Symantec

2013 Trends, Volume 19, Published April 2014

ISTR

INTERNET SECURITY THREAT REPORT
GOVERNMENT ⌖ 2014

CONTENTS

4 Introduction

5 Executive Summary

8 **2013 SECURITY TIMELINE**

9 2013 Security Timeline

11 **2013 IN NUMBERS**

12 Breaches

14 Spam

15 Bots, Email

16 Mobile

17 Web

18 Targeted Attacks – Spear Phishing

22 Targeted Attacks – Web-Based

24 **TARGETED ATTACKS + DATA BREACHES**

25 Targeted Attacks

26 Average Number of Spear-Phishing Attacks Per Day, 2011 – 2013

27 Email Campaigns, 2011 – 2013

28 Targeted Attack Key Stages

29 Top-Ten Industries Targeted in Spear-Phishing Attacks

30 Spear-Phishing Attacks by Size of Targeted Organization, 2011 – 2013

31 Risk of Job Role Impact by Targeted Attack Sent by Spear-Phishing Email

32 Ratio of Organizations in an Industry Impacted by Targeted Attack Sent by Spear-Phishing Email

33 Ratio of Organizations Targeted by Industry Size Sent by Spear-Phishing Email

33 Analysis of Spear-Phishing Emails Used in Targeted Attacks

34 Zero-day Vulnerabilities, Annual Total, 2006 – 2013

35 Top-Five Zero-day Vulnerabilities

38 Point of Sale Breach Stages

39 Data Breaches

39 Top Causes of Data Breach

40 Timeline of Data Breaches

44 **E-CRIME + MALWARE DELIVERY TACTICS**

45 E-crime and Cyber Security

46 Malicious Activity by Source: Bots, 2012–2013

47 Top-Ten Botnets

48 Ransomware Over Time

51 Top-Ten Malware

53 Threat Delivery Tactics

54 Timeline of Web Attack Toolkit Use, Top-Five

54 Top Web Attack Toolkits by Percent

55 Web Attacks Blocked Per Day

56 Most Frequently Exploited Websites

58 Zero-Day Vulnerabilities

58 Total Number of Vulnerabilities, 2006 – 2013

60 Plug-in Vulnerabilities Over Time

60 Browser Vulnerabilities, 2011 – 2013

61 Proportion of Email Traffic Containing URL Malware, 2013 vs 2012
61 Proportion of Email Traffic in Which Virus Was Detected, 2013 vs 2012
62 Top-Ten Mac OSX Malware Blocked on OSX Endpoints

63 **SOCIAL MEDIA + MOBILE THREATS**

64 Social Media
65 Social Media

69 Mobile
70 Number of Android Variants Per Family, 2013 vs 2012
70 Mobile Malware Families by Month, Android, 2013 vs 2012
72 Mobile Threat Classifications
74 Mobile Vulnerabilities by Percent
75 Top-Five Types of Madware Functionality Percentage of Ad Libraries

77 **PHISHING + SPAM**

78 Spam and Phishing
78 Phishing Rate, 2013 vs 2012
79 Number of Phishing URLs on Social Media
81 Global Spam Volume Per Day
81 Global Spam Rate, 2013 vs 2012

83 **LOOKING AHEAD**

84 Looking Ahead

86 **RECOMMENDATIONS + BEST PRACTICE GUIDELINES**

87 Best Practice Guidelines for Businesses
89 Best Practice Guidelines for Consumers
90 SANS Critical Security Controls
94 Footnotes
96 Contributors
97 About Symantec
97 More Information

Introduction

Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 41.5 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 60,000 recorded vulnerabilities (spanning more than two decades) from over 19,000 vendors representing over 54,000 products.

Spam, phishing, and malware data is captured through a variety of sources including the Symantec Probe Network, a system of more than 5 million decoy accounts, Symantec.cloud, and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before they reach customers' networks. Over 8.4 billion email messages are processed each month and more than 1.7 billion web requests filtered each day across 14 data centers. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 50 million consumers.

Symantec Trust Services provides 100 percent availability and processes over 6 billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world. These resources give Symantec analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

Executive Summary

One of the major challenges for government in 2013 has been how to prepare for attacks against the supply chain that have increased in sophistication throughout the year. In the last ISTR, Symantec identified a growing shift towards highly targeted malware attacks being sent in email to small-to-medium-sized businesses, which now appears to have reached a plateau. Moreover, although the overall volume of such email-based attacks overall has returned to 2011 levels, they have become much more subtle and harder to identify without the right technology in place. The frontline in these attacks is still moving along the supply chain; meanwhile, large enterprises may be targeted through web-based "watering-hole" attacks should email-based spear-phishing attacks fail to yield the desired results.

For the past decade, the threat landscape has been very aware of highly targeted attacks, most notably the carefully targeted spear-phishing emails that rely on sophisticated social engineering as well as state-of-the-art malware; however, this landscape is shifting and the nature of the attacks are less defined by their tactics, and more by their outcome. So when we narrow our focus on only the email aspect of targeted attacks, we may be blind to the other means by which breaches occur, such as the use of social media and watering-hole attacks.

The most important trends in 2013 were:

Data Breaches, Privacy and Trust

With privacy issues and data breach revelations dominating the headlines not only in the industry media, but also in the mainstream press, 2013 has sounded a loud clarion call for people and businesses to take a more serious look at their online information, and to keep it private and secure. The headlines in 2013 were not only peppered by the revelations about how governments were keeping track of their citizens online, but also increasingly dominated by the large number of data breaches and even larger volume of identities being leaked.

In 2013, the number of data breach incidents increased by 62 percent since 2012, with the number of online identities being exposed growing by as much as five times. It's no longer a matter of having a secure password, but who you trust to keep your credentials safe and secure. The number of incidents that resulted in 10 million or more identities being exposed was eight, compared with five in 2012. The most common cause of breach incidents was hacking, which was the reason for 35 percent of the incidents recorded in the Norton Cybercrime Index for 2013. Moreover, accidental disclosure and theft or loss of a device were close behind, making up 28 and 27 percent of breaches, respectively.

Fundamentally, the number of breach incidents is higher than ever before, and the challenge for organizations and individuals alike is to make sure they do not become counted in the next wave of statistics. Among the greatest concerns is who has access to sensitive data, and how that data may be used. A security breach at a major organization may have serious consequences not only for itself but also for its customers; personal information stolen in an online hack may later be used in the commission of fraud or to gain unauthorized access to online accounts.

As a result, the adoption of encryption technology is likely to grow in 2014/15, not only for use in securing data on devices, but also for securing online transactions. The use of personal VPNs is already growing, as concerned users become wary about the traffic that may be exposed through their Wi-Fi hotspot.

Executive Summary

VPNs are not new, but they have traditionally been the preserve of businesses seeking to safeguard its employees' data when working remotely. Newer and faster encryption protocols will also be in demand, so even if your data is exposed or your device falls into the wrong hands, you can be assured that it cannot be exploited by the criminals.

The Value of Data

The threat from governments potentially gathering our personal data in the routine business of safeguarding our national security was a major concern to many individuals and businesses. In 2013 the value of our data was also being challenged by cybercriminals, who were escalating the stakes to see how much financial value we put on our own data. Ransomware-type malware volumes increased by 500 percent from 100,000 to over 600,000 by the end of the year, an increase of over six times its previous level.

As more and more personal data is online and in the cloud than ever before and consumers are sharing more data with each other, businesses and governments have to routinely handle massive quantities of personal information safely. But do the owners of this data take sufficient protective measures to safeguard the data on their own computers and devices? Cybercriminals are increasingly seeing the value of this information for financial crime, identity theft, and other acts of fraud. Personal data is a very attractive commodity for cybercriminals, who have developed business models to sell them. Huge amounts of personal data is being harvested and sold to other malicious parties, details including names, addresses, social security numbers, health insurance details, and credit card information.

One of the biggest breaches this year was caused by an attack against a major retailer's point of sale (PoS) system. These systems handle customer transactions through cash or credit cards. When a customer swiped their credit or debit card at a PoS system, their data was sent through the company's networks in order to reach the payment processor. Depending on how the system was set up, attackers could take advantage of a number of flaws within these networks to ultimately steal their targeted data.

Targeted Spear-Phishing Emails

In 2012, we saw increasing numbers of targeted attacks using email, but when these attacks were thwarted the attackers would intensify their volume, perhaps change the social engineering, or change the exploits, or even adapt the malware. But in 2013, if a spear-phishing attack was unsuccessful, after a few attempts the attacker may be more likely to shift to a different tactic altogether such as a watering hole attack, or baiting the intended target by seeking to connect with them over social media.

The largest percentage of email-based spear-phishing attacks overall were still being directed at large enterprises (comprised of over 2,500 employees) at 39 percent compared with 50 percent in 2012, the industry sector most targeted in 2013 was Government and Public Sector (a.k.a. Public Administration), and accounted for 16 percent of all targeted spear-phishing email attacks blocked in 2013, compared with 12 percent in 2012.

In 2013, targeted email attacks aimed at Small Businesses (1-250) accounted for 30 percent of all such attacks blocked by the company, compared with 31 percent in 2012 and 18 percent in 2011. Despite the overall average being almost unchanged, the trend through the year reveals that the proportion of attacks against small businesses has increased throughout the year, peaking at 53 percent in November.

Watering-Hole Attacks and Exploiting Zero-Day Vulnerabilities

Watering-hole attacks were first described in the 2012 Symantec Internet Security Threat Report (ISTR), and as a threat they can be among the most dangerous. Watering holes are legitimate websites that have been compromised, but not by cybercriminals who have planted a traditional web-attack toolkit, such as Blackhole or Cool Exploit Kit; rather these websites are trapped with exploits for as yet undiscovered zero-day vulnerabilities. Once these exploits are discovered and the vulnerabilities patched, the perpetrators will quickly adapt by using another exploit for another zero-day. As these attacks rely on zero-day vulnerabilities in order to go undiscovered, it is all the more worrying to report an increase in the number of zero-day vulnerabilities from 14 in 2012 to 23 in 2013. There were more zero-day vulnerabilities discovered in 2013 than in any previous year since Symantec began tracking them, and more than the past two years combined.

Executive Summary

For 2013 the majority of attacks using zero-day vulnerabilities focused on Java. Not only did Java hold the top three spots in exploited zero-day vulnerabilities, it was responsible for 97 percent of attacks that used zero-day vulnerabilities after they were disclosed. When looking at the top five zero-day vulnerabilities, the average exposure window between disclosure and an official patch was 3.8 days, comprising a total of 19 days where users were left exposed.

Compromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Security Solutions division found that 77 percent of websites contained vulnerabilities. Of these, 16 percent were classified as critical vulnerabilities that could allow attackers to access sensitive data, alter the website's content, or compromise visitors' computers. This means that when an attacker looks for a site to compromise, one in eight sites makes it relatively easy to gain access.

Social Networking and Mobile Threats

Some of the most popular applications used on mobile devices are for social networking, and as the various social networking sites vie for our attention, new ones continue to emerge. These are quickly adopted by teenagers and young adults, who have little sense of loyalty to some of the more established networks, which are increasingly being dominated by the older generations and their parents. In 2013, cybercriminals have sought to exploit the data we share online through social media, and as these sites become increasingly interconnected the security of our data and personal information online becomes more important than ever. Fake offers dominated the social media landscape in 2013, making up 81 percent of all social media related attacks, up from 56 percent in 2012.

Furthermore, the greatest risk for a compromised mobile device was being spied on; this tactic was found in 60 percent of mobile threats in 2013 compared with 20 percent in 2012. Approximately 36 percent of malware was designed to steal data in 2013, compared with 46 percent in 2012. The individual can be spied on through the collection of SMS messages or phone call logs, tracking GPS coordinates, recording phone calls, or by gathering photos and video taken with the device.

Social networking also has an important role to place in the social engineering tactics employed in some targeted attacks, and not only by the cyber-criminals as revealed in some of the documents published by Edward Snowden in 2013. For example, a potential target may be exposed to a malicious social media profile that could result in malware being deployed on their computer. Social media also enables a potential attacker to find out who works for a targeted organization using professional social networking sites, such as LinkedIn. IT and network administrators may be the most attractive targets because of the type of privileged information they may have access to, due to the nature of their roles. It's through these and other means that watering-hole attacks could be expected to take the place of the more traditional email-based attacks.

Internet of Things

There has been much talk of the "Internet of Things" (or IoT) in 2013, and the first signs of attacks intended for these emerging technologies appeared in 2013. The IoT is the name given to the idea that more devices are being connected to the Internet beyond the traditional computers: Consoles, tablets and mobile devices, smart TVs and refrigerators, cameras, home security systems, and baby monitors. IoT is the way the Internet is moving, and people are as likely to become connected through tablets and smartphones as laptops and PCs, and more people will be watching TV streamed across the Internet into their living rooms rather than on their computers. As the popularity of these previously "dumb" devices increases, so will the attention they garner from security researchers. As vulnerabilities are discovered in recently-innovated internet-enabled devices, the challenge of applying patches to fix them will grow.

E-crime

In 2013 much of the efforts of cybercriminals were narrowed to carving out particular areas of focus for e-crime related activities. These criminals found themselves with a great deal to choose from; some administered web attack toolkits while others rented out botnets to third parties. Spam campaigns shifted further away from the traditional pharmaceutical spam, exploiting people's desires and needs with more adult-orientated spam. Ransomware, which grew by 500 percent (an increase of six times) in 2013 was perhaps the most notable and brazen growth areas in 2013. Cyber-criminals directly extorted money from users by holding their personal data as hostage for ransom, and even adopting alternative and anonymous payment systems such as Bitcoin.

2013 SECURITY TIMELINE

2013 Security Timeline

01 January

- Elderwood Project found using new Internet Explorer Zero-Day Vulnerability (CVE-2012-4792)
- Java Zero-Day found in Cool Exploit Kit (CVE-2013-0422)
- Android.Expresspam potentially infects thousands of devices
- Backdoor.Barkiofork used to target Aerospace and Defense industries

02 February

- Bamital botnet taken down
- Adobe zero-day used in "LadyBoyle" attack (CVE-2013-0634)
- Cross-platform toolkit for creating the remote access tool (RAT) "Frutas" discovered
- Fake Adobe Flash update discovered installing ransomware and performing click fraud
- Bit9 suffers security breach, code-signing SSL certificates stolen

03 March

- Android Malware spams victims' contacts
- "Facebook Black" scam spreads on Facebook
- Blackhole Exploit Kit takes advantage of financial crisis in Cyprus
- Several South Korean banks and local broadcasting organizations impacted by cyber attack.

04 April

- #OpIsrael hacktivism campaign targets Israeli websites
- NPR, Associated Press, and various Twitter accounts hacked by Syrian Electronic Army (SEA)
- Distributed Denial of Service attacks hit Reddit and European banks
- WordPress plugin vulnerability discovered, allowing PHP injection
- LivingSocial resets passwords for 50 million accounts after data breach

05 May

- A US Department of Labor website becomes victim of a watering-hole attack
- Cybercriminals steal more than $1 million from a Washington state hospital
- SEA hacks twitter accounts of The Onion, E! Online, The Financial Times, and Sky
- New Internet Explorer 8 Zero-Day Vulnerability used in watering-hole attack (CVE-2012-4792)
- #OpUSA hacktivism campaign launches against US websites
- Seven men were arrested in New York in connection with their role in international cyber attacks which resulted in theft of $45 million across 26 different countries.

06 June

- Microsoft and FBI disrupt Citadel botnets
- A surveillance scandal emerges in the United States, as a former Government security contractor releases classified documents
- Zero-day vulnerability found in most browsers across PC, Mac, mobile, and game consoles
- Anonymous launches #OpPetrol attack on international oil and gas companies
- 65 websites compromised to host malicious ads with ZeroAccess Trojan
- FakeAV discovered on Android phones

07 July

- Ubisoft hacked: user account information stolen
- France caught up in PRISM scandal as data snooping allegations emerge
- New exploit kit targets flaws in Internet Explorer, Java, and Adobe Reader
- FBI-style ransomware discovered targeting OSX computers
- Android Master Key vulnerability used in the wild
- Viber and Thomson Reuters latest victims of SEA attacks

2013 Security Timeline

08 August

- Channel 4 blog, New York Post, SocialFlow, Washington Post, New York Times, impacted by SEA attacks
- DNS hijack caused thousands of sites to redirect users to exploit kit
- Two new ransomware scams found: One that changes Windows login credentials on Chinese systems, another that takes advantage of the NSA PRISM controversy
- Fake 'Instagram for PC' leads to survey scam
- Attackers targeted banks' wire payment switch to steal millions
- Francophoned social engineering ushers in a new era of targeted attacks

09 September

- Syrian Electronic Army compromises US Marine Corps' website, Fox Twitter accounts, supposedly using Mac Trojan
- ATMs discovered that dispense cash to criminals
- Ransomware called "Cryptolocker" surfaces that encrypts victims' files and demands payment to decrypt them
- Symantec lifts lid on professional hackers-for-hire group Hidden Lynx
- Belgian telecom compromised in alleged cyber espionage campaign
- Symantec Security Response sinkholes ZeroAccess botnet

10 October

- The Silk Road marketplace taken offline, resurfaces by end of month
- SEA attacks GlobalPost and Qatar websites, US Presidential staff emails
- Adobe confirms security breach, 150 million identities exposed
- Blackhole and Cool Exploit Kit author arrested
- WhatsApp, AVG, Avira defaced by hacker group KDMS
- New ransomware demands Bitcoins for decryption key

11 November

- Second Android master key vulnerability discovered
- Microsoft zero-day vulnerability being used in targeted attacks and e-crime scams (CVE-2013-3906)
- SEA hacks VICE.com in retaliation for article that supposedly names members
- Anonymous claims to have hacked UK Parliament Wi-Fi during London protest
- Linux worm that targets "Internet of Things" discovered
- Target confirms data breach leading to the exposure of 110 million identities.

12 December

- Data of 20 million Chinese hotel guests leaked
- Cross-site scripting vulnerability found in wind turbine control application
- Imitation versions of Cryptolocker discovered, attempt to capitalize on original's success
- 105 million South Korean accounts exposed in credit card security breach

2013 IN NUMBERS

Breaches

Breaches With More Than 10 Million Identities Exposed

Top-Ten Types of Information Breached

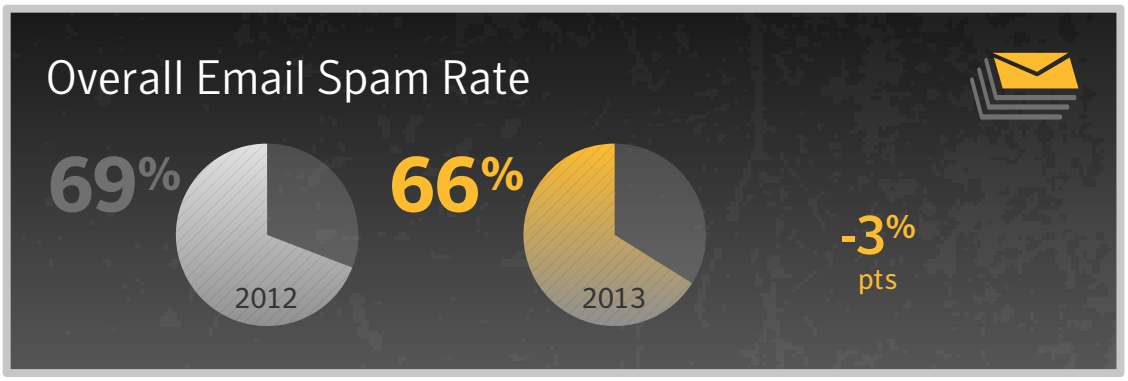
01	Real Names
02	Birth Dates
03	Government ID Numbers (Social Security)
04	Home Address
05	Medical Records
06	Phone Numbers
07	Financial Information
08	Email Addresses
09	User Names & Passwords
10	Insurance

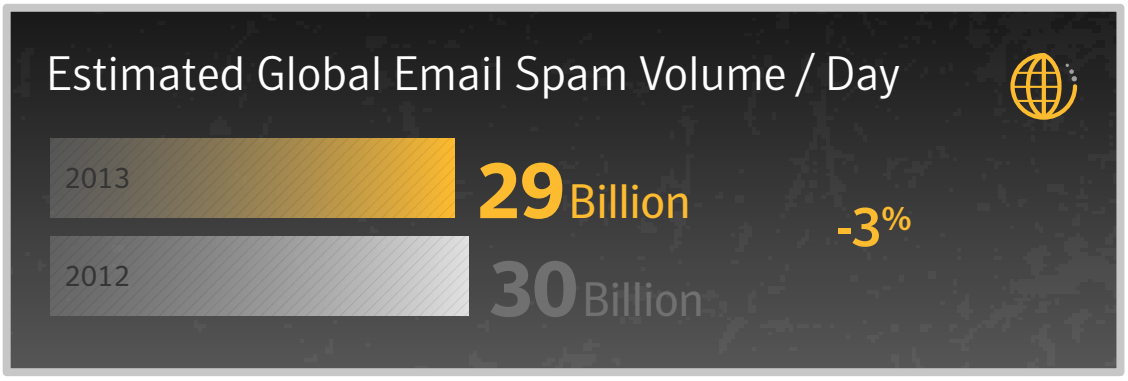
- *Mega Breaches were data breach incidents that resulted in the personal details of at least 10 million identities being exposed in an individual incident. There were eight in 2013, compared with only one in 2012.*

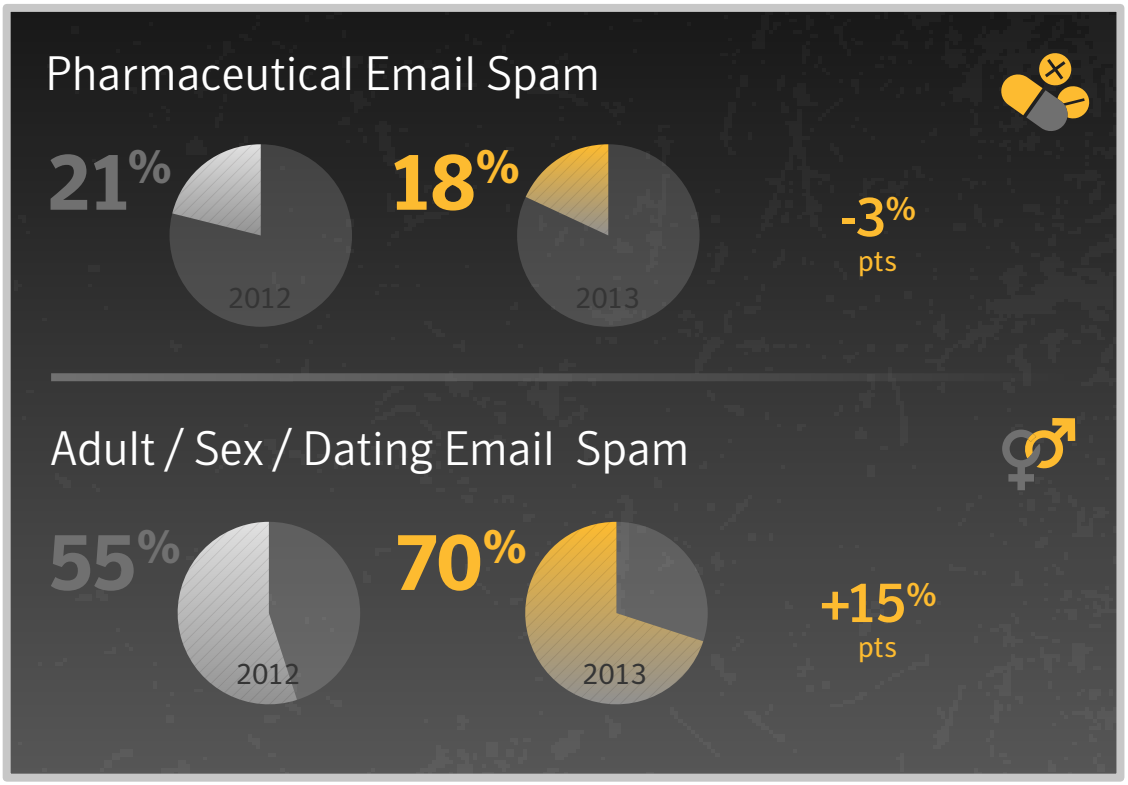
Breaches

- *Hacking continued to be the primary cause of data breaches in 2013. Hacking can undermine institutional confidence in a company, exposing its attitude to security and the loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 34 percent of data breaches in 2013.*
- *In 2013, there were eight data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 150 million identities. In contrast, 2012 saw only one breach larger than 10 million identities.*
- *Although overall average size of a breach has increased, the median number of identities stolen has actually fallen from 8,350 in 2012 to 6,777 in 2013. Using the median can be helpful in this scenario since it ignores the extreme values caused by the notable, but rare events that resulted in the largest numbers of identities being exposed.*

Spam

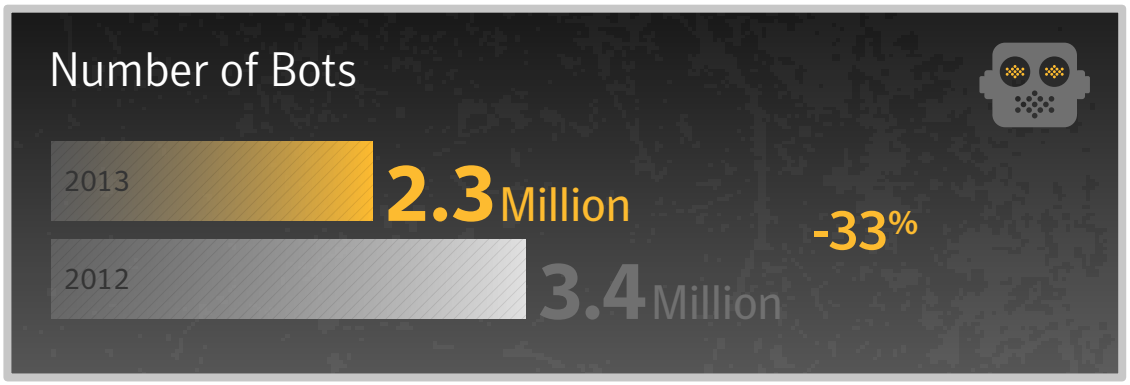


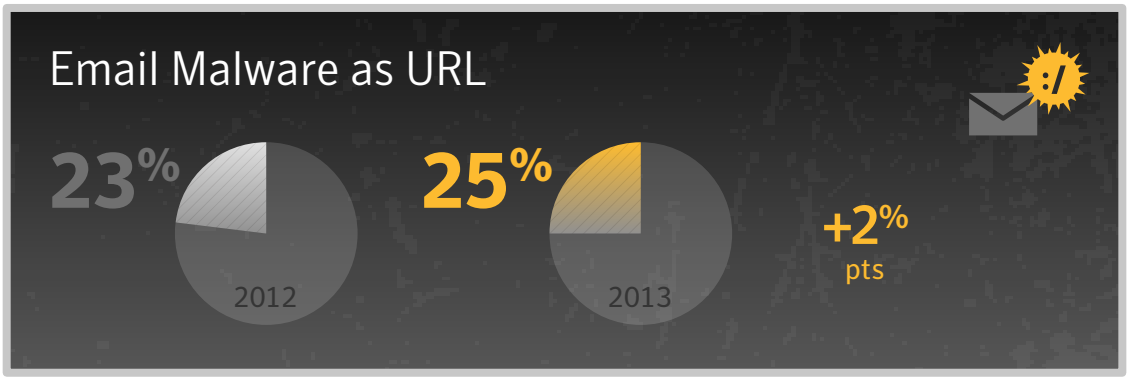


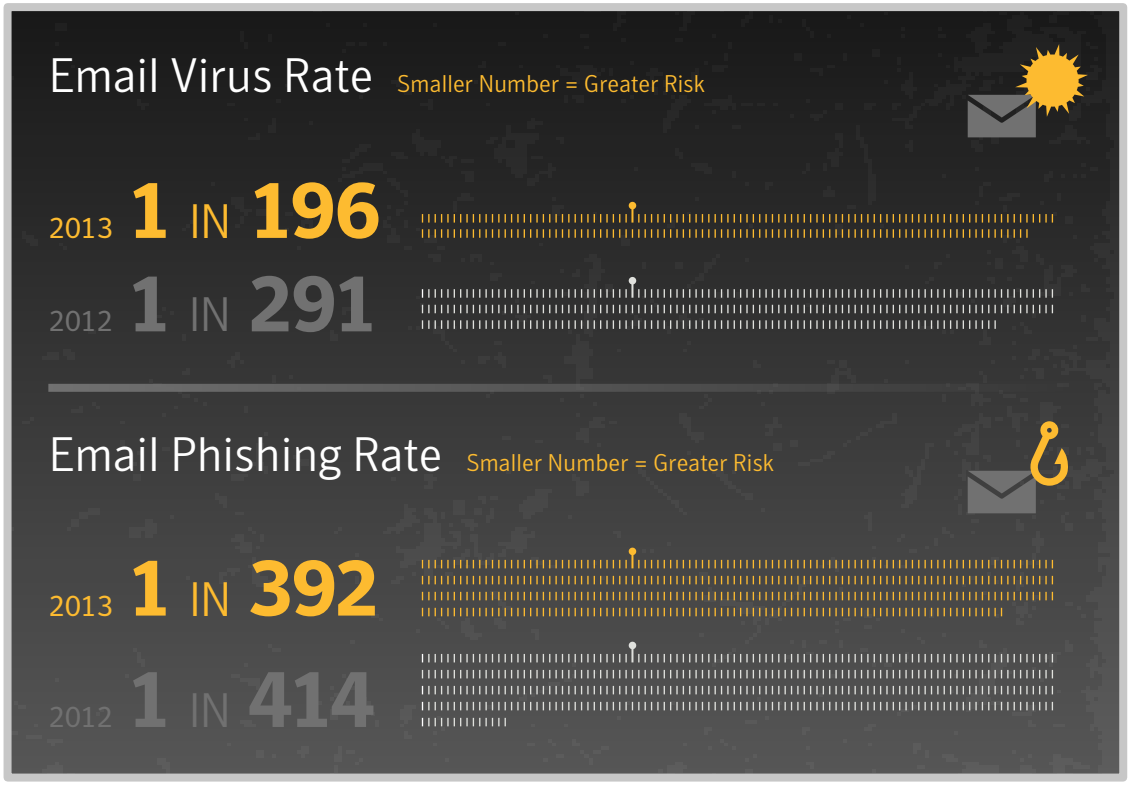


- *Approximately 76 percent of spam email was distributed by spam-sending botnets, compared with 79 percent in 2012. Ongoing actions to disrupt a number of botnet activities during the year have helped to contribute to this gradual decline.*
- *In 2013, 87 percent of spam messages contained at least one URL hyperlink, compared with 86 percent in 2011, an increase of 1 percentage point.*
- *Adult Spam dominated in 2013, with 70 percent of spam related to adult content. These are often email messages inviting the recipient to connect to the scammer through instant messaging, or a URL hyperlink where they are then typically invited to a pay-per-view adult-content web cam site. Often a bot responder, or a person working in a low-pay, offshore call center would handle any IM conversation.*

Bots, Email







- *Bot-infected computers, or bots, are counted if they are active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they may be classified as actively-attacking bots or bots that send out spam, i.e. spam zombies. During 2013, Symantec struck a major blow against the ZeroAccess botnet. With 1.9 million computers under its control, it is one of the larger botnets in operation at present. ZeroAccess has been largely used to engage in click fraud to generate profits for its controllers.*
- *In 2013, more email-borne malware comprised hyperlinks that referenced malicious code, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.*
- *71 percent of phishing attacks were related to spoofed financial organizations, compared with 67 percent in 2012. Phishing attacks on organizations in the Information Services sector accounted for 22 percent of phishing attacks in 2013*

Mobile

Android Mobile Malware Families

57
2013

-45%

103
2012

Average Number of Variants Per Family

57
2013

+50%

38
2012

Total Android Mobile Malware Variants

2013 **3,262**
2012 3,783

-14%

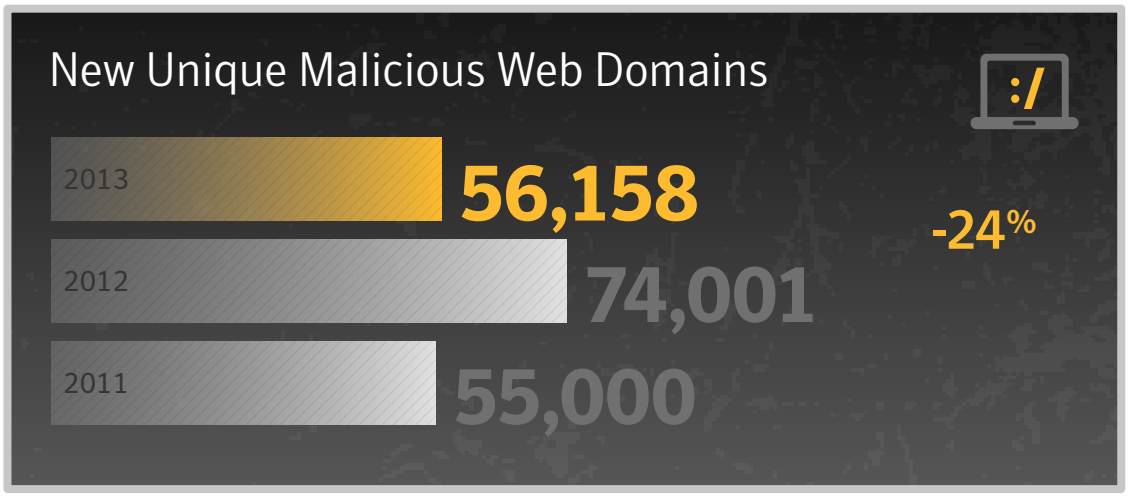
Mobile Vulnerabilities

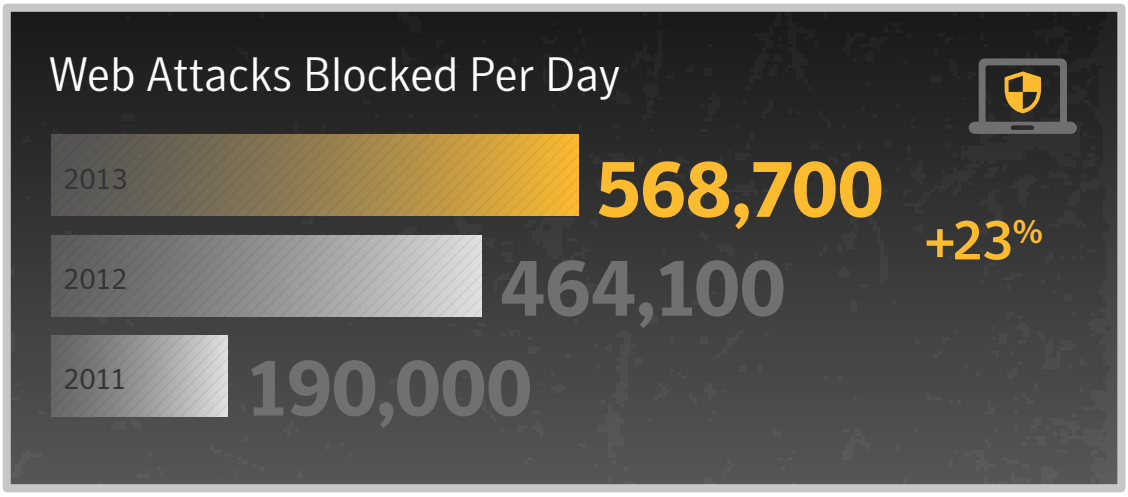
2013 **127**
2012 416

-69%

- *Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile application ("app") marketplaces in the hope that users will download and install them, often trying to pass themselves off as legitimate apps or games.*
- *Attackers have also taken popular legitimate applications and added additional code to them. Symantec has classified the types of threats into a variety of categories based on their functionality*
- *Symantec tracks the number of threats discovered against mobile platforms by tracking malicious threats identified by Symantec's own security products and confirmed vulnerabilities documented by mobile vendors.*

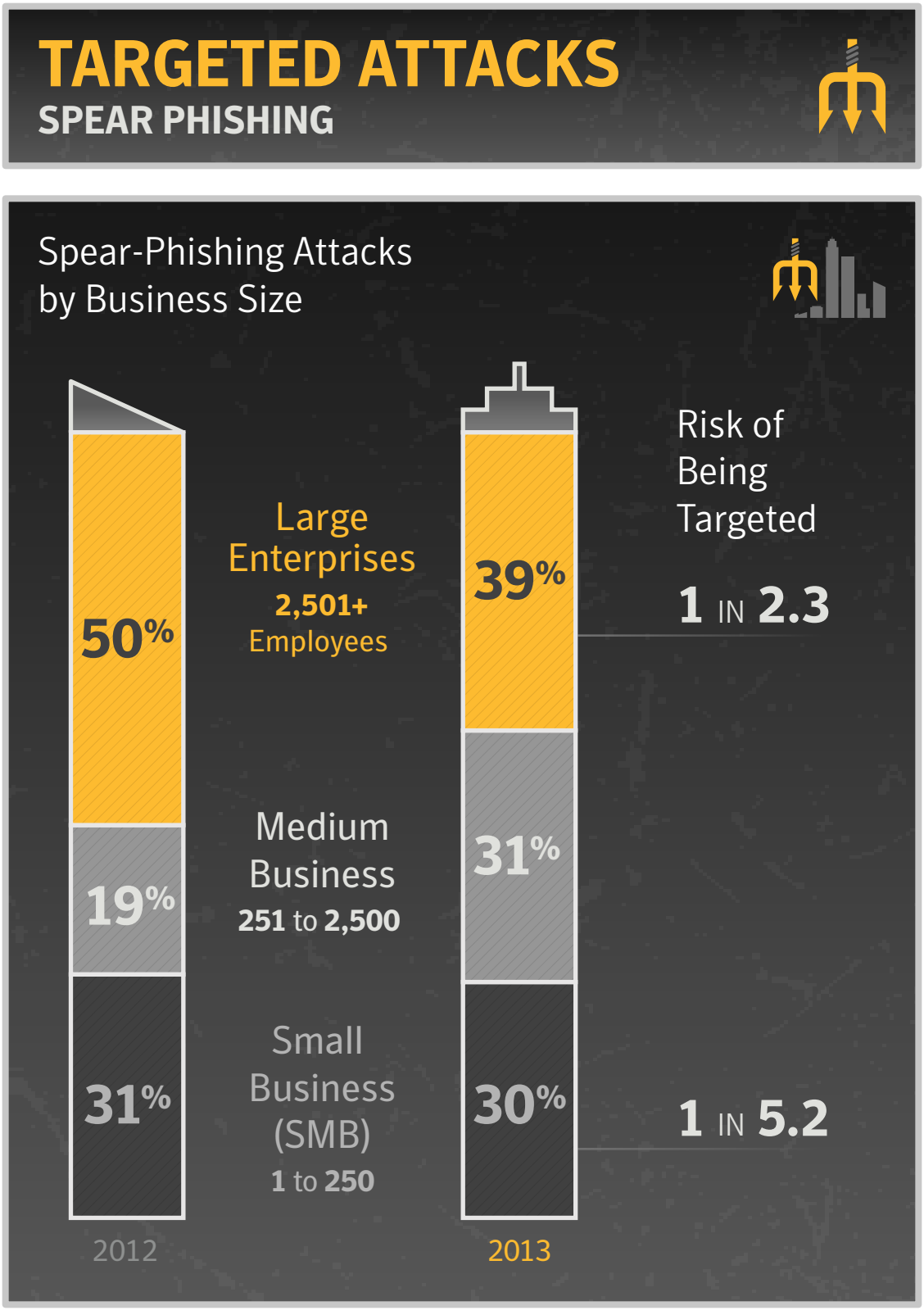
Web





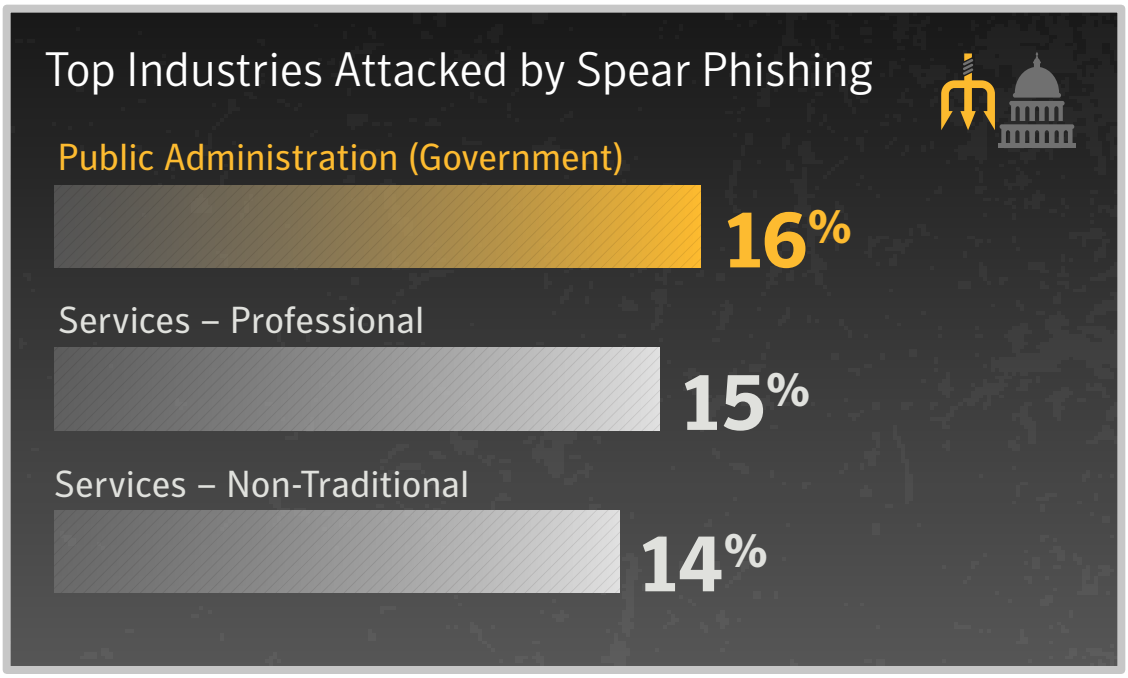
- *Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites.*
- *10 percent of malicious website activity was classified in the Technology category, 7 percent were classified in the Business category and 5 percent were classified as Hosting.*
- *73 percent of browser-based attacks were found on Anonymizer proxy websites, similarly, 67 percent of attacks found on Blogging websites involved browser-based exploits.*

Targeted Attacks – Spear Phishing



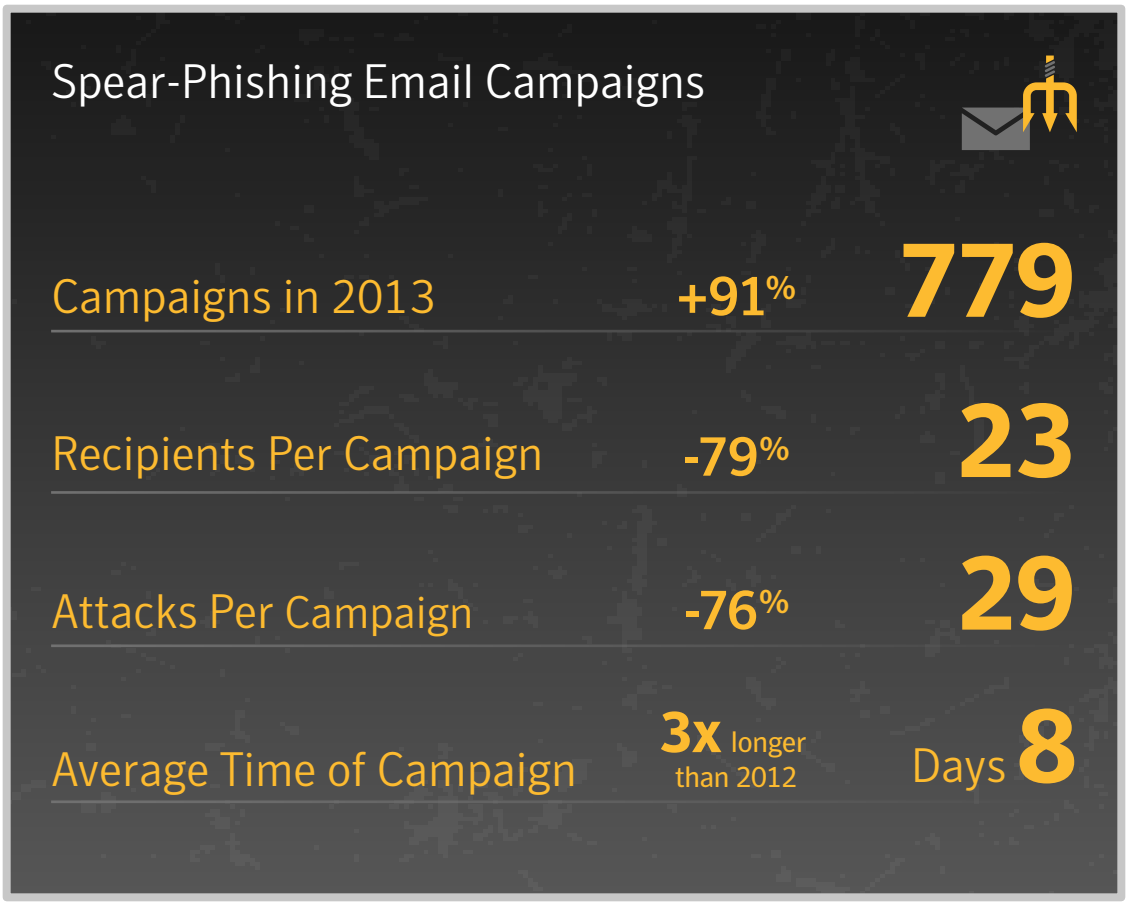
- *Targeted attacks aimed at Small Businesses (1-250) accounted for 30 percent of targeted spear-phishing attacks. 1 in 5 small business organizations was targeted with at least one spear-phishing email in 2013.*
- *39 percent of targeted spear-phishing attacks were sent to Large Enterprises comprising over 2,500+ employees. 1 in 2 of which were targeted with at least one such attack.*
- *The frontline in these attacks is moving along the supply chain and large enterprises may be targeted though web-based watering-hole attacks should email-based spear-phishing attacks fail to yield the desired results.*

Targeted Attacks – Spear Phishing



- *Approximately 1 in 3 organizations in the Mining, Public Administration and Manufacturing sectors were subjected to at least one targeted spear-phishing attack in 2013.*
- *The Government and Public Sector (aka. Public Administration) accounted for 16 percent of all targeted spear-phishing email attacks blocked in 2013, compared with 12 percent in 2012.*

Targeted Attacks – Spear Phishing

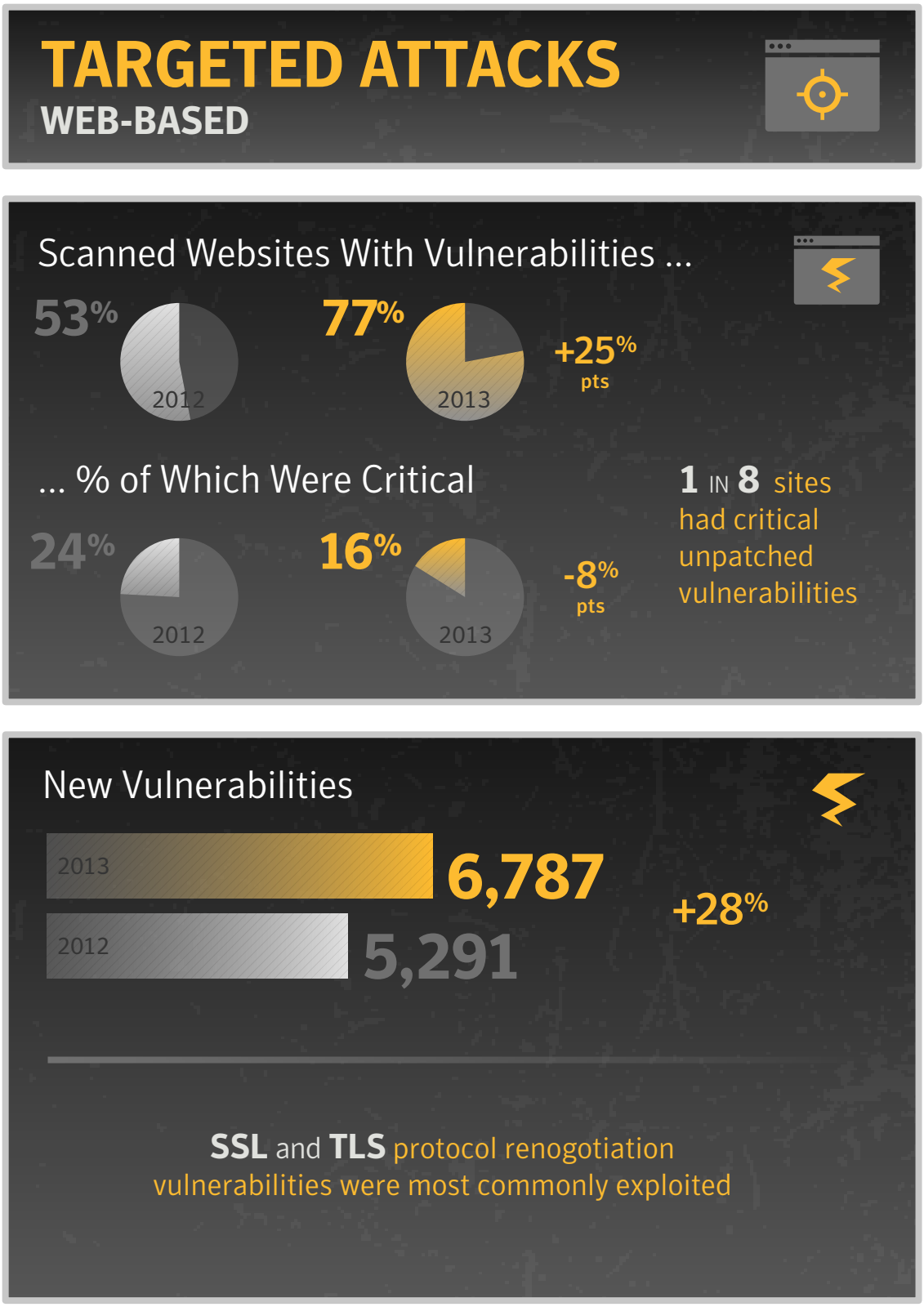


- *Attackers may target both the personal and professional email accounts of individuals concerned; a target's work-related account is likely to be targeted more often and is known as spear phishing.*
- *Over the past decade, an increasing number of users have been targeted with spear-phishing attacks and the social engineering has grown more sophisticated over time.*
- *In 2013 the volume and intensity of these attacks had changed considerably from the previous year, prolonging the duration over which a campaign may last, rather than intensifying the attacks in one or two days as had been the case previously. Consequently, the number of attacks seen each day has fallen and other characteristics of these attacks suggest this may help to avoid drawing attention to an attack campaign that may be underway.*

Targeted Attacks – Spear Phishing

- *This word cloud shows the most frequently occurring words that have been used in targeted spear-phishing email attacks throughout 2013. The larger the size of the font, the more frequently that word was used.*

Targeted Attacks – Web-Based



- *Attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site. Compromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Vulnerability Assessment Services found that 77 percent of sites contained vulnerabilities.*
- *Of this, 16 percent were classified as critical vulnerabilities that could allow attackers to access sensitive data, alter the website's content, or compromise visitors' computers. This means that when an attacker looks for a site to compromise, one in eight sites makes it relatively easy to gain access.*
- *The most commonly exploited vulnerabilities related to SSL and TLS protocol renegotiation.*

Targeted Attacks – Web-Based

Websites Found With Malware

1 IN 532 (2012)

1 IN 566 (2013)

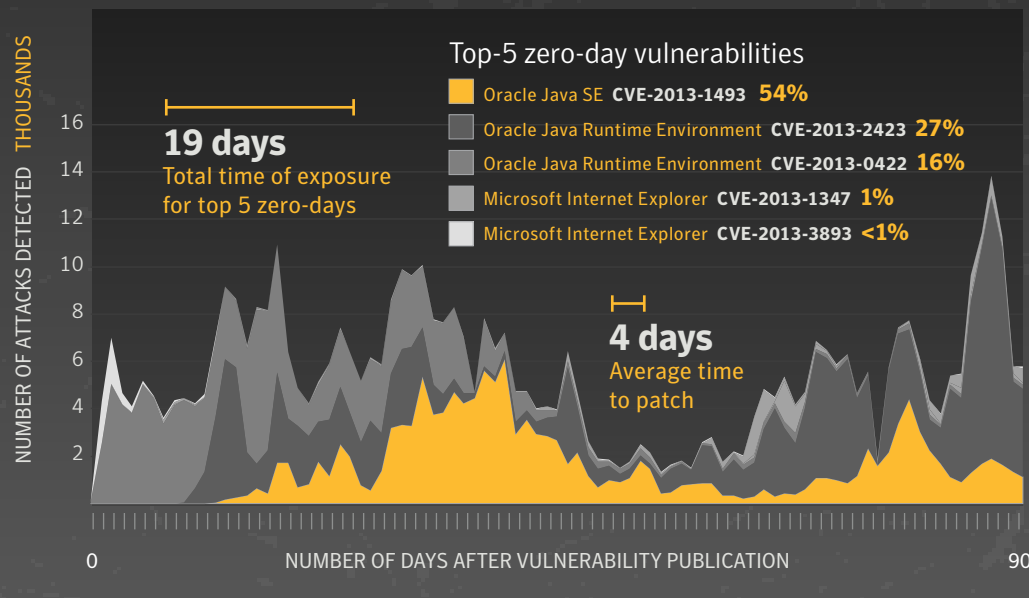
Zero-day Vulnerabilities

DAY 0

14 (2012) +64% 23 (2013)

23 software vulnerabilities were zero-day,
5 of which were for Java

97% of attacks using exploits for vulnerabilities identified as zero-day were Java-based



- *Malware was found on 1 in 566 websites scanned by Symantec's Website Vulnerability Assessment Service in combination with the daily malware scanning service.*
- *97 percent of attacks using exploits for vulnerabilities initially identified as zero-days were Java-based. The total time between a zero-day vulnerability being published and the required patch being published was 19 days for the top-five most-exploited zero-day vulnerabilities. The average time between publication and patch was 4 days.*
- *Zero-day vulnerabilities are frequently used in watering-hole web-based targeted attacks. Attackers can quickly switch to using a new exploit for an unpublished zero-day vulnerability once an attack is discovered and the vulnerability published.*

TARGETED ATTACKS + DATA BREACHES

Targeted Attacks

The use of malware specifically to steal sensitive or confidential information from organizations isn't a new trend; it's been around for at least the past decade. However the scale of these attacks has always been relatively low in order to remain below the radar of security technology used to safeguard against them. A targeted attack uses malware aimed at a specific user or group of users within a targeted organization and may be delivered through a spear-phishing email, or a form of drive-by download known as a watering-hole attack. No matter how these attacks are delivered they are designed to be low in volume, often with malicious components used exclusively in one attack. Their ultimate goal is to provide a backdoor for the attacker to breach the targeted organization.

In the past these targeted attacks have relied primarily on the spear-phishing element, an email-based phishing attack is often aimed at an individual or small group of individuals, because they may have access to sensitive information through their role at a targeted organization. An important detail with a spear-phishing email is that it often appears to come from someone the recipient knows, a source they would trust, or contain subject matter the target would be interested in or is relevant to their role. The social engineering is always refined and well-researched, hence the attack may be very difficult to recognize without the right technology in place to safeguard against it.

However, targeted attacks no longer rely as heavily on spear-phishing attacks in order to penetrate an organization's defenses. More recently the attackers have expanded their tactics to include watering-hole attacks, which are legitimate websites that have been compromised for the purpose of installing targeted malware onto the victim's computer. These attacks rely almost exclusively on client-side exploits for zero-day vulnerabilities that the attackers have in their arsenal. Once the vulnerability the hackers are using has been published, they will often quickly switch to using another exploit in order to remain undetected.

Changes in 2013

It's worth looking back at the last few years to see how previous attack trends compare to the ones in 2013. In 2012 we witnessed a 42 percent increase in the targeted-attack rate when compared to the previous year. This was a measure of the average number of targeted-attack spear-phishing emails blocked each day. In 2013 the attack rate appears to have dropped 28 percent, returning to similar levels seen in 2011.

What appears to have happened is that attacks have become more focused as the attackers have solidified and streamlined their attack methods. Looking at email-based attack campaigns in particular,[01] the number of distinct campaigns identified by Symantec is up by 91 percent compared to 2012, and almost six times higher compared to 2011. However, the average number of attacks per campaign has dropped, down 76 percent when compared to 2012 and 62 percent from 2011. This indicates that while each attack campaign is smaller, there have been many more of them in 2013.

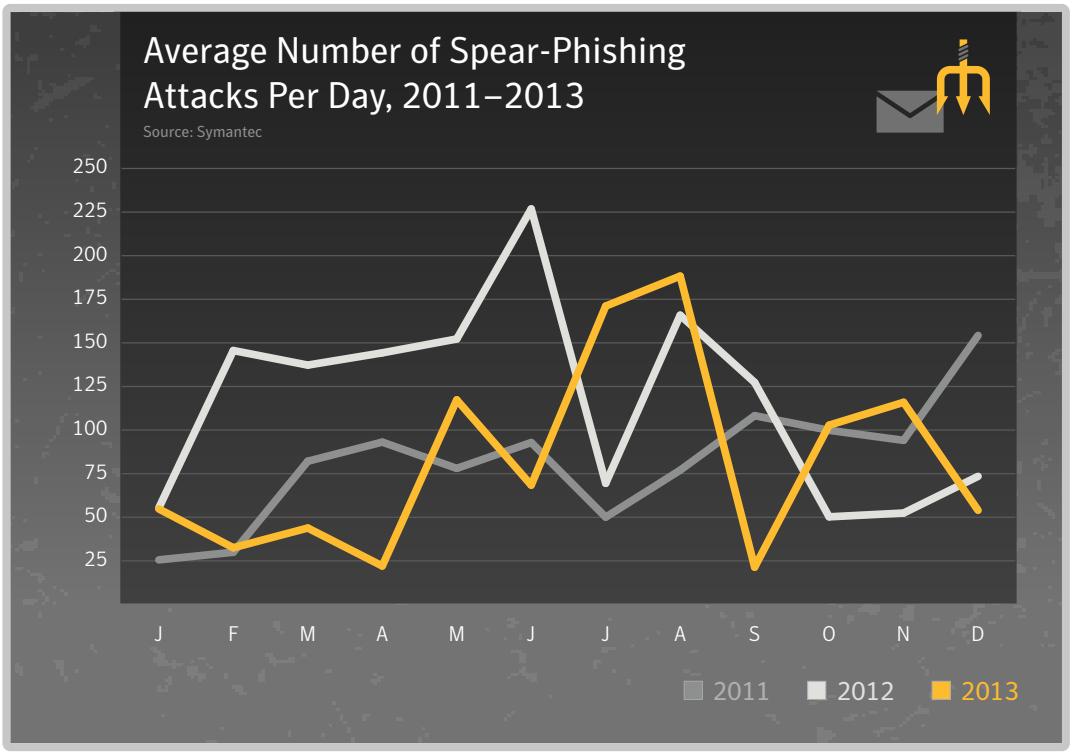
The number of recipients of spear-phishing emails during a campaign is also lower, at 23 recipients per campaign, down from 111 in 2012 and 61 in 2011. In contrast, these campaigns are lasting longer. The average duration of a campaign is 8.2 days, compared to 3 days in 2012 and 4 days in 2011. This could indicate that the attack campaigns are becoming more focused and persistent, with a reduced number of attempts over a longer period of time in order to better hide the activity.

At a Glance

- *Targeted attacks have become more focused as attackers have streamlined their attack methods.*
- *The global average number of spear-phishing attacks per day in 2013 was 83.*
- *Zero-day vulnerabilities, often used in watering-hole attacks, reached their highest levels since Symantec began tracking them.*
- *Hackers were once again responsible for more data breaches than any other source. However, accidental exposure, as well as theft or loss, grew significantly in 2013.*
- *There were over 552 million identities exposed in data breaches during 2013.*

Their ultimate goal is to provide a backdoor for the attacker to breach the targeted organization.

Fig. 1



- *The global average daily rate of targeted spear-phishing attacks is 28 percent lower than in 2012, but two percent higher than 2011. The figure for 2012 was unusually high, and attackers seem to have adjusted their tactics in 2013 in an attempt to reduce their footprint. The average rates for 2013 returned to levels on par with previous years.*
- *The global average number of spear-phishing attacks per day in 2013 was 83, compared with 116 in 2012 and 82 in 2011.*
- *The spear-phishing attack rate reached a peak of 188 attacks per day in the month of August, compared with the peak of 227 in June of the previous year.*

Spear Phishing

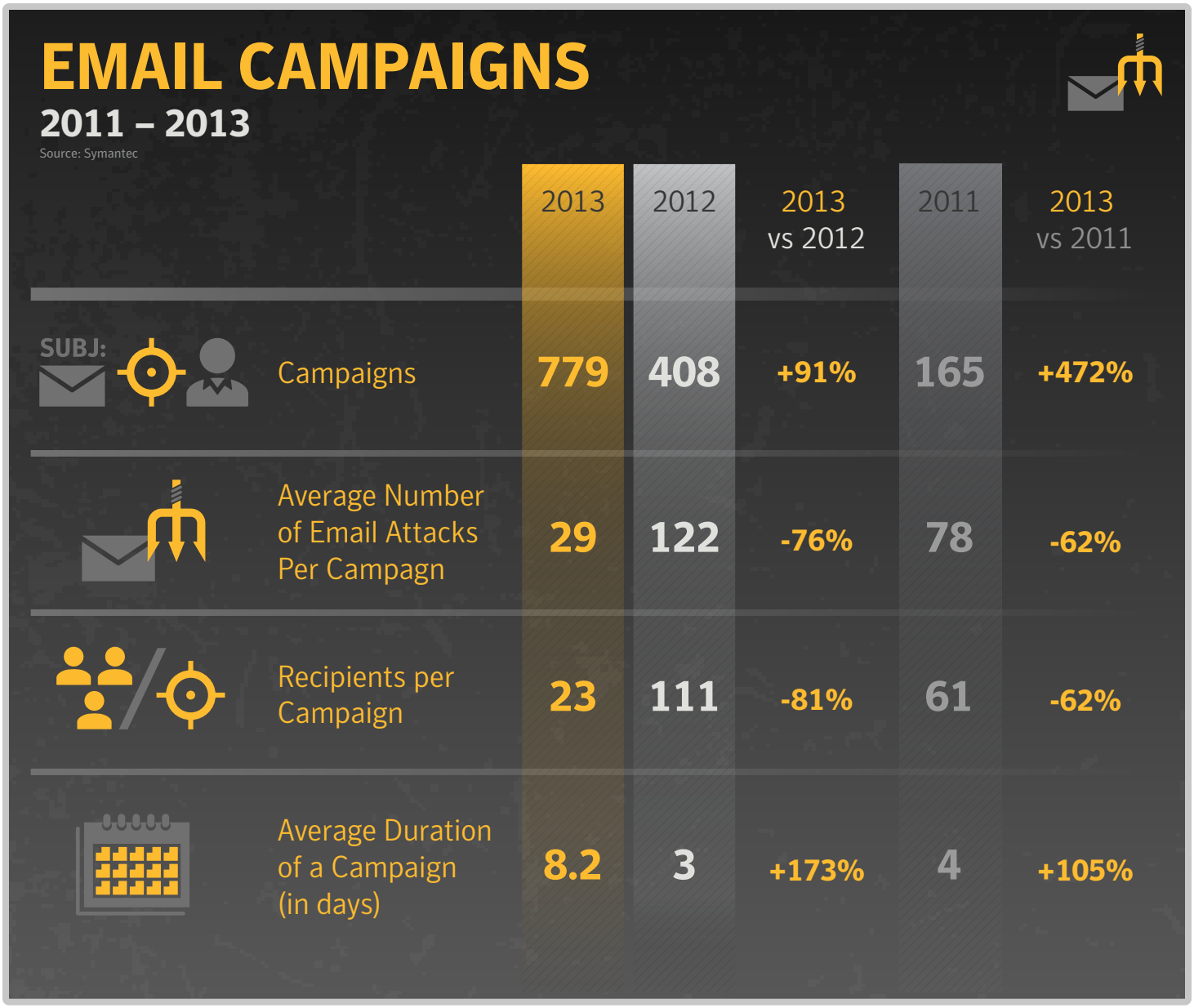
Spear-phishing attacks rely heavily on social engineering to improve their chances of success. The emails in each case are specially tailored by the attackers to spark the interest of the individual being targeted, with the hope that they will open them. For example, an attacker may send someone working in the financial sector a spear-phishing email that appears to cover some new financial rules and regulations. If they were targeting someone working in human resources, they might send spear-phishing emails that include malware-laden résumé attachments.

We've also seen some fairly aggressive spear-phishing attacks. In these cases the attacker sent an email and then followed up with a phone call directly to the target, such as the "Francophoned" attack from April 2013.[02] The attacker impersonated a high-ranking employee, and requested that the target open an attachment immediately. This assertive method of attack has been reported more often in 2013 than in previous years.

Attackers will often use both the personal and professional accounts of the individual targeted, although statistically the victim's work-related account is more likely to be targeted.

Over the past decade, an increasing number of users have been targeted with spear-phishing attacks, and the social engineering has grown more sophisticated over time. In analyzing the patterns and trends in these attacks it is important to look at the profile of the organizations concerned, most notably to which industry sector they belong, and how large their workforce is. The net total number of attacks blocked in 2013 is broken down by industry in figure 4 and organization size in figure 5.

Fig. 2



- *In 2013 the volume and intensity of spear phishing targeted email campaigns changed considerably from the previous year, extending the duration over which a campaign may last, rather than intensifying the attacks in one or two days as had been the case previously. Consequently, the number of attacks seen each day has fallen and other characteristics of these attacks suggest this may help to avoid drawing attention to an attack campaign that may be underway.*

Fig.3

TARGETED ATTACK

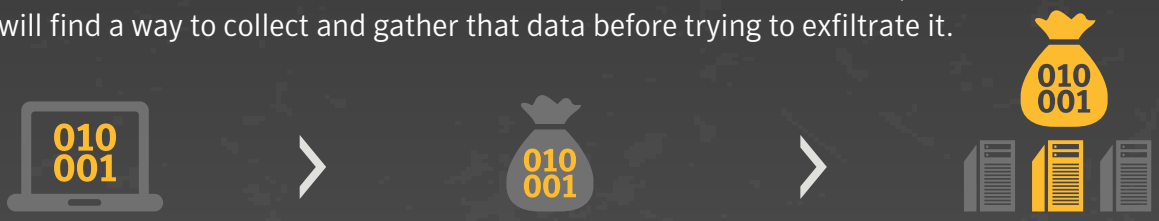
KEY STAGES

Source: Symantec

01 INCURSION The attacker gains entry to the targeted organization. This is often preceded by reconnaissance activities where the attacker is looking for a suitable social engineering tactic.

02 DISCOVERY Once the attacker has gained entry, they will seek to maintain that access as well as discover what data and other valuable resources they may wish to access.

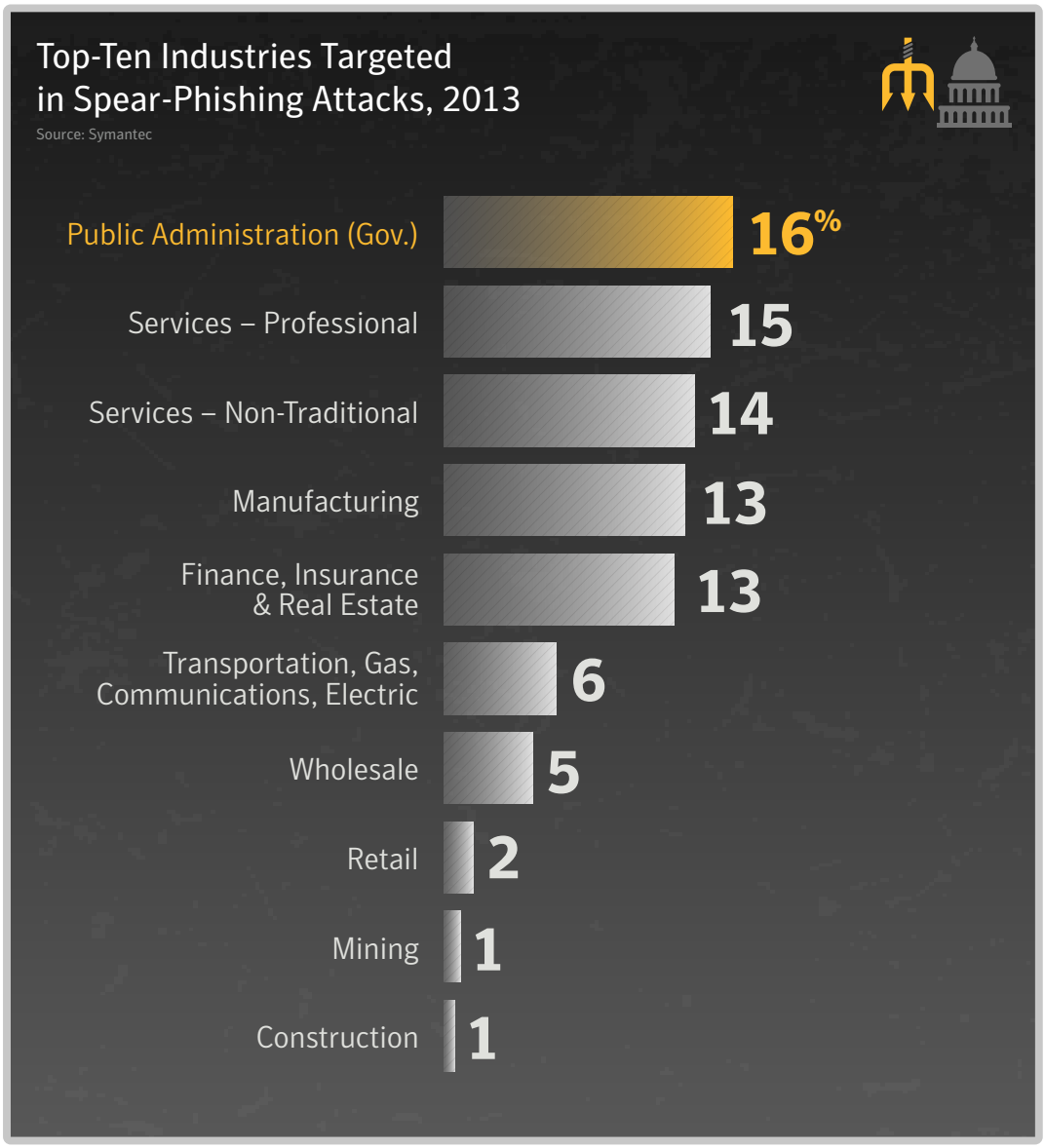
03 CAPTURE Once the valuable data has been discovered and identified, the attacker will find a way to collect and gather that data before trying to exfiltrate it.



04 EXFILTRATION The attacker will find a mechanism to steal the data from the targeted organization. This may be by uploading it to a remote server or website the attackers have access to. More covert methods may involve encryption and steganography, to further obfuscate the exfiltration process, such as hiding data inside DNS request packets.

However just because an industry or organization of a particular size receives a large number of attacks doesn't necessarily mean that it was at an elevated risk, or that someone working in that industry or organization had a high probability of being targeted. The probability was determined by looking at a group of people who have been targeted and comparing this number against a control group for that industry or organization size. Furthermore, it was important to look not only at the attacks themselves, but also to examine the email traffic of other customers in the same sectors and of the same organizational size. In this way, for the first time, Symantec was able to report on the odds of any particular organization being targeted in such an attack, based on their industry and size.

Fig. 4

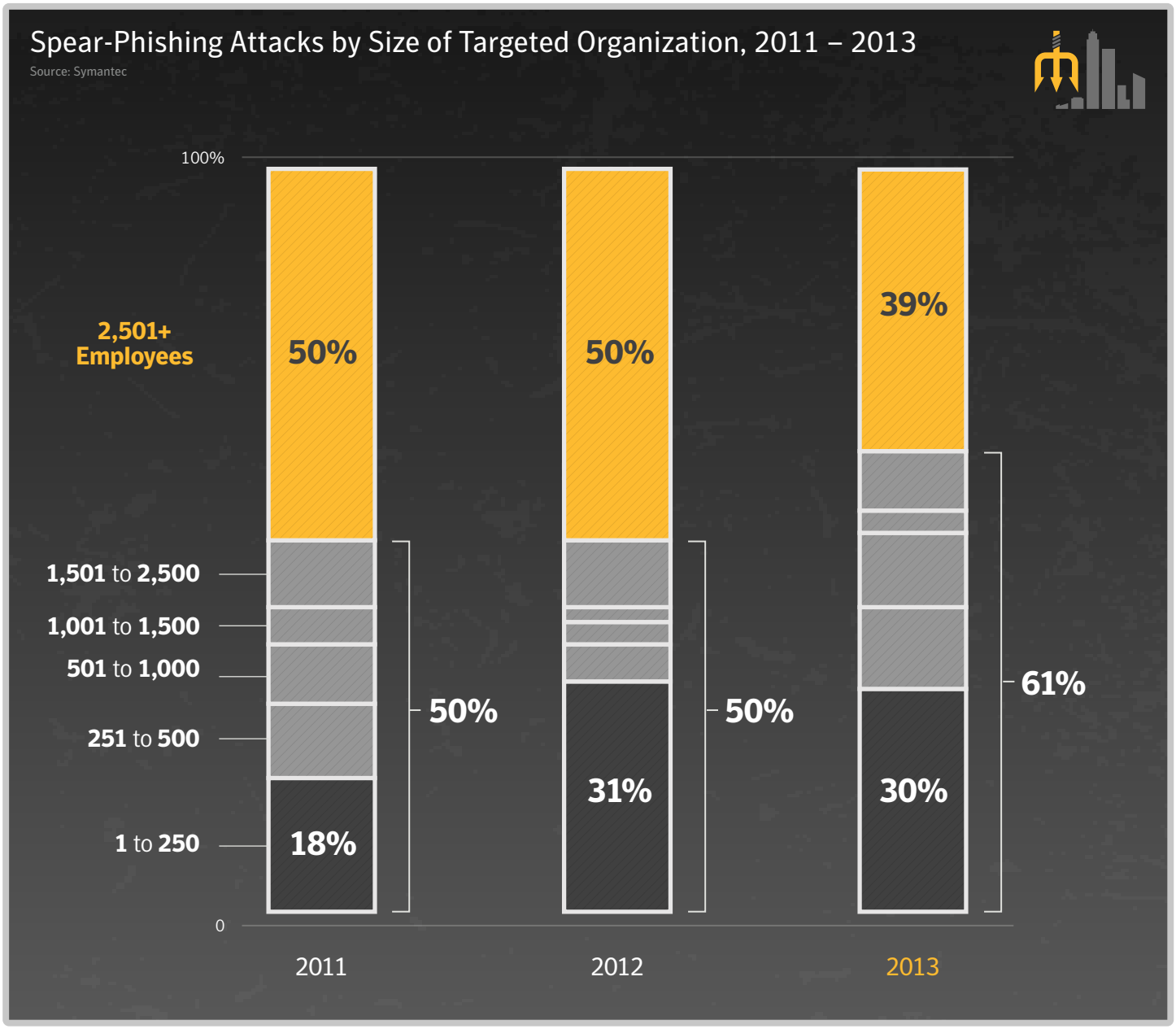


Politics and Targeted Attacks

While correlation doesn't always equal causation, it's often quite interesting never-the-less. This is especially true in the amalgamous region of targeted attacks, where it's difficult to prove motive. A good example of this came this year after negotiations concerning an energy partnership between two nation states. Sadly the negotiations broke down, but what followed was a significant increase in the number of targeted attacks against the Energy sector.

- *Public Administration[03] topped the industries targeted in 2013, comprising 16 percent of all attacks.*
- *Services, both professional and non-traditional,[04] came in second and third, respectively, in the overall number of attacks.*

Fig. 5



- *Targeted attacks aimed at small businesses (1-250 employees) in 2013 accounted for 30 percent of all such attacks, compared with 31 percent in 2012 and 18 percent in 2011. Despite the overall average being almost unchanged, the trend shows that the proportion of attacks at organizations of this size was increasing throughout the year, peaking at 53 percent in November.*
- *If businesses with 1-250 and 251-500 employees are combined, the proportion of attacks is 41 percent of all attacks, compared with 36 percent in 2012.*
- *Large enterprises comprising over 2,500+ employees accounted for 39 percent of all targeted attacks, compared with 50 percent in 2012 and 2011. The frontline in these attacks moved along the supply chain department. Large enterprises were more likely to be targeted though watering-hole attacks than through spear phishing.*

For example, in 2013, 1 in 54 Symantec.cloud customers were targeted with at least one spear-phishing email. The seriousness of attempted spear-phishing attacks is even clearer, using the same methodology, when comparing these numbers to the annual risk of an office fire. The odds of a building catching fire are, at worst, around one in 161.[05]

These odds change depending on the industry, the size of the organization, and an individual's role within the organization. This risk can be calculated using epidemiology concepts commonly applied to public health issues,[06] in this case applying them to the industry and job role. Epidemiology is frequently used in medicine to analyze how often diseases occur in different groups of people and why. In this way, if targeted attacks are considered to be disease agents, it is possible to determine which groups are more or less at risk based on exposure to the disease. In this case,

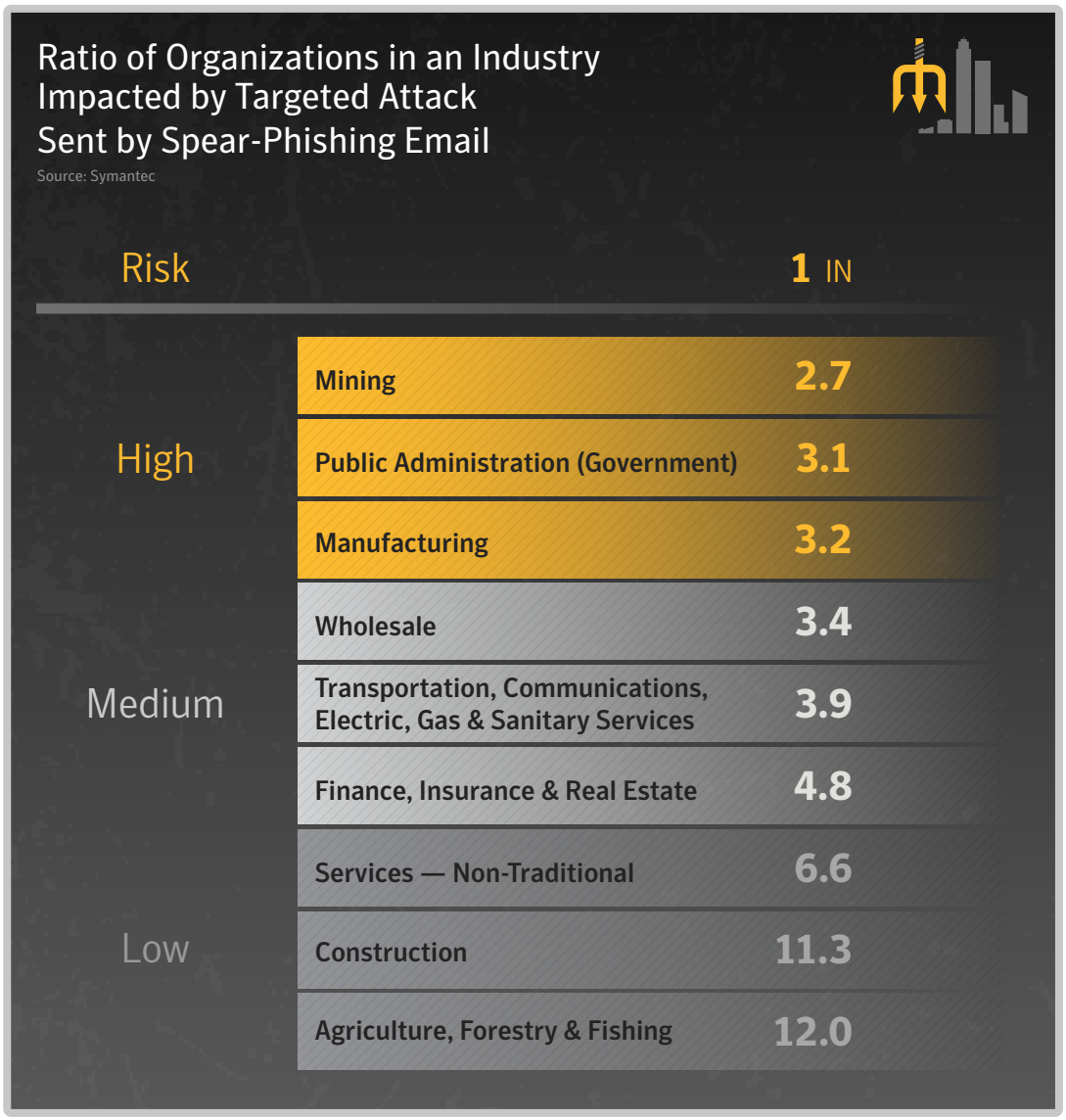
Fig. 6

- *Personal assistants, people working in the media, and senior managers are currently most at risk of being targeted by a spear-phishing campaign, based on observations in 2013.*
- *C-level executives, recruitment, and research and development are less likely to be targeted in the near future solely because of their job role.*

Theft in the Middle of the Night

On occasion, evidence of a cybercrime comes from an unexpected source. One company in the financial sector noticed an unusual early morning money transfer on a particular day, and from a particular computer. The company decided to check the CCTV footage and discovered that there was no one sitting at the computer at the time of the transaction. A back door Trojan was discovered during the examination of the computer. The threat was removed, but not before the attackers behind the attack made off with more than €60,000.

Fig. 7

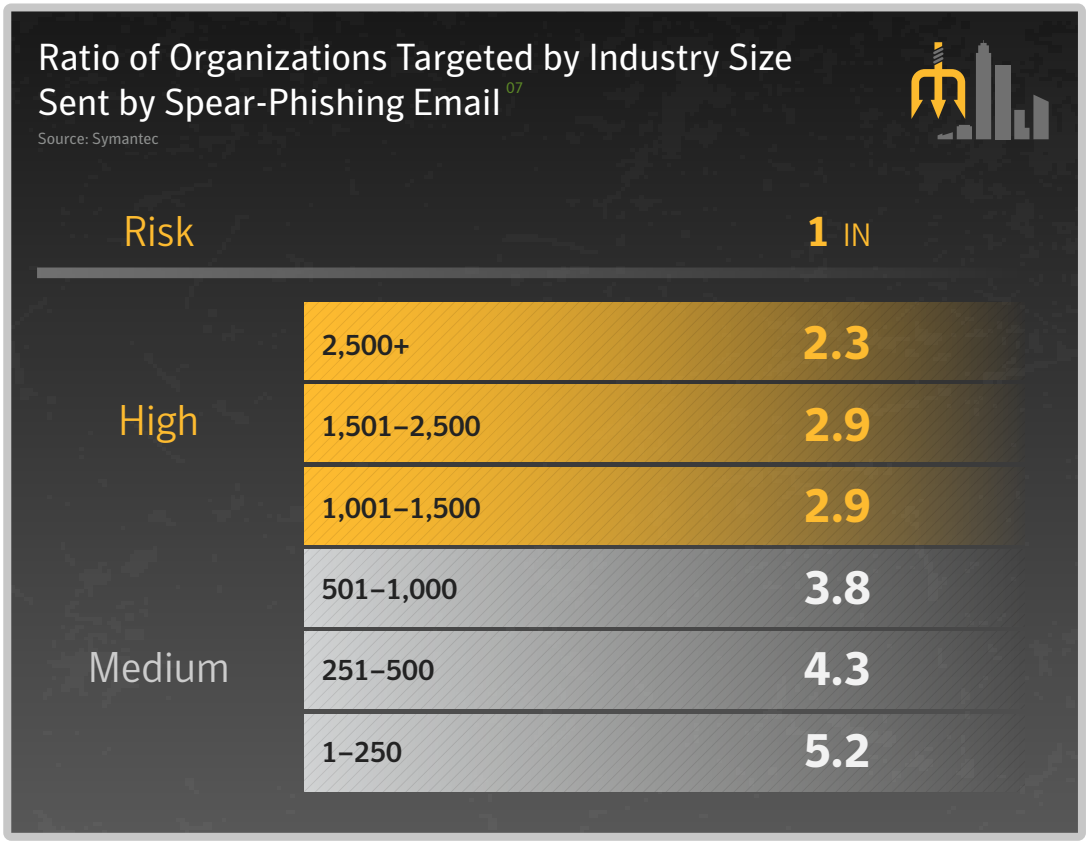


- *Mining, Manufacturing, and Public Administration were high-risk industries based on observations made in 2013. For example, approximately 1 in 3 Symantec.cloud customers in these sectors were subjected to one or more targeted spear-phishing attacks in 2013.*
- *Although only 0.9 percent (1 in 110) of all spear-phishing attacks were aimed at the Mining sector in 2013, one-third of Mining organizations were targeted at least once. This indicates a high likelihood of being targeted, but the frequency and volume of attacks is relatively low compared to other sectors.*
- *Similarly Wholesale, Transportation, and Finance may be classified as medium-risk industries.*
- *Non-traditional services, Construction, and Agriculture fell below the base line, which means that the organizations in these industry sectors were unlikely to have been targeted solely for being in that sector.*

we were not just focused on the organizations being targeted within a particular sector, but on other organizations within the same industry which may not be targeted. In this way we were able to more accurately determine the odds ratio for any one type of organization being targeted. It's similar to the way risk is calculated for diseases such as lung cancer, and calculating the probability of developing the disease from exposure to tobacco smoke.

Of course an organization's risk will either rise or fall depending on their industry and number of employees (figure 8). For the individual, another factor will be their job role, as shown in figure 6.

Fig. 8



- *The larger the company, the greater risk of receiving a spear-phishing email.*
- *One in 2.3 organizations with 2500+ employees were targeted in at least one or more spear-phishing attacks, while 1 in 5 small or medium businesses were targeted in this way.*

Fig. 9

Analysis of Spear-Phishing Emails Used in Targeted Attacks

Source: Symantec

Executable type	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

- *More than 50 percent of email attachments used in spear-phishing attacks contained executable files in 2013.*
- *Microsoft Word and PDF documents were both used regularly, making up 7.9 and 5.3 percent of attachments respectively. However, these percentages are both down from 2012.*
- *Java .class files also made up 4.7 percent of email attachments used in spear-phishing attacks.*

Watering Holes

In 2013, the most sophisticated form of targeted attacks made use of "watering holes". First documented in 2011,[08] this attack technique requires the attackers to infiltrate a legitimate site visited by their target, plant malicious code, and then lie in wait. As a drive-by download tactic, it can be incredibly potent. For example, the Hidden Lynx[09] attacks infected approximately 4,000 users in one month alone. In some cases other visitors to a watering-hole site may not be the intended target, and are therefore either served with other forms of malware or no malware at all, rather than being subjected to the attack reserved for the primary target. This illustrates that while effective, watering holes may be used as a longer-term tactic, requiring a degree of patience on the part of the attackers as they wait for their intended target to visit the site unprompted.

To set up a watering hole, attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site. Compromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Security Solutions division[10] found that 77 percent of sites contained vulnerabilities. Of these, 16 percent were classified as critical vulnerabilities that allow attackers to either access sensitive data, alter website content, or compromise a visitor's computers. This means that when an attacker looked for a site to compromise, one in eight sites made it relatively easy to gain access.

When a website is compromised, the attackers are able to monitor the logs of the compromised site in order to see who is visiting the website. For instance, if they are targeting organizations in the defense industry, they may look for IP addresses of known defense contractors. If these IP addresses are found in the traffic logs, they may then use the website as a watering hole.

Attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site.

Fig. 10

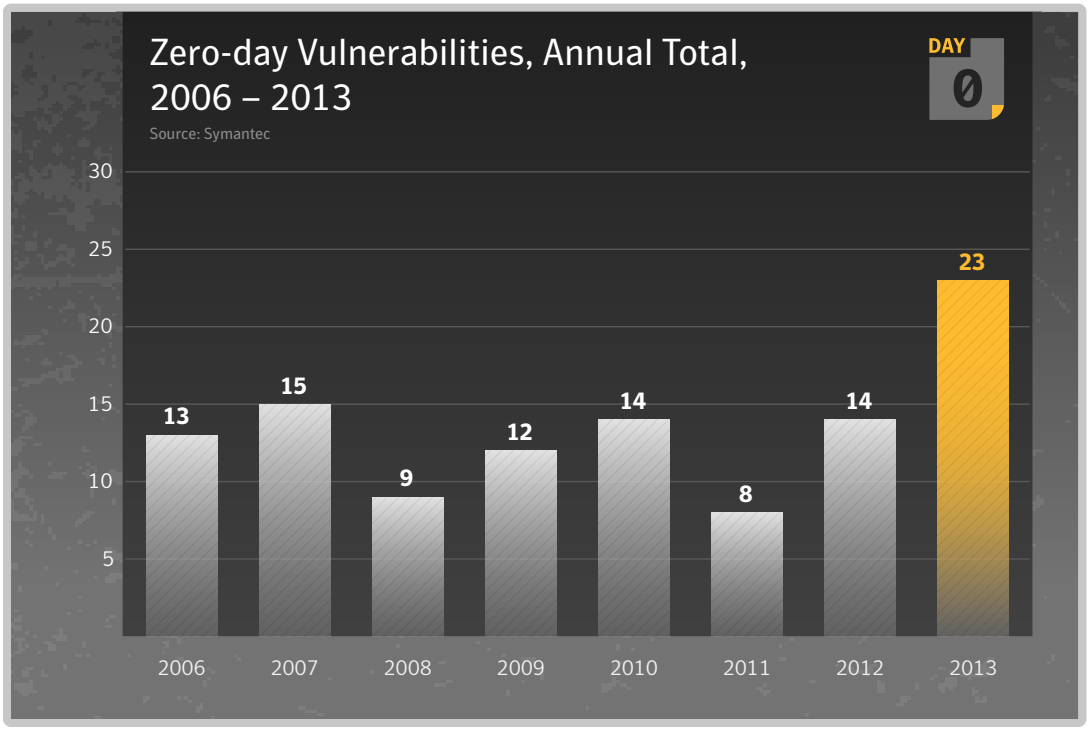
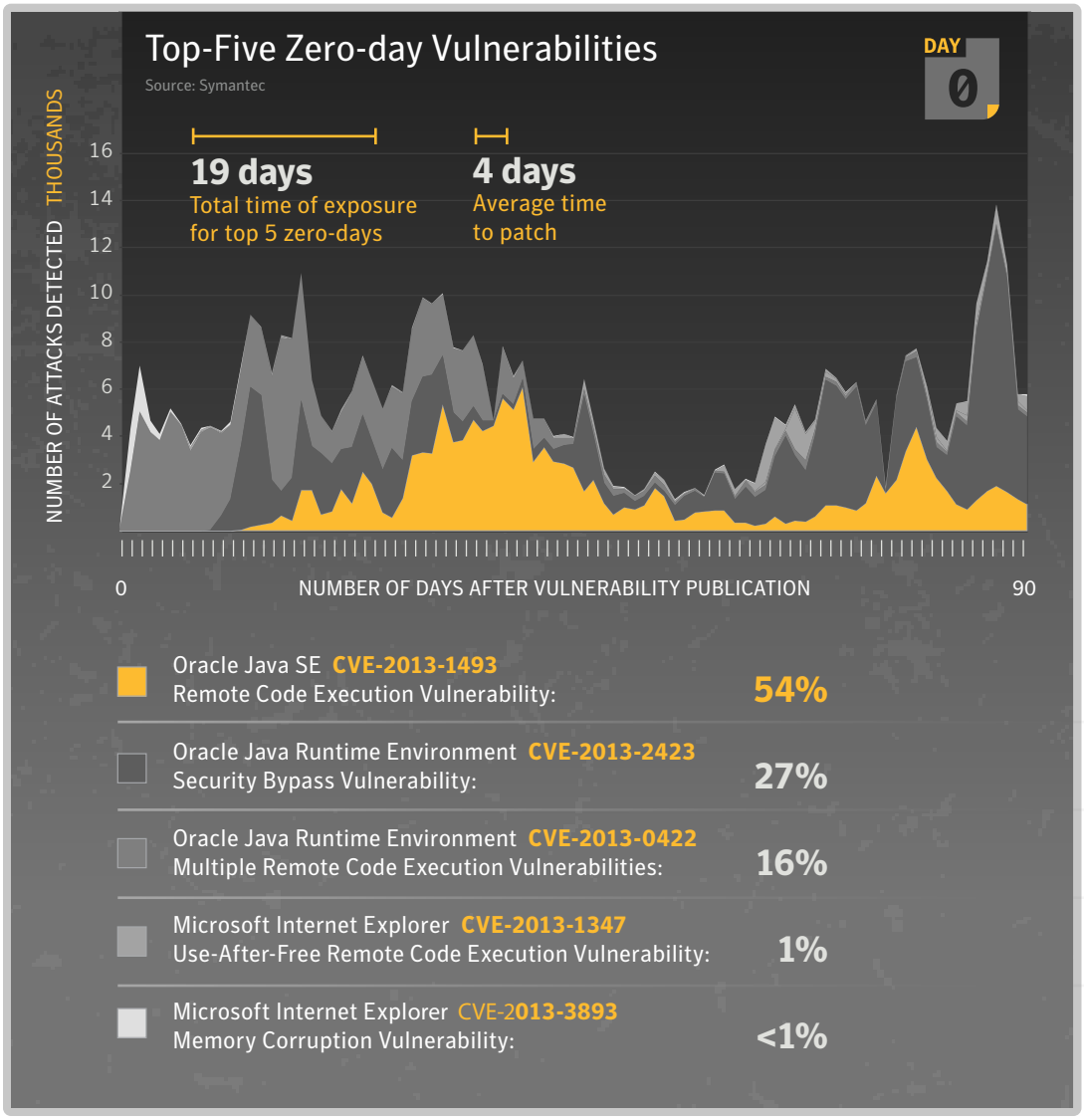


Fig. 11



- *The chart above shows the malicious activity blocked by Symantec endpoint technology for the most frequently exploited vulnerabilities that were identified as zero-days in 2013.*
- *Within the first 5-days after publication, Symantec blocked 20,813 potential attacks, which grew to 37,555 after 10 days. Within 30 days the total for the top five was 174,651.*
- *For some zero-day vulnerabilities, there was a higher amount of malicious activity very soon after publication, an indication of exploits being available in the wild before the vulnerability was documented. For example, with CVE-2013-0422 after five days Symantec had blocked 20,484 malicious actions against that vulnerability, and 100,013 after just 30 days.*

Attackers can even send the malicious payloads to particular IP address ranges they wish to target, in order to minimize the level of collateral damage from other people visiting the site which potentially draws attention to the existence of the attack.

Watering holes rely heavily on exploiting zero-day vulnerabilities because the chances of the attack being discovered are low. The number of zero-day vulnerabilities which were used in attacks during 2013 increased, with 23 new ones discovered during the year. This is an increase from the 14 that were discovered in 2012, and the highest figure since Symantec began tracking zero-day vulnerabilities in 2006.

In 2013 the majority of attacks that used zero-day vulnerabilities focused on Java. Java held the top three spots in exploited zero-day vulnerabilities, responsible for 97 percent of attacks that used zero-day vulnerabilities after they were disclosed. When looking at the top five zero-day vulnerabilities, the average exposure window between disclosure and an official patch was 3.8 days, and comprised a total of 19 days where users were left exposed.

One reason why watering-hole attacks are becoming more popular is that users aren't instinctively suspicious of legitimate websites that they know and trust. In general such attacks are set up on legitimate websites that contain specific content of interest to the individual or group being targeted. The use of zero-day vulnerabilities on legitimate websites made watering holes a very attractive method for attackers with the resources to orchestrate such an attack.

Network Discovery and Data Capture

If attackers successfully compromise an organization they may traverse the network, attempt to gain access to the domain controller, find documents of interest, and exfiltrate the data. Downloaders were popular tools used to gain further control within an organization's network. Often referred to as "stage-one back doors", these highly versatile forms of malicious code allow the download of other different malware, depending on what may be needed to carry out their objectives. The main reason that attackers use downloaders is that they're lightweight and easy to propagate. Once a downloader enters a network it will, by definition, download more traditional payloads such as Trojan horses to scan the network, keyloggers to steal information typed into compromised computers, and back doors that can send stolen data back to the attacker.

Once on the network, an attacker's goal is generally to traverse it further and gain access to various systems. Info-stealing Trojans are one of the more common payloads that an attacker will deliver. These Trojans quietly sit on compromised computers gathering account details. Password-dumping tools are used as well, especially when encountering an encrypted cache of passwords. These tools allow an attacker to copy encrypted (or "hashed") passwords and attempt to "pass the hash," as it is known, to exploit potentially vulnerable systems on the network.

The goal for the attacker is to gain elevated privileges on systems on the network that appeal to them, such as FTP access, email servers, domain controllers, and so on. Attackers can use these details to log into these systems, continue to traverse the network, or use them to exfiltrate data.

It's Not Just a Game Anymore

Video game companies have become the target of attackers, but for more than just to steal virtual currencies, as we've seen in previous years. It appears there has been a concerted effort by hacking groups to steal the source code of popular games, particularly those in the massively-multiplayer online role-playing game (MMORPG) genre. The hackers appear to have gained access through forged digital certificates, after which point they stole source code. The motive for doing so remains unclear, though it could be to monitor game users or simply to steal the intellectual property.

Case Study: Point of Sale Attacks

One of the most notable incidents in 2013 was caused by a targeted attack exploiting a retailer's point of sale (PoS) systems. This resulted in a significant breach of confidential customer records. These PoS systems handle customer transactions through cash or credit cards. When a customer swipes their credit or debit card at a PoS system, their data is sent through the company's networks in order to reach the payment processor. Depending on how the system is set up, attackers could take advantage of a number of flaws within the networks to ultimately allow them to get to their targeted data.

01 First, the attacker needs to gain access to the corporation's network that provides access to the PoS systems.

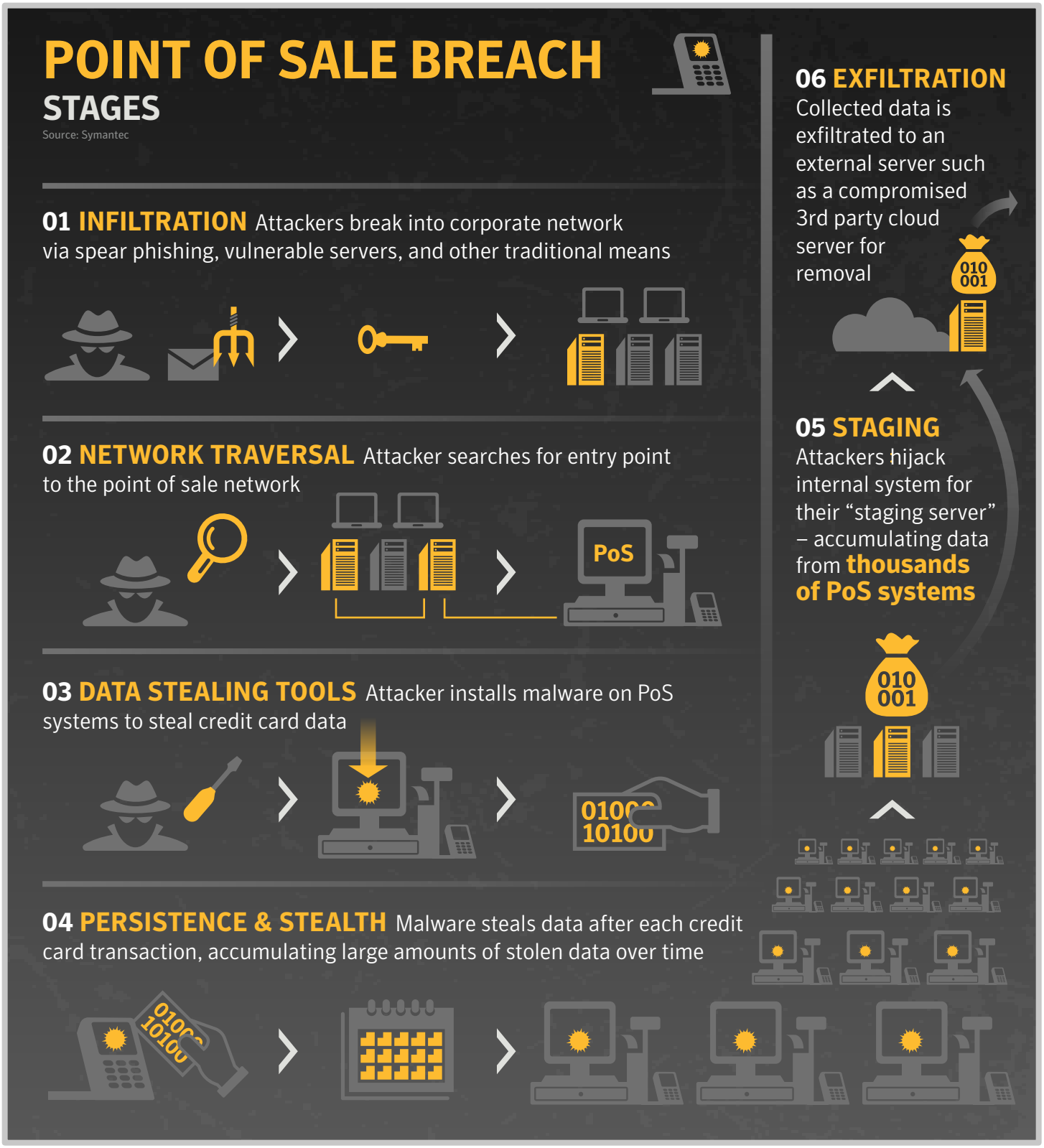
02 Once the attacker has established a beachhead into the network, they will need to get to their targeted systems. To achieve this, the attacker needs to either attempt to exploit vulnerabilities using brute-force attacks or steal privileged credentials from an employee through an information-stealing Trojan.

03 The attacker must then plant malware that steals sensitive financial data, such as network-sniffing tools, which steal credit card numbers as they move through internal unencrypted networks, or RAM-scraping malware, which gather credit card numbers as the computer reads them.

04 Once the malware is planted, the attacker needs to wait until enough financial data is collected before exfiltrating it. The stolen data is stored locally and is disguised by obfuscating file names and encrypting data. The attacker can also use the stolen administrator credentials to delete log files or disable monitoring software to cover their tracks.

05 When the time comes for the attacker to exfiltrate the data, they may use a hijacked internal system to act as their staging server. The stolen data will be passed to this server and when the time comes, the details will be transferred through any number of other internal systems before reaching an external system under the attacker's control.

Fig. 14


POINT OF SALE BREACH
STAGES
Source: Symantec
01 INFILTRATION Attackers break into corporate network via spear phishing, vulnerable servers, and other traditional means
02 NETWORK TRAVERSAL Attacker searches for entry point to the point of sale network
PoS
03 DATA STEALING TOOLS Attacker installs malware on PoS systems to steal credit card data
04 PERSISTENCE & STEALTH Malware steals data after each credit card transaction, accumulating large amounts of stolen data over time
05 STAGING
Attackers hijack internal system for their "staging server" – accumulating data from thousands of PoS systems
06 EXFILTRATION
Collected data is exfiltrated to an external server such as a compromised 3rd party cloud server for removal
010
001

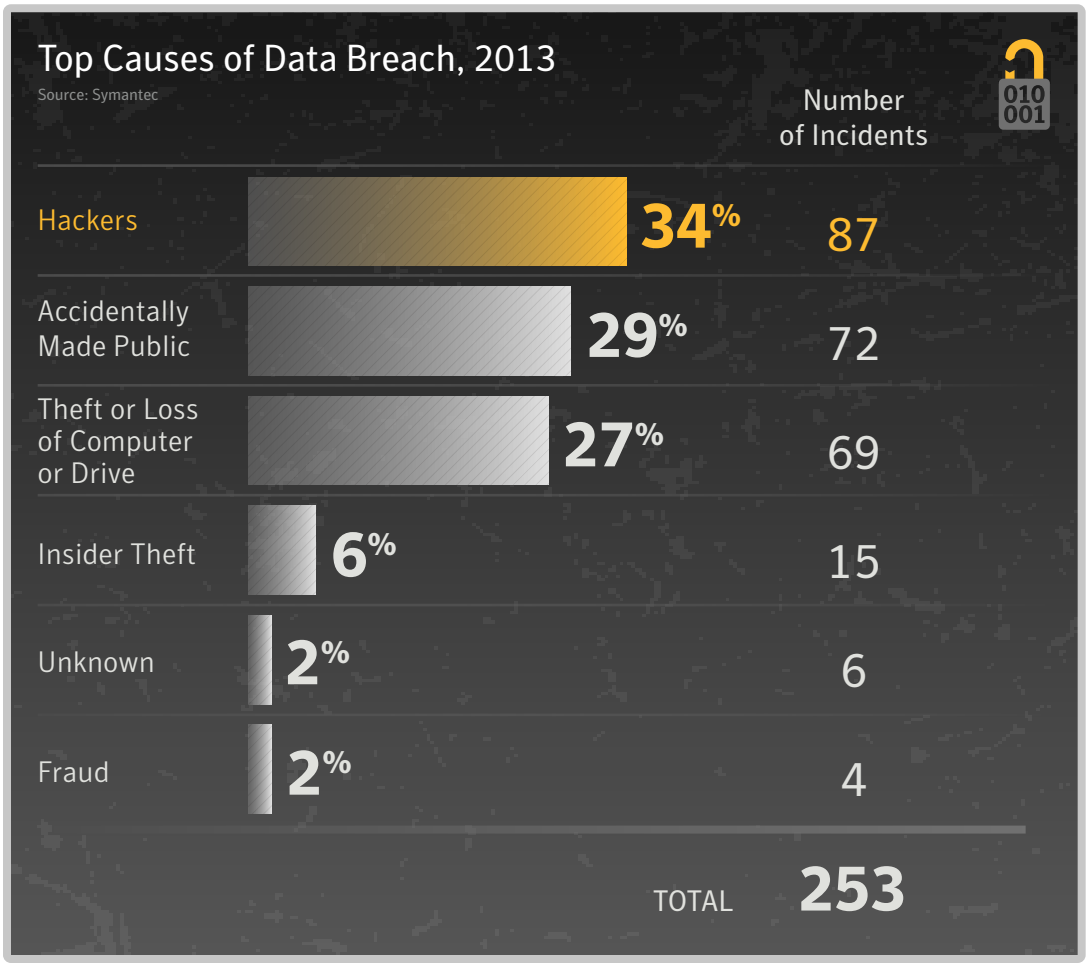
Data Breaches

We've seen a shift in 2013 in the causes of data breaches. When thinking of a data breach, what often comes to mind are outside attackers penetrating an organization's defense. Hacking continues to lead in terms of the number of breach causes, comprising 35 percent of data breaches in 2013, but this is down from 2012. At 28 percent, accidental disclosure is up 5 percentage points from 2012 and theft or loss is close behind it, up 4 percentage points to 27 percent.

There are many situations where data is exposed by the information leaving the organization silently. Sometimes it's a well-meaning employee simply hoping to work from home by sending a spreadsheet through third-party web-based email, a cloud service, or simply by copying the files to a USB drive.

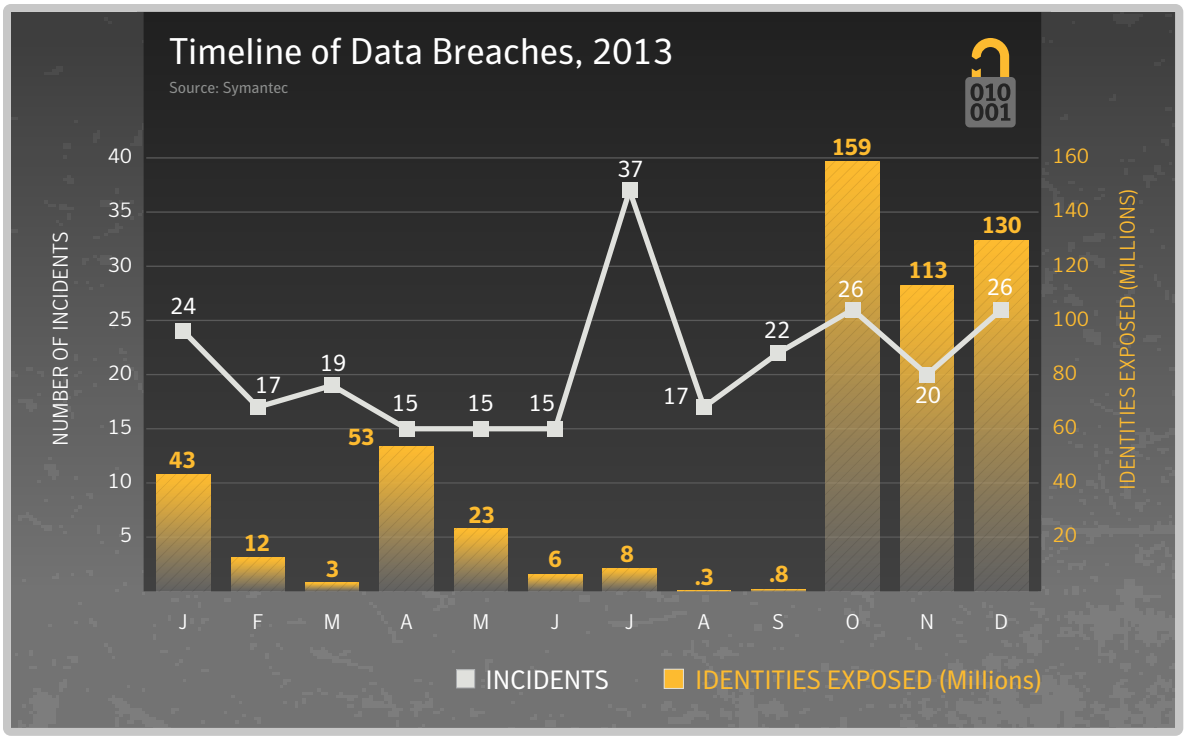
Alternatively system glitches may expose data to users who should not be able to see or share such material. For instance, users may be granted permissions on company storage resources that are higher than necessary, thus granting them too much access rather than just enough to do what they need. Privileged users, such as those granted administrative rights on work computers, are

Fig. 12



- ***Hacking was the leading source for reported identities exposed in 2013:*** *Hackers were also responsible for the largest number of identities exposed, responsible for 35 percent of the incidents and 76 percent of the identities exposed in data breach incidents during 2013.*
- *The average number of identities exposed per data breach for hacking incidents was approximately 4.7 million.*
- *Theft or loss of a device was ranked third, and accounted for 27 percent of data breach incidents.*

Fig. 13



- *There were 253 data breach incidents recorded by the Norton Cybercrime Index for 2013, and a total of 552,018,539 identities exposed as a result*
- *The average number of identities exposed per incident was 2,181,891, compared with 604,826 in 2012 (an increase of over 2.5 times)*
- *The median number of identities exposed was 6,777 compared with 8,350 in 2012. The median is a useful measure as it eliminates extreme values caused by the most notable incidents, which may not necessarily be typical.*
- *The number of incidents that resulted in 10 million or more identities being exposed in 2013 was eight, compared with only one in 2012.*

often more responsible for breaches than external hackers. These users try to access data they shouldn't have access to or tamper with protections, such as data loss prevention software meant to keep sensitive data from leaving the organization's network.

In many of these cases the employee does not believe that they are putting the company at risk. In fact, according to a survey conducted by Symantec and The Ponemon Institute, 53 percent of employees believe this practice is acceptable because it doesn't harm the company.[11]

That's not to say that attacks from hackers have suddenly slowed. In 2013 there were three record-breaking data breaches, where the numbers of identities exposed was in the hundreds of millions. These massive breaches highlight the importance of having defenses in place to keep outside intruders out as well as systems set up to stop sensitive information from leaving the network.

According to the 2013 Cost of a Data Breach study, published by Symantec and the Ponemon Institute,[12] the cost of the average consolidated data breach incident increased from US$130 to US$136. However, this number can vary depending on the country, where German and US companies experienced much higher costs at US$199 and US$188, respectively.

Consequences of a Data Breach

Data theft is not a victimless crime. Data breaches pose major consequences for both the corporations that experience them and the consumers who are victims of them.

Risks for the Corporations

If a company suffers a major data breach, it can face severe repercussions that could impact its business. First, there are the reputational damages that come with a data breach. The incident could cause consumers to lose trust in the company and move to their competitors' businesses. If the company suffered a large data breach it's likely to receive extensive media coverage, further damaging the corporation's reputation.

If the customers decide that the company was at fault for failing to protect their information from theft, they could file a class action lawsuit against the breached firm. For example, a class action lawsuit is being taken against a health insurer over the theft of two unencrypted laptop computers which held data belonging to 840,000 of its members.

Affected corporations could have other financial concerns beyond legal matters. We believe that on average, US companies paid US$188 per breached record over a period of two years. The only country hit with a bigger price tag was Germany, at US$199 per breached record. This price rose if the data breach was caused by a malicious attack. In these cases, US firms paid US$277 per breached record over two years, while German firms paid US$214 per record. These expenses covered detection, escalation, notification and after-the-fact response, such as offering data monitoring services to affected customers.

One US medical records company was driven to bankruptcy after a break-in which led to the exposure of addresses, social security numbers, and medical diagnoses of 14,000 people. When explaining its decision to file for Chapter 7 bankruptcy protection, the company said that the cost of dealing with the data breach was "prohibitive."

Data theft is not a victimless crime. Data breaches pose major consequences for both the corporations that experience them and the consumers who are victims of them.

Risks for the Consumers

Ultimately, consumers are the real victims of data breaches, as they face many serious risks as a result of this cybercrime.

One unintended risk for consumers whose data was stolen in this way is that their other online accounts could be compromised. Attackers use a victim's personal details to try to gain access to other accounts of more value, for example, through password reset features on websites. Depending on the stolen information, attackers could use the data to authorize bank account transfers to accounts under their control. They could also use victims' financial details to create fraudulent credit or debit cards and steal their money.

Consumers' own lax password habits could also cause several of their accounts to be compromised as the result of a data breach. If an attacker manages to obtain email addresses and passwords for one service as a result of a data breach, they could use this data to attempt to log in to other online services.

Medical identity theft could have a huge impact on the consumer, potentially costing victims thousands of dollars, putting their health coverage at risk, causing legal problems, or leading to the creation of inaccurate medical records. Attackers can use health insurance information, personal details, and social security numbers to make false claims on their victims' health insurance. They could take advantage of this data to get free medical treatment at the victims' cost, or even to obtain addictive prescription drugs for themselves or to sell to others. According to our data, the healthcare sector contained the largest number of disclosed data breaches in 2013 at 37 percent of those disclosed.

Medical identity theft could have a huge impact on the consumer, potentially costing victims thousands of dollars, putting their health coverage at risk, causing legal problems or leading to the creation of inaccurate medical records.

Why does it appear that the Healthcare sector is subject to a higher number of data breaches? One consideration is that few other industries can lay claim to needing to store such a variety of personally identifiable information about clients. By targeting a hospital's records, an attacker can easily gather a lot of personal information from these sources, especially if their goal is identity theft.

On the other hand, the healthcare industry is one of the most highly regulated industries, and required to disclose when and where a breach occurs. These sorts of disclosures garner lots of media attention. In contrast, many industries are less forthcoming when a breach occurs. For instance, if a company has trade secrets compromised, which doesn't necessarily impact clients or customers directly, they may not be quite as forthcoming with the information. Whatever the case, at 44 percent Healthcare continues to top our list of industries most impacted by data breaches.

Digital Privacy Concerns

If there ever was any question that governments are monitoring Internet traffic, a spotlight was cast on the subject in 2013. A variety of leaks during the year showed that, for better or for worse, there are agencies in the world who are largely gathering anything and everything they can.

In some cases it's one nation state monitoring another. In others it's a nation state monitoring the communications of its own citizens. While some governments have been thrust into the spotlight more than others, there's no question that it is happening in many places. Online monitoring was a major security and privacy talking point in 2013.

From June 2013, several news reports were released containing new information on the US National Security Agency's (NSA) data surveillance programs. More are yet to come, considering the sheer magnitude of documents leaked by Edward Snowden, the former NSA contractor who released the data. The documents claimed that over the course of several years the NSA collected metadata from phone calls and major online services, accessed the fiber-optic networks that

connected global data centers, attempted to circumvent widely-used Internet encryption technologies, and stored vast amounts of metadata gathered as part of these programs.

The US wasn't the only country engaged in cyber-espionage activities in 2013. The Snowden leaks also pointed the finger at the United Kingdom's Government Communications Headquarters (GCHQ), and the monitoring activities of other European spying agencies have come to light as well. In other parts of the globe, Symantec uncovered a professional hackers-for-hire group with advanced capabilities known as Hidden Lynx. The group may have worked for nation states, as the information that they targeted includes knowledge and technologies that would benefit other countries. Russia's intelligence forces were also accused of gaining access to corporate networks in the US, Asia, and Europe.

What's important to note is that the released data leading to many of the year's online monitoring stories was brought to the public from someone who was a contractor rather than a full-time employee, and considered a trusted member of the organization. These organizations also appeared to lack strong measures in place to prevent such data leaks, such as data loss prevention systems.

Unlike external attackers, insiders may already possess privileged access to sensitive customer information, meaning they don't have to go to the trouble of stealing login credentials from someone else. They also have knowledge of the inner workings of a company, so if they know that their organization has lax security practices they may believe that they could get away with data theft unscathed. Our recent research conducted with the Ponemon Institute says that 51 percent of employees claim that it's acceptable to transfer corporate data to their personal computers, as their organizations don't strictly enforce data security policies. Insiders could earn a lot of money for selling customer details, which may be motivation enough to risk their careers.

There are two big issues with online monitoring today, not just for governments, but also for organizations and ordinary citizens: Personal digital privacy, and the use of malware or spyware. It's clear that governments are monitoring communications on the internet, leading more Internet users to look into encryption to protect their communications and online activities. What's more troubling for those concerned about safeguarding their privacy is that nation states have largely adopted the same techniques as traditional attackers, using exploits and delivering malicious binaries. From a security perspective, there is very little difference between these techniques, targeted attacks, and cybercrime in general.

If there ever was any question that governments are monitoring Internet traffic, a spotlight has been cast on the subject in 2013

E-CRIME + MALWARE DELIVERY TACTICS

E-crime and Cyber Security

The use of computers and electronic communications equipment in an attempt to commit criminal activities, often to generate money, is generally referred to as e-crime and it continues to play a pivotal role in the threat landscape. The scope of what is covered by e-crime has also changed and expanded over the years and now includes a variety of other potentially illegal activities that may be conducted online, such as cyber bullying, the hijacking of personal data, and the theft of intellectual property.

The threats used to carry out the more traditional e-crime attacks rely heavily on social engineering in order to succeed, and may be delivered in one of two ways; through web-based activity, drive-by downloads, or by email; similar to the way spam campaigns are conducted.

The criminals behind these e-crime attacks are well organized, having a sophisticated malicious distribution network behind them. This plays out in a format where different attackers carry out different tasks. One group will focus on compromising computers, another will configure and administer those computers to carry out various malicious activities, while yet another will broker deals for renting the use of those compromised computers to other cybercriminals.

At a Glance

- *The criminals behind e-crime have set up sophisticated malicious distribution networks.*
- *The monthly volume of ransomware has increased by over six times since the beginning of 2013.*
- *Web attack toolkits continue to be a primary method for compromising computers, even with the arrest of the alleged creator of the Blackhole exploit kit in 2013.*
- *The number of vulnerabilities disclosed has reached record levels in 2013.*

Botnets and the Rental Market

Cybercriminals involved in e-crime generally start out by working to get malware onto computers, turning them into "zombies" with the aim of adding them to larger networks of similarly compromised computers, called botnets, or "robot networks". A botnet can be easily controlled from a central location, either through a command and control (C&C) server or a peer to peer (P2P) network. Zombie computers connected to the same C&C channels become part of the same botnet.

Botnets are an extremely potent asset for criminals because they can be used for a wide variety of purposes, such as sending spam emails, stealing banking information, conducting a distributed denial-of-service (DDoS) attacks against a website, or a variety of other malicious activities. They have also become a core tool for administering compromised computers that are rented to yet another third party for malicious purposes.

Botnets are an extremely potent asset for criminals because they can be used for a wide variety of purposes

Adding a computer to a botnet is generally just the first step. The attackers seek out other cybercriminals in the hope that they can lease the botnets for various purposes. This rental style gives the initial attacker a lot of leverage and flexibility concerning how they monetize and use the computers they've compromised and look after. Configurations can vary widely, focused on types of computers, regions, languages, or other features that the buyer is looking to gain access to. Prices also vary depending on the length of rental and the job for which the computers are to be used.

For example, infections in some countries are considered more valuable than others. In the case of click fraud, an infection will create fake user clicks on advertisements to earn affiliate fees. American and UK computers tend to be preferred because pay-per-click advertisers in these countries will pay more. The same applies to banking Trojans, which are generally more focused on targeting Western bank accounts.

The good news is that there were a number of takedowns that occurred in 2013. Of particular note are the efforts to take down the Bamital and ZeroAccess botnets.

Bamital was taken down in February, thanks to a cooperative effort on the part of Symantec, Microsoft, Spain's Civil Guardia, and Catalunyan CERT (CESICAT).This botnet had been responsible for a significant amount of click-fraud traffic, generating upwards of three million clicks per day at its peak.[13] To perform click fraud, the botnet would hijack the search results typed into

Fig. 1

Malicious Activity by Source: Bots, 2012–2013

Source: Symantec

Country/Region	2013 Bots Rank	2013 Bots %	2012 Bots Rank	2012 Bots %
United States	1	20.0%	1	15.3%
China	2	9.1%	2	15.0%
Italy	3	6.0%	5	7.6%
Taiwan	4	6.0%	3	7.9%
Brazil	5	5.7%	4	7.8%
Japan	6	4.3%	6	4.6%
Hungary	7	4.2%	8	4.2%
Germany	8	4.2%	9	4.0%
Spain	9	3.9%	10	3.2%
Canada	10	3.5%	11	2.0%

- *Unsurprisingly, the US and China have the most densely populated bot populations, largely owing to their large Internet populations. The US population are avid users of the Internet, with 78 percent Internet penetration, but undoubtedly their keen use of the Internet contributes to their popularity with malware authors. China also has the largest population of Internet users in the Asia region, with 40 percent Internet penetration and accounting for approximately 50 percent of the Internet users in the Asia region.*[14]
- *Italy has a lower percentage of bots in the country, but is ranked third highest in 2013, compared with fifth in 2012.*
- *The US, Germany, Spain and Canada all increased their relative proportions of the world's bots in 2013, while the proportions in the other geographies listed has diminished.*

compromised computers, redirecting the users to predetermined pay-per-click sites, with the goal of making money off those clicks. When a computer is used to perform click fraud, the user will rarely notice. The fraud consumes few computer resources to run, and at the most takes up extra bandwidth with the clicks. The attackers make money from pay-per-click advertisers and publishers—not from the user. This is in contrast with other forms of malware such as ransomware, where it is clear that an infection has occurred. A computer may be used in a click-fraud operation for an extended period of time, performing its activity invisibly during the daily operation of the computer.

The partial takedown during the year made a lasting impact on the operations of the ZeroAccess botnet. Symantec security researchers looking at the threat discovered a flaw in ZeroAccess that could allow them to sinkhole computers within the botnet. The operation succeeded in liberating approximately half a million ZeroAccess clients from the botnet network.[15]

At that time, ZeroAccess was one of the larger botnets in existence, and one that used P2P communications to maintain links between clients. These types of P2P botnets tend to be quite large overall; Helios and Zbot (a.k.a. GameOver Zeus) are two other examples of large botnets that use similar communication mechanisms. It isn't entirely clear if these botnets are big because they utilize P2P, or they utilize P2P because they're big. However, using P2P for communications does make it more difficult to take down a botnet, given the lack of a centralized C&C server.

Large botnets like Cutwail and Kelihos have made their presence felt in the threat landscape this year by sending out malicious attachments. The threats are generally like banking Trojans or downloaders, such as Downloader.Ponik and Downloader.Dromedan (also called Pony and Andromeda respectively), which download more malware.

Trojan.Zbot (a.k.a. Zeus) continues to make an impact in the botnet world. Having its malicious payload based on easy-to-use toolkits has allowed Zbot to maintain its popularity with threat actors. In 2013 we've seen Zbot being packed in different ways and at different times in order to evade detection. These packing techniques appear almost seasonal in their approach to evading detection, but underneath it all it's always the same Zeus code base.

Fig. 2

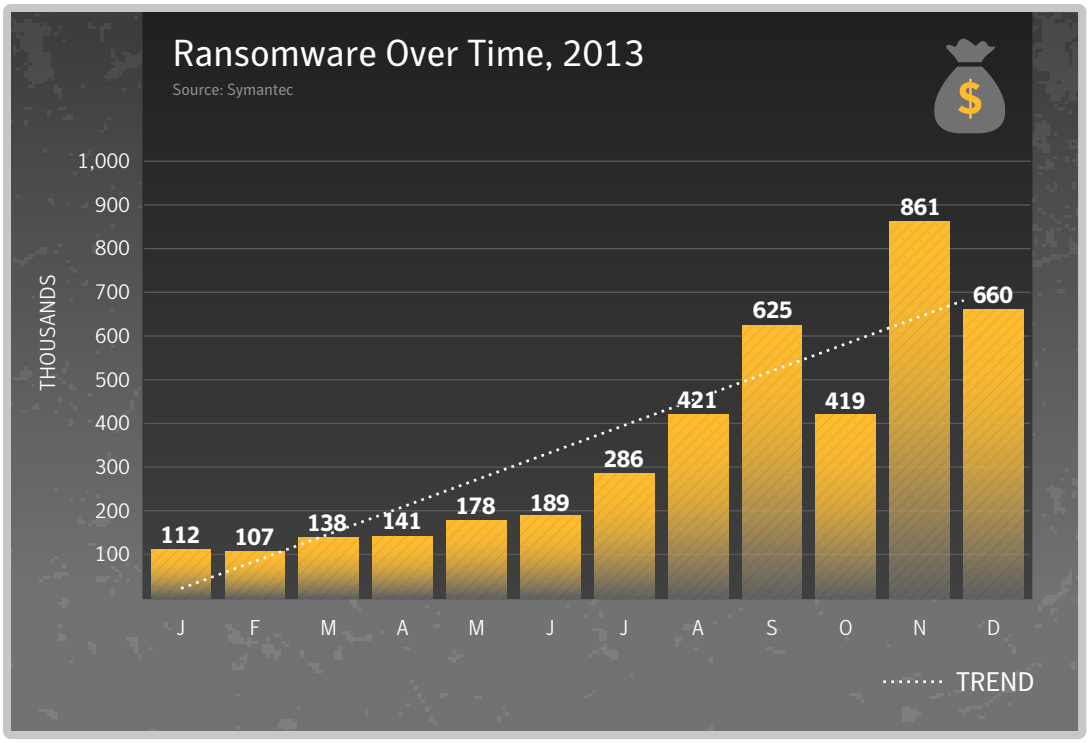
Top-Ten Botnets, 2013

Source: Symantec

Spam Botnet Name	Percentage of Botnet Spam	Estimated Spam Per Day	Top Sources of Spam From Botnet		
KELIHOS	46.90%	10.41BN	Spain 8.4%	United States 7.2%	India 6.6%
CUTWAIL	36.33%	8.06BN	India 7.7%	Peru 7.5%	Argentina 4.8%
DARKMAILER	7.21%	1.60BN	Russia 12.4%	Poland 8.3%	United States 8.1%
MAAZBEN	2.70%	598.12M	China 23.6%	United States 8.2%	Russia 4.8%
DARKMAILER3	2.58%	573.33M	United States 18.2%	France 10.4%	Poland 7.5%
UNKNAMED	1.17%	259.03M	China 35.1%	United States 10.0%	Russia 7.5%
FESTI	0.81%	178.89M	China 21.9%	Russia 5.8%	Ukraine 4.7%
DARKMAILER2	0.72%	158.73M	United States 12.6%	Belarus 8.3%	Poland 6.6%
GRUM	0.53%	118.00M	Russia 14.5%	Argentina 6.9%	India 6.9%
GHEG	0.35%	76.81M	Poland 17.4%	Vietnam 12.1%	India 11.5%

- *76 percent of spam was sent from spam botnets, down from 79 percent in 2012.*
- *It is worth noting that while Kelihos is the name of a spam-sending botnet, Waledac is the name of the malware used to create it. Similarly, Cutwail is another the spam-sending botnet and Pandex is the name of the malware involved.*

Fig. 3



- *Monthly ransomware activity increased by 500 percent from 100,000 in January to 600,000 in December, increasing to six times its previous level.*

Ransomware: When Data Becomes a Hostage to Fortune

In October 2013, the US Federal Bureau of Investigation issued a warning about a new type of malware that had appeared. The threat, known as CryptoLocker, encrypted a victim's documents and demanded payment in return for the decryption key. Two weeks later, the UK equivalent of the FBI, the National Crime Agency, also issued a public warning about CryptoLocker. It isn't often that one piece of malware mobilizes law enforcement agencies across the world, and it is indicative of the level of panic created by CryptoLocker during 2013.

Despite the hype, CryptoLocker is not a completely new malware. Instead it is the latest evolution of a family of threats known as ransomware. Ransomware first came to prominence a decade ago. The business model usually involves the victim's computer being locked. Attackers demand a ransom in order to remove the infection.

However, CryptoLocker has managed to capture the public imagination because it represents the perfect ransomware threat: It encrypts the user's data and, unlike most malware infections, no fix can rescue it. CryptoLocker uses strong encryption, meaning the victim is left with the unpalatable choice of saying goodbye to their valuable personal data or paying the attackers a ransom fee.

Symantec noticed a significant upsurge in the number of ransomware attacks during 2013. During January we stopped over 100,000 infection attempts. By December that number had risen more than six-fold. There was a noticeable uptick in detection from the month of July onwards, peaking in November.

CryptoLocker first began to circulate in September, and while CryptoLocker detections grew quickly (by 30 percent in December alone), the number of definitive CryptoLocker detections is still a very small proportion of overall ransomware detections. For example, in December only 0.2 per cent (1 in 500) of all ransomware detections by Symantec was indisputably identified as CryptoLocker.

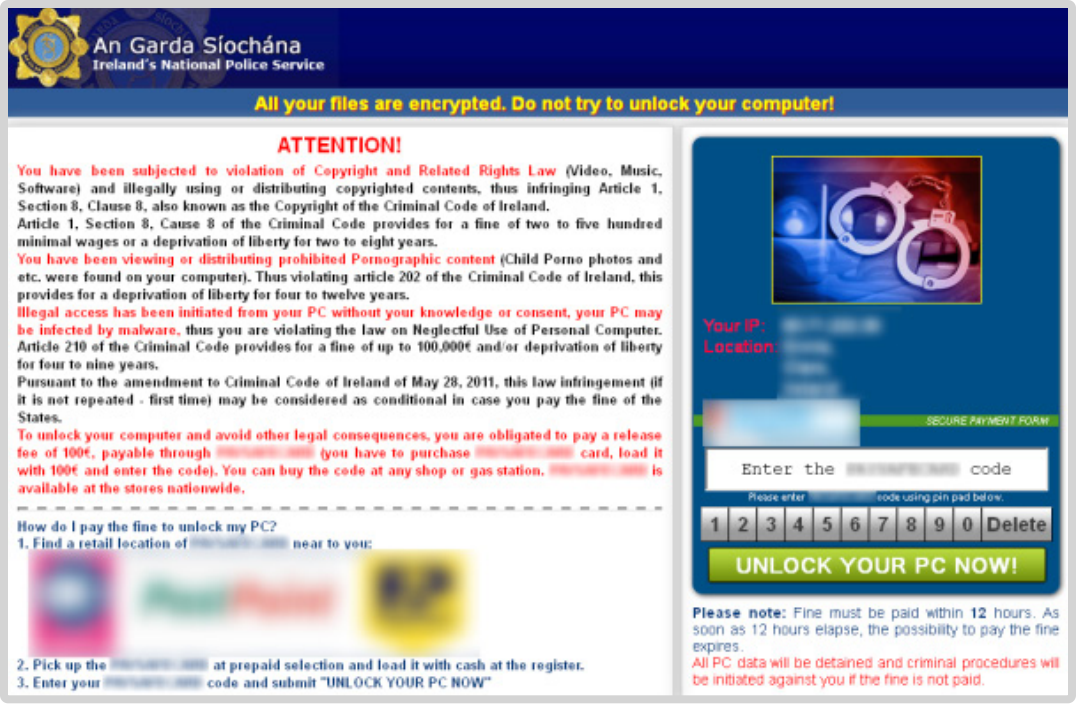


Fig. 4 Browser-based ransomware threat, Browlock.

Ransomware, including CryptoLocker, continues to prove lucrative for attackers. Symantec research indicates that on average, 3 percent of infected users will pay the ransom.

However, this statistic only tells part of the story, and its prevalence may be higher. CryptoLocker is often blocked by intrusion prevention systems (IPS) which may simply identify it as generic ransomware rather than a specific variant.

Ransomware, including CryptoLocker, continues to prove lucrative for attackers. Symantec research indicates that on average, 3 percent of infected users will pay the ransom. These figures tally with work done by other researchers.[16]

Analysis by Symantec of the ransoms demanded by CryptoLocker infections indicates that most variants demand US$100 to $400 for a decryption key. This is roughly in line with the ransom amount demanded by other ransomware variants. Although CryptoLocker is a more effective threat, attackers have yet to take advantage of this by demanding larger ransoms.

The amount of money being paid in ransom is difficult to assess, however some efforts have been made to track payments made through Bitcoin. All Bitcoin transactions are logged as public record, and searching for Bitcoin addresses used to collect ransom can yield some insight. From the small number of Bitcoin addresses analyzed, it is clear that ransomware distributors have without a doubt earned tens of millions over the last year.

Analysis of ransom amounts is complicated somewhat by the fact that many variants demand payment in Bitcoin. Our analysis of CryptoLocker ransom demands found that attackers generally seek between 0.5 and 2 Bitcoin. Lower ransom demands began appearing near the end of 2013. This reduction had less to do with any newfound altruism on the part of attackers and more to do with the soaring value of Bitcoin. The virtual currency was trading at just over US$100 when CryptoLocker first appeared in September. By December its value had increased to over US$1,000.

This suggests that attackers have concluded that US$100 to $400 is the optimum ransom amount, and they will move to adjust their demand to avoid pricing themselves out of the market. Some attackers have also refined their ransom tactics by introducing a second, larger ransom of 10 Bitcoin for victims who miss the original 72 hour deadline. The attackers appear to have concluded that some potential opportunities were left unexploited by their original business model, with some victims willing to pay significant amounts for the return of valuable data. This higher ransom tier may also have the secondary purpose of exerting additional pressure on victims to pay within the deadline.

Meanwhile, older ransomware attack techniques have started to seep into markets previously unexploited. More localized content, based on location data, has started to appear in Latin American countries. In many ways, this form of ransomware is similar to what has been seen in English-speaking countries in previous years. The reasons behind this are likely precipitated by the increasing availability of online payment providers in these regions. With easy options for payment, ransomware has begun to appear in these areas, with the Reventon and Urausy versions already having been discovered with Spanish variants.

In the grand scheme of the threat landscape, ransomware does not make up a huge percentage of overall threats, but it clearly does serious damage particularly to the victims who may not have backed-up their data to begin with. In the future, new ransomware schemes may emerge. Since some groups have had success with it, others may jump on the bandwagon. Toolkits for creating these types of ransomware have been developed. Browser-based ransomware also began to appear near the end of the year, which uses JavaScript to prevent a user from closing the browser tab,[17] and more of these ransomware-type scams will likely be seen in the future.

In the grand scheme of the threat landscape, ransomware does not make up a huge percentage of overall threats, but it clearly does serious damage, particularly to the victims who may not have backed-up their data to begin with.

Banking Trojans and Heists

Banking Trojans are a fairly lucrative prospect for attackers. Today's threats continue to focus on modifying banking sessions and injecting extra fields in the hope of either stealing sensitive banking details or hijacking the session. Some of the more common banking Trojans include Trojan.Tiylon[18] and a variant of the Zbot botnet, called Gameover Zeus. Symantec's State of Financial Trojans 2013 whitepaper[19] concluded that in the first three quarters of 2013, the number of banking Trojans tripled. More than half of these attacks were aimed at the top 15 financial institutions, though over 1,400 institutions have been targeted in 88 countries. While browser-based attacks are still common, mobile threats are also used to circumvent authentication through SMS messages, where the attacker can intercept text messages from the victim's bank.

The most common form of attack continues to be financial Trojans which perform a Man-In-The-Browser (MITB) attack on the client's computer during an online banking session. Symantec analyzed 1,086 configuration files of 8 common financial Trojans. The malware was configured to scan for URLs belonging to 1,486 different organizations. All of the top 15 targeted financial institutions were present in more than 50 percent of the analyzed configuration files.

In addition to those attacks, Symantec observed an increase in hardware-supported attacks in 2013. Besides the still popular skimming attacks, a new piece of malware was discovered named Backdoor.Ploutus which targeted ATMs. Initially discovered in Mexico, the malware soon spread to other countries, with English versions emerging later.

The malware allows for criminals to effectively empty infected ATMs of cash. The malware is applied to the ATM by physically inserting a malicious CD-ROM and causing the machine to boot from it. While booting, the malware is installed onto the system. The attacker can then use specific key combinations on the keypad to interact with the malware and initiate the ultimate goal – to

dispense all available cash from the cassettes. Later variants allow cash to be dispensed by sending a special SMS to an installed GSM modem at the ATM.

Meanwhile in Britain, a gang attempted to steal millions from a bank in London by attaching a KVM wireless switch to computers at one of the bank's branches. They infiltrated the branch by posing as computer repair personnel. This allowed them to remotely control these computers over a wireless link, most likely with intent to leverage this access to defraud the bank. However, the attack was foiled and the police arrested 12 men involved in this scam. A similar attack on another bank in London resulted in eight arrests. In this case the attackers were successful in transferring funds of around £1.3 million from the bank through KVM-controlled machines. The wireless transmitter packages were installed a day earlier by an attacker disguised as an IT technician.

These examples highlight the trend that attackers are increasingly targeting physical systems directly at financial institutions. This is similar to the trend that what we have observed with attacks against point of sale (PoS) systems at retailers.

Another popular method employed last year was to use DDoS attacks as distractions while the attackers conducted the fraudulent transactions. A construction company and its bank in California were attacked using this method: While a classic Zeus Trojan started to transfer US$900,000 out of clients' accounts, the attackers started a DDoS attack against the bank to obfuscate their actions and to keep the bank's Computer Emergency Readiness Team (CERT) busy.

Attackers are trying to extract every last bit of money possible by utilizing every monetization option at their disposal with the compromised computers they control.

Monetization: Malware as a Commodity

E-crime in 2013 can be summed up as follows: Attackers are trying to extract every last drop of cash available, using every monetization option at their disposal with the compromised computers they control. Compromised computers have essentially become just another commodity, where attackers work to maximize the ways they make money from them.

Fig. 5

Top-Ten Malware, 2013

Source: Symantec

Rank	Name	Overall Percentage
1	W32.Ramnit	15.4%
2	W32.Sality	7.4%
3	W32.Downadup	4.5%
4	W32.Virut	3.4%
5	W32.Almanahe	3.3%
6	W32.SillyFDC	2.9%
7	W32.Chir	1.4%
8	W32.Mabezat	1.2%
9	W32.Changeup	0.4%
10	W32.Xpaj	0.2%

The attackers will generally monitor the compromised computers, often through a back door connection to an administration tool such as a botnet dashboard, to determine what malicious faucets they can tap. For instance, they may start with a banking Trojan and wait to see if they can gather any banking details entered into the compromised computer. If nothing is captured by the banking Trojan, they may try ransomware with a pornographic theme, in the hope that they can extort money from the user through the ransom attempt.

In one such scenario, an attack group may compromise computers and initially install a downloader followed by a banking Trojan. The attackers monitor to see what financial institutions the user interacts with, in the hopes they connect to a bank in a specific region. If they don't see any banking activity over a period of a week or two, the attack group will change tactics and install ransomware using the original downloader. If the victim pays the ransom, they'll then install a spam Trojan and convert the computer into a spam bot, which will run behind the scenes without the user's knowledge.

While the payouts from cybercrime can be high, so too can the punishment for getting caught. 2013 saw several cases where arguably harsh punishments were handed out to cybercriminals. While punishments like the 18-year sentence given to a Ukrainian cybercriminal found guilty of running a website where stolen financial data was bought and sold may seem deserved, others have been more questionable. For instance a man from the US was given two years federal probation and a hefty fine of US$183,000 for his part in a DDoS attack against a multinational corporation. The guilty man in this case used the *Low Orbit Ion Cannon* DDoS tool for approximately 60 seconds as part of a larger group of hacktivists taking part in an Anonymous campaign. Whether or not people think these punishments are fitting of the crimes, one thing is clear—Law makers and enforcers now realize the potential and actual impact cybercrime can have.

The attackers will generally monitor the compromised computers, often through a back door connection to an administration tool such as a botnet dashboard, to determine what malicious faucets they can tap.

Threat Delivery Tactics

Toolkits

A major shift in the realm of toolkits happened in early October of 2013 with the arrest of the Blackhole and Cool Exploit Kit author, nicknamed "Paunch". The Blackhole exploit kit has dominated the web attack toolkit charts for the last few years and looked poised to do so again, based on the numbers leading up to and including October.

It appears that Blackhole has largely fallen off the map, while other toolkits have stepped in to take its place. For instance, the attackers behind the Cutwail botnet, who used to rely heavily on Blackhole, appear to have switched to the Magnitude exploit kit (a.k.a. Popads).[20] The Styx and Nuclear kits have been picked up by the attackers distributing Trojan.Shylock.[21] The authors of the ransomware threats such as Revention (Trojan.Ransomlock.G) have moved to the WhiteHole kit.[22]

It's possible that in the near future, the source code for the Blackhole toolkit will appear online and new people will pick it up, create their own version, and help to develop it. Releasing source code like this can help someone mask their trail from investigators.

Eventually, the void left by Blackhole will be filled by another toolkit. Much like the arrest of a drug kingpin causes lower ranking criminals to scramble to fill the void, so too will the chaos caused by the arrest of the apparent Blackhole author eventually settle and a new toolkit will take its place.

Eventually, the void left by Blackhole will be filled by another toolkit. Much like the arrest of a drug kingpin causes lower ranking criminals to scramble to fill the void, so too will the chaos caused by the arrest of the Blackhole author eventually settle and a new toolkit will take its place.

Business Model

Years ago, web-attack toolkits were sold on underground forums, where one person would sell it for a set amount to an associate, who would sell it on to another associate, and so on. The distribution worked in a black market sense, but the developer of the attack toolkit would miss a large percentage of revenue, where someone who simply possessed the code could profit without doing much work.

In the last few years, the Blackhole toolkit changed all that by introducing a service model that has grown to become the dominate way toolkits operate. In this service-style model, the web-attack toolkit developer maintains control of the code and administers the toolkit.

The kit can be locked down to a compromised computer of the attacker's choice, but the owners of the toolkit will offer access as a service where they will administer the kit. This way the developer maintains control of the kit code, rather than releasing it in underground forums.

Web Attacks Blocked per Day

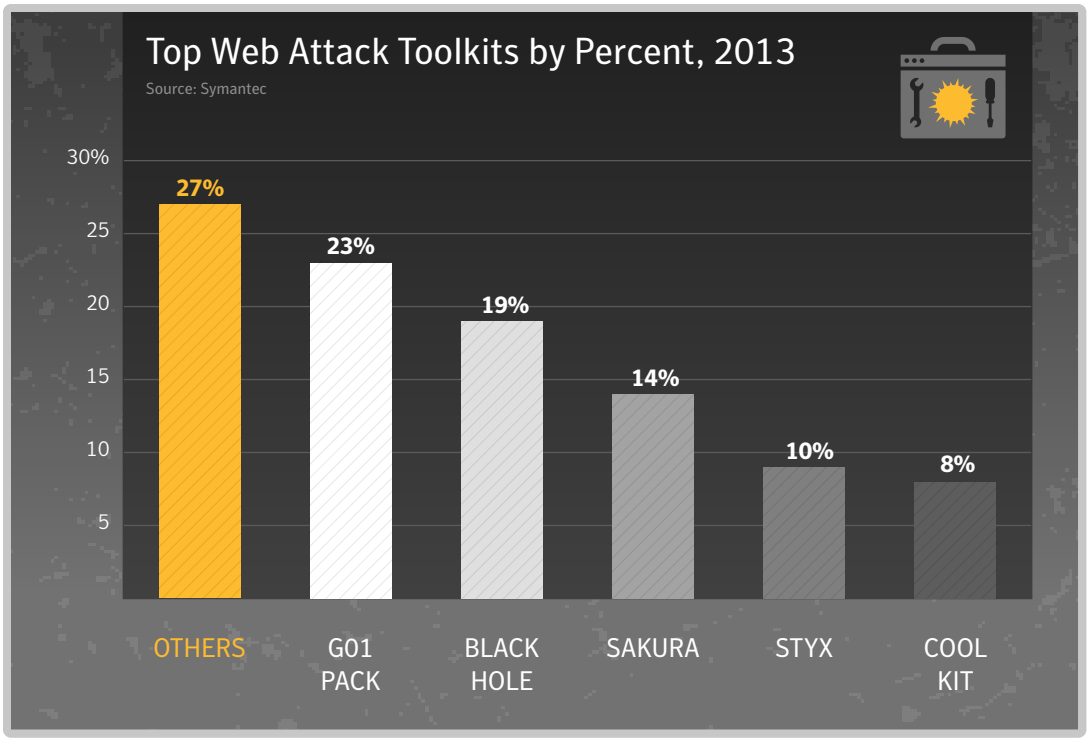
This sort of setup has allowed toolkit owners to experiment with different service offerings. This ranges from end-to-end coverage where the toolkit administrator sets everything up, to a less hands-on approach where tech support services are available to help the purchaser if they encounter configuration issues.

For advanced attacker clientele with some level of technical know-how, there is access to redirect their traffic from computers they've compromised to the web attack toolkit. However, in the case of setups like Blackhole, the toolkit uses legitimate PHP obfuscators, protecting the toolkit developers "intellectual property." This means that even if someone has access to a system running Blackhole, the code is unreadable without the proper keys to decode it.

When the primary work is handled by the toolkit owner, it requires far less administration on the attacker's side, or even knowledge of how to set up the attacks. In fact today's toolkit clients are usually of limited technical expertise when compared

Continued on p.57 ...

Fig. 6



- *The earlier dominance of the Blackhole toolkit had all but disappeared by the end of 2013 when the alleged person responsible for it was arrested in October. Blackhole was ranked first in 2013 with 44.3 percent of total attacks blocked; however, The G01Pack Exploit Kit was ranked first in 2013 with 23 percent of attacks blocked.*
- *The Sakura toolkit that ranked second in 2012, accounting for 22 percent of attacks is now ranked third with 14 percent in 2013.*
- *Many of the more common attack toolkits were updated in 2013 to include exploits for the Java Runtime Environment, including CVE-2013-0422, CVE-2013-2465 and CVE-2013-1493 and the Microsoft Internet Explorer vulnerability CVE-2013-2551.*

Fig. 7

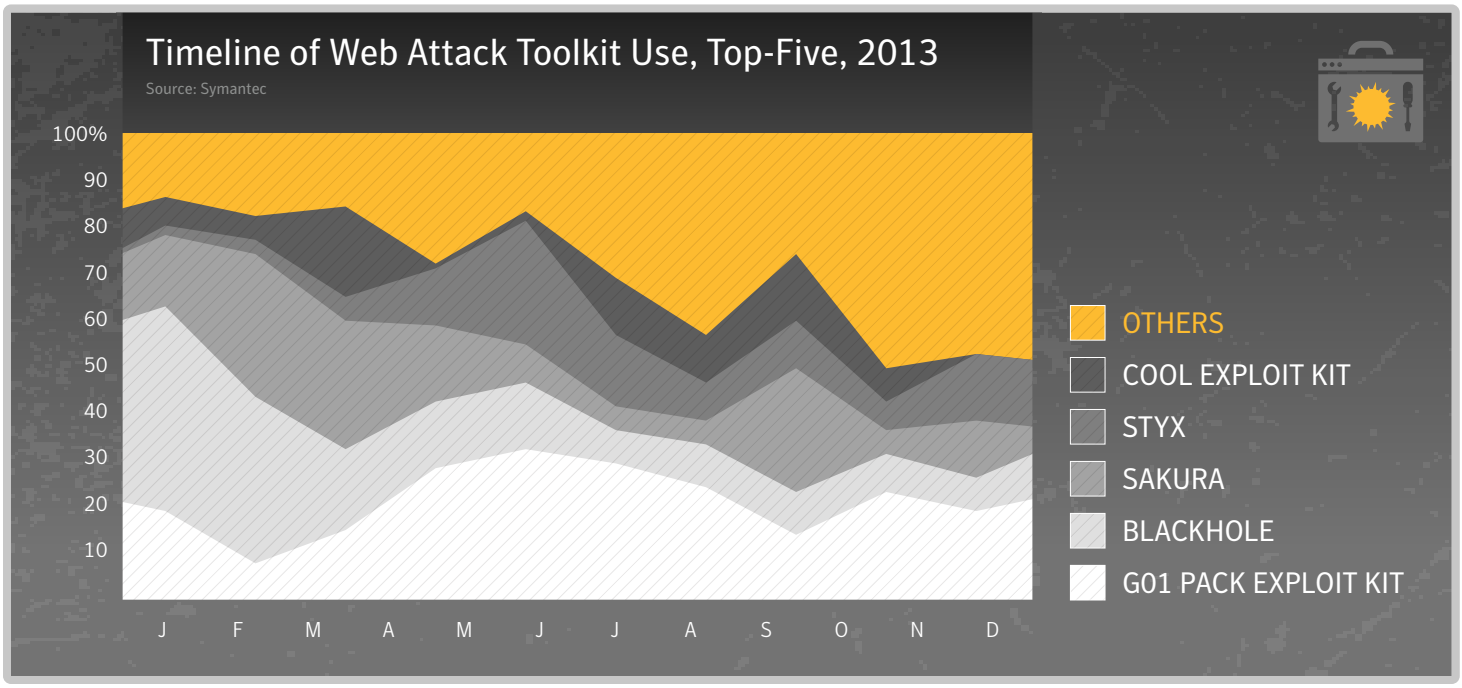
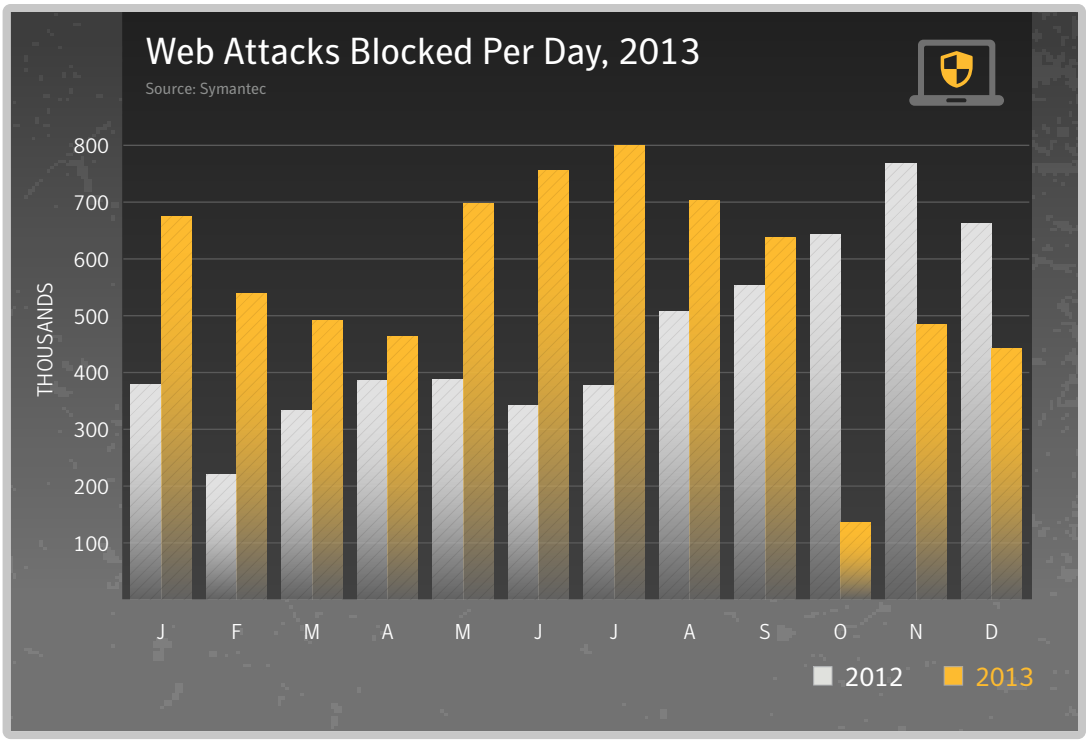


Fig. 8



- *The average number of malicious websites blocked each day rose by approximately 22.5 percent from approximately 464,100 in 2012 to 568,700 in 2013.*
- *The highest level of activity was in July, with approximately 799,500 blocks per day.*
- *The lowest rate of malicious activity was 135,450 blocks per day in October 2013; this is likely to have been connected to the arrest in Russia of "Paunch," the alleged author of the Blackhole and Cool Exploit web attack toolkits. Blackhole operated as a software-as-a-service toolkit, which was maintained in the cloud. With no one around to update it, Blackhole quickly became less effective, leaving a space for other operators to move in.*

Classification of Most Frequently Exploited Websites in 2013

- The malicious URLs identified by the Norton Safe Web technology were classified by category using the Symantec Rulespace[23] technology, and the most frequently abused sites for malicious code were listed in the table above.
- Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites that could be classified, compared with 61 percent in 2012. This figure excludes URLs that contained just an IP address and did not include general domain parking and pay-per-click websites.

Fig. 9

Most Frequently Exploited Websites, 2013

Source: Symantec

Rank	Top 10 Most Frequently Exploited Categories of Websites	Percent of Total Number of infected Websites
1	Technology	9.9%
2	Business	6.7%
3	Hosting	5.3%
4	Blogging	5.0%
5	Illegal	3.8%
6	Shopping	3.3%
7	Entertainment	2.9%
8	Automotive	1.8%
9	Educational	1.7%
10	Virtual Community	1.7%

- The Technology category accounted for 9.9 percent of malicious Website activity identified
- The Illegal category is for sites that fall into the following sub-categories: Activist Groups, Cyber-bullying, Malware Accomplice, Password Cracking, Potentially Malicious Software and Unwanted Programs, Remote Access Programs, and several other phishing and spam-related content.
- Analysis of websites that were used to deliver drive-by fake antivirus attacks revealed that four percent of threats found on compromised Art and Museum sites were related to fake antivirus software. Moreover, 50 percent of fake antivirus attacks were found on compromised Art and Museum sites. Additionally, 42 percent of attacks found on compromised Shopping sites were fake antivirus software.
- Analysis of websites that were used to deliver attacks using browser exploits revealed that 21 percent of threats found on compromised Anonymizer sites were related to browser exploits. Furthermore, 73 percent of browser-exploit attacks were found on compromised Anonymizer sites and 67 percent of attacks found on compromised Blogging sites involved browser exploits.
- Finally, 17 percent of attacks used on social networking sites were related to malware hosted on compromised Blogging sites. This is where a URL hyperlink for a compromised website is shared on a social network. Similarly, hosting websites accounted for 4 percent of social networking related attacks. Hosting covers services that provide individuals or organizations access to online systems for websites or storage, often using free cloud-based solutions.

to those offering toolkit services. At most they know enough to set up and administer the kit, but probably don't have the skills to write the code themselves. They're simply out to make money through using the services being provided.

Of course, the Achilles heel for this system is the locked-down software-as-a-service model. This is exactly what led to the colossal disruption that the Blackhole toolkit experienced when "Paunch" was arrested. Since the toolkit was run and administered by a small group of developers, the toolkit collapsed when they were arrested.

Spam, Compromised Sites, and Malvertising

The vast majority of infections that occur through web attack toolkits are spam-relays, compromised websites, and malvertisments. None of these techniques are new, pointing again to the fact that age-old techniques continue to reap rewards for attackers.

The area of the most growth in 2013 has been in malvertising. Malvertising is the process of serving up malicious code through advertising programs. When successful, this allows attackers to serve up specially-crafted ads on legitimate websites, often bypassing security mechanisms that may be set up on the primary site because the content comes from a third party.

For instance, near the end of the year a large malvertising campaign was used to spread the Browlock ransomware threat.[24] This form of attack is extremely difficult to block, because attackers are signing up with advertisers, and initially serve up perfectly legitimate ads on legitimate websites. After a few weeks of apparent legitimate activity, the attackers switch over to serving up malicious ads. It's a long-term strategy that pays off due to the large amount of traffic it can gather very quickly. Lots of hits may come through within a few hours before the website discovers the malicious ad in question and blocks it from their advertising network.

Advertising companies are aware of this behavior and are taking action to prevent it, including forming organizations to investigate this behavior such as the Online Trust Alliance.[25] Ad companies check IP addresses of registered accounts and share suspicious addresses. They also look for activity on registered domain names which domains advertisers direct their ads towards. If the domain has only recently been registered a week or two, they may deny access to the ad network.

Social Engineering Toolkits: From RATs to Creepware

While web-attack toolkits tend to dominate the discussion in the threat landscape, they are not the only type of toolkits out there. There are also toolkits designed for penetration testing and detecting vulnerabilities that are open to exploits, often used legitimately by the whitehat community, but are often also employed by blackhat cybercriminals.

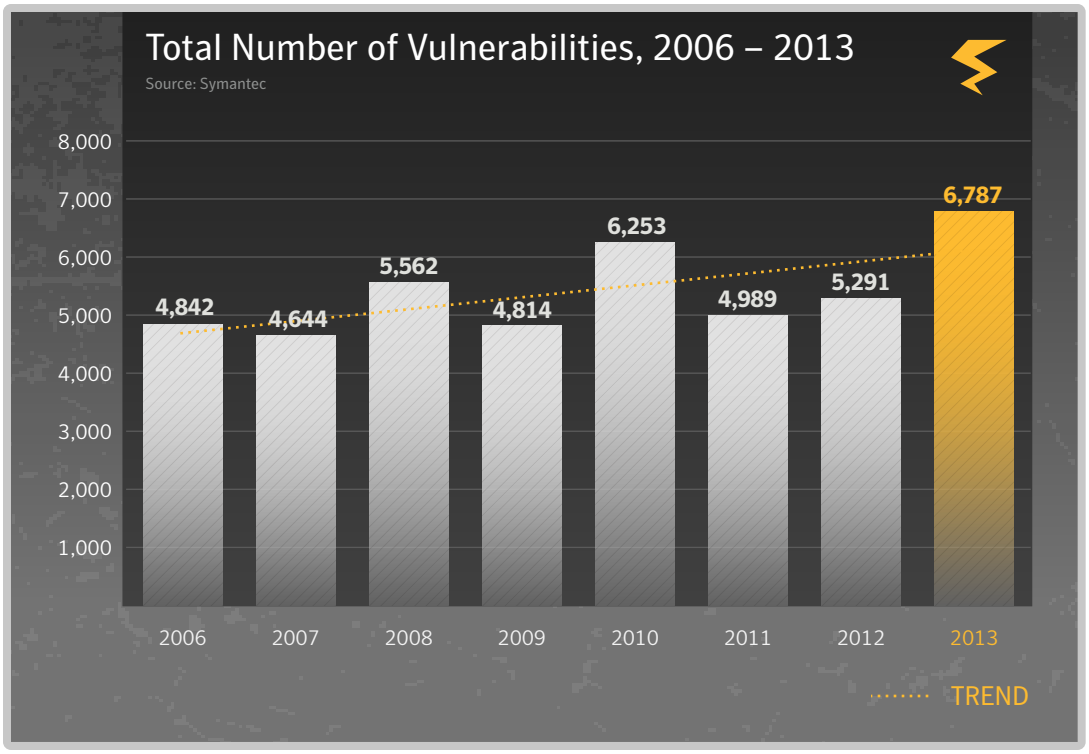
Probably the second most commonly known type of toolkit is the remote administration tool (RAT). These toolkits have been around for many years, such as the RATs behind the Zeus botnet, and are often used to create payload Trojans with various features as well as to obfuscate the binaries in an attempt to evade antivirus detection.

Social Engineering toolkits can be used to create phishing sites such as fake Facebook login pages. These are essentially web-design tools with extra features for hacking. For instance, an attacker can specify the type of information they want to collect on the back end of the website.

Creepware is a type of threat that uses toolkits. These threats are usually installed through social engineering and allow attackers to spy on the victims.[26] In many cases, the attackers administer their creepware by using toolkits that allow them to carry out various activities through the toolkit control panel.

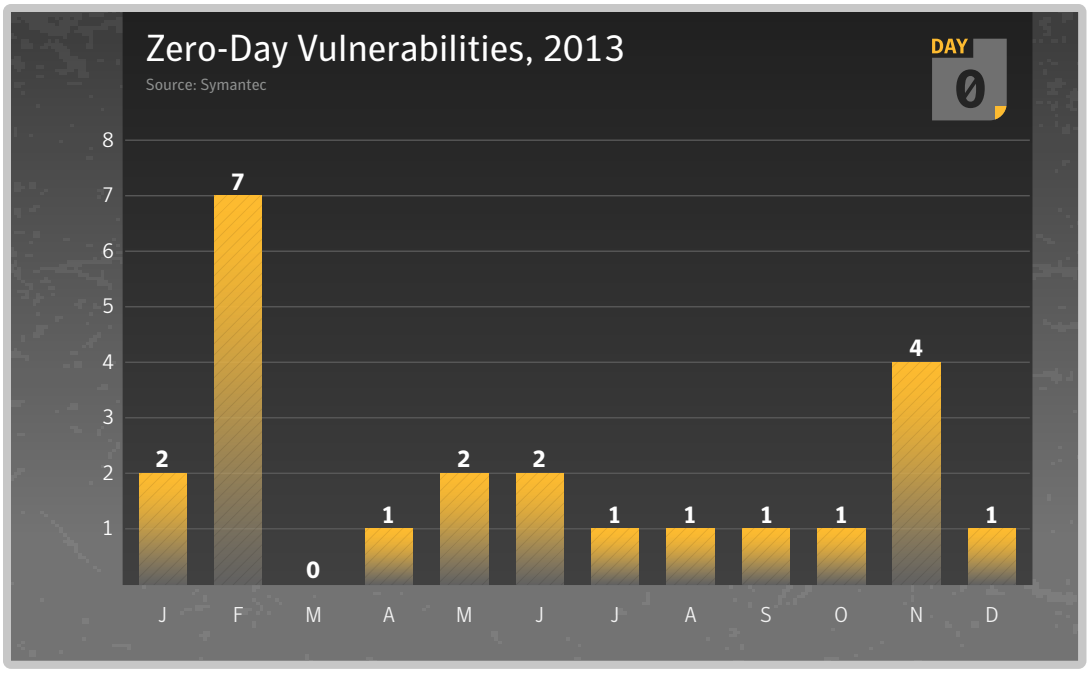
The vast majority of infections that occur through web attack toolkits are spam, compromised websites, and malvertisments. None of these techniques are new, pointing again to the fact that age-old techniques continue to reap rewards for attackers.

Fig. 10



- *There were 6,787 vulnerabilities disclosed in 2013, compared with 5,291in 2012.*
- *In 2013 there were 32 public SCADA (Supervisory Control and Data Acquisition) vulnerabilities, compared with 85 in 2012 and 129 in 2011.*

Fig. 11



- *A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available.*
- *The total number of zero-day vulnerabilities reported in 2013 was 23, compared with 14 in 2012.*
- *The peak number reported in one month for 2013 was 7 (in February), compared with a monthly peak of 3 (June) in 2012.*

Vulnerabilities: The Path to Exploitation

Vulnerabilities continue to be one of the core choices for the delivery of malicious code. Vulnerabilities are being exploited to serve up all sorts of threats such as ransomware, Trojans, backdoors, and botnets. The total number of vulnerabilities disclosed in 2013 supports this - at 6787 vulnerabilities disclosed, the number is higher than any year previously reported.

The number of vulnerabilities being exploited in zero-day attacks was up in 2013, often used in watering-hole attacks. This increase in the number of zero-day vulnerabilities occurred for the most part in the first half of the year. The reduction in the latter half of the year could have a lot to do with the complexity of exploitation for the zero-days discovered later in the year. This could point to a future landscape where vulnerability exploitation becomes more difficult.

Once a zero-day is disclosed, further exploits are developed and incorporated into toolkits within a matter of days, as attackers scramble to take advantage of the window of exploitation between disclosure, the patch release, and the time it takes organizations and individuals to patch their computers.

For the top-five zero-day vulnerabilities disclosed in 2013, the top 3 accounted for 97 percent of all attacks against zero-day vulnerabilities in 2013. Moreover, for the top-five zero-day vulnerabilities, the average time between publication and the requisite patch being made available by the vendor was approximately 4 days; however, there were a total of 19 days during which time no patch was available.

Bug bounties are also bringing more researchers out of the underground and allowing them to participate in the public dialog, where finders can get paid through discovery bounties rather than be tempted to sell them to malicious actors for use in attacks.

Browser vulnerabilities have declined this year, where four of the top five browsers reported fewer vulnerabilities than they did in 2012. The exception is Internet Explorer, which saw an increase in reported vulnerabilities from 60 to 139. While Safari reported the most vulnerabilities in 2012, the Chrome browser came out on top in 2013, with 212 vulnerabilities.

Oracle's Java platform had the highest number of reported plug-in vulnerabilities. However, this may not point to an increased weakness in the Java platform, but rather to the way in which Oracle has responded to Java security issues, increasing the release of security patches. Security improvements in other popular browser plug-ins have also contributed to this, with attackers continuing to exploit Java vulnerabilities where users have not upgraded to newer, more secure Java versions. Adobe added sandboxing technology to its products a few years ago, and has seen the benefits of such a strategy. Sandboxing executes code within a controlled environment, preventing an application for making programmatic calls outside its own environment. This has made it increasingly difficult to run malicious code within environments using the latest versions of the software. On top of that, Google has created mechanisms that actively test the Flash content being served up in search results to determine if exploits are being used on sites before showing it to users. This effectively limits the use of the platform as an easily-exploitable piece of the threat landscape.

Vulnerabilities continue to be one of the core choices for the delivery of malicious code. Vulnerabilities are being exploited to serve up all sorts of threats, ranging from ransomware, Trojans, backdoors, and botnets.

Fig. 12

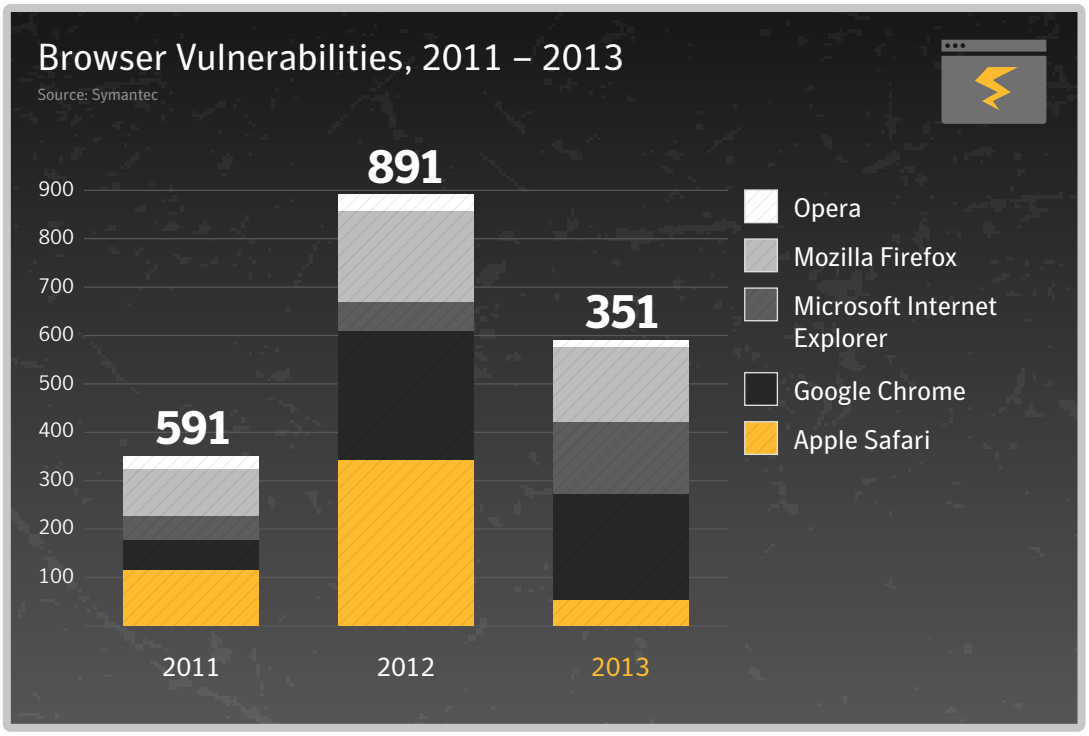
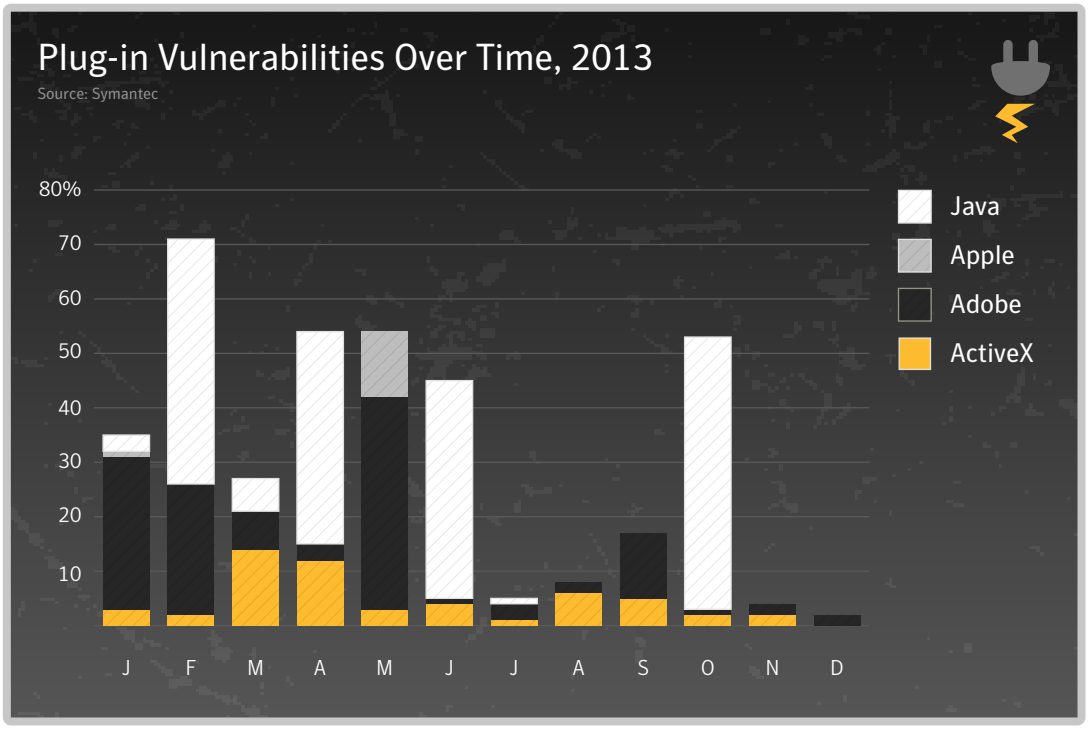
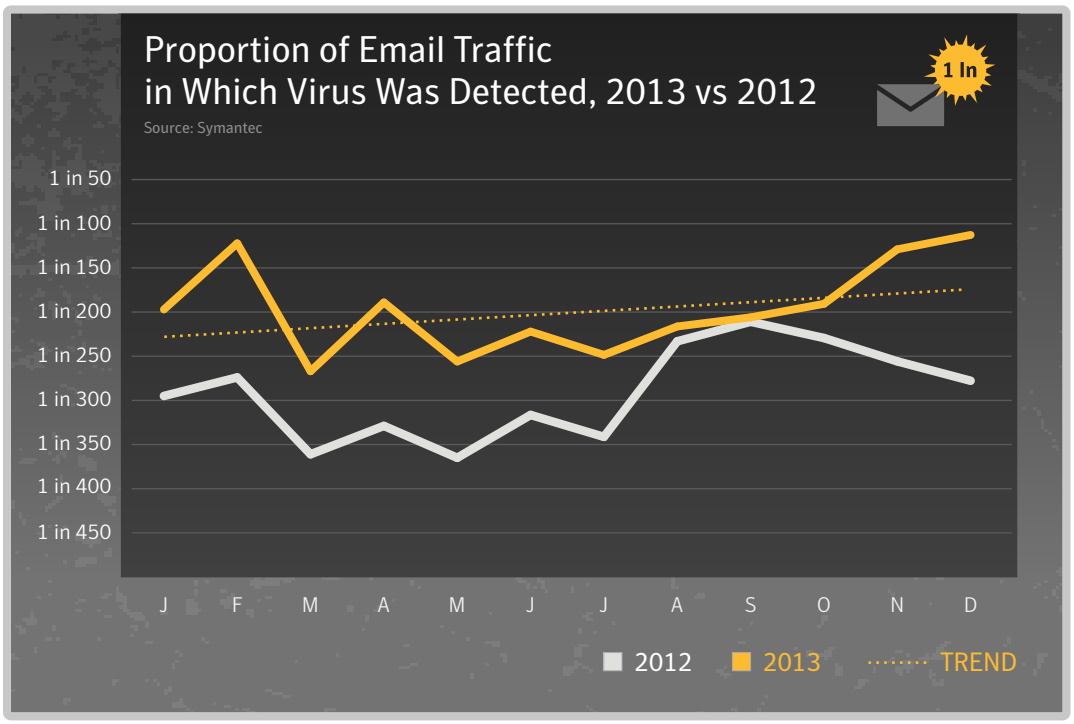


Fig. 13



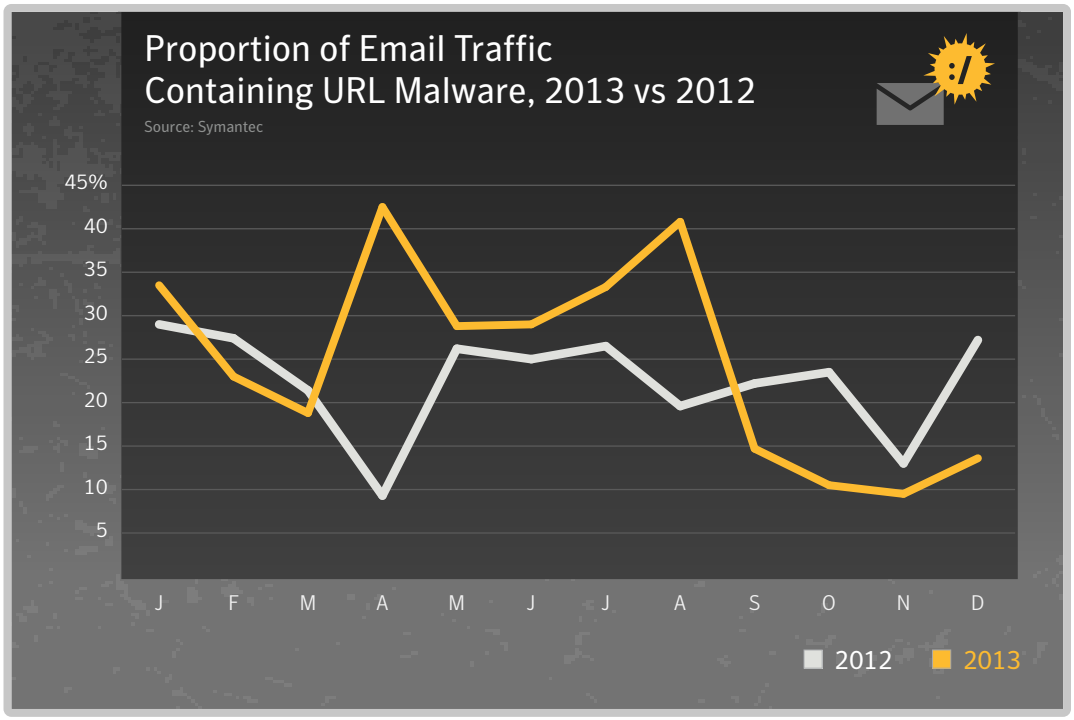
- *In 2013, 375 vulnerabilities affecting browser plug-ins were documented by Symantec, an increase compared to 312 vulnerabilities affecting browser plug-ins in 2012.*
- *ActiveX vulnerabilities decreased in 2013.*
- *Java vulnerabilities increased in 2013. This upward trend was already visible in 2012, and is also reflected in its usage in attack toolkits which have focused around Adobe Flash Player, Adobe PDF Reader and Java in 2013.*
- *Although the number of Java vulnerabilities was significantly higher in 2013, the number of new vulnerabilities being reported against the other plug-ins decreased throughout the year.*
- *Java is a cross-platform application, and as such any new vulnerability may potentially be exploited on a variety of different operating systems and browsers. This makes Java especially attractive to cyber-criminals and exploits against Java are likely to quickly find their way in the various web-attack toolkits.*

Fig. 14



- *Overall email-based malware numbers increased in 2013, with 1 in 196 emails containing malware, compared with 1 in 291 in 2012.*

Fig. 15



- *The proportion of email traffic that contains a malicious URL has increased in 2013 from 23 to 25 percent.*
- *There were two spikes in 2013 where more than 40 pecent of malicious emails contained URL links to malicious websites, rather than attachments, resulting in a higher rate for 2013 overall.*

Email Malware

Windows executable files still dominate the realm of malicious email attachments, and Java attachments have grown in number. In fact, attackers have found these attachments so successful that they're no longer trying to mask them within web attack toolkits. In 2013, Symantec identified executable Java files being sent through email both as .jar and .class attachments because, assuming a Java runtime environment is installed, both file types are launched by double-clicking them. It's possible this shift could be based on a desire to get past attachment restrictions in large corporations where traditional executables are not allowed as attachments, or it could simply be taking advantage of the average user's lack of awareness of the threat.

Malware sent through email increased in 2013, where 1 in 196 emails contained a malicious attachment. This is up from 1 in 290.7 in 2012. December saw the largest ratio for the year, at 1 in 112.7, generally during a time of year when the virus rate is in decline.

Apple Macs Under Attack

There has been an increase in Enterprise-level adoption of Macs as many organizations are allowing their work force to choose between PCs and Macs.

Although Macs still represent a small proportion of the overall operating system market, Macs could be considered more valuable if higher profile targets adopt the operating system for work purposes. Since the data available on these Macs may be considered more valuable, more resources are being turned towards attacking the Mac platform.

The challenge for Macs is similar to the challenges surrounding BYOD (bring your own device) initiatives within an organization. How do you manage the risk of another device type without compromising user performance? Unfortunately many Mac end users may still be under the impression that they are protected against malware attacks and don't require basic protection. As with any Internet-connected device that is used to access sensitive information, security countermeasures should always be included for Macs.

Ultimately, Macs are an accepted part of the IT fabric for an organization, and any strong security architecture plans must include them. As the demand for Macs in the Enterprise increases and they are used to access sensitive data, so too will the amount of Mac malware.

Fig. 16

Top-Ten Mac OSX Malware Blocked on OSX Endpoints, 2013

Source: Symantec

Malware Name	Percent of Mac Threats Detected on Macs
OSX.RSPlug.A	35.2%
OSX.Flashback.K	10.1%
OSX.Flashback	9.0%
OSX.HellRTS	5.9%
OSX.Crisis	3.3%
OSX.Keylogger	3.0%
OSX.MacControl	2.9%
OSX.FakeCodec	2.3%
OSX.Iservice.B	2.2%
OSX.Inqtana.A	2.1%

- *Approximately 1 in 924 (0.11 percent) of malware detected on Mac OSX endpoints was actually Mac-based malware. The remainder was mostly Windows based (i.e. Mac computers encountering Windows-based malware). This figure was 2.5 percent in 2012, largely due to the initial spread of the Flashback malware in 2012, which exploited a vulnerability in Java and reportedly affected as many as 600,000 Macs at the time.*
- *Flashback was first identified in 2012 and was still being detected on Macs in 2013.*

SOCIAL MEDIA + MOBILE THREATS

Social Media

Social media continued to work its way deeper into our digital lives in 2013. The importance of social media has also grown in the past year, and its cultural significance has been reflected in the financial markets' acceptance of mobile as an increasingly popular platform for global business. During 2013 a number of newer, niche platforms garnered enough users to make their way into popular consciousness, while more-established platforms realized the financial success that comes with IPOs. Popularity and profit appear to be central to the social media world this year.

Many of the recent entrants into social media have grown by narrowing their focus in comparison with better-established platforms, fulfilling an apparent desire for straightforward, simple-to-use social media apps, such as time-limited photos, short videos, micro blogging, or free alternatives to text messaging. The sites are often designed specifically for mobile use and the target audience is generally younger. It is these early adopters—the "cool kids" —who often start new trends, quickly bringing more users with them. These are the sort of users that scammers identify as their prime targets. Unfortunately, widespread popularity draws scammers to these social networking platforms, as per the saying, "If you build it, they will come." If a social network attains a certain level of popularity, scammers will find a way to exploit it. In 2012 the shift in spam and phishing towards social media was already underway, although these threats were harder to recognize than their email counterparts. Symantec identified new scams targeting some of these up-and-coming social networks during 2013.

The central goal of the scammer is profit. A lot of scam activity is carried out through traditional click-through campaigns that lead to survey scams, in contrast to the more complex setups found in other areas of the threat landscape. While they aren't making such large amounts of money as the hackers behind threats such as ransomware, a scammer in the world of social media can still make thousands of dollars in a month, thereby providing a regular income.

It is easy for a scammer to get started in this field because setting up social media accounts is largely free. A scammer can set up accounts on the sites, cultivate a group of followers, create and release free apps or browser plug-ins, and even host external pages on free sites. From there all the scammer has to do is figure out a topic that users might click on and then deploy the campaigns.

Techniques

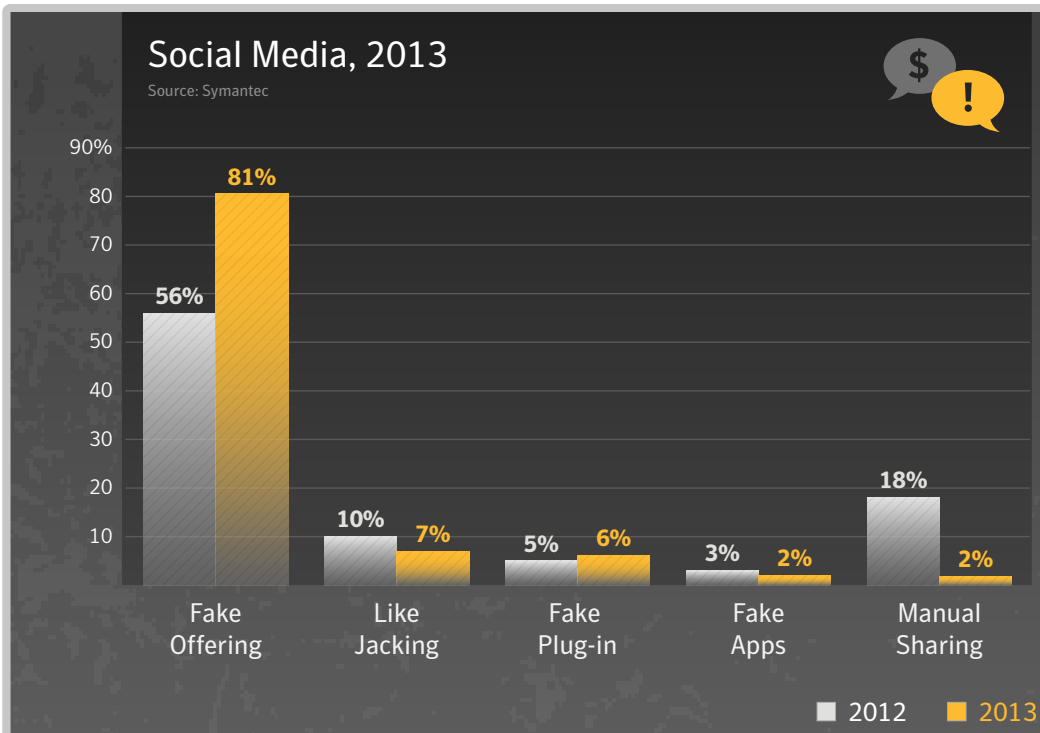
Phishing and spam is evolving, moving further away from email and into the social media landscape. These social media campaigns include the same lures that are seen in phishing and spam email. The types of material being offered remains similar to past years: gift cards, electronics, concert tickets, and DVD box sets are just a few of the fake offers seen this year. The fake profiles set up by scammers include pictures of attractive people looking to be friends and more. In other cases, a scam may center around posting a single photo or theme on a series of compromised accounts.

At a Glance

- *Fake offers lead the types of scams on social media again this year, accounting for 81 percent of scams identified in 2013.*
- *Click-through campaigns that lead to online surveys are a common tactic used by scammers.*
- *Mobile attackers are repackaging their threats more often, as the average number of variants per family is up in 2013.*
- *Tracking users is most common type of activity found in mobile threats.*

Phishing and spam is evolving, moving further and further away from email and into the social media landscape. The campaigns include the same lures that are seen in phishing and spam email.

Fig. 1



Fake Offers These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

Manual Sharing Scams These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

Fake Plug-in Scams Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions, but when installed steal sensitive information from the infected machine.

Fake App Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

- *Fake Offers accounted for the largest number of social media based attacks in 2013, with 81 percent, compared with 56 percent in 2012.*
- *Manual sharing scams have also decreased in 2013, from 18 percent in 2012 to 2 percent.*
- *Micro-blogging based scams accounted for one percent of total attacks detected for the social media category, for both 2012 and 2013.*

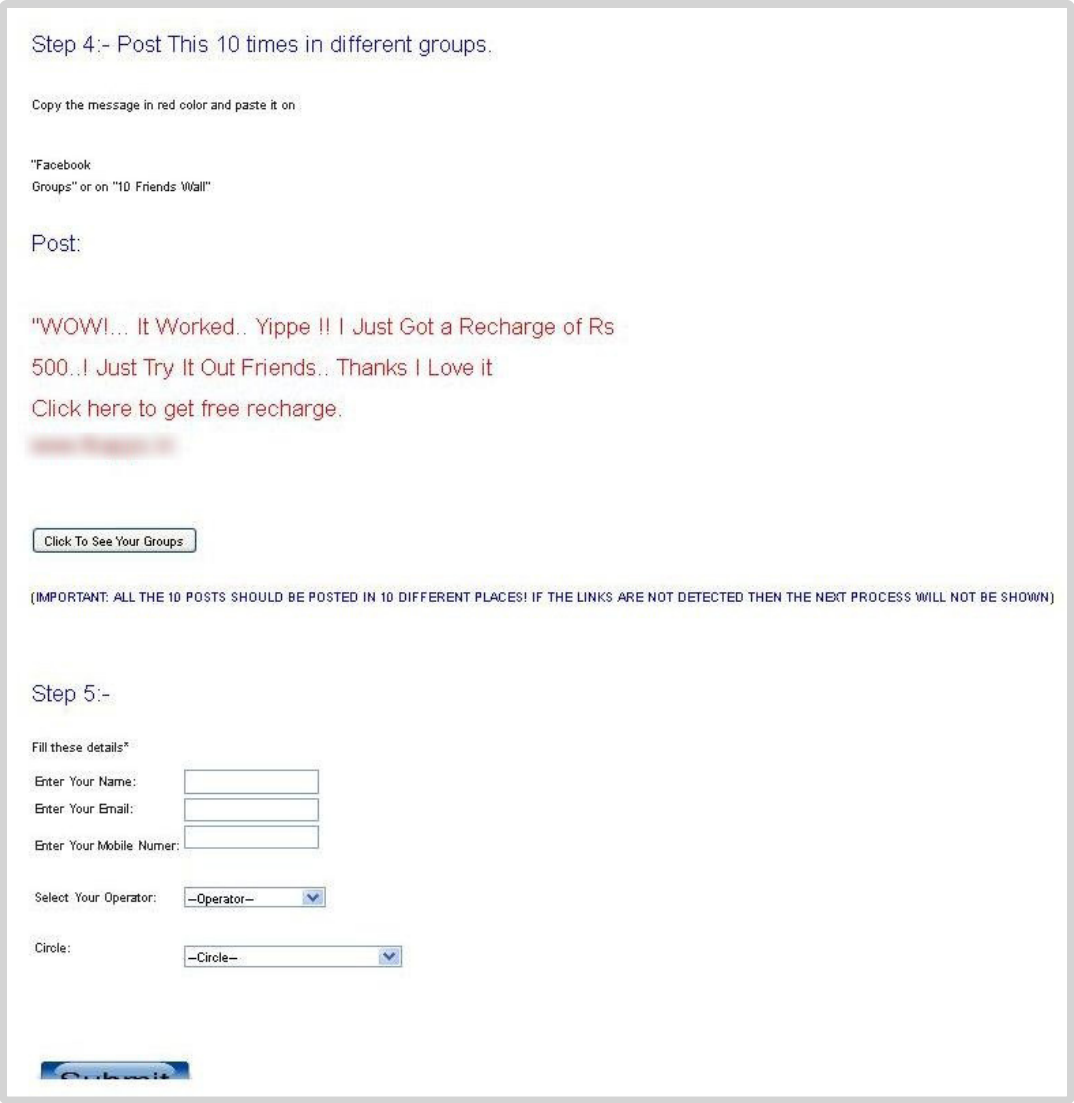


Fig. 2 Social media scam offering free cell phone minutes.

A scam could be advertised as a cool app to check out, or offer a download of a song from a favorite artist. If a user clicks on it, the scam often asks the user to enter his or her social media login details.

One example that came to light involved a login- and password-stealing scam that advertised a cool app for users to check out, or offered a download of a song from a favorite artist. If a user clicked on it, the scam asked the user to enter their social media credentials. They then stole this and redirected the user back to the social network without providing the promised app, download, or service.

In addition to stealing credentials, phishing sites encouraged victims to spam information about supposed phishing apps. This appeared to work well as a propagation technique for the scam, allowing it to spread from the original victim to their friends. These were often coupled with supposed incentives, like credits or points to be given to the users within the fake app.

For example, phishers offered a bogus app that claimed to deliver free cell phone minutes to social media users. The offer allegedly was available only if a user entered their login credentials and then forwarded it to at least ten friends. Thus, phishers aimed at multiplying the number

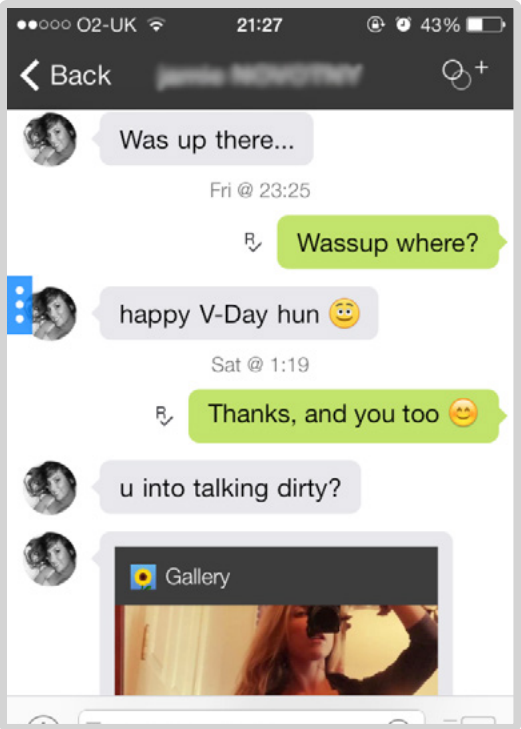


Fig. 3 Dating scam, where scammers send racy photos if the user agrees to install apps of their choosing.

of victims exponentially by blending their phishing attack with spam.

Social media scams are generally delivered through posts in the social network's feed, though if the service offers it they may also spread through private messages. Scammers don't limit their messages to the latest posts either, often replying to posts across the user's history sometimes months, if not years earlier. The messages generally linked to resources outside of the social network, such as compromised websites that the scam is being promoted upon.

Social media attackers were often seeking account credentials in the hope of using the account as a platform to spread their scams. A compromised profile allowed them to send messages to the victim's friends which appear to come from a reliable source. Another area of concern wasn't just a user's friends; it's who they chose to follow. Celebrities and other popular accounts or pages became prime targets of scammers who have hacked into their accounts. A simple word of caution in these cases: If the material posted seems contrary to the celebrity in question (e.g. A well-known academic hawking miracle diets) a user should not click any links presented.

Social media sites with a particular activity focus, like dating, also continued to be a location where scammers attempted to prey upon users. Fake users will often send messages to those genuinely attempting to meet a romantic partner. However, a common tell is that they generally come on quite strong. For instance, a scammer may send a user a message saying "Hey you're cute," hoping to strike up a conversation. The scammers send provocative photos, eventually followed by a link that leads to a webcam site. Only the site requires registration and the user is asked to hand over credit card information on this cam site. They may benefit from a few days of free access, but will eventually be charged at very high prices.

It's not just the specific social media sites to be concerned about. The growth in aggregate social media sites which allow users to quickly publish posts across multiple sites opened new avenues for attackers to take control of many points in a social profile at once. If these sites are hacked, as has already happened, they may not have gained direct access to users' various social media account details, but if they could send messages through the service it worked just as well in helping them accomplish their mischievous goals.

Another lure we continued to see was enticing users to participate in scams by suggesting they could gain likes. For example, "Gain 100 followers by clicking this link and filling out a survey" or "Install this mobile app and gain 100 followers." In many cases, the app the user is directed to is legitimate, but the scammer made money from the download through affiliate programs. It's worth noting that the affiliate may not have been aware of the scam. In the end no followers or likes were given, but the scammer didn't care; they've achieved their objective.

In some cases, a scam did indeed increase followers. However, the followers may not have been the types of accounts that the user would have desired. The scammers generally had a large group of compromised or fake accounts which they used to like or follow the user's account. The InstLike app, that was removed from popular app marketplaces near the end of 2013, was one such example. The app allowed a user to purchase likes and followers and also requested the user's login details, which was then used to "auto-like" and "auto-follow" other InstLike users.[27]

This focus on identity theft increased in scams, though the underlying motive was still financially rooted, albeit more indirectly. Well-established markets where phishers were able to sell such information on to other criminals were in abundance. These markets provided an easier and less risky method to make money as they gathered and sold personal details, in contrast to having attempted to use the information directly.

This highlights why such scams were so popular and prevalent. The chief risk for a cybercriminal was capitalizing on their ill-gotten gains. This is often what exposed them to potential detection and capture. Selling information and details to others who have established networks for cashing out (i.e. money laundering) reduced the risk. This is why a credit card had a value on the black market that seemed lower than its potential value in real terms: The higher the value, the greater the risk.

In the overall threat landscape, social networking scammers were low on the food chain. Their margins were much less, but so was their risk. They made money by doing what they do in large volumes: spam run through compromised accounts, URL comment scams, fake profiles with the same details, along with other methodologies.

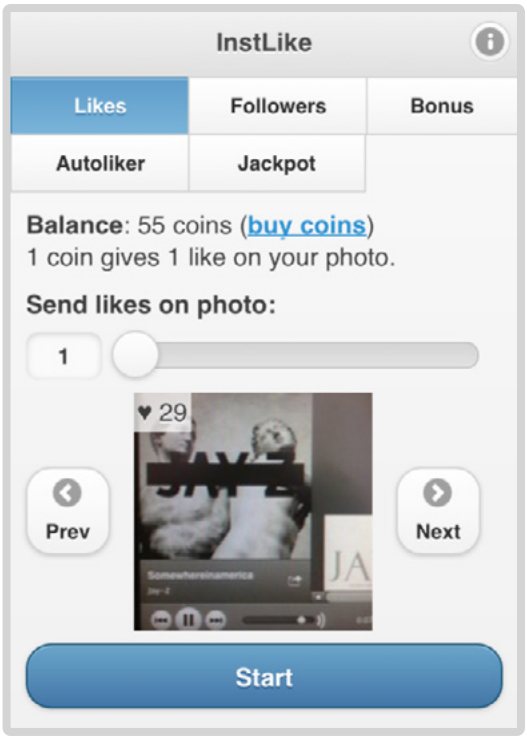


Fig. 4 *The InstLike application*

Well-established markets, where phishers are able to sell such information on to other criminals, are in abundance. These markets provide an easier and less risky method to making money as they gather and sell personal details, in contrast to attempting to use the information directly.

Mobile

Transition from Desktop

Mobile malware has been around for a number of years, and has multiplied with the widespread adoption of the Android platform. When Android gave smartphone users more freedom to install software from outside their official marketplace, it also opened the doors to malware authors, who have spent years honing their techniques. Much of the focus has been around stealing information from the device, although a variety of threats that have traditionally been found on desktop systems have begun to appear more regularly in the mobile landscape.

In the middle of 2013 remote access Trojan (RAT) toolkits began to appear for Android.[28] At first, attackers began to circulate Java-based RAT threats using email attachments, which were traced back to a toolkit designed to create threats that work across multiple platforms so long as a Java Runtime Machine is present.[29] RAT toolkits began to be developed for the Android operating system shortly thereafter, such as in a threat called Android.Dandro.[30] This toolkit type, called a "binder," allowed an attacker to take a Trojan and package it with a legitimate app. The idea was simple; to take the Trojan and the legitimate app, put them together and attempt to get them onto as many mobile devices as possible while hoping users do not notice the extended permissions requested by the Trojanized app.

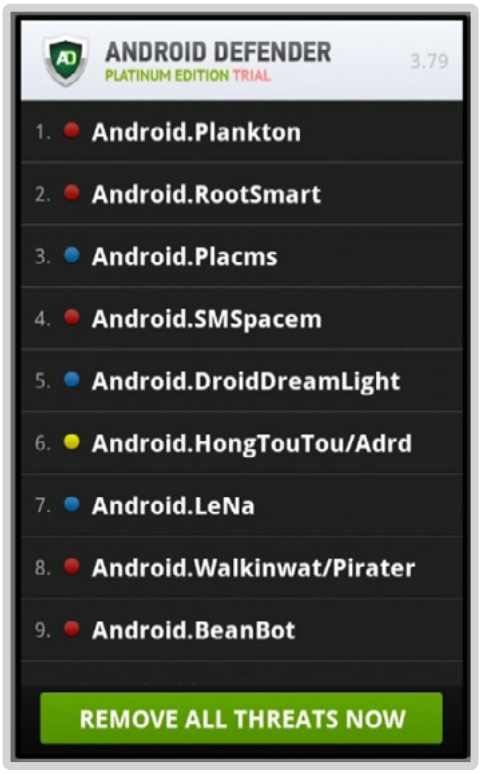


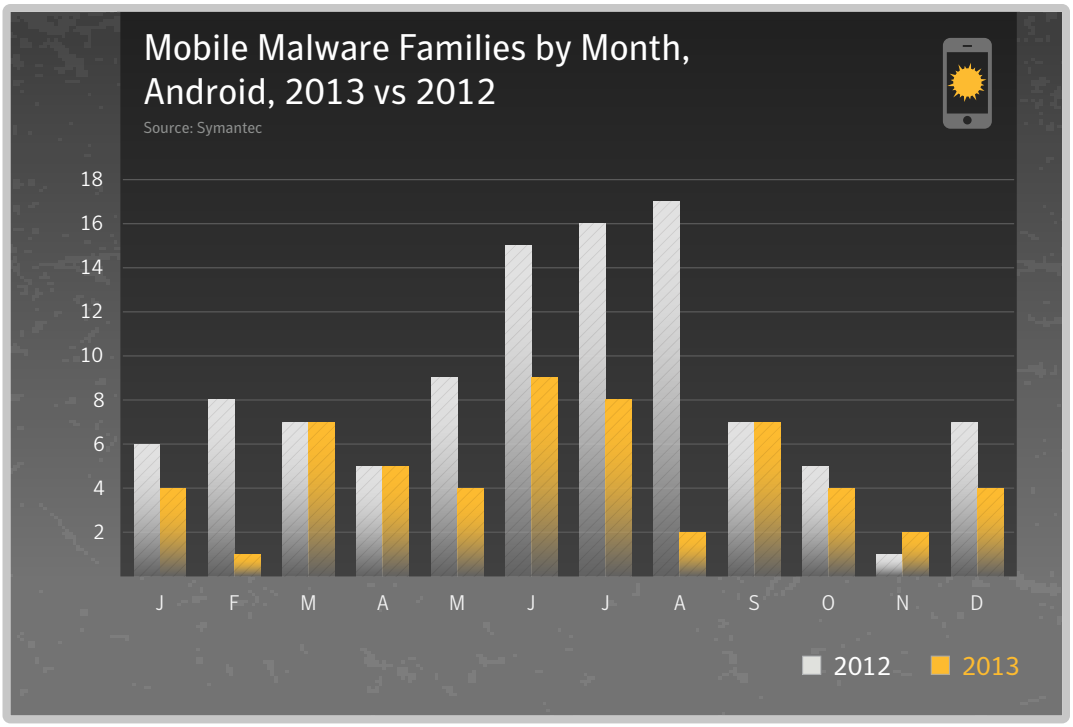
Fig. 5 Android.Fakedefender showing fake threats.

In 2012, Symantec's Norton Report[31] showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger. The 2013 Norton Report[32] showed this number rising to 57 percent. How did this awareness of security software decline? It seems that a lack of education among mobile users has contributed at least in part to this, or that people who had previously had feature phones (and therefore limited need for security software) were becoming smartphone users – but hadn't been made aware of the need to install a security app. The pool of people using mobile devices grew in 2013 as well, and many of these users were later adopters, who tend to be less digitally literate and less aware of the risks.

It appears that most mobile device users are just not aware of mobile threats, and as if to play into this lack of knowledge, rogue security software has been discovered on these devices; the first of which was identified in June. Android.Fakedefender did everything expected from fake security software: it ran a scan, warned the user of non-existent threats that the software found on the device, then attempted to coerce the user into paying for the fake app in order to remove them.[33] Moreover, while desktop fake security software is annoying, it generally doesn't prevent someone from using

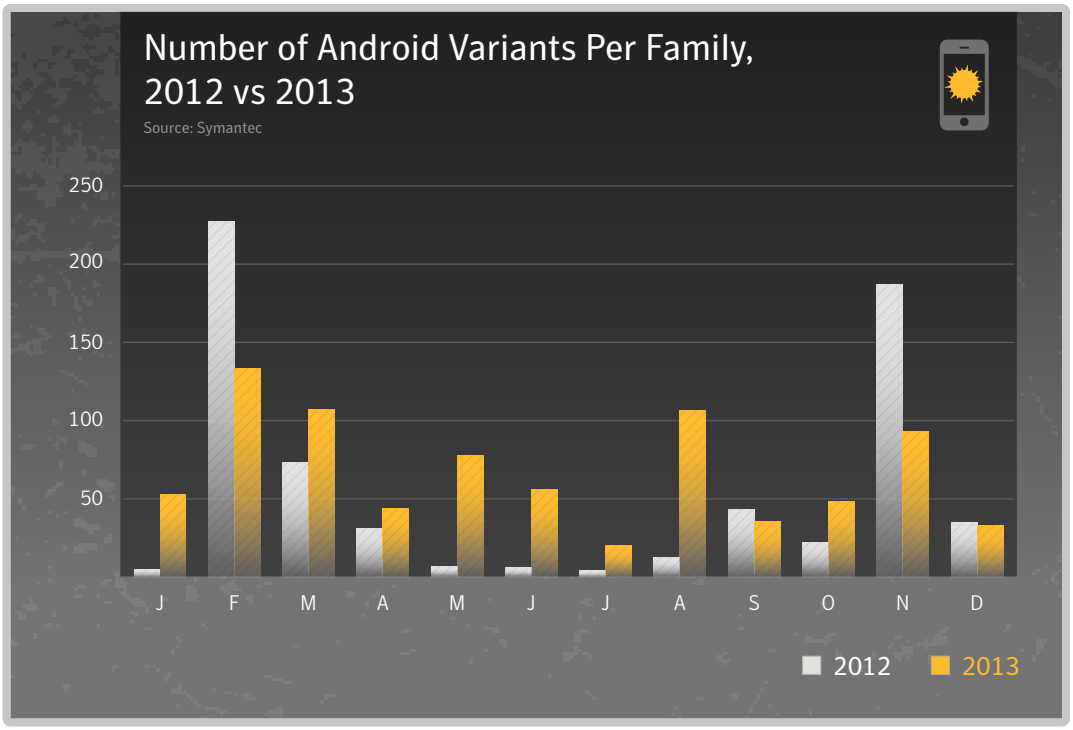
In 2012, Symantec's Norton Report showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger.

Fig. 6



- *The average number of mobile malware families discovered per month in 2013 was 5, compared with 9 in 2012.*
- *June and July were the most active months in 2013, when 9 and 8 families were identified each month.*

Fig. 7



- *The average number of variants within each family has increased since 2012. The average number of variants per family in 2012 was 1:38, increasing to 1:57 in 2013.*
- *March and June were the most active months for identifying new variants, with 748 and 504 variants being discovered, respectively.*

the computer. Fakedefender[34] took it one stage further, preventing the user from using the device altogether. This is reminiscent of the ransomware frequently found on desktops, though it's difficult to determine whether this was truly intentional. The code behind Fakedefender was buggy and caused the device to crash. On the one hand, it might have been a trick to make the user think the phone was infected; on the other it may simply have been shoddy programing on the attacker's part. Regardless, it appears there may be more threats like this on the horizon, potentially having greater impact on mobile users as attackers improve them.

Phishing pages were also developed for mobile devices. These campaigns were hosted on standard websites, and simply designed in such a manner to lend themselves to mobile devices - smaller images, less text, and so on.

Mobile users are already very familiar with the idea of downloading applications (or apps) onto their smartphones for the convenience and added functionality they provide. Consequently, cybercriminals have sought new ways to hide their malicious code inside mobile apps and make them attractive to potential users; sometimes they will repackage malicious code within legitimate apps, or simply create new malicious apps that pretend to contain some useful functionality while carefully masking their malicious purpose.

This highlights a key factor of the mobile landscape: App marketplaces are a quick way to get an application out to a large audience. Mobile users have become familiar with these marketplaces and the process of finding, downloading and installing new apps is a fast and painless process, whilst the cost is often small or even free. During the height of the desktop operating system's dominance, there was never such a simplified software marketplace quite like the app markets of today. In the past a developer would have to sign on with a software distributor, or would have to generate traffic to their own website for their customers to download applications.

This shift to app marketplaces was also helpful for cyber criminals. Attackers were likely to spend the time trawling through app marketplaces to find out what is popular, and then attempt to repackage malicious code with such apps. For instance, the release of an instant messaging application by a well-known smartphone vendor on the Android platform was greeted with much fanfare, and it quickly climbed to the top of the download charts. Attackers in turn took advantage of the popularity of the new app and released a variety of counterfeit versions bundled with adware. These apps were quickly removed from the Android marketplace, but not before accumulating a large number of downloads.

This trend appeared in our stats when we compared new mobile malware families to variants. The number of new families per month dropped from an average of 8.5 per month in 2012 to 4.8 in 2013. In comparison, while a huge number of variants was discovered in February of 2012, the median number of variants discovered per month increased 25 percent in 2012, from 170.5 per month to 213.

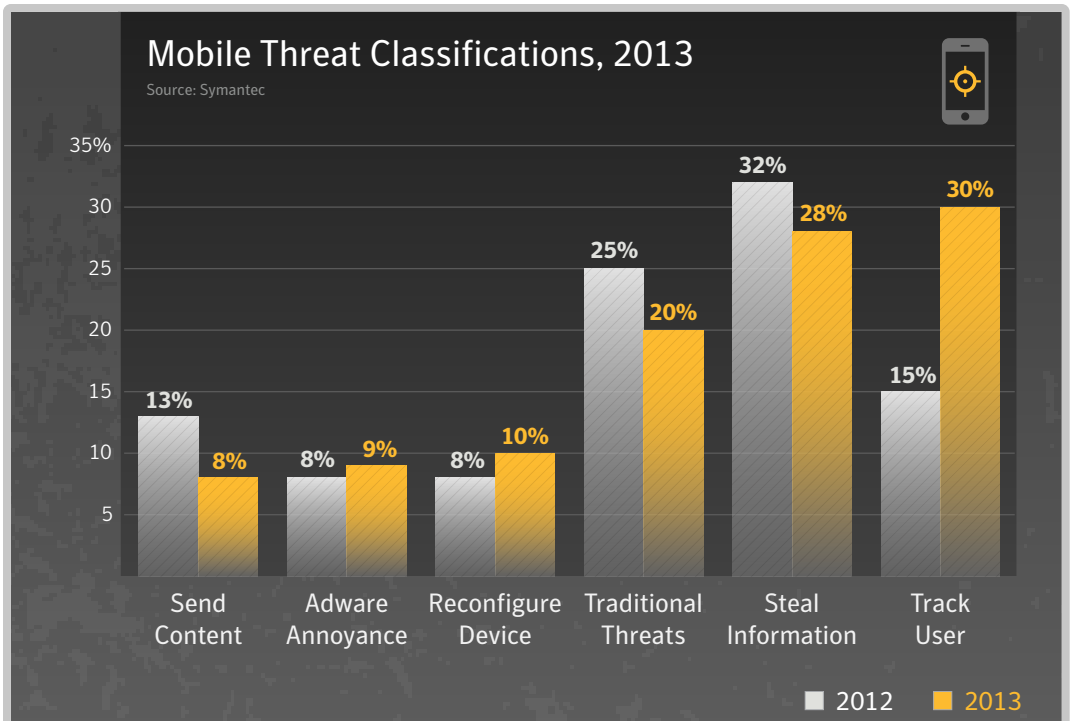
Also of note in 2013 is that mobile malware seemed almost exclusively focused on the Android platform. In fact only one new family was discovered outside this operating system—an information stealing Trojan for the Windows mobile platform.

Regional Landscapes

The type of attacks and the material attackers are pursuing often depends on the geographic region they're targeting. For example, there was a cluster of malicious mobile activity in Japan, which could be based on the presence of an advanced mobile infrastructure in the country. There are mobile services prevalent in Japan that are less common in other countries, as well as leading-edge, mobile-based purchasing methods.

The draw of mobile to attackers is clearly based on the size of the user base today. Yet it's also based on the amount of personal information that's easily attainable, once an attacker is on the device.

Fig. 8



Track User Risks that spy on the individual using the device, collecting SMS messages or phone call logs, tracking GPS coordinates, recording phone calls, or gathering pictures and video taken with the device.

Steal Information This includes the collection of both device- and user-specific data, such as device information, configuration data, or banking details.

Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

Reconfigure Device These types of risks attempt to elevate privileges or simply modify various settings within the operating system.

Adware/Annoyance Mobile risks that display advertising or generally perform actions to disrupt the user.

Send Content These risks will send text messages to premium SMS numbers, ultimately appearing on the bill of the device's owner. Other risks can be used to send spam messages.

- *The number of threats that track users has increased in 2013, from 15 to 30 percent, effectively doubling since 2012. This is perhaps an indication that this type of data is of more commercial value to the cybercriminals.*
- *In contrast, the largest type of mobile threat in 2012, those that steal information off the device, has actually decreased nine percentage points from 32 percent to 23 percent.*

Fig. 9 A Japanese mobile spam message, used to spread Android.Expespam.[35]

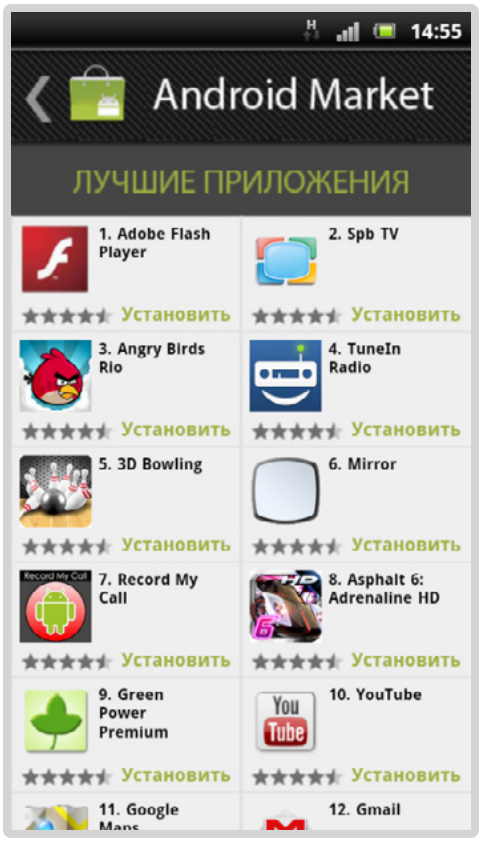


Fig. 10 A fake Russian app market, offering threats masked as popular apps.

One popular method for spreading malicious apps was through a mobile email account.[36] The emails provided a link and asked the user to download and install an app. If installed, information like contact details was gathered from the phone and the invitation messages were spammed out to other users in the recipient's address book. Similar attacks were carried out in South Korea as well, though these used SMS instead.

Another type of attack also surfaced this year in South Korea. A legitimate Korean app developer was compromised by attackers, which resulted in their app being replaced with a variant of Android.Fakeguard.[37] Users of the app were notified of an update to the app through normal means, and downloaded the revised, malicious code thinking it was a standard update. China is also another area where malicious versions of software are prevalent. However, this malicious activity has been driven due to a less robust version of official app marketplaces being available in the country. As a result, users have become inclined to install apps from unknown sources that have the functionality they desire, putting themselves at risk in less-stringent marketplaces, where threats may not be identified as readily.

A similar problem was present in Russia, where the presence of counterfeit app marketplaces, designed to look like official ones, hosting malicious apps was commonplace. Many sites offered a variety of malware-laden apps, though in some cases they went a simpler route and created an app install page hosting only one app.

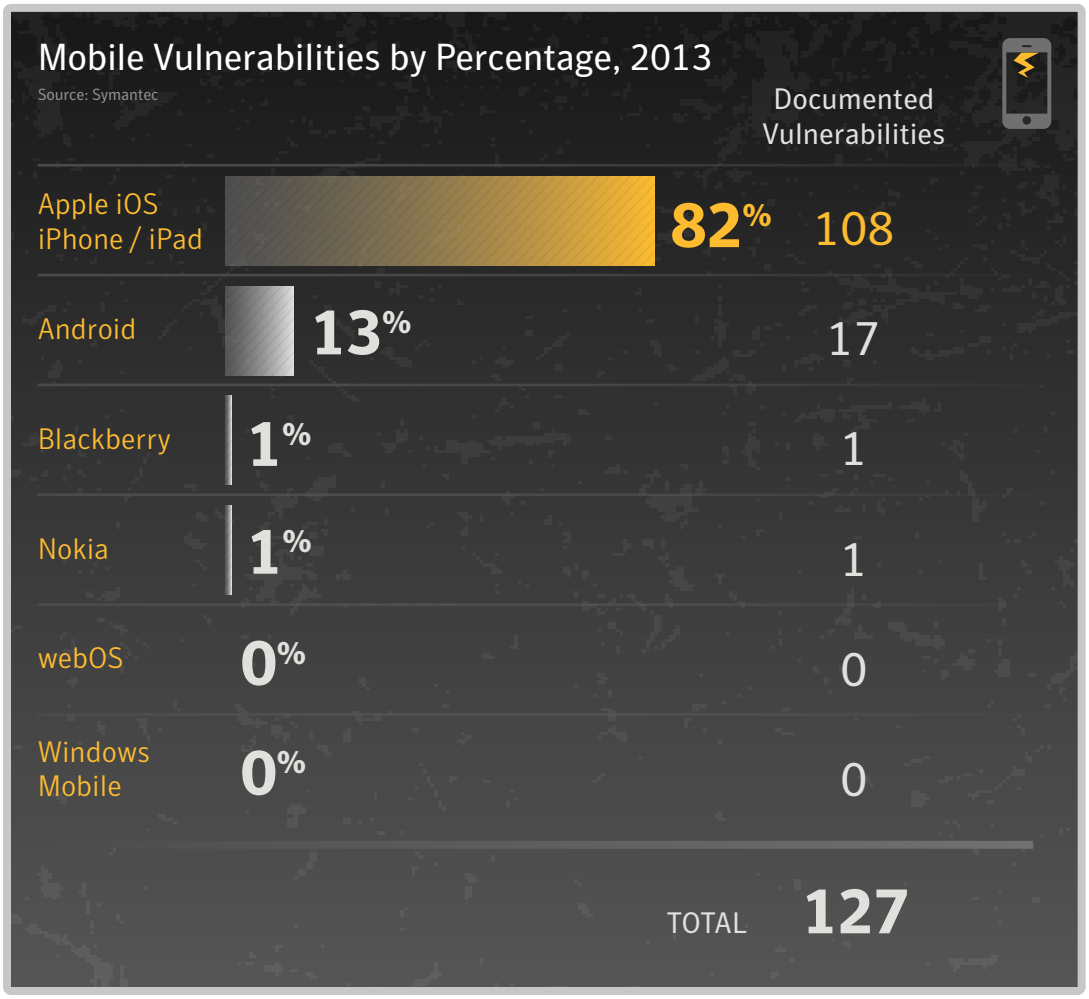
Vulnerabilities

It still appears that the mobile threat landscape is under development. Attackers are researching what they can do on Android, and their attacks are becoming more sophisticated. For instance, we've seen threats like Android.Obad,[38] which used exploits to elevate its privileges, and then once installed, hid all traces of itself on the device.

The discovery of a vulnerability that allowed attackers to inject malicious code into apps without invalidating the digital signature is one example. This "Master Key" vulnerability allowed an attacker to modify apps to include malicious code, yet looked identical to legitimate apps in terms of their signature. In essence, the operating system had no way to tell the modified app from the original.

Disclosed vulnerability numbers are lower in 2013 than the previous year, down almost 68 percent. September saw the largest number of disclosed vulnerabilities. This increase coincided with the release of Apple's iOS7, which included a number of patches for vulnerabilities discovered in iOS6. Similarly, the Android platform saw the release of version 4.3 in July and 4.4 in November.

Fig. 11



- *As we have seen in previous years, a high number of vulnerabilities for a mobile operating system does not necessarily lead to malware that exploits those vulnerabilities. Overall, there were 127 mobile vulnerabilities published in 2013, compared with 416 in 2012, a decrease of 69 percent.*

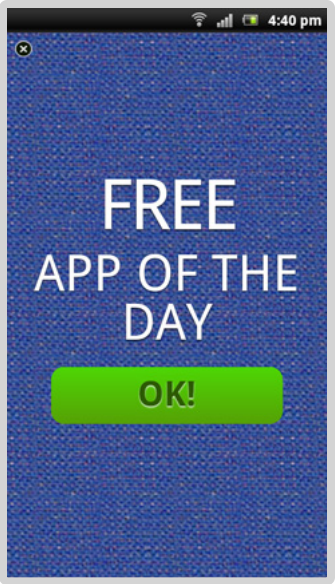


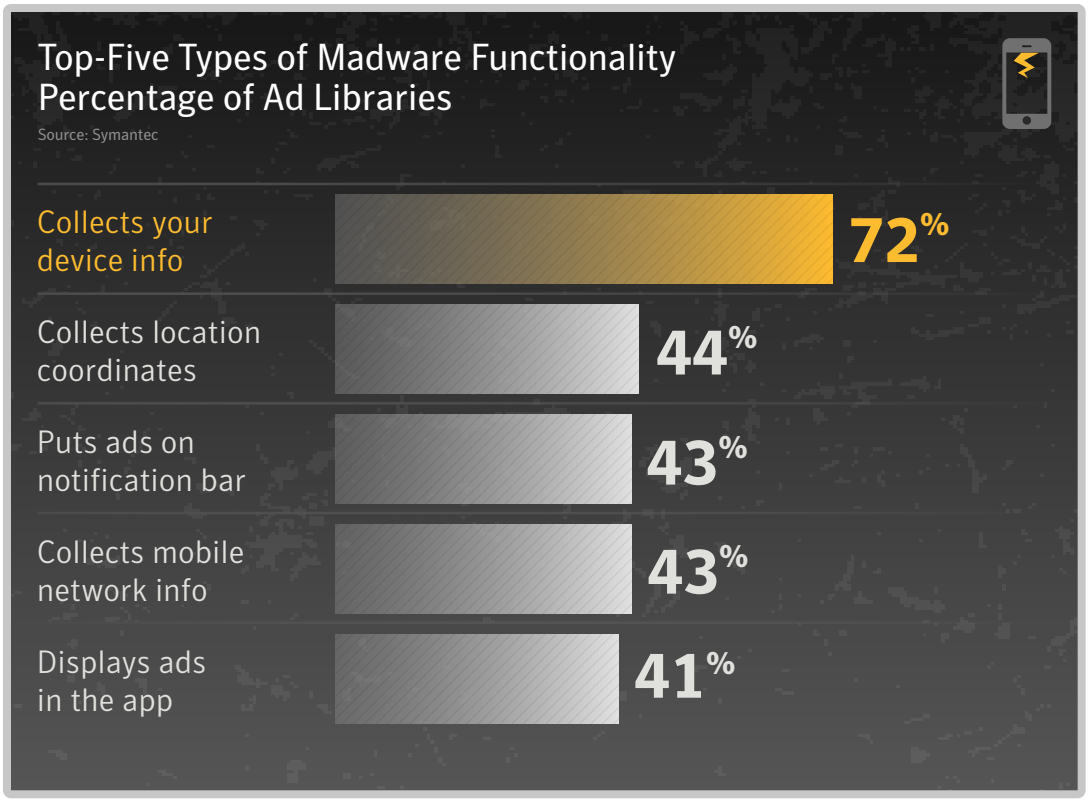
Fig. 12 Example madware pop-up advertisement.

Mobile Adware ("Madware")

There's another risk to the mobile landscape that grew in 2013. Advertising is a core part of the free app business model; however, some developers aren't content with keeping their advertisements held within the bounds of their application. Some developers have taken to displaying ads in the notification bar, or suggest the user install other apps. This type of risk is called mobile adware – or "madware."

The problem is that madware is common on app stores and appears to be growing. In October of 2013, 65 ad libraries were identified.[39] This number increased to 88 ad libraries by the end of 2013. That's not to say the market owners aren't quick to pull apps that exhibit some of the more aggressive madware traits. However, an app like this can rack up a modest number of installs before it's discovered and removed.

Fig. 13



Hybrid Threats

Another new development we've seen is malware threats and campaigns targeted at both Android and Windows. In the case of the Android.Stels Trojan,[40] which was distributed via a malicious email campaign, the payload varied depending on the device type. If the malicious URL in the email was opened on a PC, then a PC version of the malware was installed. If it was opened on a mobile device, a mobile version was served up. Other threats contained payloads for both device types in one package. If an Android device was connected to a compromised PC, it spread to the device.[41]

Motivations

The attraction of the mobile environment to attackers is clearly based on the size and growth rate of the user base today. Yet it's also based on the amount of personal information that's easily attainable once an attacker is on the device. With the right permissions the device's phone number, GPS coordinates, camera, and other information become readily available.

Access to various features and data on a device is the key here. Mobile devices offer attackers a much wider attack surface: Cameras, near field communication (NFC), GPS and other location services, Bluetooth, and wireless are all common features present in most smartphones. All apps have to ask for access permissions to access these features on the device. Fortunately mobile operating systems are usually quite verbose in detailing which permissions are requested when installing an app. Still, most users don't examine these permissions carefully, opting to just accept the request rather than reading through the details, in much the same way many users approach EULAs. Given this behavior, malicious app developers find it simple to persuade users that they should grant unnecessary permissions to a malicious app.

The attraction of the mobile environment to attackers is clearly based on the size and growth rate of the user base today. Yet it's also based on the amount of personal information that's easily attainable once an attacker is on the device.

PHISHING + SPAM

Spam and Phishing

In the mid-to-late 2000s, most phishing attempts were carried out through email for financial gain. Over time, phishing attacks have expanded in the scope of their targets from not only banks, credit unions and other financial institutions, to a variety of other organizations. The social engineering involved has also grown more sophisticated in recent years and recent examples include phishing for online accounts of customers of domestic energy companies and loyalty card programs. More energy utility companies are encouraging their customers to move to paperless billing, enabling an attacker to retrieve utility bills. They can potentially use these bills in the money laundering process such as in creating a bank account in someone else's name and using the online bill as proof of identity.

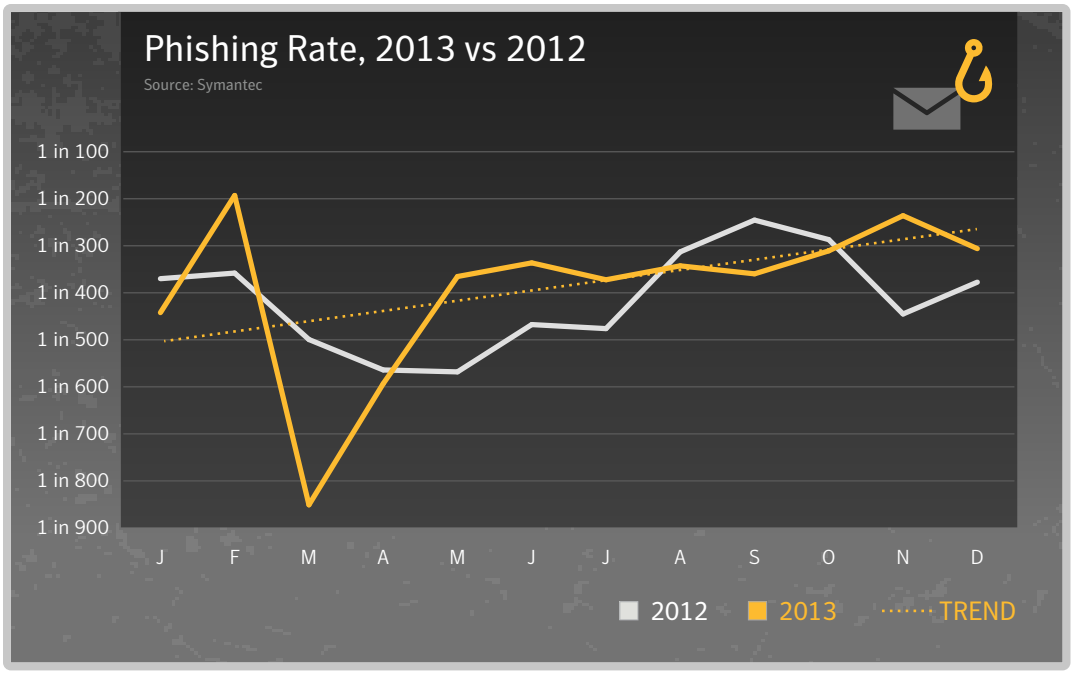
The phishing rate for the year has increased, from 1 in 414.3 emails per day, to 1 in 392.4. The busiest month of the year was February, where the rate rose to 1 in 193.0 emails.

Many of these phishing attempts consist of fake login pages for popular social networks. In addition to just spoofing login pages of legitimate sites, phishers began introducing baits relevant to current events to add flavor to the phishing pages. Celebrity promotions, popular community pages, social networking applications, and other related material were introduced into phishing sites as bait.

At a Glance

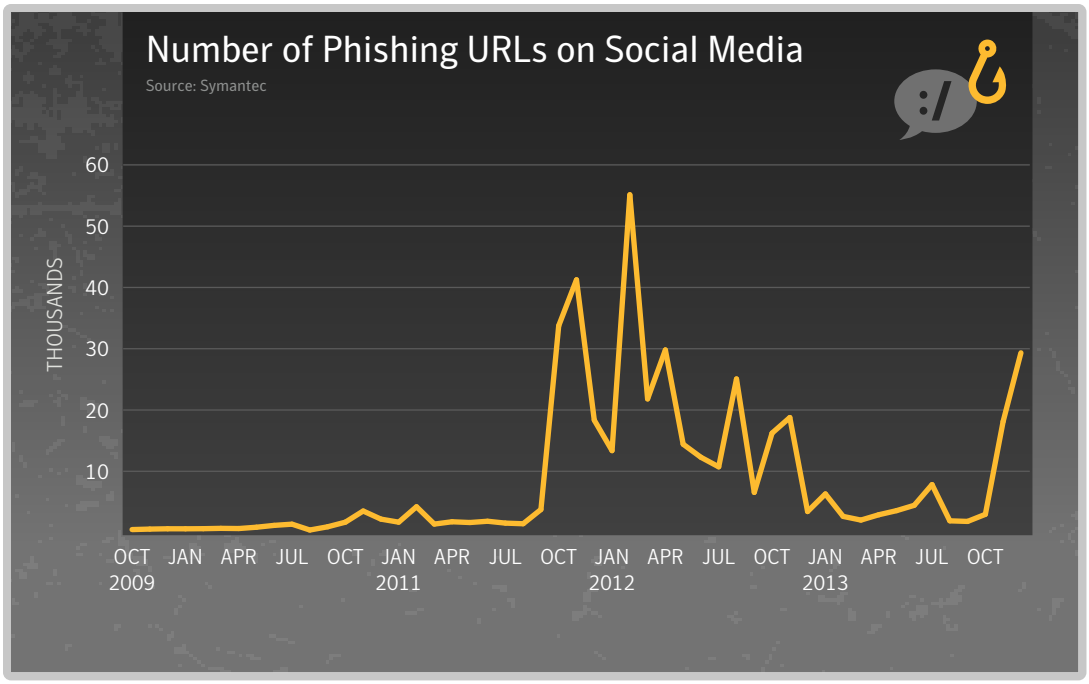
- *The phishing rate has increased in 2013, from 1 in 414 for 2012 to 1 in 392 in 2013.*
- *Login credentials for various accounts are the primary type of information sought by phishers.*
- *Spam rates are down 3 percentage points in 2013, making up 66 percent of email traffic.*
- *Scammers are working to compromise websites in order to help spread their scams.*

Fig. 1



- *The global average phishing rate has increased from 2012 from 1 in 414 to 1 in 392.*

Fig. 2



- *This chart represents number of URLs detected on social media websites per month.*

Phishers also began exploring new up-and-coming social networks. During the past five years, the number of social media sites that phishers have used in their attempts to gather sensitive information has increased to roughly three times its earlier figure.

Social networking is bringing down the overall impact of email phishing attempts as scammers post their messages and campaigns through social media instead. For instance, in October 2013 Symantec noted one such phishing campaign being propagated using social media messages. This phishing attack in particular used URLs with the .pw top-level domain (TLD), a TLD frequently utilized by scammers in 2013. The number of phishing URLs originating from social media sources increased six-fold in November 2013 as compared to the previous month. Out of these links, 84 percent of URLs had the .pw TLD.

That's not to say that attackers have abandoned email for spam and phishing attempts; these still make up a large percentage of email traffic. Spammers still hawk their wares and phishers still try to steal information.

Login credentials for accounts seem to be the main information phishers are looking for. Email campaigns often include socially-engineered text and links to web pages that are designed to impersonate popular social networking sites, while others may look almost identical to a bank's website. The email text might hint at a problem with a user's account or a special limited-time offer, the goal being to convince users that the web page is legitimate so that they will enter their credentials. Once entered, compromised social media accounts can be used to spread phishing and spam campaigns, or banking information can be used to access an individual's finances. In total, the 2013 Norton Report demonstrated that 12 percent of those surveyed said that someone has hacked their social media account.[42]

Social networking is bringing down the overall impact of email phishing attempts as scammers post their messages and campaigns through social media instead.

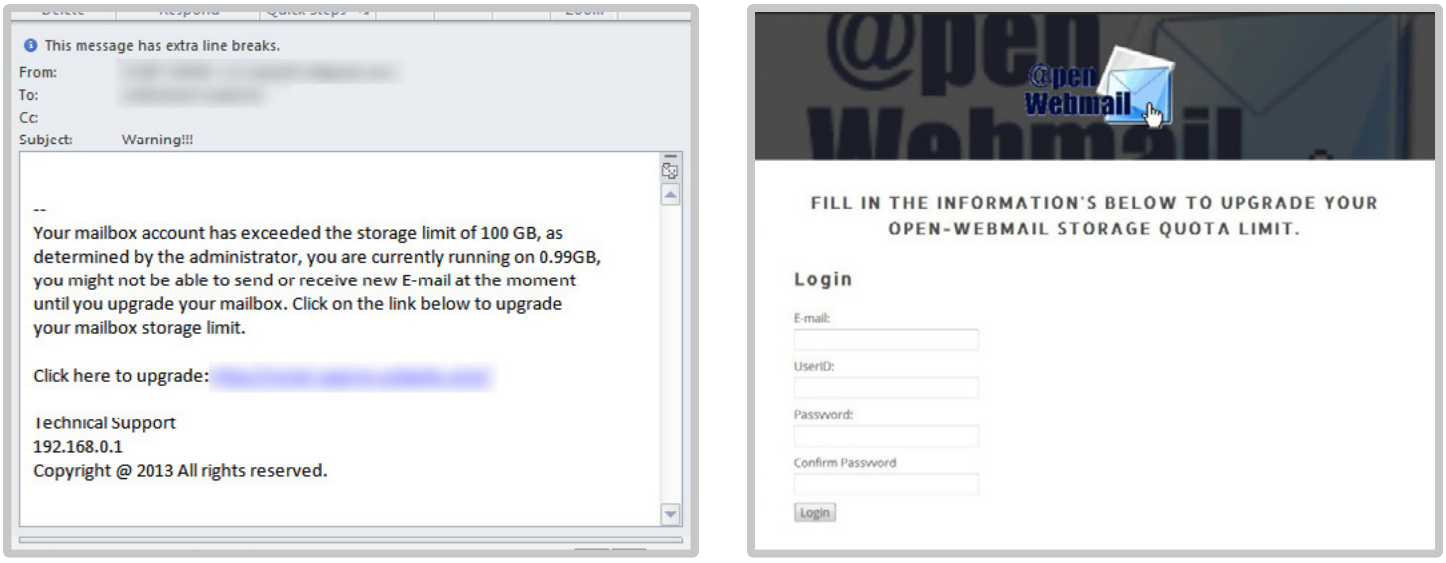


Fig. 3 Example quota phishing email and website.

Phishers also continued to spoof webmail accounts during 2013. One popular attack method played off the idea that a mailbox has exceeded its quota. A victim is directed to a site where they are asked to "confirm" email, user name and password. However, no further information is provided about the quota issue and the account is compromised, leaving it open to be used to send spam.

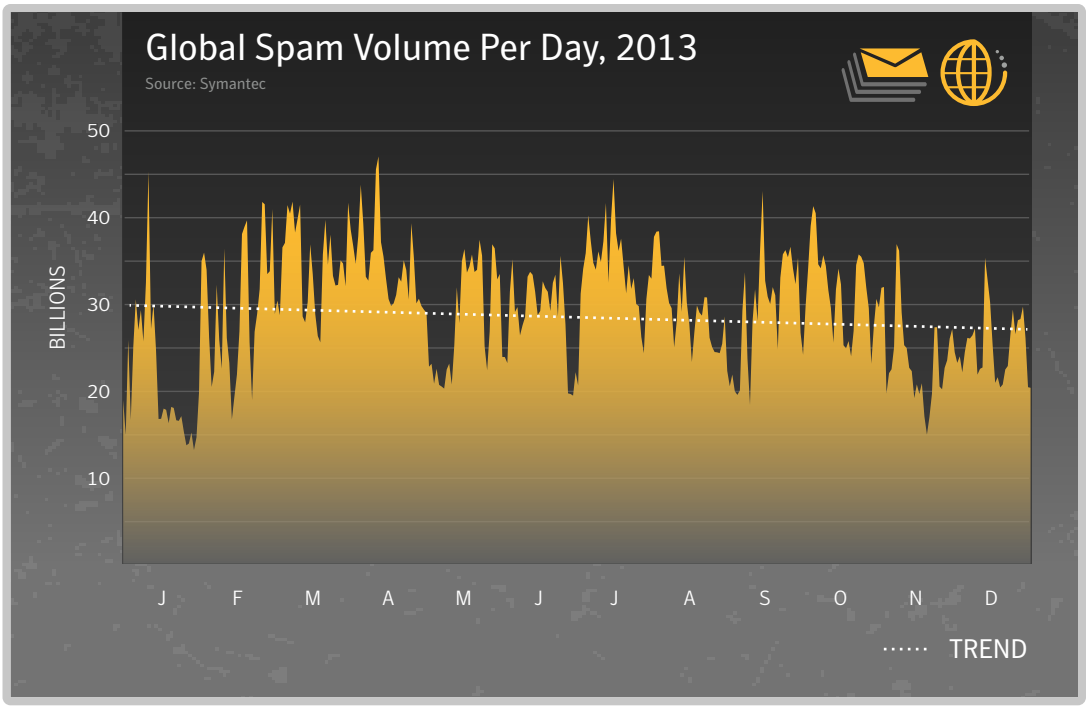
One of the latest findings from analysis of phishing activity in 2013 was the emergence of campaigns targeting information not usually associated with more traditional phishing activities. These include attempts to steal frequent flyer and loyalty card accounts, online credentials for utility accounts, and cloud-based storage account details. More concerning perhaps was that some of these may be used in identity fraud. For instance, a utility bill is often a requirement as a proof of address. Many people today use paperless billing, so if phishers gained access to a utility account they could have feasibly changed the account address and used it to fraudulently obtain goods and services in the victim's name.

In other cases, scammers preyed upon people's dreams of living in another country. Someone looking to travel or emigrate, particularly to countries with tight visa restrictions may have been willing to reveal sensitive information if they thought that it would help them to gain entry to the country in question.

With all the new phishing scams, the more traditional financial phishing has not declined. There were a number of new angles that became popular in 2013. Bitcoin wallet account details, tax information, welfare and benefit details, and payday loan accounts were all examples of campaigns targeting a victim's finances.

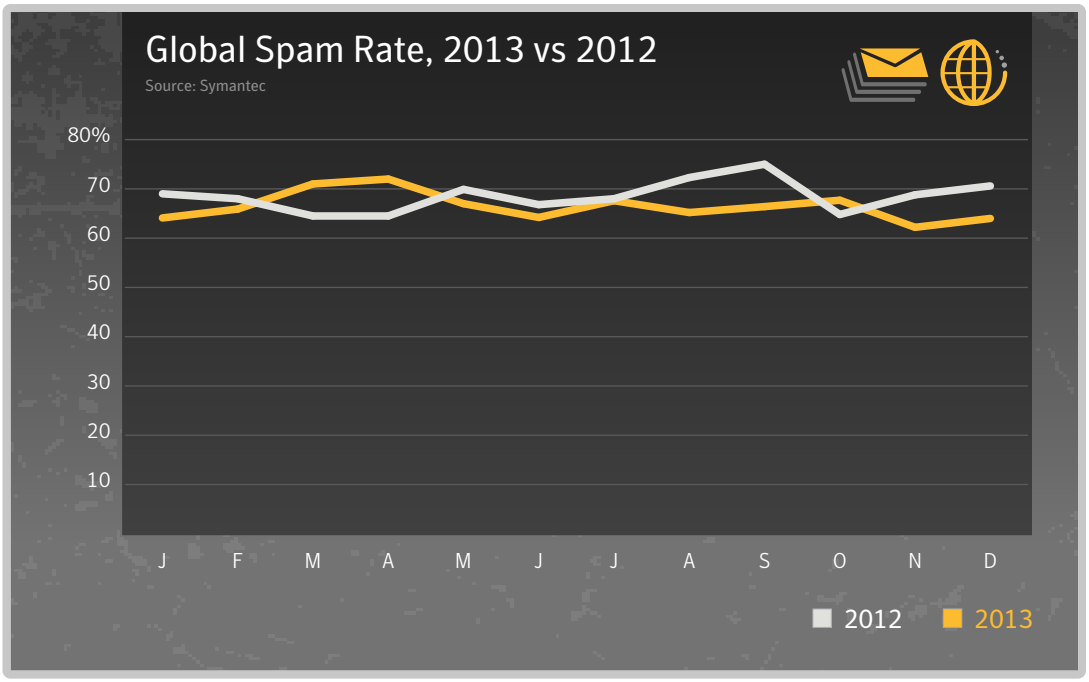
In terms of spam campaign strategies, some were quite blatant, clearly selling pills, whilst in other cases the message entirely unrelated topics - such as subject lines referencing replica watches, while the email body linked to pornographic sites.

Fig. 4



- *The estimated projection of global spam volumes for spam in business email traffic decreased marginally by 3 percent, from 30 billion spam emails per day in 2012, to 29 billion in 2013.*
- *Spam volumes were highest in March and April, with approximately 34.3 billion and 35.3 billion spam emails per day.*

Fig. 5



- *The global average spam rate for 2013 was 66 percent, compared with 69 percent in 2012; a decrease of 3 percentage points.*
- *Pharmaceutical spam accounts for 18 percent of all spam, but the Adult/ Dating category accounts for approximately 70 percent of spam. Pharmaceutical spam in 2013 declined by approximately 3 percentage points compared with 2012.*
- *Adult/Dating spam in 2013 increased by approximately 15 percentage points compared with 2012.*

The overall spam rate appeared to be down by 3 percentage points for the year, from 69 percent in 2012 to 66 percent in 2013. There was a period of time during 2013 where the spam rate did surpass rates for similar time periods during 2012. For approximately six months of the year, the global spam rate exceeded the equivalent rate for the same month in the previous year, despite the fact that the annual average was actually lower.

Lots of spam and phishing attacks use URL shortening, a method where a longer URL is shortened to save space, but still resolves to the original page. However, the use of shortened URLs also masks the original URL, allowing attackers to hide malicious links behind them. This technique was still popular and for much of 2013 its use remained fairly stable.

The use of shortened URLs also masks the original URL, allowing attackers to hide malicious links behind them. This technique was still popular and for much of 2013 its use remained fairly stable.

Compromised Sites

Many ordinary users and small businesses are comfortable managing their own web servers, whether internally or externally hosted, since it's now easier to do and relatively inexpensive. However, while the ease of installation and cost of maintenance may have decreased, many new administrators are perhaps not familiar with how to secure their servers against attacks from the latest web attack toolkits. Nor are they diligent about keeping their sites secure and patched with the latest software updates. Updating popular applications such as content management systems or blogging software on the web server is a necessity. These services have become major targets for abuse by hackers, and a single vulnerability may be used across thousands of sites.

Scammers are also attacking web hosting sites that provide hosting platforms as a service. If an attacker can figure out a way to successfully breach a company that provides such services, they can gain access to multiple sites hosted by the compromised company. It's possible for thousands of sites to be impacted in such breaches. Hackers can also use popular search engines to quickly discover potentially vulnerable websites that they may be able to compromise. In this way, a website may be easily hijacked if any software vulnerabilities can be exploited by the attackers.

Beyond hijacking websites in order to spread spam, scammers continue to attack Autonomous Systems (ASes) using the Border Gateway Protocol (BGP), as first discussed in last year's ISTR. In these situations, attackers hijack entire blocks or ranges of IP addresses that may belong to a business and re-route them to a new destination URL of their choosing. The spammers then use those IP addresses to send spam for a brief period, where the spam appears to come from the legitimate business. This topic is covered in detail in Appendix C of this report, New Spam Tread: BGP Hijacking.

- *For more information on spam and phishing trends, see the Spam and Phishing appendix.*

LOOKING AHEAD

Looking Ahead

Privacy and Trust

Many factors helped to shape the threat landscape during 2013, and some will have an enduring impact by altering our thinking about how we behave and conduct ourselves online. For some, the attitude regarding online privacy may be a factor of our age and perhaps to some extent how long we have been online; however, the general attitudes regarding online trust and privacy changed more during 2013 than in any other time.

In one sense, anything published online may be there forever; our proudest moments may sit alongside our most embarrassing mistakes. It is when the personal information we casually share falls into what we call "the wrong hands" that we are most concerned. We are increasingly sharing more data about ourselves that we may not even think about; for example, if it will lower our insurance premiums, we are willing to share GPS tracking information with an insurance provider to prove that we don't drive recklessly. So much of what we do is online and linked across many different environments, social media applications, and devices. What we do in one area is quickly shared with another.

One of the key drivers for the adoption of cloud-based technology has been the widespread use of social media; social networking sites, applications and mobile apps all use the cloud. Without Internet access, a smartphone is just a phone. Widespread cloud adoption has essentially enabled rapid growth to occur on an enormous scale, and as a result of some of the headlines in 2013 some people are already asking questions: "Do we still trust the cloud?" "Who should we trust to look after our personal data?" We have seen limited impact, but it remains to be seen whether this will influence the social media and mobile app revolution in any meaningful way over the coming months. In 2014 and beyond we can expect social networking organizations and other online service providers to seek to win back the hearts and minds of their users by making online privacy and data security core to their offerings. The worst case scenario is that people will become even more lackadaisical about online privacy to the detriment of their own personal security.

The adoption of encryption technology is expected to grow in 2014 and beyond, not only for securing data on personal devices but for online transactions including emails. The use of personal VPNs is also likely to increase as concerned users become wary about the traffic that may be exposed through their Wi-Fi hotspot, or simply to prevent their ISP from being able to track their activity. More up-to-date, faster encryption protocols will be in demand to secure these devices, so even if data is exposed or a device falls into the wrong hands, users can be assured that it cannot be exploited by the criminals.

Targeted Attacks and Data Breaches

The huge scale of breaches dominated the headlines during 2013, and has forced both businesses and home users to seriously consider how they secure their confidential information to keep it both private and secure. The sheer number of data breaches and even larger volume of identities being leaked was alarming, and the majority of these were caused by hacking. As the pressure mounts not to become the next victim, businesses are looking more towards trusted security vendors as a one-stop solution provider to take care of all their data protection needs. Not only will the focus be on safeguarding against an attack by hardening the perimeter, but also on minimizing the potential impact of any breach should one occur. The wider adoption of encryption technology will be at the core of securing personal data, intellectual property, and company secrets. It has often been considered difficult to implement a robust and comprehensive encryption policy within an organization, hence the growing demand for such technology to become a seamless part of the underlying infrastructure rather than an add-on only used by a few.

As more personal information is stored in the cloud and accessible online, we routinely share more data with each other. Businesses and governments need to routinely handle massive quantities of personal information securely. Important questions are now being asked by the owners of this data, such as whether the caretakers are taking sufficient protective measures to safeguard it, irrespective of whether information is on their own computers and devices or in the cloud?

E-crime and Malware Delivery

In the short term, e-crime will continue to grow. This will lead to greater cooperation between law enforcement and industry, and make it increasingly difficult for cybercriminals to operate. Rather than disappearing, e-crime is likely to move towards a new, more professional business model.

At the end of 2013 there are still many users on Windows XP using older, more vulnerable web browsers and plug-ins; in many ways this combination can be the Achilles heel of security.

Looking Ahead

Microsoft is sun-setting their support for Windows XP in 2014 and it will be interesting to see how this affects people's attitudes towards online security. On the one hand, those that continue to use the retired operating system will no longer get patches directly from Microsoft. On the other, it may precipitate a large move to newer and more secure operating systems.

The next two or three years may bear witness to a divergence in the threat landscape; as people move to newer, more secure operating systems and modern web browsers, it will naturally become more easy to avoid falling victim to a casual malware attack. The success or failure of these attacks will be increasingly determined by the level of social engineering involved, which in turn may drastically affect the overall shape of the online security landscape.

Finally, as the "Internet of Things" becomes more an everyday reality, items like TVs, telephones, security cameras, and baby monitors as well as wearable technology and even motor cars will become woven into the fabric of the Internet. This in turn increases the attack surface, presenting new opportunities for researchers and attackers alike. The Internet of Things could soon become the next battleground in the threat landscape.

Social Media and Mobile

So much of what we now do in our daily lives is being tracked and recorded online. The public has a seemingly insatiable appetite for personal lifestyle apps that help do things better than before and help achieve our goals faster than we could imagine. This may open more avenues for cybercriminals to exploit and allow them to take advantage of potential victims. While there may still be a number of activities in our lives that aren't currently shared online, this is likely to diminish in the near future. Wearable technology such as interactive wristwatches and other accessories will make interacting with these apps less like being online and simply a part of everyday life. Users who are less aware of the potential risks and dangers may soon find themselves victims. The importance of online security education and awareness-raising for these users will be greater than ever.

In the future, expect more traditional malware threats being "ported" to mobile devices. Fake security software has already appeared in this environment, and ransomware could soon be developed for the mobile platform too, given how lucrative it has proved on desktop and laptop computers.

The latest mobile devices also contain a large number of entry points, including Wi-Fi, Bluetooth, and near field communication (NFC), as well as USB. There may be plenty of opportunities to compromise these devices through new methods not fully explored at this stage. So far, mobile threats are still mainly aimed at consumers rather than enterprises. Only a few cases have been discovered where a mobile threat has targeted corporate users. Targeted attacks can be expected to take advantage of the mobile landscape in the near future, especially since the potential for surveillance or counter surveillance measures are even higher on devices that include in-built cameras and microphones that may be switched on and off with ease.

RECOMMENDATIONS + BEST PRACTICE GUIDELINES

Best Practice Guidelines for Businesses

01
Employ defense-in-depth strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

02
Monitor for network incursion attempts, vulnerabilities, and brand abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

03
Antivirus on endpoints is not enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints;
- Browser protection for avoiding obfuscated web-based attacks;
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

04
Secure your websites against MITM attacks and malware infection

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL (SSL protection on your website from logon to logoff);
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for any vulnerabilities (in 2013 1 in 8 websites scanned by Symantec was found to have vulnerabilities);
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

05
Protect your private keys

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures;
- Secure keys in secure, tamper-proof, cryptographic hardware devices;
- Implement physical security to protect your assets from theft.

06
Use encryption to protect sensitive data

Implement and enforce a security policy whereby any sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization. Use Data Loss Prevention to help prevent data breaches: Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss. Data loss prevention should be implemented to monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.

- DLP should be configured to identify and block suspicious copying or downloading of sensitive data;
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

Best Practice Guidelines for Businesses

07
Ensure all devices allowed on company networks have adequate security protections

If a bring your own device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

08
Implement a removable media policy

Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

09
Be aggressive in your updating and patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plug-ins. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

10
Enforce an effective password policy

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

11
Ensure regular backups are available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

12
Restrict email attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

13
Ensure that you have infection and incident response procedures in place

- Keep your security vendor contact information handy, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

14
Educate users on basic security protocols

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
- Deploy web browser URL reputation plug-in solutions that display the reputation of websites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendor website;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or the task manager.

Best Practice Guidelines for Consumers

01
Protect yourself

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing;
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
- Browser protection to protect against obfuscated web-based attacks;
- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines;
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.[43]

02
Update regularly

Keep your system, program, and virus definitions up-to-date – always accept updates requested by the vendor. Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

03
Be wary of scareware tactics

Versions of software that claim to be free, cracked or pirated can expose you to malware, or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

04
Use an effective password policy

Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites. Use complex passwords (upper/lowercase and punctuation) or passphrases.

05
Think before you click

Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plug-in.
- Use a web browser plug-in or URL reputation site that shows the reputation and safety rating of websites before visiting. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, bitTorrent, and any other peer-to-peer (P2P) exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only.

06
Guard your personal data

Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates.

- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

SANS Critical Security Controls:

How to Protect Your Organization from Cyber Attack

01

Introduction

The goal of the annual Symantec Internet Security Threat Report (ISTR) is not only to raise awareness of cyber threats and educate business users and consumers about the changing nature of the cyber security threat landscape, but also to provide guidance and advice about how to secure your critical assets, including your personal data to help reduce the impact of any potentially harmful incidents.

There are a number of good best practice guidelines that, if followed, can help to reduce the risk from cyber threats – many of these have been outlined in this report. However, for businesses and organizations especially, the implementation of a more methodological approach to hardening their security profile can bring additional benefits as well. There are a variety of frameworks that can help, and each one may suit different organizations in different ways. Generally a standard framework will need to be continually maintained, and adapted to new threats and challenges. Moreover, your business will benefit from the wealth of experience and lessons learned by other organizations that are also using these standards and frameworks, and building on them in turn. This approach will help you to prioritize the areas that you need to focus on first, and also to harden your existing defenses and develop the right security posture to help prevent the most common and potentially most harmful types of attack from damaging your business.

In the United States, the National Institute of Standards and Technology (NIST) recently published the "Framework for Improving Critical Infrastructure Cybersecurity," and Symantec has played a central role in shaping it. The NIST framework is not designed to be a standard or set of controls, nor is it a checklist; instead, it is a tool to help organizations assess and improve their cybersecurity programs, or to help develop such a program if they don't already have one in place. Symantec also works with the SANS Institute[44], one of the largest sources for information security training and certification, which operates the SANS Top 20 Critical Security Controls. The SANS CSC is comprised of a detailed list of controls that any organization can implement and adapt quickly, and each one is specifically designed to address particular areas of concern. For more information on the SANS CSC, please visit www.sans.org/critical-security-controls/guidelines. Additional details about the new NIST framework can also be found here: www.nist.gov/cyberframework.

How to Apply the SANS Critical Security Controls

In order to apply the controls effectively, it's not always necessary to try to implement everything at once. By identifying some "quick wins," you should be able to quickly implement the relevant controls that will have the greatest impact and reduce the exposure of your organization to the greatest threats more quickly.

For example, in order to tighten the controls that will help reduce the likelihood of a website being breached; you may wish to consider the following controls: 3, 4 and 5 to begin with and then 6 and 11 when that is fully operational. Additional controls may then be introduced later, once you have the basics in place and operating effectively.

Following is a list of potential controls that could be implemented to safeguard against some of the most important types of threats discussed in the Symantec ISTR.

CRITICAL CONTROL 01

PROTECTION PRIORITIES

Source: Sans.org, Symantec

	HARDEN DEFENSES	ENHANCE DETECTION	REDUCE IMPACT
Data Breaches	02 03 04 05 06 10 11 07	01 14 16 09 18 20	08 12 17 13 15 19
Targeted Attacks	02 03 04 05 06 11	01 14 16 18 20	12 17 13 15
Web-Based Attacks	02 03 04 05 06	01 14 16	12 13 15 17
Safeguarding Web Servers	02 03 04 05 06 10 11	01 14 16 18 20	08 12 17 13
Mobile Threats	02 03 04 05 06 07	01	08 17
Malware Threats	02 03 04 05	01 14 16 09 18 20	08 12 17 13
Spam + Phishing	02 05	01 09 20	12 13
Bots	02 03 04 05	01 14 18	17 13 19

01

01
Inventory of Authorized and Unauthorized Devices

Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

02
Inventory of Authorized and Unauthorized Software

Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

03
Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

04
Continuous Vulnerability Assessment and Remediation

Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

05
Malware Defense

Block malicious code from tampering with system settings or content, capturing sensitive data, or from spreading:

Use automated antivirus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis.

Prevent network devices from using auto-run programs to access removable media.

06
Application Software Security

Neutralize vulnerabilities in web-based and other application software: Carefully test internally-developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).

07
Wireless Device Control

Protect the security perimeter against unauthorized wireless access: Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

08
Data Recovery Capability

Minimize the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more frequently.

Regularly test the restoration process.

09
Security Skills Assessment and Appropriate Training to Fill Gaps

Find knowledge gaps, and eradicate them with exercises and training: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

10
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

11
Limitation and Control of Network Ports, Protocols, and Services

Allow remote access only to legitimate users and services: Apply host-based firewalls, port-filtering, and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

01

12 Controlled Use of Administrative Privileges

Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious email, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

13 Boundary Defense

Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish a multi-layered boundary defense by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").

14 Maintenance, Monitoring, and Analysis of Security Audit Logs

Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.

15 Controlled Access Based on the Need to Know

Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.

16 Account Monitoring and Control

Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

17 Data Loss Prevention

Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

18 Incident Response Management

Protect the organization's reputation, as well as its information: Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

19 Secure Network Engineering

Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

20 Penetration Tests and Red Team Exercises

Use simulated attacks to improve organizational readiness: Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defense and response capabilities.

Footnotes

Targeted Attacks + Data Breaches

01 An attack campaign is defined as a series of emails that:
A.) Show clear evidence that the subject and target has been deliberately selected.
B.) Contain at least 3 or 4 strong correlations to other emails such as the topic, sender address, recipient domain, source IP address, etc.
C.) Are sent on the same day or across multiple days.

02 http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack

03 In previous years, this category was labeled as Government.

04 The Professional category includes Engineering, Accounting, Legal, and Heath-related services. The Non-Traditional category includes Business, Amusement, and Repair-related services.

05 Fires in workplace premises: risk data. Holborn et. al.(2002) Fire Safety Journal 37 303-327. The full range is from 1:161 and 1:588.

06 These are frequently referred to as case-control studies, which compare a group of subjects with a disease (cases) to a similar group without the disease (the controls). The resulting ratio shows the risk of contracting the disease. In the case of spear phishing, we simply substitute “afflicted with a disease” for “received at least one spear-phishing email in 2013.”

07 This represents the proportions of organizations within the same sector that were subjected to one or more targeted attacks within the year.

08 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

09 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf

10 http://www.symantec.com/en/aa/theme.jsp?themeid=ssl-resources

11 http://www.symantec.com/about/news/release/article.jsp?prid=20130206_01

12 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

Ecrime, Malware + Malware Delivery Tactics

13 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_bamital.pdf

14 http://internetworldstats.com/

15 http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet

16 http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

17 http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware

18 http://www.symantec.com/security_response/writeup.jsp?docid=2012-111612-5925-99

19 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf

20 http://www.secureworks.com/resources/blog/research/cutwail-spam-swapping-blackhole-for-magnitude-exploit-kit/

21 http://www.threattracksecurity.com/it-blog/shylock-caphaw-drops-blackhole-for-styx-and-nuclear/

22 http://www.scmagazine.com/criminals-move-quickly-to-other-exploit-kits-after-arrest-of-blackhole-author/article/315629/

23 For more details about Symantec Rulespace, please visit http://www.symantec.com/theme.jsp?themeid=rulespace

24 http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware

25 https://otalliance.org/resources/malvertising.html

26 http://www.symantec.com/connect/blogs/creepware-who-s-watching-you

Footnotes

Social Media + Mobile Threats

27 http://www.symantec.com/connect/blogs/instagram-users-compromise-their-own-accounts-likes

28 http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder

29 http://www.symantec.com/connect/blogs/rise-java-remote-access-tools

30 http://www.symantec.com/security_response/writeup.jsp?docid=2013-012916-2128-99

31 http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

32 http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

33 http://www.symantec.com/connect/blogs/fakeav-holds-android-phones-ransom

34 http://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99

35 http://www.symantec.com/connect/blogs/androidexprespam-authors-revamp-gcogle-play-android-express-s-play

36 In Japan email is often used instead of SMS, through special email addresses provided by mobile carriers. While primarily accessed and used through mobile devices, these email addresses can send and receive email from standard email addresses.

37 http://www.symantec.com/security_response/writeup.jsp?docid=2012-102908-3526-99

38 http://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99

39 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf

40 http://www.symantec.com/security_response/writeup.jsp?docid=2013-032910-0254-99

41 http://www.symantec.com/connect/blogs/windows-malware-attempts-infect-android-devices

Phishing + Spam

42 http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

Best Practice Guidelines

43 For more information about Norton Online Family, please visit https://onlinefamily.norton.com/

SANS Critical Controls

44 www.sans.org

Contributors

Credits

Paul Wood, Executive Editor
Ben Nahorney, Editorial Content
Kavitha Chandrasekar, Analyst
Scott Wallace, Graphics & Design
Kevin Haley, Technical Advisor

Contributors

Anand Kashyap
Andrew Horbury
Arman Catacutan
Bartlomiej Uscilowski
Candid Wueest
Chau Mai
Con Mallon
Dick O'Brien
Eric Chien
Eric Park
Gavin O'Gorman
Hon Lau
John-Paul Power
Joji Hamada
Kari Ann Sewell
Laura O'Brien
Mathew Maniyara
Olivier Thonnard
Nicholas Johnston
Orla Cox
Peter Coogan
Pierre-Antoine Vervier
Quentin Liu
Satnam Narang
Stephen Doherty
Tim Gallo

With Support From

Andrew Watson
Chintan Trivedi
Himanshu Dubey
Jason Theodorson
Jeffrey Wilhelm
John Gunalan
John Swick
Kevin Thompson
Manish Khorgade
Mat Nisbet
Parveen Vashishtha
Paul Thomas
Phil Ivers
Prasanna N
Rahul Sharma
Rajesh Sethumadhavan
Tony Zhu

Special Thanks To

Alejandro Borgia
Cheryl Elliman
Darragh Cotter
Elizabeth Soares
Jasmin Kohan
Jeannie Warner
Linda Smith Munyan
Rebecca Donaldson
Richard Clooke
Sondra Magness
Jennifer Duffourg

2013 Trends, Volume 19, Published April 2014

ISTR

INTERNET SECURITY THREAT REPORT
GOVERNMENT APPENDIX ⌖ 2014

CONTENTS

101 **APPENDIX :: A**
THREAT ACTIVITY TRENDS

102 Threat Activity Trends

103 Malicious Activity by Source

104 Malicious Activity by Source: Overall Rankings, 2012–2013

104 Malicious Activity by Source: Malicious Code, 2012–2013

105 Malicious Activity by Source: Phishing Hosts, 2012–2013

105 Malicious Activity by Source: Spam Zombies, 2012–2013

106 Malicious Activity by Source: Web Attack Origins, 2012–2013

106 Malicious Activity by Source: Bots, 2012–2013

107 Malicious Activity by Source: Network Attack Origins, 2012–2013

108 Malicious Web-Based Attack Prevalence

108 Malicious Website Activity, 2012–2013

110 Analysis of Malicious Web Activity by Attack Toolkits

110 Malicious Website Activity: Attack Toolkit Trends

111 Malicious Website Activity: Overall Frequency of Major Attack Toolkits

112 Analysis of Web-Based Spyware, Adware, and Potentially Unwanted Programs

112 Potentially Unwanted Programs: Spyware and Adware Blocked

113 Analysis of Web Policy Risks from Inappropriate Use

113 Web Policies that Triggered Blocks, 2012–2013

115 Analysis of Website Categories Exploited to Deliver Malicious Code

115 Malicious Web Activity: Categories that Delivered Malicious Code

116 Malicious Web Activity: Malicious Code By Number of Infections per Site for Top-Five Most Frequently Exploited Categories

116 Malicious Web Activity: Malicious Code by Number of Infections per Site

117 Malicious Web Activity: Fake Antivirus by Category

118 Malicious Web Activity: Browser Exploits by Category

119 Malicious Web Activity: Social Networking Attacks by Category

120 Bot-Infected Computers

120 Top-Ten Bot Locations by Average Lifespan of Bot, 2012–2013

122 Denial of Service Attacks

126 Analysis of Mobile Threats

126 Android Mobile Threats: Newly Discovered Malicious Code, 2012–2013

127 Mobile Threats: Malicious Code by Platform, 2013

127 Android Mobile Threats: Average Number of Malware Variants per Family, 2012–2013

128 Mobile Threats: Malicious Code Actions in Malware, 2012–2013

128 Mobile Threats: Malicious Code Actions – Additional Detail, 2012–2013

129 Mobile Threats: Documented Mobile Vulnerabilities by Platform

129 Mobile Threats: Documented Mobile Vulnerabilities by Month

132 Quantified Self – A Path to Self-Enlightenment or Just Another Security Nightmare?

133 Data Breaches that could lead to Identity Theft

134 Timeline of Data Breaches Showing Identities Breached in 2013, Global

135 Data Breach Incidents by Sector

136 Identities Exposed by Sector

137 Average Number of Identities Exposed per Data Breach by Notable Sector

138 Top Causes for Data Breach by Number of Breaches

138 Top Causes for Data Breaches by Number of Identities Exposed

139 Types of Information Exposed by Data Breach
139 Average Number of Identities Exposed per Data Breach, by Cause

140 Threat of the Insider

141 Gaming Attacks

142 The New Black Market

144 Footnotes

145 **APPENDIX :: B**
MALICIOUS CODE TRENDS

146 Malicious Code Trends

147 Top Malicious Code Families
148 Overall Top Malicious Code Families
149 Relative Proportion of Top-Ten Malicious Code Blocked in Email Traffic by Symantec.cloud in 2013, by Percentage and Ratio
149 Malicious Code Blocked in Email Traffic by Symantec.cloud, 2012–2013
150 Relative Proportion of Top-Ten Malicious Code Blocked in Web Traffic by Symantec.cloud in 2013, by Percentage and Ratio

152 Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
153 Proportion of Email Traffic Identified as Malicious by Industry Sector
153 Proportion of Email Traffic Identified as Malicious by Organization Size

154 Propagation Mechanisms
154 Propagation Mechanisms

156 Email-Targeted Spear-Phishing Attacks Intelligence
164 Miniduke Sample of Email Subjects, Documents, and MD5s
167 Elderwood Sample of Email Subjects, Documents, and MD5s
170 APT1 Sample of Email Subjects, Documents, and MD5s

172 Footnotes

173 **APPENDIX :: C**
SPAM + FRAUD ACTIVITY TRENDS

174 Spam and Fraud Activity Trends

175 Analysis of Spam Activity Trends
175 Global Spam Volume in Circulation
176 Proportion of Email Traffic Identified as Spam, 2012–2013

177 Analysis of Spam Activity by Geography, Industry Sector, and Company Size
177 Proportion of Email Traffic Identified as Spam by Industry Sector
178 Proportion of Email Traffic Identified as Spam by Organization Size
178 Proportion of Email Traffic Identified as Spam by Geographic Location

179 Analysis of Spam Delivered by Botnets
179 Top Sources of Botnet Spam by Location
180 Analysis of Spam-Sending Botnet Activity at the End of 2013

181 Significant Spam Tactics
181 Frequency of Spam Messages by Size
181 Proportion of Spam Messages Containing URLs
182 Analysis of Top-Level Domains Used in Spam URLs

183 Analysis of Spam by Categorization
184 Spam by Category

185 Phishing Activity Trends
185 Phishing Rate, 2012–2013
186 Phishing Category Types, Top 200 Organizations
186 Tactics of Phishing Distribution

188 Analysis of Phishing Activity by Geography, Industry Sector, and Company Size
188 Proportion of Email Traffic Identified as Phishing by Industry Sector
188 Proportion of Email Traffic Identified as Phishing by Organization Size
189 Proportion of Email Traffic Identified as Phishing by Geographic Location

190 New Spam Trend: BGP Hijacking

195 Footnotes

196 **APPENDIX :: D**
VULNERABILITY TRENDS

197 Vulnerability Trends

198 Total Number of Vulnerabilities
198 Total Vulnerabilities Identified 2006–2013
199 New Vulnerabilities Month-by-Month, 2012–2013
199 Most Frequently Attacked Vulnerabilities

201 Zero-Day Vulnerabilities
201 Volume of Zero-Day Vulnerabilities, 2006–2013
202 Zero-Day Vulnerabilities Identified

204 Web Browser Vulnerabilities
204 Browser Vulnerabilities, 2011–2013

205 Web Browser Plug-in Vulnerabilities
205 Browser Plug-In Vulnerabilities, 2012–2013

207 Web Attack Toolkits

208 SCADA Vulnerabilities
208 SCADA Vulnerabilities Identified

210 Footnotes

211 **APPENDIX :: E**
GOVERNMENT THREAT ACTIVITY TRENDS

212 Government Threat Activity Trends

213 Malicious Activity by Critical Infrastructure Sector
213 Malicious Activity by Critical Infrastructure Sector

214 Sources of Origin for Government-Targeted Attacks
214 Sources of Origin for Government-Targeted Attacks

215 Attacks by Type – Notable Critical Infrastructure Sectors
216 Attacks by Type: Overall Government and Critical Infrastructure Organizations
217 Attacks by Type: Notable Critical Infrastructure Sectors

218 Footnotes

219 About Symantec

219 More Information

APPENDIX :: A
THREAT ACTIVITY TRENDS

Threat Activity Trends

The following section of the Symantec Global Internet Security Threat Report provides an analysis of threat activity, data breaches, and web-based attacks, as well as other malicious actions that Symantec observed in 2013. The malicious actions discussed in this section also include phishing, malicious code, spam zombies, bot-infected computers, and attack origins. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Source
- Malicious Web-Based Attack Prevalence
- Analysis of Malicious Web Activity by Attack Toolkits
- Analysis of Web-Based Spyware, Adware, and Potentially Unwanted Programs
- Analysis of Web Policy Risks from Inappropriate Use
- Analysis of Website Categories Exploited to Deliver Malicious Code
- Bot-Infected Computers
- Denial of Service Attacks
- Analysis of Mobile Threats
- Quantified Self – A Path to Self-Enlightenment or Just Another Security Nightmare?
- Data Breaches That Could Lead to Identity Theft
- Threat of the Insider
- Gaming Attacks
- The New Black Market

Malicious Activity by Source

Background

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, including faster speeds, the potential of constantly connected systems, and a typically more stable connection. Symantec categorizes malicious activities as follows:

- **Malicious code:** This includes programs such as viruses, worms, and Trojans that are covertly inserted into programs. The purpose of malicious code includes destroying data, running destructive or intrusive programs, stealing sensitive information, and compromising the security or integrity of a victim's computer data.
- **Spam zombies:** These are remotely controlled, compromised systems specifically designed to send out large volumes of junk or unsolicited email messages. These email messages can be used to deliver malicious code and phishing attempts.
- **Phishing hosts:** A phishing host is a computer that provides website services in order to illegally gather sensitive user information while pretending that the attempt is from a trusted, well-known organization by presenting a website designed to mimic the site of a legitimate business.
- **Bot-infected computers:** Malicious programs have been used to compromise computers to allow an attacker to control the targeted system remotely. Typically, a remote attacker controls a large number of compromised computers over a single reliable channel in a botnet, which can then be used to launch coordinated attacks.
- **Network attack origins:** This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- **Web-based attack origins:** This measures attack sources that are delivered via the web or through HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Methodology

These metrics assess the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, namely: malicious code reports, spam zombies, phishing hosts, bot-infected computers, network attack origins, and web-based attack origins. The proportion of each activity originating in each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question, and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Fig. A.1

Malicious Activity by Source: Overall Rankings, 2012–2013

Source: Symantec

Country/Region	2013 World Rank	2013 Overall Average	2012 World Rank	2012 Overall Average	Change
United States	1	20.3%	1	22.7%	-2.4%
China	2	9.4%	2	11.0%	-1.6%
India	3	5.1%	3	6.5%	-1.4%
Netherlands	4	3.5%	7	2.7%	0.8%
Germany	5	3.3%	6	3.4%	-0.2%
Russia	6	2.6%	11	2.2%	0.4%
United Kingdom	7	2.6%	9	2.4%	0.2%
Brazil	8	2.5%	5	4.0%	-1.5%
Taiwan	9	2.5%	10	2.3%	0.1%
Italy	10	2.3%	8	2.4%	-0.1%

Fig. A.2

Malicious Activity by Source: Malicious Code, 2012–2013

Source: Symantec

Country/Region	2013 Malicious Code Rank	2013 Malicious Code Percentage	2012 Malicious Code Rank	2012 Malicious Code Percentage	Change
United States	1	16.9%	1	17.2%	-0.3%
India	2	15.3%	2	16.2%	-0.9%
China	3	5.9%	3	6.1%	-0.1%
Indonesia	4	4.0%	4	3.9%	0.1%
Japan	5	3.4%	5	3.4%	0.0%
Vietnam	6	2.8%	6	3.0%	-0.1%
United Kingdom	7	2.8%	8	2.7%	0.1%
Netherlands	8	2.8%	12	2.1%	0.7%
Germany	9	2.7%	10	2.5%	0.3%
Brazil	10	2.6%	7	2.9%	-0.2%

Fig. A.3

Malicious Activity by Source: Spam Zombies, 2012–2013

Source: Symantec

Country/Region	2013 Spam Rank	2013 Spam Percentage	2012 Spam Rank	2012 Spam Percentage	Change
India	1	9.8%	1	17.1%	-7.4%
Netherlands	2	8.2%	3	6.5%	1.7%
Russia	3	6.6%	10	2.7%	3.8%
Taiwan	4	5.5%	17	2.2%	3.2%
Iran	5	5.3%	18	1.5%	3.7%
China	6	5.1%	9	3.1%	2.0%
Vietnam	7	5.0%	13	2.5%	2.5%
Peru	8	4.5%	12	2.6%	1.9%
United States	9	4.3%	5	4.2%	0.1%
Italy	10	3.2%	20	1.5%	1.8%

Fig. A.4

Malicious Activity by Source: Phishing Hosts, 2012–2013

Source: Symantec

Country/Region	2013 Phishing Hosts Rank	2013 Phishing Hosts Percentage	2012 Phishing Hosts Rank	2012 Phishing Hosts Percentage	Change
United States	1	39.4%	1	50.0%	-10.6%
Germany	2	6.5%	2	6.2%	0.3%
United Kingdom	3	3.8%	3	3.9%	-0.1%
Canada	4	2.8%	6	2.9%	-0.1%
France	5	2.6%	7	2.7%	-0.1%
Netherlands	6	2.5%	9	2.3%	0.2%
Russia	7	2.5%	8	2.4%	0.1%
Brazil	8	2.2%	4	3.6%	-1.4%
China	9	2.2%	5	3.2%	-1.1%
Poland	10	1.8%	10	1.6%	0.2%

Fig. A.5

Malicious Activity by Source: Bots, 2012–2013

Source: Symantec

Country/Region	2013 Bots Rank	2013 Bots Percentage	2012 Bots Rank	2012 Bots Percentage	Change
United States	1	20.0%	1	15.3%	4.7%
China	2	9.1%	2	15.0%	-5.9%
Italy	3	6.0%	5	7.6%	-1.6%
Taiwan	4	6.0%	3	7.9%	-1.9%
Brazil	5	5.7%	4	7.8%	-2.1%
Japan	6	4.3%	6	4.6%	-0.3%
Hungary	7	4.2%	8	4.2%	0.0%
Germany	8	4.2%	9	4.0%	0.1%
Spain	9	3.9%	10	3.2%	0.7%
Canada	10	3.5%	11	2.0%	1.5%

Fig. A.6

Malicious Activity by Source: Web Attack Origins, 2012–2013

Source: Symantec

Country/Region	2013 Web-Attacking Countries Rank	2013 Web Attacking Countries Percentage	2012 Web Attacking Countries Rank	2012 Web Attacking Countries Percentage	Change
United States	1	26.2%	1	34.4%	-8.2%
China	2	7.4%	3	9.4%	-2.0%
Netherlands	3	2.8%	6	2.4%	0.3%
India	4	1.6%	7	1.7%	0.0%
Germany	5	1.6%	5	2.6%	-1.0%
Japan	6	1.4%	8	1.6%	-0.2%
Korea, South	7	1.4%	4	3.0%	-1.6%
United Kingdom	8	1.0%	10	1.5%	-0.4%
Russia	9	0.9%	9	1.5%	-0.6%
Brazil	10	0.9%	11	1.3%	-0.4%

Fig. A.7

Malicious Activity by Source: Network Attack Origins, 2012–2013

Source: Symantec

Country/Region	2013 Network Attacking Countries Rank	2013 Network Attacking Countries Percentage	2012 Network Attacking Countries Rank	2012 Network Attacking Countries Percentage	Change
China	1	26.6%	1	29.2%	-2.6%
United States	2	15.2%	2	14.9%	0.3%
Netherlands	3	3.9%	6	2.6%	1.3%
United Kingdom	4	3.3%	4	3.1%	0.2%
Russia	5	3.1%	3	3.7%	-0.6%
Vietnam	6	2.7%	23	0.8%	1.9%
France	7	2.6%	10	2.3%	0.4%
Brazil	8	2.6%	5	3.0%	-0.4%
India	9	2.4%	8	2.4%	0.0%
Japan	10	2.2%	7	2.4%	-0.2%

Commentary

- **In 2013, the United States and China remained the top two sources overall for malicious activity.** The overall average proportion of attacks originating from the United States in 2013 decreased by 2.4 percentage points compared with 2012, while the same figure for China saw a decrease by 1.6 percentage points compared with 2012. Countries ranking in the top-ten for 2012 continued to appear in the same range in 2013.
- The United States remains ranked in first position for the source of all activities except for spam zombies and network attacks. India remains in first position for spam zombies and China remains primary for network attacks.
- **20 percent of bot activity originated in the United States:** The United States was the main source of bot-infected computers, an increase of 4.7 percentage points compared with 2012. The US population are avid users of the Internet, with 78 percent Internet penetration, and undoubtedly their keen use of the Internet contributes to their popularity with malware authors.
- **26.2 percent of Web-based Attacks originated in the United States:** Web-based attacks originating from the United States decreased by 8.2 percentage points in 2013.
- **26.6 percent of network attacks originated in China.** China has the largest population of Internet users in the Asia region, with its Internet population growing to approximately 618 million Internet users by the end of 2013[1], 81 percent of which connecting via mobile, making it the country with the largest Internet population in the world.
- **39.4 percent of phishing websites were hosted in the United States.** In 2013, with approximately 256 million Internet users[2], the United States was has the second largest population of Internet users in the world.
- **9.8 percent of spam zombies were located in India,** a decrease of 7.4 percentage points compared with 2012. The proportion of spam zombies located in the United States rose by 0.1 percentage points to 4.3 percent, resulting in the United States being ranked in 9th position in 2013, compared with 5th position in 2012.
- **16.9 percent of all malicious code activities originated from the United States,** a decrease of 0.3 percentage points compared with 2012, overtaking India as the main source of malicious code activity in 2013. With 15.3 percent of malicious activity originating in India, the country was ranked in second position. India has approximately 205 million Internet users,[3] with the third largest population of Internet users in the world.

Malicious Web-Based Attack Prevalence

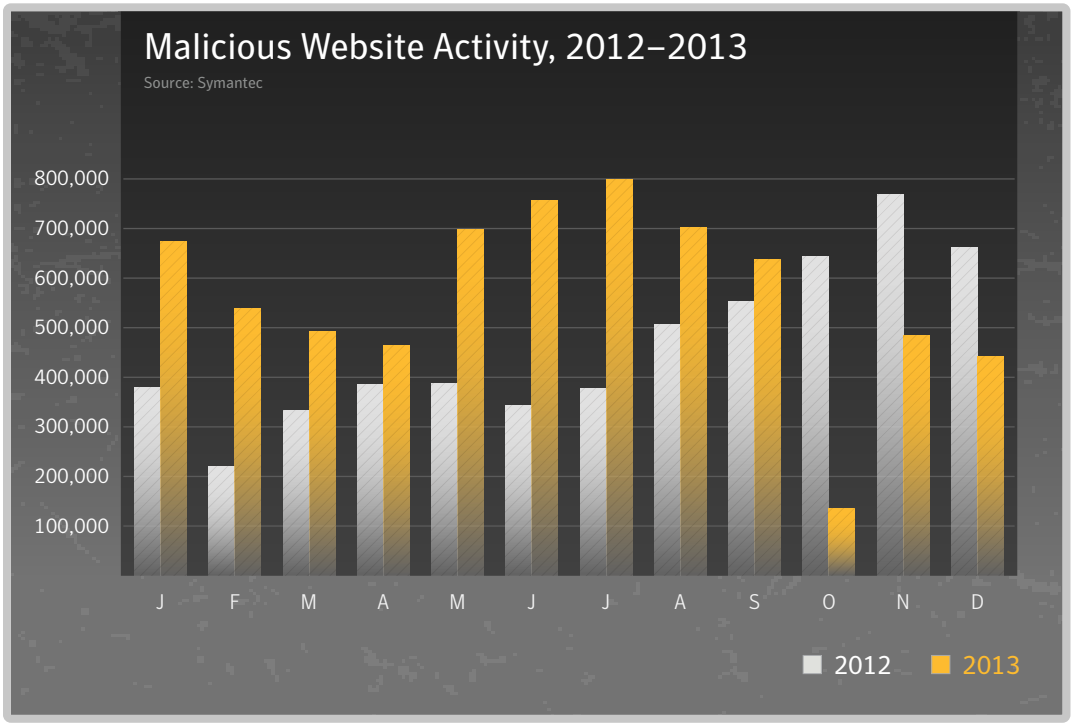
Background

The circumstances and implications of web-based attacks vary widely. They may target specific businesses or organizations, or they may be widespread attacks of opportunity that exploit current events, zero-day vulnerabilities, or recently patched and publicized vulnerabilities that many users have yet to protect themselves against. While major attacks may have individual importance and often receive significant attention when they occur, examining overall web-based attacks provides insight into the threat landscape and how attack patterns may be shifting. Analysis of the underlying trend can provide insight into potential shifts in web-based attack usage, and can assist in determining whether attackers are more or less likely to employ these attacks in the future. To see which vulnerabilities are being exploited by web-based attacks, see Appendix D: Vulnerability Trends.

Methodology

This metric assesses changes to the prevalence of web-based attack activity by comparing the overall volume of malicious activity in each month during the current and previous reporting periods. The data is obtained from Symantec Endpoint Protection and Norton Network Threat Protection IPS Signature detections.

Fig. A.8



Commentary

- The average number of malicious websites blocked each day rose by approximately 22.5 percent from approximately 464,100 in 2012 to 568,700 in 2013.
- The highest level of activity was in July, with approximately 799,500 blocks per day.
- The lowest rate of malicious activity was 135,450 blocks per day in October 2013; this is likely to have been connected to the arrest in Russia of "Paunch," the alleged author of the Blackhole and Cool Exploit web attack toolkits. Blackhole operates as a software-as-a-service toolkit, which is maintained in the cloud. With no one around to update it, it quickly became less effective, leaving a space for other operators to move in.
- Further analysis of malicious code activity may be found in Appendix B: Malicious Code Trends - Top Malicious Code Families.

Analysis of Malicious Web Activity by Attack Toolkits

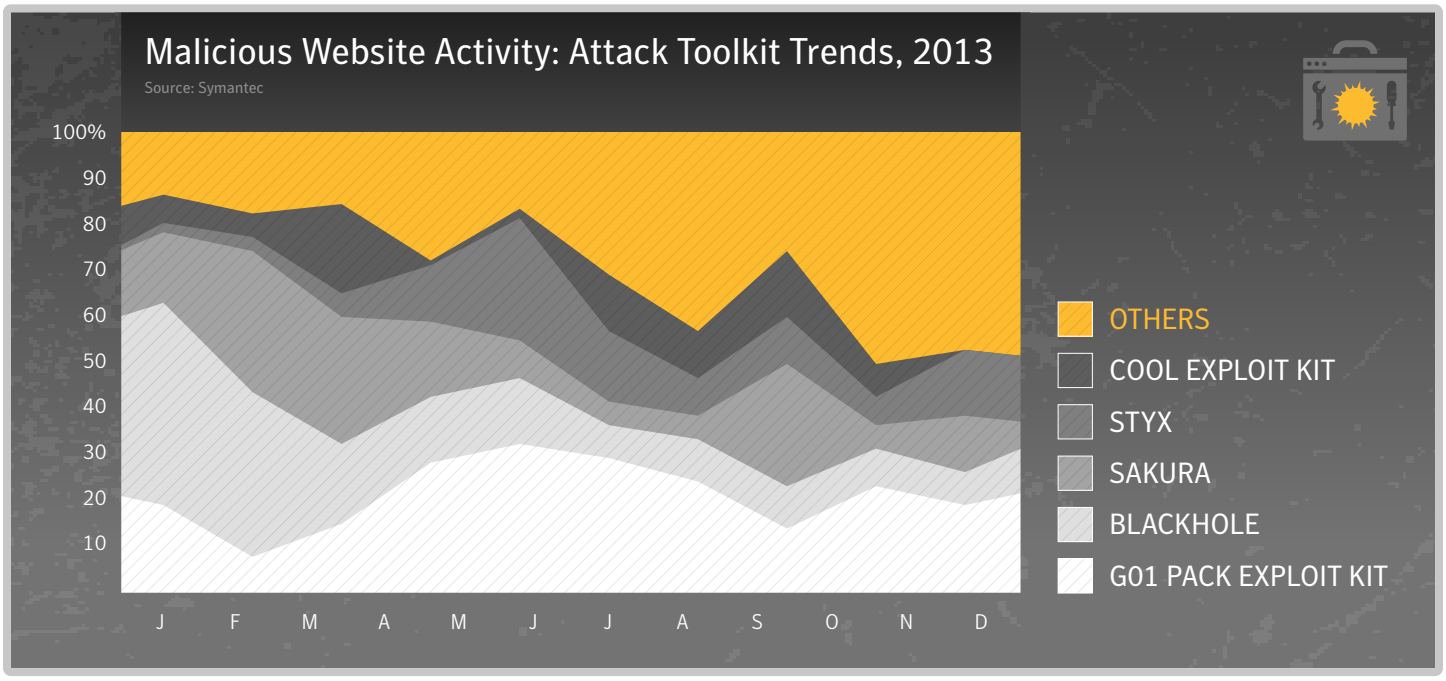
Background

The increasing pervasiveness of web browser applications, along with increasingly common, easily exploited web browser application security vulnerabilities, has resulted in the widespread growth of web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers. These attacks work by infecting enterprises and consumers that visit mainstream websites hosting web attack toolkits, and silently infect them with a variety of malware. Symantec analyzes attack activity to determine which types of attacks and attack toolkits attackers are utilizing. This can provide insight into emerging web attack trends and may indicate the types of attacks with which attackers are having the most success.

Methodology

This metric assesses the top web-based attack activity grouped by exploit "web-kit" families. These attacks originated from compromised legitimate sites and intentionally malicious sites set-up to target Internet users in 2013. To determine this, Symantec ranked attack activity by the number of associated incidents associated with each given web kit.

Fig. A.9



Commentary

- Blackhole virtually disappears from the detections of web attack kits in 2013, while ranked first in 2013 with 44.3 percent of total attacks blocked. G01 Pack Exploit Kit ranked first in 2013 with 23 percent of attacks blocked. The Sakura toolkit that ranked second in 2012, accounting for 22 percent of attacks is seen third place in 2013 with 14%.
- Many of the more common attack toolkits were updated in 2013 to include exploits for the Java Runtime Environment, including CVE-2013-0422, CVE-2013-2465 and CVE-2013-1493 and the Microsoft Internet Explorer vulnerability CVE-2013-2551.

Fig. A.10

Malicious Website Activity: Overall Frequency of Major Attack Toolkits, 2013

Source: Symantec

Toolkit	Percentage of Attacks
G01 PACK EXPLOIT KIT	22.7%
BLACKHOLE	18.8%
SAKURA	14.0%
STYX	9.9%
COOL EXPLOIT KIT	7.5%
OTHERS	27.0%

Analysis of Web-Based Spyware, Adware, and Potentially Unwanted Programs

Background

One of the main goals of a drive-by web-based installation is the deployment of malicious code, but often a compromised website is also used to install spyware or adware code. This is because the cybercriminals pushing the spyware and adware in this way are being paid a small fee for each installation. However, most adware vendors, such as those providing add-in toolbars for web browsers, are not always aware how their code came to be installed on users' computers; the expectation is that it is with the permission of the end-user, when this is typically not the case in a drive-by installation and may be in breach of the vendors' terms and conditions of use.

Methodology

This metric assesses the prevalence of web-based spyware and adware activity by tracking the trend in the average number of spyware and adware related websites blocked each day by users of Symantec.cloud web security services. Underlying trends observed in the sample data provide a reasonable representation of overall malicious web-based activity trends.

Fig. A.11

Potentially Unwanted Programs: Spyware and Adware Blocked, 2013

Source: Symantec.cloud

Rank	Name	Percent
1	Adware.Singalng	56.5%
2	Adware.DealPly	19.2%
3	Adware.Adpeak.E	13.6%
4	Adware.BHO.WVF	3.8%
5	Adware.Adpeak.C	2.6%
6	Adware.Adpeak.F	1.0%
7	Adware.GoonSquad	0.7%
8	Adware.Gamevance.AV	0.6%
9	Adware.BHO.BProtector.E	0.2%
10	Application:Android/Counterclank.A	0.2%
	Total spyware detected generically	1.8%

Commentary

- It is sometimes the case that "Potentially Unwanted Programs" are legitimate programs that have been installed as part of a drive-by download and the installation is performed without the permission of the user. This is typically when the third-party behind the installation is being rewarded for the number of installations of a particular program, irrespective of whether the user has granted permission. It is often without the knowledge of the original vendor, and may be in breach of their affiliate terms and conditions.
- The most frequently blocked installation of potentially unwanted programs in 2013 was for the adware Singalng.
- In 2013, nine of the top-ten potentially unwanted programs were classified as adware, compared with four in 2012.
- 1.8 percent of spyware and adware was detected using generic techniques compared with 80.9 percent in 2012.

Analysis of Web Policy Risks from Inappropriate Use

Background

Many organizations implement an acceptable usage policy to limit employees' use of Internet resources to a subset of websites that have been approved for business use. This enables an organization to limit the level of risk that may arise from users visiting inappropriate or unacceptable websites, such as those containing sexual images and other potentially illegal or harmful content. Often there will be varying degrees of granularity imposed on such restrictions, with some rules being applied to groups of users, while other rules may only apply at certain times of the day; for example, an organization may wish to limit employees access to video sharing websites to only Friday lunchtime, but may also allow any member of the PR and Marketing teams access at any time of the day. This enables an organization to implement and monitor its acceptable usage policy and reduce its exposure to certain risks that may also expose the organization to legal difficulties.

Methodology

This metric assesses the classification of prohibited Web-sites blocked by users of *Symantec.cloud Web security services*. The policies are applied by the organization from a default selection of rules that may also be refined and customized. This metric provides an indication of the potential risks that may arise from uncontrolled use of Internet resources.

Fig. A.12

Web Policies that Triggered Blocks, 2012–2013

Source: Symantec.cloud

Rank	Category	2013	2012	Change
1	Social Networking	39.0%	24.1%	14.9%
2	Advertisement & Popups	24.4%	31.8%	-7.4%
3	Streaming Media	5.2%	9.0%	-3.8%
4	Computing & Internet	4.5%	4.0%	0.5%
5	Hosting Sites	3.7%	2.8%	0.9%
6	Chat	2.9%	4.7%	-1.8%
7	Search	2.8%	1.7%	1.1%
8	Peer-To-Peer	2.7%	3.3%	-0.6%
9	Games	2.6%	1.9%	0.7%
10	News	1.3%	1.7%	-0.4%

Commentary

- The most frequently blocked traffic was categorized as **Social Networking, and accounted for 39 percent of policy-based filtering activity that was blocked**, equivalent to approximately one in every 2.5 websites blocked. Many organizations allow access to social networking websites, but in some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.
- **24 percent of web activity blocked through policy controls was related to advertisement and popups.** Web-based advertisements pose a potential risk though the use of "malvertisements," or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless website.
- **Activity related to streaming media policies resulted in 9 percent of policy-based filtering blocks in 2012.** Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This figure was likely to have been higher in 2012 due to the staging of the London Olympics.

Analysis of Website Categories Exploited to Deliver Malicious Code

Background

As organizations seek to implement appropriate levels of control in order to minimize risk levels from uncontrolled web access, it is important to understand the level of threat posed by certain classifications of websites and categories. This helps provide a better understanding of the types of legitimate websites that may be more susceptible to being compromised, that would potentially expose users to greater levels of risk.

Methodology

This metric assesses the classification of malicious websites blocked by users of Norton Safe Web[4] technology. Data is collected anonymously from customers voluntarily contributing to this technology, including through Norton Community Watch. Norton Safe Web is processing billions of rating requests each day, and monitoring millions of daily software-downloads.

This metric provides an indication of the levels of infection of legitimate websites that have been compromised or abused for malicious purposes. The malicious URLs identified by the Norton Safe Web technology were classified by category using the Symantec Rulespace[5] technology. RuleSpace proactively categorizes websites into nearly 100 categories in 30 languages.

Fig. A.13

Malicious Web Activity: Categories that Delivered Malicious Code, 2013

Source: Symantec.cloud

Rank	Top-Ten Most Frequently Exploited Categories of Websites	Percent of Total Number of infected Websites	2012	Change
1	Technology	9.9%	24.1%	14.9%
2	Business	6.7%	31.8%	-7.4%
3	Hosting	5.3%	9.0%	-3.8%
4	Blogging	5.0%	4.0%	0.5%
5	Illegal	3.8%	2.8%	0.9%
6	Shopping	3.3%	4.7%	-1.8%
7	Entertainment	2.9%	1.7%	1.1%
8	Automotive	1.8%	3.3%	-0.6%
9	Educational	1.7%	1.9%	0.7%
10	Virtual Community	1.7%	1.7%	-0.4%

Fig. A.14

Malicious Web Activity: Malicious Code By Number of Infections per Site for Top-Five Most Frequently Exploited Categories, 2013

Source: Symantec.cloud

Rank	Top-Five Most Frequently Exploited Categories of Websites	Average Number of Threats Found on Infected Website	Top-Three Threat Types Detected		
1	Technology	1.9	Malware: 38%	Malicious Site: 17%	Fake AV: 14%
2	Business	2.1	Malware: 42%	Fake AV: 27%	Malicious Site: 14%
3	Hosting	1.4	Scam: 35%	Malicious Site: 21%	Malware: 19%
4	Blogging	1.6	Browser Exploit: 25%	Scam: 17%	Web Attack: 17%
5	Illegal	1.3	Malicious Site: 51%	PHISH: 25%	Malware: 6%

Fig. A.15

Malicious Web Activity: Malicious Code by Number of Infections per Site, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites	Average Number of Threats Found on Infected Website	Major Threat Type Detected
1	Automated Web Application	3.4	Malware: 82%
2	Placeholder	2.9	Pay Per Click: 68%
3	Automotive	2.9	Pay Per Click: 63%
4	Kids	2.8	Malware: 67%
5	Cult	2.6	Fake Antivirus: 49%
6	Military	2.5	Malware: 60%
7	Hate	2.4	Malware: 54%
8	Humor	2.3	Malware: 31%
9	Forums	2.2	Scam: 28%
10	Weapons	2.2	Fake Antivirus: 38%

Fig. A.16

Malicious Web Activity: Fake Antivirus by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Fake Antivirus	Percentage of Threats Found Within Same Category	Percentage of Fake AV Attacks Found Within Top-Ten Categories
1	Art and Museums	50%	4%
2	Cult	49%	0.2%
3	Alcohol	40%	2%
4	Religion	39%	9%
5	Weapons	38%	1%
6	Shopping	37%	42%
7	Drugs	36%	0.2%
8	Entertainment	35%	34%
9	Glamour	34%	2%
10	Food and Restaurants	33%	7%

- The fake antivirus (fake AV) threat has been explicitly analyzed and the above top-ten website categories have been generated and ranked based on the percentage of fake AV threats that each of them account for.
- Art and Museum websites rank at the top with 50 percent of all threats being fake AV. But this website category accounts to only 4 percent of this threat when compared with other categories in the top-ten list.
- It shows that the majority of threats from Art and Museum websites are fake AV but the volume of such threats is very low. Entertainment has the highest volume of fake AV threats.

Fig. A.17

Malicious Web Activity: Browser Exploits by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Browser Exploits	Percentage of Threats Found Within Same Category	Percentage of Browser Exploits Found Within Top-Ten Categories
1	Anonymizer	73%	21%
2	Blogging	27%	67%
3	Dynamic	20%	4%
4	Violence	11%	0.005%
5	Filesharing	10%	2%
6	Portal	10%	1%
7	Humor	10%	0.1%
8	Pornography	8%	4%
9	Hacking	7%	0.1%
10	Automated Web Application	7%	0.01%

- The browser exploit threat has been explicitly analyzed and the above top-ten website categories have been generated and ranked based on the percentage of browser exploit threats that each of them account for.
- Websites catergorized as Anonymizer rank at the top with 73 percent of all threats being browser exploits. But this website category accounts for only 21 percent of this threat when compared with other categories in the top-ten list.
- It shows that the majority of threats from anonymizer type websites are browser exploits, although the volume of such threats is not the highest. Blogging has the highest volume of browser exploit threats.

Fig. A.18

Malicious Web Activity: Social Networking Attacks by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Social Networking	Percent Used To Deliver Social Networking Attacks
1	Blogging	17%
2	Hosting	4%
3	Illegal	3%
4	Technology	2%
5	News	1%

Commentary

- Approximately 67 percent of websites used to distribute malware were identified as legitimate but compromised websites, an increase of four percentage points compared with 2012. This figure excluded URLs that contained just an IP address and did not include general domain parking and pay-per-click websites.
- 9.9 percent of malicious website activity was classified in the Technology category.
- Websites classified as automated web application were found to host the greatest number of threats per site than other categories, with an average of 3.4 threats per website, the majority of which related to Malware (82 percent).
- Analysis of websites that were used to deliver drive-by fake AV attacks revealed that 4 percent of fake AV threats were found on compromised Art and Museum sites. Additionally, 50 percent of threats found on compromised Art and Museum sites were fake AV. 42 percent of threats found on compromised Shopping sites were also fake AV.
- Analysis of websites that were used to deliver attacks using browser exploits revealed that 21 percent of threats found on compromised anonymizer sites were related to browser exploits. 73 percent of browser exploit attacks were found on compromised anonymizer sites. 67 percent of attacks found on compromised blogging sites involved browser exploits.
- 17 percent of attacks on social networking sites were related to malware hosted on compromised blogging sites. This is where a URL hyperlink for a compromised website is shared on a social network. Websites dedicated to the discussion of hosting accounted for 4 percent of social networking attacks.
- The Dynamic category is used to classify websites that have been found to contain both appropriate and inappropriate user-generated content, such as social networking or blogging websites. Also, websites in which the page content changes based on how the user is interacting with it (for example, an Internet search).
- The Illegal category includes sites that fall into the following sub-categories: Activist Groups, Cyberbullying, Malware Accomplice, Password Cracking, Potentially Malicious Software and Unwanted Programs, Remote Access Programs, and several other phishing- and spam-related content.
- The Placeholder category refers to any domain name that is registered, but may be for sale or has recently expired and is redirected to a domain parking page.
- The Automated Web Application category refers to sites which allow a computer to automatically open an HTTP connection for various reasons including checking for operating system or application updates.

Bot-Infected Computers

Background

Bot-infected computers, or bots, are programs that are covertly installed on a user's machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet relay chat (IRC), P2P, or hyper-text transfer protocol (HTTP). These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers —all of which can lead to serious financial and legal consequences. Attackers favor bot-infected computers with a decentralized C&C[6] model because they are difficult to disable and allow the attackers to hide in plain sight among the massive amounts of unrelated traffic occurring over the same communication channels, such as P2P. Most importantly, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate.

Methodology

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; a single such computer can be active on a number of different days. A distinct bot-infected computer is a distinct computer that was active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they can be classified as active attacker bots or bots that send out spam, i.e. spam zombies.

Distributed denial-of-service (DDoS) campaigns may not always be indicative of bot-infected computer activity, DDoS activity can occur without the use of bot-infected computers. For example, the use of publically available software such as "Low Orbit Ion Cannon" (LOIC) when used in a coordinated effort may disrupt some businesses' website operations if used in sufficiently large numbers.

The following analysis reveals the average lifespan of a bot-infected computer for the highest populations of bot-infected computers. To be included in the list, the geography must account for at least 0.1 percent of the global bot population.

Fig. A.19

Top-Ten Bot Locations by Average Lifespan of Bot, 2012–2013

Source: Symantec.cloud

Rank	Country/Region	Average Lifespan of Bot (Days) - 2013	Average Lifespan of Bot (Days) - 2012	Percentage of World Bots - 2013	Percentage of World Bots - 2012
1	Romania	20	24	0.19%	0.16%
2	Indonesia	15	12	0.12%	0.12%
3	Bulgaria	14	17	0.12%	0.10%
4	United States	13	13	20.01%	15.34%
5	Egypt	11	10	0.11%	0.11%
6	Colombia	11	6	0.10%	0.12%
7	Switzerland	10	8	0.31%	0.28%
8	Philippines	10	10	0.16%	0.16%
9	New Zealand	10	6	0.15%	0.16%
10	Ukraine	9	10	0.15%	0.15%

Commentary

- Bots located in Romania were active for an average of 20 days in 2013, compared with 24 days in 2012; 0.19 percent of bots were located in Romania, compared with 0.16 percent in 2012.
- Although it still takes longer to identify and clean a bot-infected computer in Romania than it does in the United States, the number of infections in the United States is more than a hundred times greater than that of Romania. One factor contributing to this disparity may be a low level of user-awareness of the issues involved, combined with the lower availability of remediation guidance and support tools in the Romanian language.
- In the United States, which was home to 20 percent of the world's bots in 2013, the average lifespan for a bot was still 13 days, unchanged from 2012.
- Additionally, in China, which was ranked second for bot activity in 2013 and was host for 9 percent of the world's bots, the average lifespan for a bot was 5 days.
- All other countries outside the top-ten had a lifespan of 9 days or less. The overall global average lifespan was 6 days, unchanged from 2012.

Botnets, which are large networks of malware-infected computers, continued to be a significant feature of the threat landscape in 2013. By pooling the power of infected computers, attackers have a powerful tool that allows them to engage in activities such as Distributed Denial of Service (DDoS) attacks, click fraud or Bitcoin mining.

Symantec actively initiates and supports clean-up actions against botnets. However, botnets are becoming resilient against takedowns. We believe that even if a takedown operation does not remove a botnet completely, it does at least make it harder for cybercriminals. It might lead to arrests and they are forced to rebuild, losing revenue in the process.

During 2013, Symantec struck a major blow against the ZeroAccess botnet. With 1.9 million computers under its control, it is one of the larger botnets in operation at present. ZeroAccess has been largely used to engage in click fraud to generate profits for its controllers. The gang also experimented with a Bitcoin-mining module, but appear to have deemed it not profitable and removed it again.

One of the key features of the ZeroAccess botnet is that it uses a peer-to-peer (P2P) framework for its command and control (C&C) architecture. This makes ZeroAccess highly resilient. Because there is no central C&C, the botnet cannot be disabled by simply targeting C&C servers.

While analyzing the ZeroAccess malware Symantec discovered a weakness in the protocol used by the botnet and put in place plans for a takedown operation. When ZeroAccess' controllers started to address this weakness by updating their software, Symantec immediately began sinkholing computers while the opportunity lasted. Roughly half a million computers were liberated from the botnet during the operation.

A number of other botnet takedowns and sinkhole initiatives took place in 2013. Among them was a combined Microsoft/FBI attempt to disrupt the Citadel botnet and the takedown of the Bamital botnet by Symantec and Microsoft. This might explain part of the reduction in the number of bots we observed. The number of infected computers decreased from 3.4 million in 2012 to 2.3 million in 2013 (a reduction of 32.8 percent). However, newer forms of botnets also emerged in 2013, utilizing low-powered devices such as routers, and other hardware.

Denial of Service Attacks

The size of denial of service attacks underwent a dramatic increase in 2013, with one attack in particular reaching over 300Gbps. This increase is due in part to changes in the techniques used by attackers, with old tricks that worked well in the past seeing a resurgence. Internet access and quality is constantly improving and reaching previously unconnected or poorly connected parts of the globe. This new access also brings with it poorly configured infrastructure and computers with little or no security, which is good news for malicious actors who see commodities waiting to be utilized.

The number of attacks is increasing year over year, with Akamai seeing 250 attacks in 2011, compared to 768 in 2012.[7] With their final quarterly report for 2013 still to be released, Akamai have so far seen 807 attacks,[8] a clear sign that DDoS attacks are an increasingly popular method of attack.

Throughout 2012 the size of DDoS attacks, in terms of bandwidth, averaged in the realm of double digits. That all changed in 2013, when the triple digit mark of 100Gbps was not only reached but was exceeded more than threefold. In March the anti-spam organization Spamhaus was targeted with a DDoS attack that peaked at over 300Gbps. An attack of this magnitude was made possible by a method known as DNS reflection, also known as DNS amplification. In this type of attack, an attacker sends a request with a spoofed source IP address matching that of the target to a large number of recursive DNS resolvers. The resolvers then respond to the request, but the response is much larger in size, which means the attacker can effectively amplify their attack to many times that of the bandwidth they have available. DNS reflection attacks are made possible by poorly configured domain name servers that have recursion enabled and will respond to anyone, these are referred to as open resolvers or open DNS recursors. There are millions of open resolvers[9] online that need to be locked down and secured, and until this problem is addressed DNS reflection attacks will not only continue but increase in size.

Network Time Protocol (NTP) reflection attacks also saw a significant increase last year with December seeing a major spike in activity.[10] NTP is used to sync time between computers on the Internet and, if not updated, can be used in DDoS attacks. As with DNS reflection attacks, an attacker can send a small packet of data to an NTP server which then sends a large amount of data to the target IP address. The recent attacks against the servers of several well-known online games[11] used this technique, and it seems set to continue to be used by attackers in 2014, with one major NTP reflection attack this year already reported to have reached 400Gbps.[12]

Use of reflection attack methodology means there may be less need for tools such as the Low Orbit Ion Cannon or large botnets with DDoS capabilities because fewer individual computers are now needed to undertake larger attacks.

The increased use of reflection attacks doesn't mean that other methods have disappeared. An attack against one the world's largest Bitcoin exchanges - the cryptocurrency being a prime target for DDoS attacks in 2013 - used a SYN flood attack and still reached over 100Gbps. Rather than using a huge botnet of compromised computers for this attack, it is believed those responsible used a network of compromised servers. This is another tactic that is becoming increasingly popular. Compromising unsecured servers gives hackers access to far more bandwidth than they would get from even a modest size botnet with DDoS functionality.

The increase in DDoS size also means an increase in severity, reflected by the reported slowdown of the Internet due to the Spamhaus attack in March. Denial of service attacks are one of the largest threats to the Internet. As we become more reliant on devices that are connected to the Internet,

these attacks will not only increasingly threaten governments, organizations, and businesses, but also individuals using the Internet for their everyday activities. A prime example of this was the attack against the Chinese registry,[13] which caused many .cn websites to go offline for several hours.

Mobile devices are becoming alternative tools for launching DDoS attacks. Symantec detected several mobile applications that allow the user to simply enter the target information and, at the press of a button, start the attack. Users can join large DDoS groups and pool their efforts, making this similar to older computer-based tools such as the LOIC. It is predicted that close to one billion smartphones[14] were sold in 2013. That is a huge number of potential recruits for DDoS attacks.

Approximately 45 percent of the world's population is now covered by a 3G mobile network[15] and the cost of mobile data is continually falling, with unlimited data plans becoming commonplace. It was forecasted that 4G/LTE networks will account for 1 in 5 mobile broadband subscriptions in 2017,[16] compared to 1 in 25 in 2012. LTE networks will increase connection speeds dramatically with an estimated average speed of 3,898kbps projected by 2017,[17] compared to 189kbps in 2010. Attacks emanating from mobile devices will likely increase in 2014 as more people migrate to mobile devices and networks around the world continue to improve connection speeds and reduce the cost of mobile data.

DDoS as a service

It is now easier than ever to carry out a DDoS attack regardless of someone's technical knowledge. DDoS as a service is sold online on underground hacking forums and attacks of varying sizes can be organized for the right price. Websites or businesses that offer DDoS as a service, referred to as stressers, can be found online with relative ease. These services are commonly offered in the gaming community to temporarily get rid of competing players during critical gaming sessions.

While some services say their business is only for "stress testing your own website" others are more blatant about what they are offering.

Prices range from US$5 to over $1,000 depending on the length and magnitude of the attack.

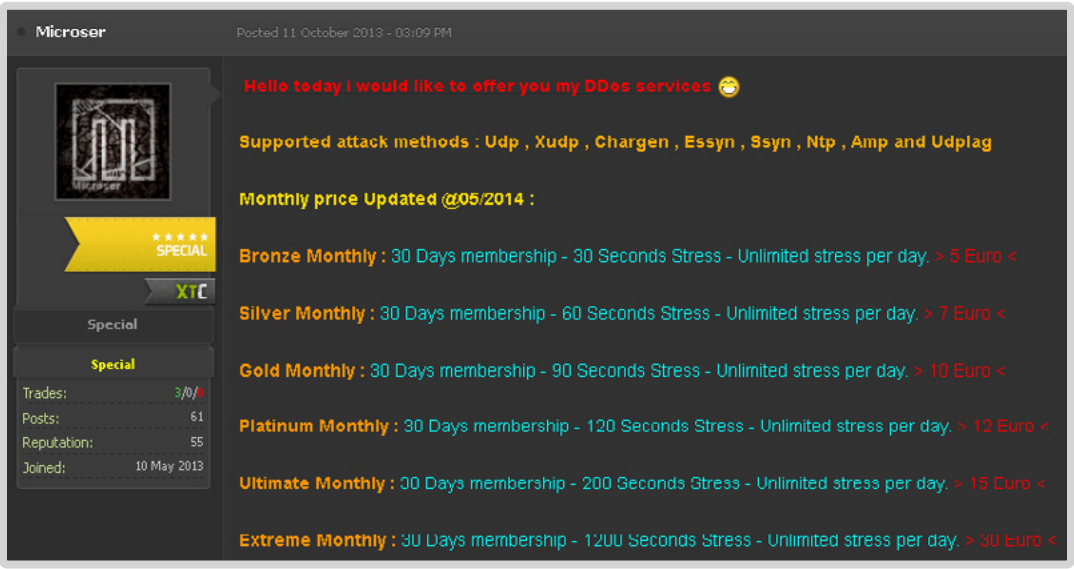


Fig. A.20 DDoS Service options

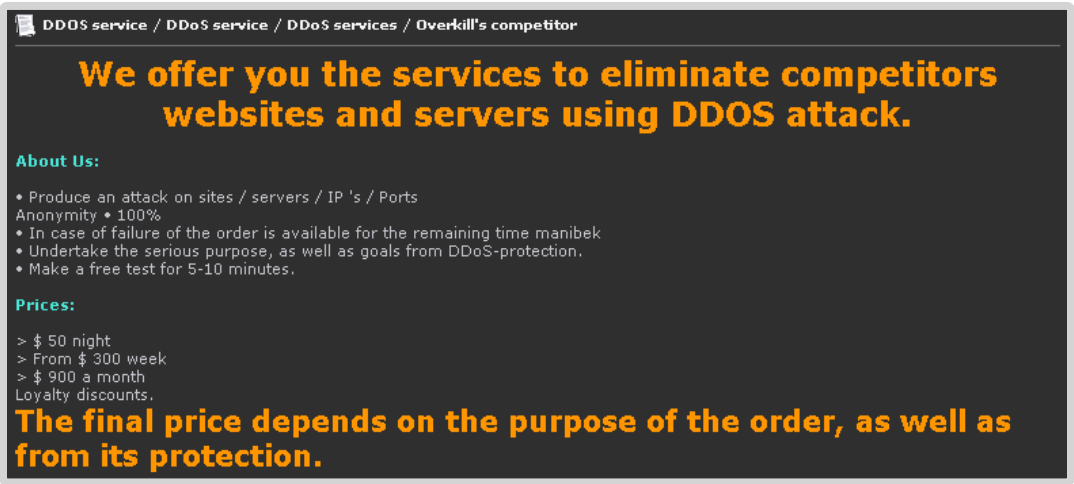


Fig. A.21 DDoS Service example

Hacktivism

Improved Internet access can help people who may not have been heard in the past to voice their opinions and political views. Unfortunately, some individuals and groups feel that cybercrime is a better way to get their message across. When discussing hacktivist collectives, one of the largest and best-known is Anonymous. While this loosely associated network of individuals and groups is still making its mark, its campaigns are failing to create the impact they once did. The second assault against Israel in April 2013, which promised to "wipe Israel off the map of the Internet", failed to cause much disruption. The same was true for other campaigns such as #OpUSA. While attacks under the Anonymous banner still pose a major risk, it is another hacktivist group that has taken the limelight recently.

Rise of the SEA

The pro-Bashar al-Assad hacktivist collective the Syrian Electronic Army (SEA), was quite prolific throughout 2013.

Although active since 2011, the SEA became increasingly active in 2013, compromising a multitude of high-profile websites and social media accounts. The SEA is usually happy with posting political messages on hacked social media accounts or websites by defacement or redirection, but it has also been known to steal information. However this does not seem to be its preferred modus operandi. Whether or not data breaches by the SEA will become more common in 2014 remains to be seen.

When it comes to security the SEA know that the weakest link in the chain is often users themselves and the hacktivist group uses this to its advantage. Phishing attacks are used to obtain the login credentials for social media accounts of target organizations, and due to many users within an organization having access to the same accounts it greatly improves the chances of getting the credentials in this manner. Often the same credentials are used for more than one account, so a successful phishing attack can grant attackers access to several accounts. The global phishing rate reflects the popularity of this method of attack; it has increased from 2012, when 1 in 414 emails per day were actual phishing attacks, to 1 in 392.4 emails being phishing attempts in 2013.

The widespread use of social media by companies and organizations has made it an ideal target for hacktivists and this will no doubt continue in 2014. The 2013 Norton Report[18] revealed that 12 percent of social media users admit to having their accounts hacked and a staggering 25 percent of people shared their account credentials with others. While two-factor authentication (2FA) is slowly becoming commonplace, it is often not practical for companies that share social media accounts across several geographical regions. For instance, if a social media account allows only one mobile phone number to be registered for 2FA purposes, it will limit the authentication to one region. This type of restriction means that enterprises with shared accounts are often less secure than individual users. If at all possible, users must take advantage of 2FA and other security measures, such as single sign-on technology[19] and multiple permission levels, before social media hacking is placed out of the reach of hackers like the SEA.

While some may view defacement attacks by hacktivist groups as relatively harmless, this was not the case when in April 2013 the Twitter account belonging to a well-known news agency was hacked. The SEA tweeted that two explosions had gone off in the White House. This news caused the US stock market to panic and the Dow Jones to drop by 143 points. The news agency quickly reported the hack and the stock market recovered but this highlights the power that social media hacking can wield in today's world.

Analysis of Mobile Threats

Background

Since the first smartphone arrived in the hands of consumers, speculation about threats targeting these devices has abounded. While threats targeted early "smart" devices such as those based on Symbian and Palm OS in the past, none of these threats ever became widespread and many remained proof-of-concept. Recently, with the growing uptake in smartphones and tablets, and their increasing connectivity and capability, there has been a corresponding increase in attention, both from threat developers and security researchers.

While the number of immediate threats to mobile devices remains relatively low in comparison to threats targeting PCs, there have been new developments in the field; and as malicious code for mobile begins to generate revenue for malware authors, there will be more threats created for these devices, especially as people increasingly use mobile devices for sensitive transactions such as online shopping and banking.

As with desktop computers, the exploitation of a vulnerability can be a way for malicious code to be installed on a mobile device.

Methodology

In 2013, there was a decrease in the number of vulnerabilities reported that affected mobile devices. Symantec documented 132 vulnerabilities in mobile device operating systems in 2013, compared to 416 in 2012 and 315 in 2011; a decrease of 68 percent.

Symantec tracks the number of threats discovered against mobile platforms by tracking malicious threats identified by Symantec's own security products and confirmed vulnerabilities documented by mobile vendors.

Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile application ("app") marketplaces in the hope that users will download and install them, often trying to pass themselves off as legitimate apps or games. Attackers have also taken popular legitimate applications and added supplementary code to them. Symantec has classified the types of threats into a variety of categories based on their functionality.

Fig. A.22

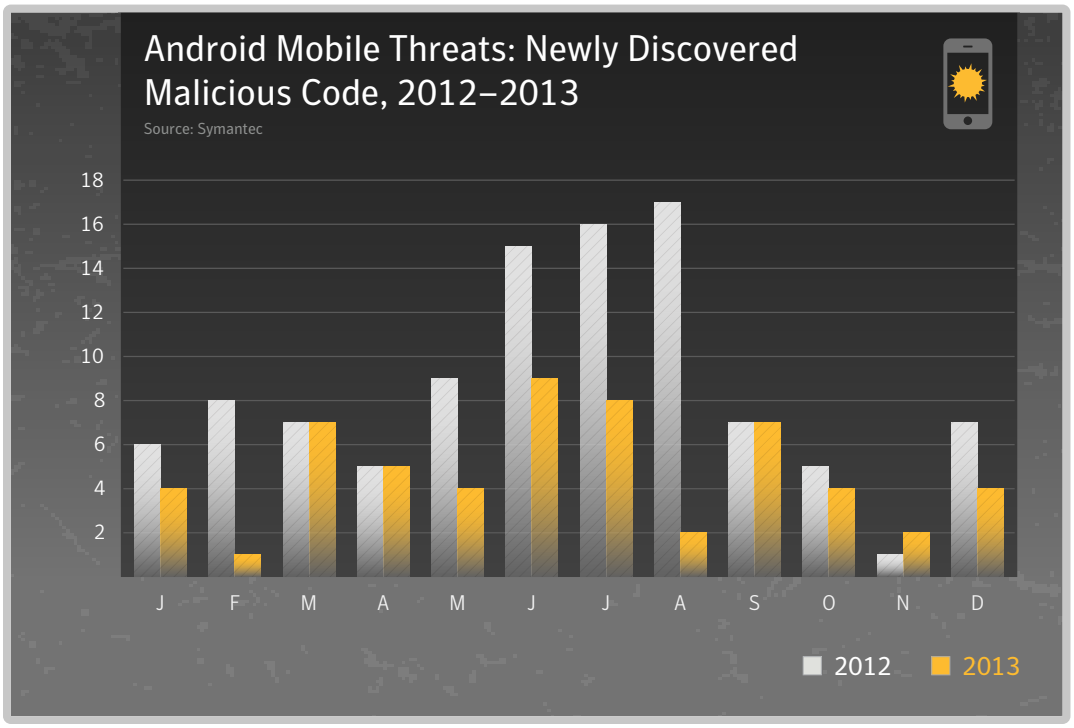


Fig. A.23

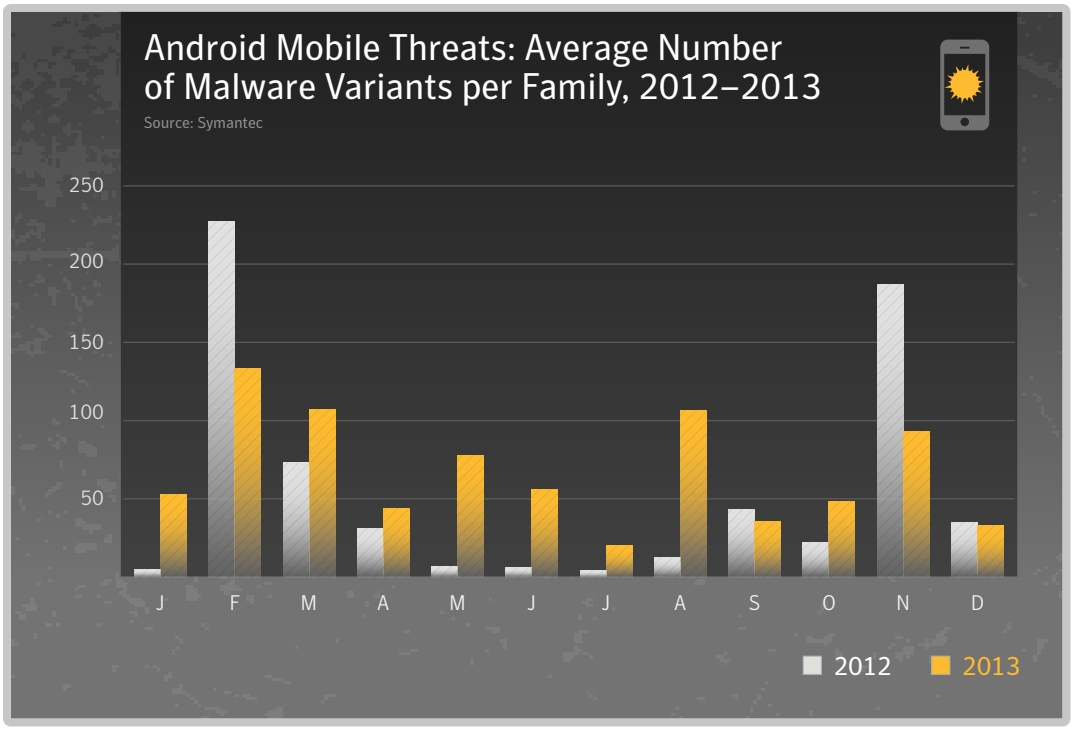


Fig. A.24

Mobile Threats: Malicious Code by Platform, 2013

Source: Symantec

Platform	Number of Threats	Percent of Threats
Android	57	97%
Symbian	1	2%
Windows	1	2%
iOS	0	0%

Fig. A.25

Mobile Threats: Malicious Code Actions in Malware, 2012–2013

Source: Symantec

High-level Risk Categories	Track User	Steal Information	Send Content	Traditional Threats	Reconfigure Device	Adware/ Annoyance
Percent of actions found in threats (2012)	15%	32%	13%	25%	8%	8%
Percent of actions found in threats (2013)	30%	23%	8%	20%	10%	9%

Fig. A.26

Mobile Threats: Malicious Code Actions – Additional Detail, 2012–2013

Source: Symantec

Detailed Threat Categories	Percent Found in Threats, 2013	Percent Found in Threats, 2012
Steals Device Data	17%	27%
Spies On User	28%	12%
Sends Premium SMS	5%	11%
Downloader	8%	11%
Back door	12%	13%
Tracks Location	3%	3%
Modifies Settings	8%	5%
Spam	3%	2%
Steals Media	3%	2%
Elevates Privileges	2%	3%
Banking Trojan	3%	2%
Adware/ Annoyance	9%	8%
DDOS Utility	0%	1%
Hacktool	0%	1%

Fig. A.27

Mobile Threats: Documented Mobile Vulnerabilities by Platform, 2013

Source: Symantec

Platform	Documented vulnerabilities	Percentage
Apple iOS/iPhone/iPad	108	82%
Android	17	13%
BlackBerry	1	1%
Nokia	1	1%

Fig. A.28

Mobile Threats: Documented Mobile Vulnerabilities by Month, 2013

Source: Symantec

Month	Documented Vulnerabilities
January	16
February	4
March	9
April	7
May	22
June	5
July	4
August	3
September	45
October	5
November	7
December	1

The following are specific definitions of each subcategory:

- **Steals Device Data**—gathers information that is specific to the functionality of the device, such as IMEI, IMSI, operating system, and phone configuration data.
- **Spies on User**—intentionally gathers information from the device to monitor a user, such as phone logs and SMS messages, and sends them to a remote source.
- **Sends Premium SMS**—sends SMS messages to premium-rate numbers that are charged to the user's mobile account.
- **Downloader**—can download other risks on to the compromised device.
- **Backdoor**—opens a back door on the compromised device, allowing attackers to perform arbitrary actions.
- **Tracks Location**—gathers GPS information from the device specifically to track the user's location.
- **Modifies Settings**—changes configuration settings on the compromised device.
- **Spam**—sends spam email messages from the compromised device.
- **Steals Media**—sends media, such as pictures, to a remote source.
- **Elevates Privileges**—attempts to gain privileges beyond those laid out when installing the app bundled with the risk.
- **Banking Trojan**—monitors the device for banking transactions, gathering sensitive details for further malicious actions.
- **SEO Poisoning**—periodically sends the phone's browser to predetermined URLs in order to boost search rankings.

Mobile applications ("apps") with malicious intentions can present serious risks to users of mobile devices. These metrics show the different functions that these bad mobile apps performed during the year. The data was compiled by analyzing the key functionality of malicious mobile apps.

Symantec has identified five primary mobile risk types:

Steal Information. Most common among bad mobile apps was the collection of data from the compromised device. This was typically done with the intent to carry out further malicious activities, in much the way an information-stealing Trojan might. This includes both device- and user-specific data, ranging from configuration data to banking details. This information can be used in a number of ways, but for the most part it is fairly innocuous, with IMEI[20] and IMSI[21] numbers taken by attackers as a way to uniquely identify a device. More concerning is data gathered about the device software, such as operating system (OS) version or applications installed, to carry out further attacks (say, by exploiting a software vulnerability). Rarer, but of greatest concern is when user-specific data, such as banking details, is gathered in an attempt to make unauthorized transactions. While this category covers a broad range of data, the distinction between device and user data is given in more detail in the subcategories below.

Track User. The next most common purpose was to track a user's personal behavior and actions. These risks take data specifically in order to spy on the individual using the phone. This is done by gathering up various communication data, such as SMS messages and phone call logs, and sending them to another computer or device. In some instances they may even record phone calls. In other cases these risks track GPS coordinates, essentially keeping tabs on the location of the device (and their user) at any given time. Gathering pictures taken with the phone also falls into this category.

Send Content. The third-largest in the group of risks is apps that send out content. These risks are different from the first two categories because their direct intent is to make money for the attacker. Most of these risks will send a text message to a premium SMS number, ultimately appearing on the mobile bill of the device's owner. Also within this category are risks that can be used as email spam relays, controlled by the attackers and sending unwanted emails from addresses registered to the device. One threat in this category constantly sent HTTP requests in the hope of bumping certain pages within search rankings.

Traditional Threats. The fourth group contains more traditional threats, such as backdoors and downloaders. Attackers often port these types of risks from PCs to mobile devices.

Change Settings. Finally there are a small number of risks that focus on making configuration changes. These types attempt to elevate privileges or simply modify various settings within the OS. The goal for this final group seems to be to perform further actions on the compromised devices.

Commentary

- There were 57 new Android malware families identified in 2013, compared with 103 in 2012
- The average number of variants per family in 2013 was 57, compared with 38 in 2012. Although the overall number of new mobile malware families was much lower than in the previous year, the number of variants for each family is now much higher. This is likely to be a result of mobile malware toolkits allowing the attackers to repackage and customize their malware variants more easily, and in so doing using them much more widely.
- As we have seen in previous years, a high number of vulnerabilities for a mobile OS do not necessarily lead to malware that exploits those vulnerabilities. Overall, there were 127 mobile vulnerabilities published in 2013, compared with 416 in 2012, a decrease of 69 percent.
- Further analysis of mobile malware and spyware indicated the highest type of activity undertaken on a compromised device was to spy on the user, 28 percent in 2013 compared with 12 percent in 2012. 17 percent of malicious mobile activity was designed to steal data in 2013, compared with 27 percent in 2012.

Quantified Self – A Path to Self-Enlightenment or Just Another Security Nightmare?

In recent years, the idea of collecting and analysing data about a person's activities and status has really taken off. A new term had been coined for this activity and it is known as the concept of the Quantified Self[22] (QS) – also known as life tracking.

At its core, the QS describes the notion of collection and analysis of all types of data about a person on an ongoing and often real-time basis. The goal is usually some high-minded aspiration such as to live better or improve oneself in some shape or form. While we are hearing a lot more about QS these days, it is not a new concept by any means. In the past, this type of monitoring was something that was mostly done by professional athletes to enhance training and performance or medical patients for managing life-threatening conditions. Today, improved technology, innovative startups and lower costs are all driving forward the current wave of the QS movement at breakneck speed and creating a tsunami of data in its wake.

It's Personal Data, But Not as We've Known It

We are all familiar with the collection and use of the traditional types of personal information in the form of the name, address, date of birth, and so on. We as users have been sharing this type of information with businesses for decades. When we talk of "personal information" this is typically what we think of. But now, new technologies enable us to collect much more information at a deeper and more personal level. Data generated by quantified self devices and services (also known as first-party data) is highly personal and could reveal a lot more about ourselves to others than we may like.

The types of data typically generated by QS applications include:

- GPS location
- Heart rate
- Height/weight
- Calorie/alcohol intake
- Mood
- Sleep times/patterns
- Body temperature

Users need to understand what's being collected, how it is being stored and shared, and be comfortable with this fact and its implications and potential applications before proceeding.

A Burgeoning Sector

Despite the many potential security landmines in the field of QS, public interest in it has mushroomed in the past year few years. One indicator of this interest is in the amount of startup business activity in this area. According to CB Insights, funding for QS related startups reached US$318 million[23] in 2013, up 165 percent from 2012. Businesses in this category track nearly every aspect of human activity. A lot of the data that is collected will be done with active user consent – the person will install the app, then sign up and consent for services that collect and analyze the data. But there will also be cases where data may be collected without user consent or knowledge, and we as users of these new technologies and services will have to proceed with caution.

Data Breaches that could lead to Identity Theft

Background

Hacking continued to be the primary cause of data breaches in 2013. In 2013, there were eight data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 150 million identities. In contrast, 2012 saw only one breach larger than 10 million identities. As a result the overall average number of identities exposed has increased significantly, from 604,826 identities per breach in 2012 to 2,181,891 in 2013.

As the overall average size of a breach has increased, the median number of identities stolen has actually fallen from 8,350 in 2012 to 6,777 in 2013. Using the median can be helpful in this scenario since it ignores the extreme values caused by the notable, rare events that resulted in the largest numbers of identities being exposed. In this way, the median may be more representative of the underlying trend. While the number of incidents is rising, the number of identities exposed is still in in the order of thousands, but there were also more incidents that resulted in extremely large volumes of identities being exposed in 2013 than in the previous year.

Hacking was the chief cause of most data breaches in 2013, and consequently received a great deal of media attention. Hacking can undermine institutional confidence in a company, exposing its attitude to security. The loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 34 percent of data breaches in 2013 according to the Norton Cybercrime Index data.[24] As data breach notification legislation becomes more commonplace, we are likely to see the number of data breaches rising. Such legislation is often used to regulate the responsibilities of organizations after a data breach has occurred and may help to mitigate against the potential negative impact on the individuals concerned.

The Healthcare, Education, and the Public Sector were ranked highest for the number of data breach incidents in 2013; the top three accounted for 58 percent of all data breaches. However, the Retail, Computer Software and Financial sectors accounted for 77 percent of all the identities exposed in 2013.

Methodology

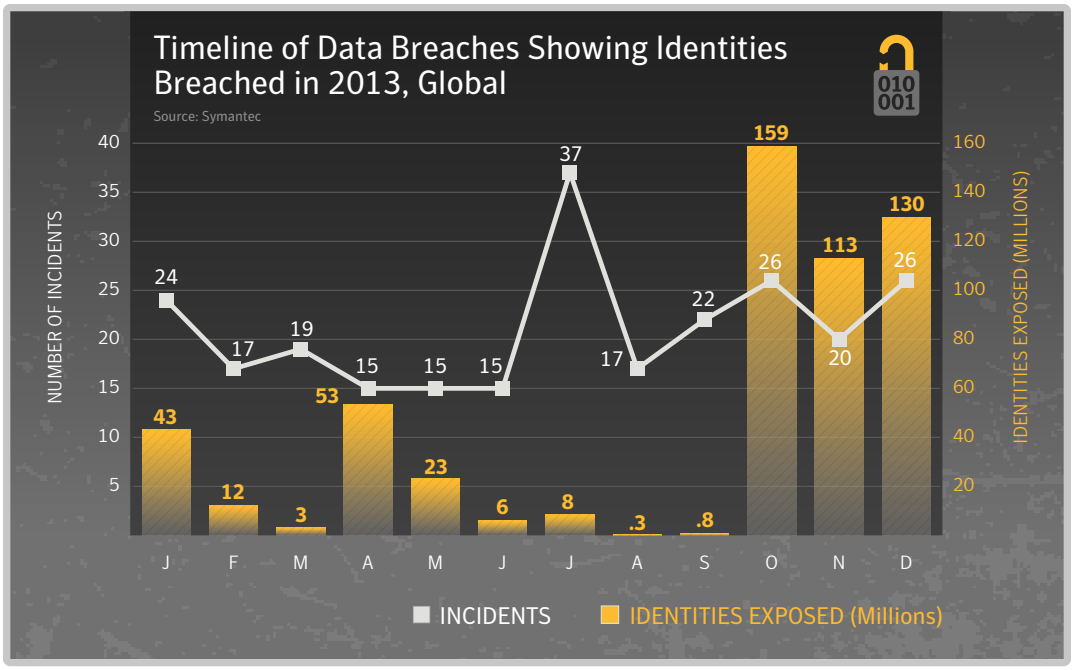
The information analysed regarding data breaches that could lead to identity theft is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model which measures the levels of threats including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. Data for the CCI is primarily derived from Symantec Global Intelligence Network and for certain data from ID Analytics.[25] The majority of the Norton CCI's data comes from Symantec's Global Intelligence Network, one of the industry's most comprehensive sources of intelligence about online threats. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information, including name, address, Social Security numbers, credit card numbers, and medical history. Using publicly available data the Norton CCI determines the sectors that were most often affected by data breaches, as well as the most common causes of data loss.

The sector that experienced the loss, along with the cause of loss that occurred, is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

The data also reflects the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data. An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach. Data may include names, government-issued identification numbers, credit card information, home addresses, or email information. A data breach is considered deliberate when the cause of the breach is due to hacking, insider intervention, or fraud. A data breach is considered to be caused by hacking if data related to identity theft was exposed by attackers, external to an organization, gaining unauthorized access to computers or networks.

It should be noted that some sectors may need to comply with more stringent reporting requirements for data breaches than others do. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[26] Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are neither required nor encouraged to report data breaches may be under-represented in this data set.

Fig. A.29



- There were 253 data breach incidents recorded by the Norton Cybercrime Index for 2013 and a total of 552,018,539 identities exposed as a result.
- The average number of identities exposed per incident was 2,181,891 compared with 604,826 in 2012 (an increase of more than 2.6 times).
- The median number of identities exposed was 6,777 compared with 8,350 in 2012. The median is a useful measure as it eliminates extreme values caused by the most notable incidents, which may not necessarily be typical.
- The number of incidents that resulted in 10 million or more identities being exposed was eight, compared with only one in 2012.

Fig. A.30

Data Breach Incidents by Sector, 2013

Source: Norton Cybercrime Index

Industry Sector	Number of Incidents	Percentage of Incidents
Healthcare	93	36.8%
Education	32	12.6%
Government and Public Sector	22	8.7%
Retail	19	7.5%
Accounting	13	5.1%
Computer software	12	4.7%
Hospitality	10	4.0%
Insurance	9	3.6%
Financial	9	3.6%
Transportation	6	2.4%
Information technology	5	2.0%
Telecom	4	1.6%
Law enforcement	4	1.6%
Social networking	3	1.2%
Agriculture	2	0.8%
Community and non-profit	2	0.8%
Administration and human resources	2	0.8%
Military	2	0.8%
Construction	1	0.4%
Utilities and energy	1	0.4%
Computer hardware	1	0.4%

Fig. A.31

Identities Exposed by Sector, 2013

Source: Norton Cybercrime Index

Industry Sector	Identities Exposed	Percentage of Identities Exposed
Retail	165,154,040	29.9%
Computer software	153,134,178	27.7%
Financial	106,958,000	19.4%
Social networking	48,250,000	8.7%
Information technology	22,501,152	4.1%
Hospitality	20,342,323	3.7%
Telecom	12,117,143	2.20%
Accounting	8,760,912	1.6%
Healthcare	6,279,270	1.1%
Education	3,208,557	0.6%
Government and Public Sector	2,197,646	0.4%
Transportation	1,460,340	0.3%
Insurance	1,032,973	0.2%
Administration and human resources	301,300	0.1%
Computer hardware	100,000	0.02%
Agriculture	74,000	0.01%
Community and non-profit	69,228	0.01%
Military	53,000	0.01%
Law enforcement	4,477	0.001%

- Healthcare, Education, and the Public Sector were ranked highest for the number of data breach incidents in 2013; the top three accounted for 58 percent of all data breaches
- The Retail, Computer Software and Financial sectors accounted for 77 percent of all the identities exposed in 2013.
- This highlights that sectors involved in the majority of data breaches don't necessarily result in the largest caches of stolen identities.

Fig. A.32

Average Number of Identities Exposed per Data Breach by Notable Sector

Source: Norton Cybercrime Index

Cause of Breach	Average Identities per Incident
Accounting	673,916
Administration and human resources	150,650
Agriculture	37,000
Community and non-profit	34,614
Computer hardware	100,000
Computer software	12,761,182
Education	100,267
Financial	11,884,222
Government	99,893
Healthcare	67,519
Hospitality	2,034,232
Information technology	4,500,230
Insurance	114,775
Law enforcement	1,119
Military	26,500
Retail	8,692,318
Social networking	16,083,333
Telecom	3,029,286
Transportation	243,390
Construction	20,000

- The highest average number of identities exposed per breach in 2013 was in the Social Networking and Computer Software categories, with between 16 million and 12 million identities exposed in each breach, on average.
- The largest breach incident in 2013 occurred in the Computer Software sector, with an incident resulting in 15 million identities reportedly exposed.

Fig. A.33

Top Causes for Data Breach by Number of Breaches

Source: Norton Cybercrime Index

Cause of Breach	Number of Incidents	Percentage of Incidents
Hackers	87	34.4%
Accidentally made public	72	28.5%
Theft or loss of computer or drive	69	27.3%
Insider theft	15	5.9%
Unknown	6	2.4%
Fraud	4	1.6%

Fig. A.34

Top Causes for Data Breaches by Number of Identities Exposed

Source: Norton Cybercrime Index

Cause of Breach	Number of Identities Exposed	Percentage of Identities Exposed
Hackers	408,432,788	74.0%
Insider theft	112,435,788	20.4%
Accidentally made public	22,350,376	4.1%
Theft or loss of computer or drive	6,231,790	1.1%
Fraud	2,417,320	0.4%
Unknown	150,477	0.03%

Fig. A.35

Average Number of Identities Exposed per Data Breach, by Cause

Source: Norton Cybercrime Indexx

Cause of Breach	Average Identities per Incident
Hackers	4,694,630
Insider theft	7,495,719
Accidentally made public	310,422
Theft or loss	90,316
Fraud	604,330
Unknown	25,080

- **Hacking was the leading cause of reported identities exposed in 2013:** Hackers were also responsible for the largest number of identities exposed, responsible for 34 percent of the incidents and 74 percent of the identities exposed in data breach incidents during 2013.
- The average number of identities exposed per data breach for Hacking incidents was approximately 4.7 million.

Fig. A.36

Types of Information Exposed, by Data Breach

Source: Norton Cybercrime Index

Type of Information	Number of Incidents	Percentage of Data Types
Real Names	181	71.5%
Birth Dates	109	43.1%
Government ID numbers (incl. Social Security)	100	39.5%
Home Address	95	37.5%
Medical Records	85	33.6%
Phone Numbers	48	19.0%
Financial Information	45	17.8%
Email Addresses	39	15.4%
Usernames & Passwords	30	11.9%
Insurance	15	5.9%

- The most common type of personal information exposed in data breaches during 2013 was real names, where 84 percent of the incidents in 2013 included this type of information being exposed
- Birth dates were identified in 51 percent of the identity breaches during 2013, compared with usernames and passwords, which were exposed in 14 percent of incidents
- Government ID numbers, including social security numbers, were exposed in 47 percent of breach incidents during 2013

Threat of the Insider

For many companies, the leaked NSA documents have shown how an insider can easily gain access to confidential information and the damage that leaked information can cause. This issue was further highlighted when three South Korean credit card firms announced that they suffered a major data breach that affected tens of millions of customers. The cause of the breach, which is believed to be the largest ever recorded in South Korea, was due to one employee at a company that produces credit scores. This insider stole names, resident registration numbers (a Government identification number), and credit card details simply by copying this data to a USB stick which was then sold on to marketing firms.

Unlike external attackers, insiders may already possess privileged access to sensitive customer information, meaning they don't have to go to the trouble of stealing login credentials from someone else. They also have knowledge of the inner workings of a company, so if they know that their firm has lax security practices, they may believe that they will get away with data theft unscathed. Our recent research conducted with the Ponemon Institute suggests that 51 percent of employees claim it's acceptable to transfer corporate data to their personal computers, as their companies don't strictly enforce data security policies. Insiders could earn a lot of money by selling customer details, which may be sufficient motivation to risk their careers.

Outside of leaking information for the insider's personal gain, insider data breaches may also be the result of an accident. There were several cases last year in which company laptops were lost, potentially exposing personal information. Employees may not have had adequate data-handling training, meaning that they may have stored or shared data on insecure channels.

Accidental data breaches were most prevalent in 2013. We estimate that 28.5 percent of all data breaches were cases where records were accidently made public. This was the second biggest cause of data breaches all year.

German companies are the most likely to experience a malicious or criminal attack, according to our recent research with the Ponemon Institute, followed by Australia and Japan. Brazilian companies were most likely to experience data breaches caused by human error. All companies should be aware that, in addition to protecting their data from outsider threats, they should also keep an eye on those on the inside and strengthen their data protection policies in light of this.

Gaming Attacks

While gaming services may not seem like an obvious target for cybercriminals, account information such as usernames and passwords are valuable in themselves. In addition to this, in-game items have a real world value, making them a target for theft.

A console game vendor in Asia had 24,000 accounts relating to its reward program broken into by a brute force attack which involved around 5 million login attempts. One week later a similar attack against a Japanese computer game vendor resulted in 35,000 accounts being compromised. In this case, four million password guesses were required.

It would appear that it took around 160 password guesses on average per account to guess the password. This is a clear indication that many users still use easy-to-guess passwords.

In addition to this, attackers are re-using data from data breaches on other services. At least three large online game vendors fell victim to such breaches in 2013, revealing millions of account records. These events helped motivate some gaming companies to move to two-factor authentication for their login process.

The attackers behind gaming Trojans have also begun to expand their focus and move outside of the gaming sector. For example, Trojan.Grolker is a common gaming Trojan that has now started to target customers of a major South Korean bank.

Attacks are not just motivated by account theft. In some instances the attacker just wants to disrupt the game. For example, during the Christmas holiday, a group of attackers used NTP amplification DDoS attacks to bring down a handful of popular online games. On Twitter the group said they were doing it just for fun.

DDoS attacks require relatively little technical expertise to mount and the main obstacle for the attacker is finding enough bots or an amplifier to use. A new development is the emergence of DDoS services customized for gamers. Those so called “booter” services start at around US$2.50 for short-burst attacks.

Online games can also suffer from vulnerabilities like any other software. Researchers have found[27] multiple vulnerabilities such as buffer overflows in many of the popular game engines. Successful exploitation could lead to the compromise of the gaming server or even to remote code execution on all connected clients.

The gaming sector has also not been immune to the attention of state-sponsored attackers. Leaks to the media have revealed that a number of popular online gaming platforms were monitored by intelligence agencies, who were fearful that in-game communication tools were being used by terrorists for covert communications.

The New Black Market

One of the most notable developments of 2013 was the emergence of new underground markets for drugs and other illegal goods. The oldest and best known of these marketplaces is Silk Road. Launched in 2001, it maintained a relatively low profile until last year, when it emerged into the public's consciousness and gathered significant media attention before it was temporarily shut down by the US Federal Bureau of Investigation (FBI) in October.

Silk Road epitomizes the growing professionalization of the cybercrime underground. It borrows the business model of legitimate e-commerce marketplaces such as Amazon and eBay, incorporating features such as vendor feedback, escrow payments and dispute resolution.

Where Silk Road and other sites differ is in the degree of anonymity they afford their users. Most of these sites operate on Tor, a network designed to facilitate anonymous access to the Internet. Transactions are conducted through virtual currency Bitcoin, which is largely unregulated.

If these measures led users to believe that they could operate with impunity, that illusion was shattered by the FBI raids in October. A man alleged to be the founder of the website was arrested and Bitcoins worth more than US$28 million were seized.

Law enforcement moves have yet to deter the online narcotics trade completely. In the aftermath of the raid, business moved to a number of copycat marketplaces such as Black Market Reloaded and Sheep. Before the end of the year Silk Road itself was re-launched by former administrators of the original site.

These developments indicate that the new black market has a high degree of resilience. While the original Silk Road employed numerous measures to preserve the anonymity of its users, its alleged founder did make several mistakes that allowed the FBI to discover his identity. A new generation of black marketeers may be more careful about guarding their identity. If so, other marketplaces will prove more difficult to dismantle.

The evolution of the new black market model closely resembles the growth of online music and video piracy. Early ad hoc sales were followed by the construction of a trading platform. When the original marketplace falls foul of the law, it is succeeded by a host of copycat services, each seeking to perfect the business model and enhance security.

On this basis, it would appear that the new black market is still in its infancy and could prove to be a persistent threat for years to come. While such marketplaces in themselves do not represent an information security threat, they have the potential to facilitate other criminal activity, such as providing further income for cybercrime gangs or acting as a platform for scams and fraud.

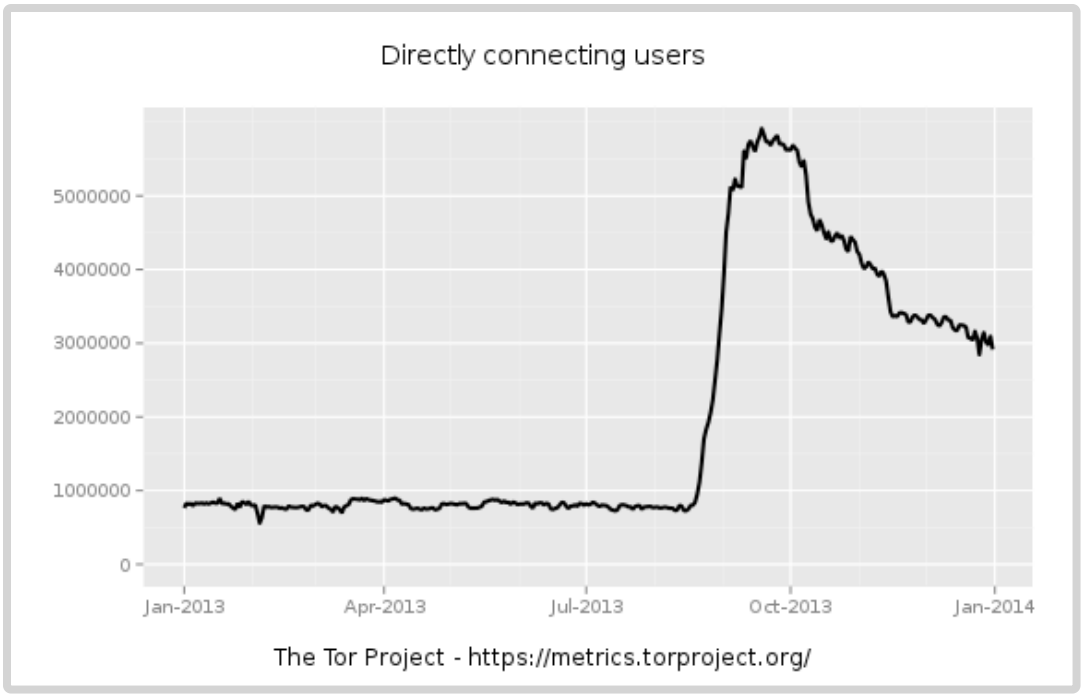


Fig. A.37 *Directly connected Tor users in 2013.*

The narcotics trade has traditionally been controlled by powerful and violent criminal gangs. If these new online marketplaces continue to gain popularity, it is likely that these gangs will not easily cede their market share to new arrivals, leading to potential for conflict and violence.

Tor is the most popular means of accessing these underground sites, but other networks like I2P or Freenet also became popular in 2013. The Tor network was more popular than ever, promoted as the best way to stay anonymous on the Internet. In August the number of active users grew from 1 million to 5 million in just two weeks. But some of that growth might have been related to the botnet Backdoor.Mevede,[28] which switched to use Tor as its command infrastructure.

Footnotes

01 http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201401/P020140116395418429515.pdf

02 http://data.worldbank.org/indicator/IT.NET.USER.P2 and http://www.prb.org/DataFinder/Topic/Rankings.aspx?ind=14

03 http://www.iamai.in/PRelease_detail.aspx?nid=3222&NMonth=11&NYear=2013

04 For more details about Norton Safe Web, please visit http://safeweb.norton.com

05 For more details about Symantec Rulespace, please visit http://www.symantec.com/theme.jsp?themeid=rulespace

06 Command and control

07 http://www.akamai.com/dl/whitepapers/akamai_soti_q412.pdf?curl=/dl/whitepapers/akamai_soti_q412.pdf&solcheck=1&

08 http://www.akamai.com/dl/akamai/akamai-soti-q313.pdf?WT.mc_id=soti_Q313

09 http://openresolverproject.org

10 http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

11 http://arstechnica.com/security/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol

12 http://www.informationweek.com/security/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787

13 http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend

14 https://www.gartner.com/login/loginInitAction.do?method=initialize&TARGET=http://www.gartner.com/document/2622821

15 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/b#3g-or-better

16 http://www.gsmamobileeconomy.com/GSMA Mobile Economy 2013.pdf

17 http://www.gsmamobileeconomy.com/GSMA_ME_Report_2014_R2_WEB.pdf

18 http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

19 http://en.wikipedia.org/wiki/Single_sign-on

20 International Mobile Equipment Identity

21 International Mobile Subscriber Identity

22 http://en.wikipedia.org/wiki/Quantified_Self

23 http://www.cbinsights.com/blog/trends/quantified-self-venture-capital

24 http://www.nortoncybercrimeindex.com

25 http://www.idanalytics.com

26 For example, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) of California. For more on this act, please see: http://www.privacyrights.org/fs/fs6a-facta.htm. Another example is the Health Insurance Portability and Accountability Act of 1996. For more information see: http://www.cms.hhs.gov/HIPAAGenInfo

27 http://revuln.com/files/ReVuln_Game_Engines_0days_tale.pdf

28 http://www.symantec.com/security_response/writeup.jsp?docid=2013-090611-2333-99

APPENDIX :: B
MALICIOUS CODE TRENDS

Malicious Code Trends

Symantec collects malicious code information from our large global customer base through a series of opt-in anonymous telemetry programs, including Norton Community Watch, Symantec Digital Immune System and Symantec Scan and Deliver technologies. Millions of devices, including clients, servers and gateway systems, actively contribute to these programs. New malicious code samples, as well as detection incidents from known malicious code types, are reported back to Symantec. These resources give Symantec's analysts unparalleled sources of data to identify, analyze, and provide informed commentary on emerging trends in malicious code activity in the threat landscape. Reported incidents are considered potential infections if an infection could have occurred in the absence of security software to detect and eliminate the threat.

Malicious code threats are classified into four main types — backdoors, viruses, worms, and Trojans:

- Backdoors allow an attacker to remotely access compromised computers.
- Viruses propagate by infecting existing files on affected computers with malicious code.
- Worms are malicious code threats that can replicate on infected computers or in a manner that facilitates them being copied to another computer (such as via USB storage devices).
- Trojans are malicious code that users unwittingly install onto their computers, most commonly through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.

Many malicious code threats have multiple features. For example, a backdoor will always be categorized in conjunction with another malicious code feature. Typically, backdoors are also Trojans, however many worms and viruses also incorporate backdoor functionality. In addition, many malicious code samples can be classified as both worm and virus due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.

The following malicious code trends were analyzed for 2013:

- Top Malicious Code Families
- Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
- Propagation Mechanisms
- Email Targeted Spear-Phishing Attacks Intelligence

Top Malicious Code Families

Background

Symantec analyzes new and existing malicious code families to determine attack methodologies and vectors that are being employed in the most prevalent threats. This information also allows system administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and new threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may be deployed, such as gateway or cloud-based filtering.

Methodology

A malicious code family is initially comprised of a distinct malicious code sample. As variants to the sample are released, the family can grow to include multiple variants. Symantec determines the most prevalent malicious code families by collating and analyzing anonymous telemetry data gathered for the reporting period.

Malicious code is classified into families based on variants in the signatures assigned by Symantec when the code is identified. Variants appear when attackers modify or improve existing malicious code to add or change functionality. These changes alter existing code enough that antivirus sensors may not detect the threat as an existing signature.

Overall, the top-ten list of malicious code families accounted for 40.1 percent of all potential infections blocked in 2013.

Fig. B.1

Overall Top Malicious Code Families, 2013

Source: Symantec

Rank	Name	Type	Propagation Mechanisms	Impacts/Features	Percent Overall
1	W32.Ramnit	Virus/Worm	Executable files and removable drives	Infects various file types, including executable files, and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	15.4%
2	W32.Sality	Virus/Worm	Executable files and removable drives	Uses polymorphism to evade detection. Once running on an infected computer it infects executable files on local, removable and shared network drives. It then connects to a P2P botnet, downloads and installs additional threats. The virus also disables installed security software.	7.4%
3	W32.Downadup	Worm/Backdoor	P2P/CIFS/remote vulnerability	The worm disables security applications and Windows Update functionality and allows remote access to the infected computer. Exploits vulnerabilities to copy itself to shared network drives. It also connects to a P2P botnet and may download and install additional threats.	4.5%
4	W32.Virut	Virus/Backdoor	Executables	Infects various file types including executable files and copies itself to local, removable, and shared network drives. It also establishes a backdoor that may be used to download and install additional threats.	3.4%
5	W32.Almanahe	Virus/Worm	CIFS/mapped drives/ removable drives/ executables	Disables security software by ending related processes. It also infects executable files and copies itself to local, removable, and shared network drives. The worm may also download and install additional threats.	3.3%
6	W32.SillyFDC	Worm	Removable drives	Downloads additional threats and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	2.9%
7	W32.Chir	Worm	SMTP engine	Searches across the network and accesses files on other computers. However, due to a bug, these files are not modified in any way.	1.4%
8	W32.Mabezat	Virus/Worm	SMTP/CIFS/removable drives	Copies itself to local, removable, and shared network drives. Infects executables and encrypts various file types. It may also use the infected computer to send spam email containing infected attachments.	1.2%
9	W32.Changeup	Worm	Removable and mapped drives/File sharing programs/Microsoft Vulnerability	The primary function of this threat is to download more malware on to the compromised computer. It is likely that the authors of the threat are associated with affiliate schemes that are attempting to generate money through the distribution of malware.	0.4%
10	W32.Xpaj	Virus	Executables/removable, mapped, and network drives	Infects .dll, .exe, .scr, and .sys files on the compromised computer.	0.2%

Fig. B.2

Relative Proportion of Top-Ten Malicious Code Blocked in Email Traffic by Symantec.cloud in 2013, by Percentage and Ratio

Source: Symantec.cloud

Rank	Malware	Percentage of Email Malware	Equivalent Ratio in Email	Percentage Overall
1	Trojan.Zbot-SH	24%	1 in 4.2	15.4%
2	Trojan.Zbot	11%	1 in 8.7	7.4%
3	Exploit/Link.D	3%	1 in 33.2	4.5%
4	Exploit/Link-Downloader	2%	1 in 41.1	3.4%
5	Exploit/LinkAlias	2%	1 in 42.8	3.3%
6	w32/NewMalware-30e9	2%	1 in 50.6	2.9%
7	Exploit/LinkAlias.fu	1%	1 in 71.7	1.4%
8	Exploit/Link.G	1%	1 in 81.6	1.2%
9	Exploit/Link-30e9	1%	1 in 85.1	0.4%
10	Exploit/MimeBoundary003	1%	1 in 105.8	0.2%

Fig. B.3

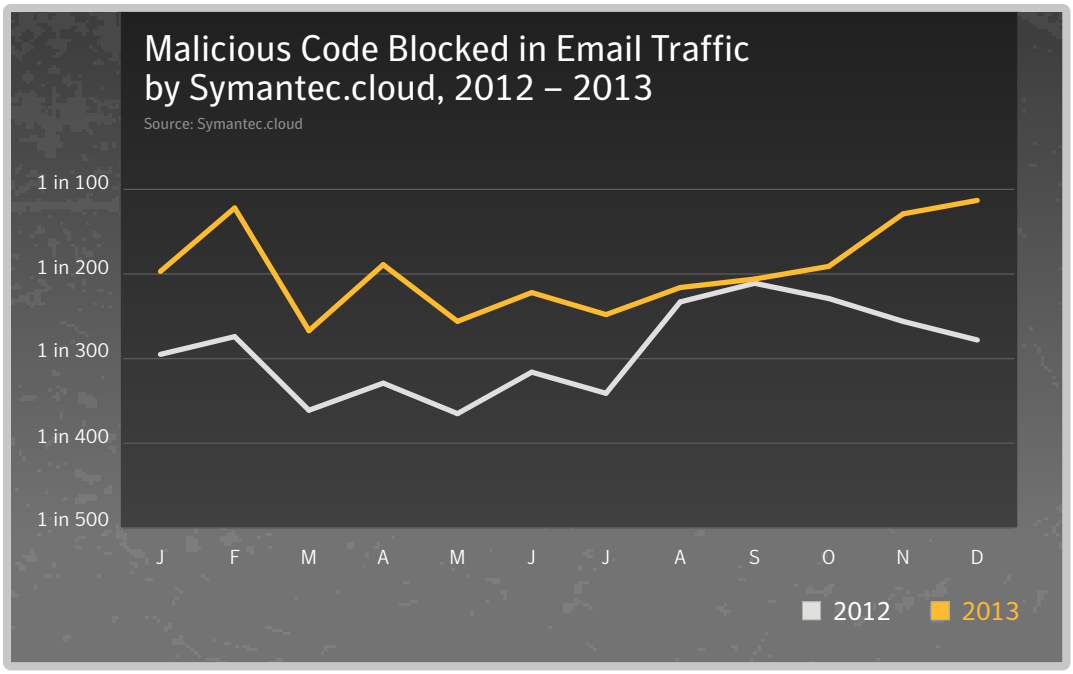


Fig. B.4

Relative Proportion of Top-Ten Malicious Code Blocked in Web Traffic by Symantec.cloud in 2013, by Percentage and Ratio

Source: Symantec.cloud

Rank	Malware Name	Percentage of Web Malware	Equivalent Ratio
1	Trojan.Iframe.BMY	5.6%	1 in 17.8
2	Bloodhound.Exploit.281	2.4%	1 in 42.1
3	Trojan.Malscript	1.8%	1 in 56.8
4	EML/Worm.AA.dam	1.7%	1 in 58.1
5	URL.Malware	1.1%	1 in 87.6
6	Trojan.Maljava	1.0%	1 in 96.0
7	IFrame.Exploit	1.0%	1 in 96.5
8	Trojan.HTML.Redirector.CH	0.6%	1 in 165.0
9	JS:Trojan.JS.Iframe.AM	0.6%	1 in 166.0
10	JS:Trojan.Crypt.KA	0.6%	1 in 181.6

Commentary

- Ramnit overtook Sality again to become the most prevalent malicious code family in 2013. Ranked first in 2011 and 2012, it was the top malicious code family by volume of potential infections again in 2013.[1]
- Samples of the Ramnit family of malware were responsible for significantly more potential infections (15.4 percent) than the second ranked malicious code family in 2013, Sality[2] (7.4 percent).
- First discovered in 2010, W32.Ramnit has remained a prominent feature of the threat landscape.
- Ramnit spreads by encrypting and then appending itself to DLL, EXE and HTML files. It can also spread by copying itself to the recycle bin on removable drives and creating an AUTORUN.INF file so that the malware is potentially automatically executed on other computers. This can occur when an infected USB device is attached to a computer. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Ramnit and Sality (as well as SillyFDC[3] and others) effective vehicles for installing additional malicious code on computers.
- The Sality family of malware remains attractive to attackers because it uses polymorphic code that can hamper detection. Sality is also capable of disabling security services on affected computers. These two factors may lead to a higher rate of successful installations for attackers. Sality propagates by infecting executable files and copying itself to removable drives such as USB devices. Similar to Ramnit, Sality also relies on AUTORUN.INF functionality to potentially execute when those drives are accessed.
- Downadup gains some momentum: Downadup (a.k.a. Conficker) was ranked in third position in 2013 and 2012. Downadup propagates by exploiting vulnerabilities in order to copy itself to network shares.
- Overall in 2013, 1 in 196.4 emails was identified as malicious, compared with 1 in 291 in 2012; 25.4 percent of email-borne malware comprised hyperlinks that referenced malicious code, in contrast with malware that was contained in an attachment to the email. This figure was 22.5 percent in 2012, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.

- In 2013, 10.5 percent of malicious code detected in 2013 was identified and blocked using generic detection technology. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked. By deploying techniques such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.
- Trojan.Zbot-SH was the most frequently blocked malware in email traffic by Symantec.cloud in 2013, with Trojan.Zbot taking the second position.
- Trojan.Iframe.BMY was the most frequently blocked malicious activity in web traffic filtered by Symantec.cloud in 2013, accounting for 5.6 percent. Detection for a malicious IFrame is triggered in HTML files that contain hidden HTML IFrame elements with JavaScript code that attempts to perform malicious actions on the computer; for example, when visiting a malicious web page, the code attempts to quietly direct the user to a malicious URL while the current page is loading.
- Bloodhound.Exploit.281 ranks second with 2.4 percent of detections.
- Trojan.Malscript ranks third with a detection of 1.8%.

Data Ownership: Targeting the User's Information Directly

Many people believe that only after they hand over their data to a company for purposes such as social networking and shopping, this data is under threat. If we continue with this logic, it could lead us to assume that, as long as a person does not give any of their personal data to third-party services, they're safe. However, this is not necessarily the case. There are several forms of malware that specifically target data that resides on the user's computer.

Stealing Information Directly

Infostealer malware, as the name implies, specifically focuses on stealing information directly from the user's computer. This malware could log keystrokes or take screenshots to steal login credentials, financial information and other personally identifiable information.

Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size

Background

Malicious code activity trends can also reveal patterns that may be associated with particular geographical locations, or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace that can drive down prices, increasing adoption rates. There may be other factors at work based on the local economic conditions that present different risk factors. Similarly, the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a malicious attack by virtue of the relationships they have with other organizations; for example, a company may be subjected to an attack because they are a supplier to a larger organization, and attackers may seek to take advantage of this relationship in forming the social engineering behind subsequent attacks to the main target using the SMB as a springboard for these later attacks. SMBs are perceived to be a softer target as they are less likely to have the same levels of security as a larger organization, which is likely to have a larger budget applied to their security countermeasures.

Methodology

Analysis of malicious code activity on geography, industry, and size are based on the telemetry analysis from Symantec.cloud clients for threats detected and blocked against those organizations in email traffic during 2013.

This analysis looked at the profile of organizations being subjected to malicious attacks, in contrast to the source of the attack.

Fig. B.5

Proportion of Email Traffic Identified as Malicious by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013	2012
Public Sector	1 in 95.4	1 in 72.2
Education	1 in 233.0	1 in 163.1
Accommodation and Catering	1 in 247.3	1 in 236.4
Marketing/Media	1 in 291.8	1 in 234.6
Non-Profit	1 in 328.4	1 in 272.3
Estate Agents	1 in 360.2	1 in 291.4
Recreation	1 in 370.8	1 in 315.1
Prof Services	1 in 396.5	1 in 315.1
Agriculture	1 in 415.5	1 in 329.7
Finance	1 in 426.8	1 in 218.3

Fig. B.6

Proportion of Email Traffic Identified as Malicious by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013	2012
1-250	1 in 332.1	1 in 299.2
251-500	1 in 359.4	1 in 325.4
501-1000	1 in 470.3	1 in 314.2
1001-1500	1 in 356.9	1 in 295.0
1501-2500	1 in 483.5	1 in 401.9
2501+	1 in 346.5	1 in 252.1

Fig. B.7

Proportion of Email Traffic Identified as Malicious by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013	2012
United Kingdom	1 in 198.9	1 in 163.2
South Africa	1 in 272.8	1 in 178.1
Austria	1 in 300.7	1 in 262.9
Hungary	1 in 306.8	1 in 289.8
Italy	1 in 370.3	1 in 385.3
Netherlands	1 in 379.5	1 in 108.0
China	1 in 380.8	1 in 358.0
Australia	1 in 399.6	1 in 245.9
United Arab Emirates	1 in 420.6	1 in 462.3
Germany	1 in 429.2	1 in 196.1

Commentary

- The rate of malicious attacks carried out by email has increased for two of the top-ten geographies being targeted and decreased for the other eight; malicious email threats fell in 2013 for organizations in United Kingdom, South Africa, Austria, Hungary, Netherlands, China, Australia and Germany.
- Businesses in the United Kingdom were subjected to the highest average ratio of malicious email-borne threats in 2013, with 1 in 198.9 emails blocked as malicious, compared with 1 in 163.2 in 2012.
- Globally, organizations in the Government and Public sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 95.4 emails blocked as malicious in 2013, compared with 1 in 72.2 for 2012.
- Malicious email threats have decreased for all sizes of organizations, with 1 in 346.5 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2013, compared with 1 in 252.1 in 2012.
- 1 in 332.1 emails were blocked as malicious for small to medium-sized businesses with between 1-250 employees in 2013, compared with 1 in 299.2 in 2012.

Propagation Mechanisms

Background

Worms and viruses use various means to spread from one computer to another. These means are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), simple mail transfer protocol (SMTP), common Internet file system (CIFS), peer-to-peer file transfers (P2P), and remotely exploitable vulnerabilities.[4] Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a backdoor server and using it to upload and install itself.

Methodology

This metric assesses the prominence of propagation mechanisms used by malicious code. To determine this, Symantec analyzes the malicious code samples that propagate and ranks associated propagation mechanisms according to the related volumes of potential infections observed during the reporting period.[5]

Fig. B.8

Propagation Mechanisms

Source: Symantec

Rank	Propagation Mechanisms	2013	Change	2012
1	**Executable file sharing:** The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	70%	-1%	71%
2	**File transfer, CIFS:** CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within. Malicious code creates copies of itself on shared directories to affect other users who have access to the share.	32%	-1%	33%
3	**Remotely exploitable vulnerability:** The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	23%	-3%	26%
4	**File transfer, email attachment:** The malicious code sends spam email that contains a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	8%	+0%	8%
5	**File transfer, HTTP, embedded URI, instant messenger:** The malicious code sends or modifies instant messages with an embedded URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	3%	+0%	3%
6	**File transfer, non-executable file sharing:** The malicious code infects non-executable files.	3%	+0%	3%
7	**Peer-to-peer file sharing**	3%	+0%	3%
8	**SQL:** The malicious code accesses SQL servers, by exploiting a latent SQL vulnerability or by trying default or guessable administrator passwords, and copies itself to the server.	1%	+2%	1%
9	**File transfer, instant messenger:** The malicious code sends or modifies instant messages that contain a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	1%	+0%	1%
10	**File transfer, HTTP, embedded URI, email message body:** The malicious code sends spam email containing a malicious URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	<1%	=	<1%

Commentary

As malicious code continues to become more sophisticated, many threats employ multiple mechanisms.

- Executable file-sharing activity decreases: In 2013, 70 percent of malicious code propagated as executables, a small decrease from 71 percent in 2012. This propagation mechanism is typically employed by viruses and some worms to infect files on removable media. For example, variants of Ramnit and Sality use this mechanism, and both families of malware were significant contributing factors in this metric, as they were ranked as the two most common potential infections blocked in 2013.
- Remotely exploitable vulnerabilities decrease: The percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2013 at 23 percent was 3 percentage points lower than in 2012. Examples of attacks employing this mechanism include Downadup, which gained some momentum and is still a major contributing factor to the threat landscape, ranked in third position in 2012.
- File transfer using CIFS is in decline: The percentage of malicious code that propagated through CIFS file transfer fell by 1 percentage point between 2012 and 2013, a smaller decline than that seen in 2012. Fewer attacks exploited CIFS as an infection vector in 2013.
- File transfer via email attachments remains the same: It is worth noting that file transfer via email attachments remains the same in 2013 compared to 2012. This is justified by 1 in 196.4 emails being identified as malicious in 2013, compared with 1 in 291 in 2012. In 2013, 25.4 percent of email attacks used malicious URLs, compared with 22.5 percent in 2012, which is also an increase.

Email-Targeted Spear-Phishing Attacks Intelligence

Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Over the year 2013, Symantec identified about thirty-thousand spear-phishing emails that were deemed targeted by our threat analysts. Some of these originate from malicious actors that have different skills, exhibit various behaviors and pursue different goals. To get a better understanding of this threat landscape it is important to be able to differentiate them and identify series of related attacks that might have been sourced by the same (group of) attackers. This will help get a better understanding of attackers' tactics, techniques and procedures (TTPs) as well as their motivation, which can ultimately be used to proactively detect or predict when attackers are coming back with new exploits, or if they use slightly adapted techniques in attempts to compromise other customers.

However, finding groups of related attacks and attributing them to a specific threat actor or hacker group, based solely on intrusion activity or logging data, is challenging. The main reason is that skilled attackers can and will update at least part of their attack tools and methodology in order to maximize their chance of successfully compromising the organizations they are targeting. While changing all aspects of their attack tools or exploit kits might have a prohibitive cost, there is a strong chance that they will adapt their methods over time by investing resources in developing new exploits and adapting their intrusion tools.

As a result it can be challenging for us, as defenders, to determine whether any two spear-phishing attacks were conducted by the same person, by different persons who are collaborating, or by two unrelated hackers who decided independently to compromise the same company or computer. Nevertheless, with enough information, analytical experience, and technological tools to piece it all together, it is possible to reconstruct attack campaigns from raw email data and additional metadata on the malware, or the exploit crafted together with the email. Consider an analogy with a serial killer in the real world who leaves behind traces of his crime at different crime scenes. While individual crimes may vary in many details (such as the crime location, the victim gender and age, the weapon or vehicle used, the various signs left on the crime scene and how it was framed by the criminal), investigators might be able to collect different pieces of evidence which, when put together appropriately, can enable them to reconstruct the whole puzzle and ultimately identify which criminal was behind a series of crimes, based on the identified *modus operandi* and through the combination of all available pieces of evidence.

How Symantec is Able to Differentiate Distinct Targeted Attack Campaigns Using the Advanced TRIAGE Technology

Symantec advanced TRIAGE[6] data analytics technology aims at reproducing, in an automated fashion, a forensics methodology similar to the one performed by crime investigators, but in the digital world. This framework has been designed to help analysts answer fundamental questions about cyber-attacks, such as:

- *Campaign analysis:* which series of attacks might be related with each other, even though they may be targeting different organizations – on the same or different dates – and use different malware or different exploits?
- What are the attackers' tactics, techniques and procedures (TTPs)? How many different groups of attackers can we identify based on their *modus operandi?*

- What are the *characteristics* and *dynamics* of attack campaigns run by the same hacker groups? Example, what is their prevalence, their size and scale, or their sophistication?

Symantec uses the term *attack campaign* to refer to a series of spear-phishing emails (or email intrusions) that:

1. Show clear evidence that the subject and target has been deliberately selected.
2. Contain at least 3 to 4 strong correlations to other emails, such as the email topic, sender address, recipient domain, source IP address, attachment MD5, etc.

Attack campaigns may be sent on a single day or spread across multiple days, however emails within the same campaign are always linked by a number of similar traits and thus form a "chain of attacks".

One of the challenges in identifying such attack campaigns is that intrusions sourced by the same attackers (or group) may have varying degrees of correlation. Without knowing in advance which features or indicators one should use to correlate attacks, it can be very tedious for analysts to identify groups of related attacks. Figure B.9 illustrates graphically this challenge of varying correlations between three different intrusions that were identified as part of the same campaign. For example, intrusions 1 and 2 are linked by a different set of email features than intrusions 2 and 3. This means that attackers may change any one feature when targeting different companies over time. Since we don't know in advance what might be the next move, we have to rely on advanced correlation mechanisms that enable us to identify groups of related attacks (i.e. originating from a specific threat group) without knowing which set of features should be used to associate these attacks to a particular group.

Phase	Email feature	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	**Recipient**	[user1]@org1.**gov.xy**	[user2]@**org2.gov.xy**	[user3]@**org2.gov.xy**
Weaponization	**Attach_name**	**Global Pulse Project***.pdf**		Agenda – G20***.pdf
	Attach MD5	**dd2ed3f7dead4a[***]**		2e36081dd7f62e[***]
Delivery	**Date**	2011-05-13	2011-05-14	2011-07-02
	From addr.	[Att1]@domain1.com	[Att2]@domain2.com	
	Sender IP	**74.125.83.*** **		74.125.82.***
	Subject	FW:Project Document	Project Document	G20 Ds Finance Key Info – Paris July 2011
	Email body	[body1]		[body2]
Exploitation	**AV signature**	**CVE-2011-0611.C**		
Persistence	**C&C domains**	www.webserver.***		[N/A]

Fig. B.9 Illustration of varying correlations between different intrusions of the same campaign

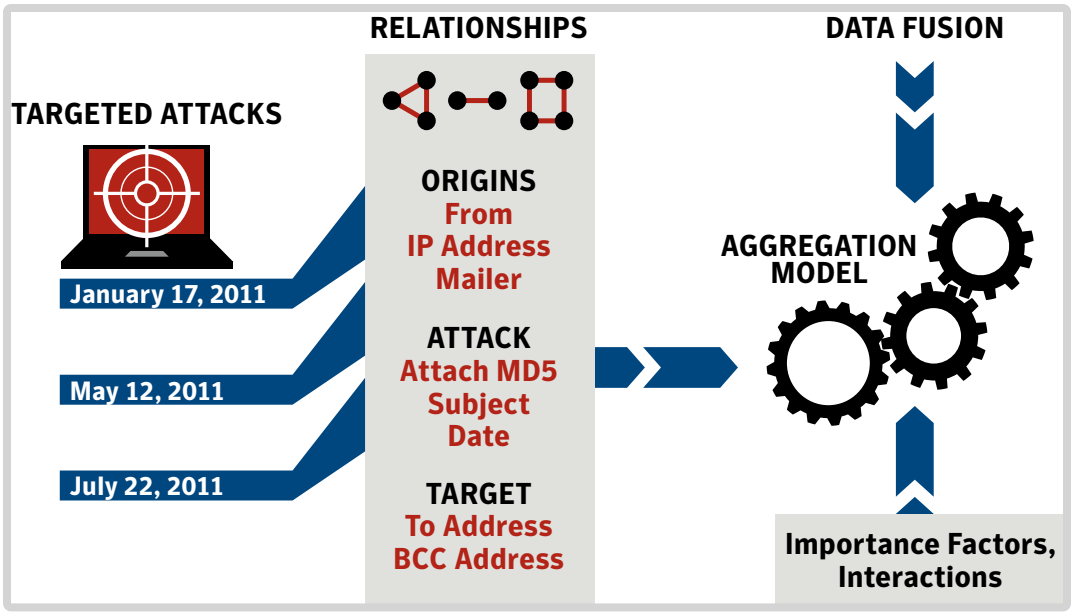


Fig. B.10 Illustration of TRIAGE methodology

By leveraging our TRIAGE data analytics technology, targeted attacks can be automatically grouped together based upon common elements which are likely to reflect the same root cause. As a result, we are able to identify complex patterns showing various types of relationships among series of targeted attacks, giving insights into the manner by which attack campaigns are orchestrated by various threat actors. The TRIAGE approach is illustrated in Figure B.10.

It is worth mentioning that our TRIAGE framework was recently enhanced with novel visualizations thanks to VIS-SENSE,[7] a European research project aiming at developing visual analytics technologies for network security applications. Since its original conception, TRIAGE has been successfully used to analyze the behavior of cybercriminals involved in various types of Internet attack activities, such as rogue antivirus websites,[8] spam botnet operations,[9] scam campaigns,[10] and targeted attacks performed via spear-phishing emails[11,12].

Insights into targeted attack campaigns

In 2013 Symantec's TRIAGE technology has identified 779 clusters of spear-phishing attacks (named hereafter "attack campaigns", as defined previously), which are quite likely to reflect different waves of attacks launched by the same groups of individuals. Indeed, within the same cluster, attacks are linked by at least 3 to 4 characteristics among the following:

- The origins of the attack (like the email 'From' address and source IP address used by the attacker).
- The attack date.
- The characteristics of the malicious file attached to the email (MD5 checksum, AV signature, file name and some metadata coming from both static and dynamic analysis, such as document type or domains and IP addresses contacted by the malware).
- The email subject.
- The targeted recipient ('To:' or 'Bcc:' address fields in the email).

Figure B.11 and Figure B.12 highlight some global metrics calculated across all attack campaigns identified by TRIAGE. To give more perspective to these figures, we compare them to statistics calculated in the past two years (2011-2012), which can generate some insight concerning the characteristics and evolution of spear-phishing campaigns. More specifically, we can clearly identify the following new trends:

- Spear-phishing campaigns seem to be more widespread, with a significant increase in the number of distinct campaigns compared to 2011-2012.
- The average number of attacks per campaign has significantly decreased, which suggests campaigns are becoming more diverse, and possibly more automated. While we have not gathered conclusive evidence about this aspect, we anticipate that attackers are increasingly relying on exploit toolkits such as the Social Engineering Toolkit (SET), the Metasploit framework, and also the large availability of exploit codes on the Internet, which enable more threat groups to leverage this attack vector (spear-phishing emails).
- We observe also that the average duration of a spear-phishing campaign has increased (8.2 days on average), which suggests that these campaigns are much more persistent.

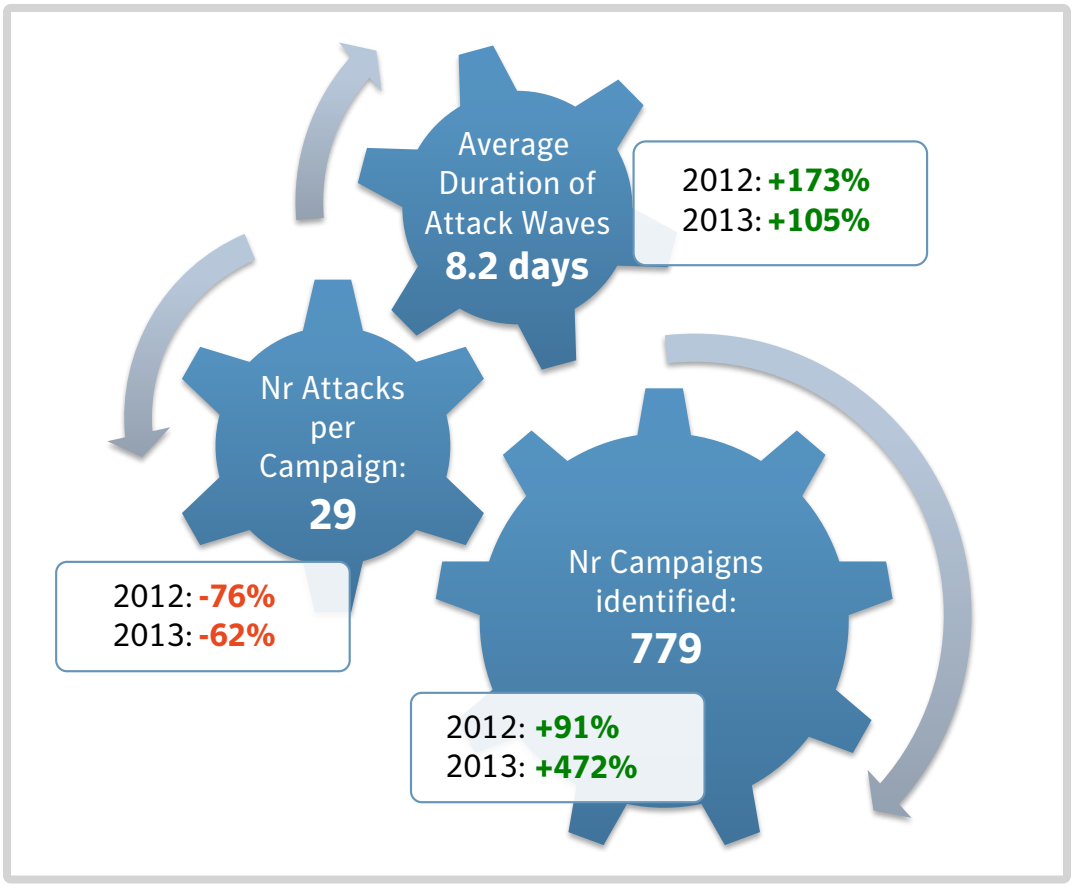


Fig. B.11 Global metrics calculated across all identified campaigns (1)

Figure B.12 highlights other interesting aspects of these targeted attack campaigns:

- The average number of recipients targeted during the same campaign has dropped significantly compared to 2011-2012. This means the vast majority of spear-phishing campaigns are now more focused, and targeted specifically at a small set of companies and individuals.
- Similarly, we observed that the average number of distinct droppers used in the same campaign has decreased by 84 and 60 percent compared to 2012 and 2011, respectively. This suggests that attackers try to be stealthier, and avoid sending attacks in large volumes during the same campaign. On average they will use only two different droppers in the same campaign. However, note that these two different droppers may sometimes contain the very same exploit, which was simply re-packed in two different documents (pdf, doc, xls, etc.)
- Finally, looking at the average number of different industries[13] targeted during the same campaign, we note that this number has increased by 33 and 11 percent compared to 2012 and 2011 respectively, showing an increased prevalence and broader diversification in spear-phishing attacks.

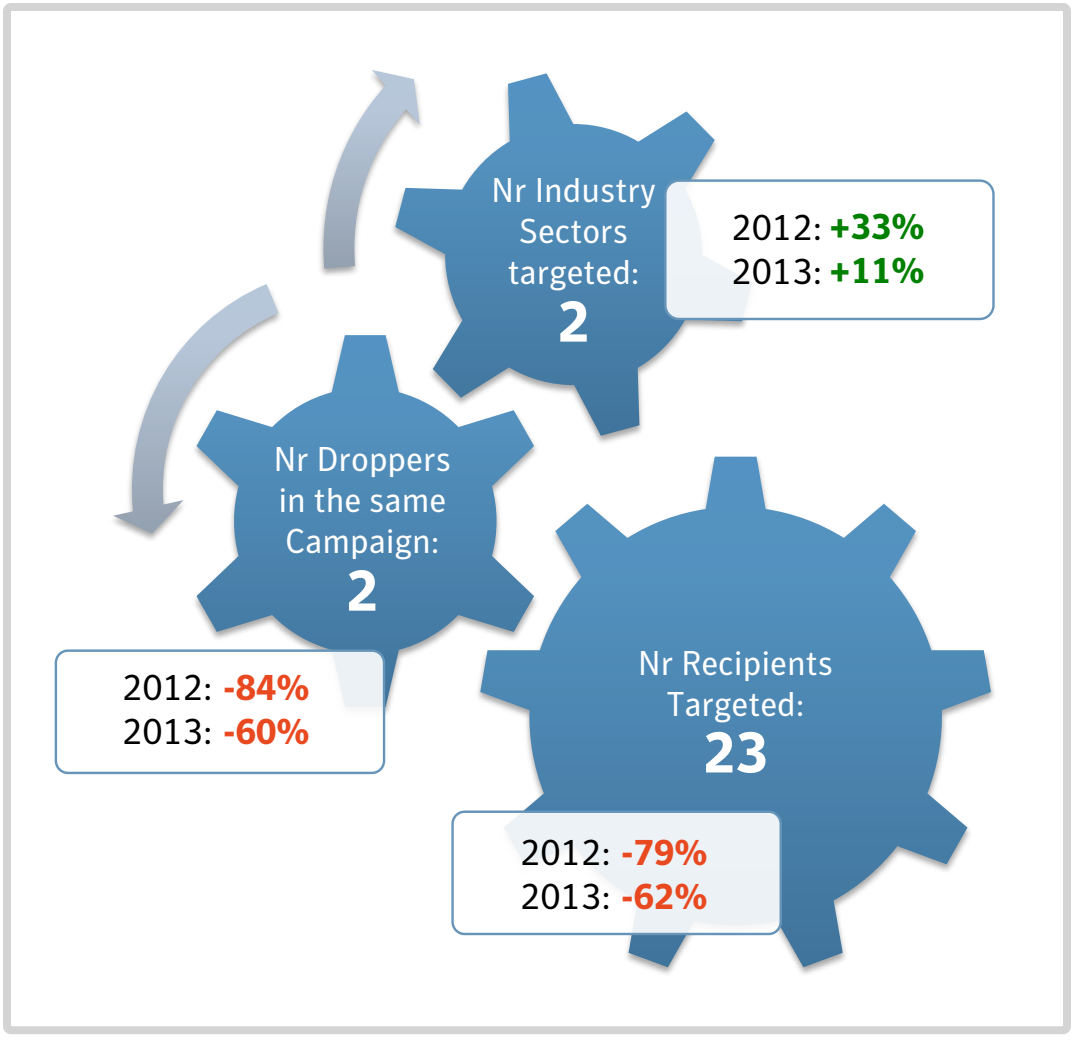


Fig. B.12 Global metrics calculated across all identified campaigns (2)

Highly focused versus Mass-scale campaigns

The 779 distinct campaigns of spear-phishing attacks were then classified into two groups:

- **Type 1:** Highly focused and targeted campaigns
- **Type 2:** Mass-scale Organizational Targeted Campaigns (MOTA)

To this end, we used a combination of two criteria on the number of targeted companies and the number of distinct industry sectors associated to them. Type 1-campaigns are defined as spear-phishing campaigns that had targeted five (or less) distinct companies, in five (or less) different sectors. Spear-phishing campaigns not matching these criteria were deemed as 'Type 2" campaigns, i.e., they fit the profile of so-called *Mass-scale Organizational Targeted Campaigns* (MOTA) because they target a more significant set of different industries having very different lines of business.

Based on the classification defined previously, we found that in 2013 about two-thirds of spear-phishing campaigns were highly focused and targeted a reduced set of companies active in the same or closely related sectors. The other one-third of the campaigns were still targeted (in the sense of being in low-copy number and showing some evidence of a selection of a subject in relation with the recipient activity), but these campaigns instead involved more large-scale attacks, in the sense that they were targeting a more significant number of companies and organizations active in different sectors.

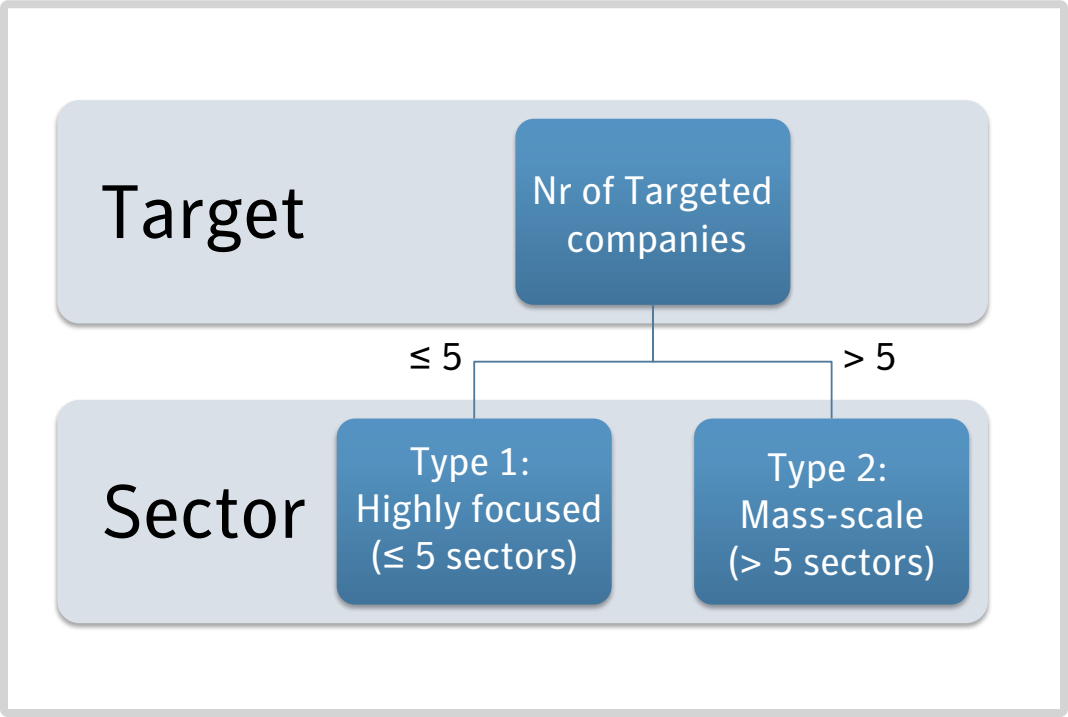


Fig. B.13 Criteria used to classify targeted attack campaigns according to their scale

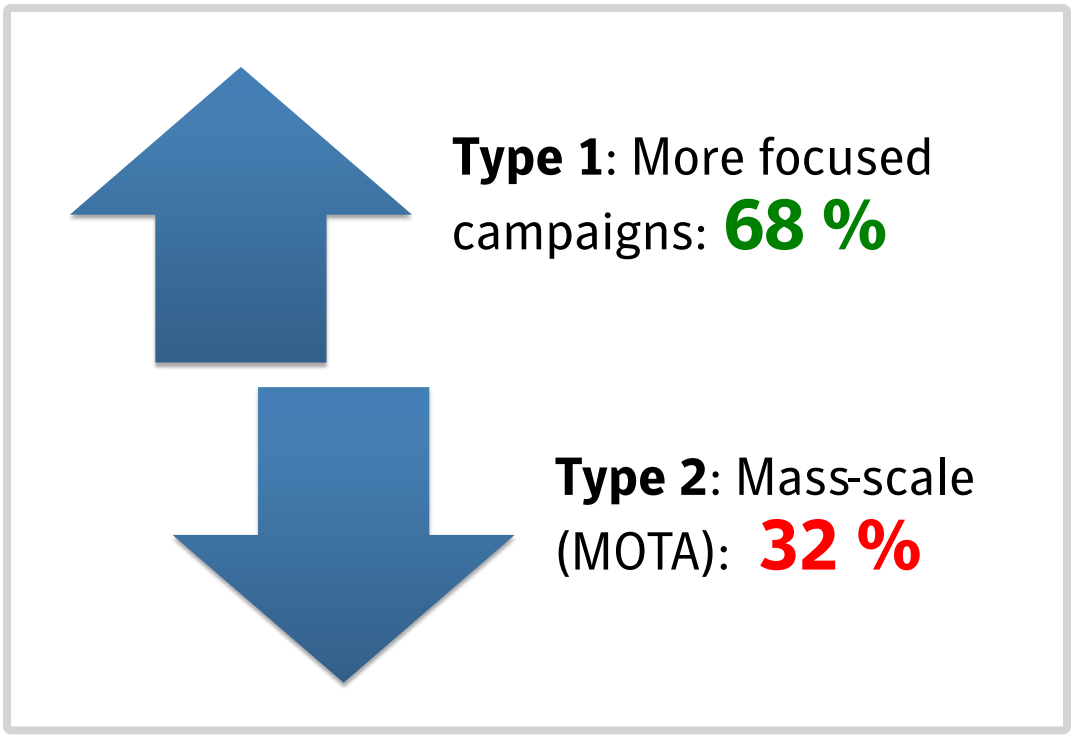


Fig. B.14 Types of campaigns

Type 1 – Highly targeted campaigns

As we have seen, 68 percent of spear-phishing attacks are forming rather small campaigns, meaning they are organized on a relatively small scale and tend to focus on specific targets. One example of such campaigns took place on January 1, 2013 and targeted a global energy research company – hence dubbed the "New Year campaign". As illustrated in Figure B.15, a first wave of spear-phishing emails was sent from two distinct Freemailer accounts to 291 individuals at the targeted company. All receiving email addresses started with a letter between G and R, covering half of the alphabet. Whether there was a second wave of emails using the other half of the alphabet or whether the attackers only got their hands on part of the address book remains unknown.

All emails had either the subject line "2013,Obama QE4! Merry Christmas !" or "2013,Obama QE4!". It is common to see spear-phishing attacks take place around holidays, as people are receiving more emails during these times and are less likely to perform due diligence while opening them. All of the emails contained the same Trojan.Dropper disguised as an attachment with the filename AVP.dll.

The malware itself drops a malicious Downloader "clbcatq.dll" into a newly created "wuauclt" directory, posing as Windows update and taking advantage of the DLL search order hijack weakness in order to load the malicious code in Windows. The same family of dropper was used in previous targeted attacks against other sectors, indicating that a group with multiple interests is behind the attacks. The backdoor provided full access to the compromised computers.

A week later, on January 7, 2013, the group attacked the same company again with another wave of spear-phishing emails (which appears quite clearly in the graph diagram in Figure B.15). Seventy emails were sent to 58 individuals using either "2012-13 NFL Playoffs Schedule" or "Re: 2012-13 NFL Playoffs Schedule" as a subject line. In this wave, the attackers used a similar AVP.dll to the one used before. In some of the emails, an additional CHM file with an old exploit was used in an effort to maximize the chances of a successful infection.

After this second wave, the attack ceased. It is unknown whether the attackers successfully retrieved the information they were seeking, if they installed other backdoor Trojans or gained passwords that allowed them to directly access the computers, or if they had given up on the target. Nevertheless, this "New-Year campaign" illustrates quite well how persistent and determined attackers can be in this type of focused, highly targeted campaign.

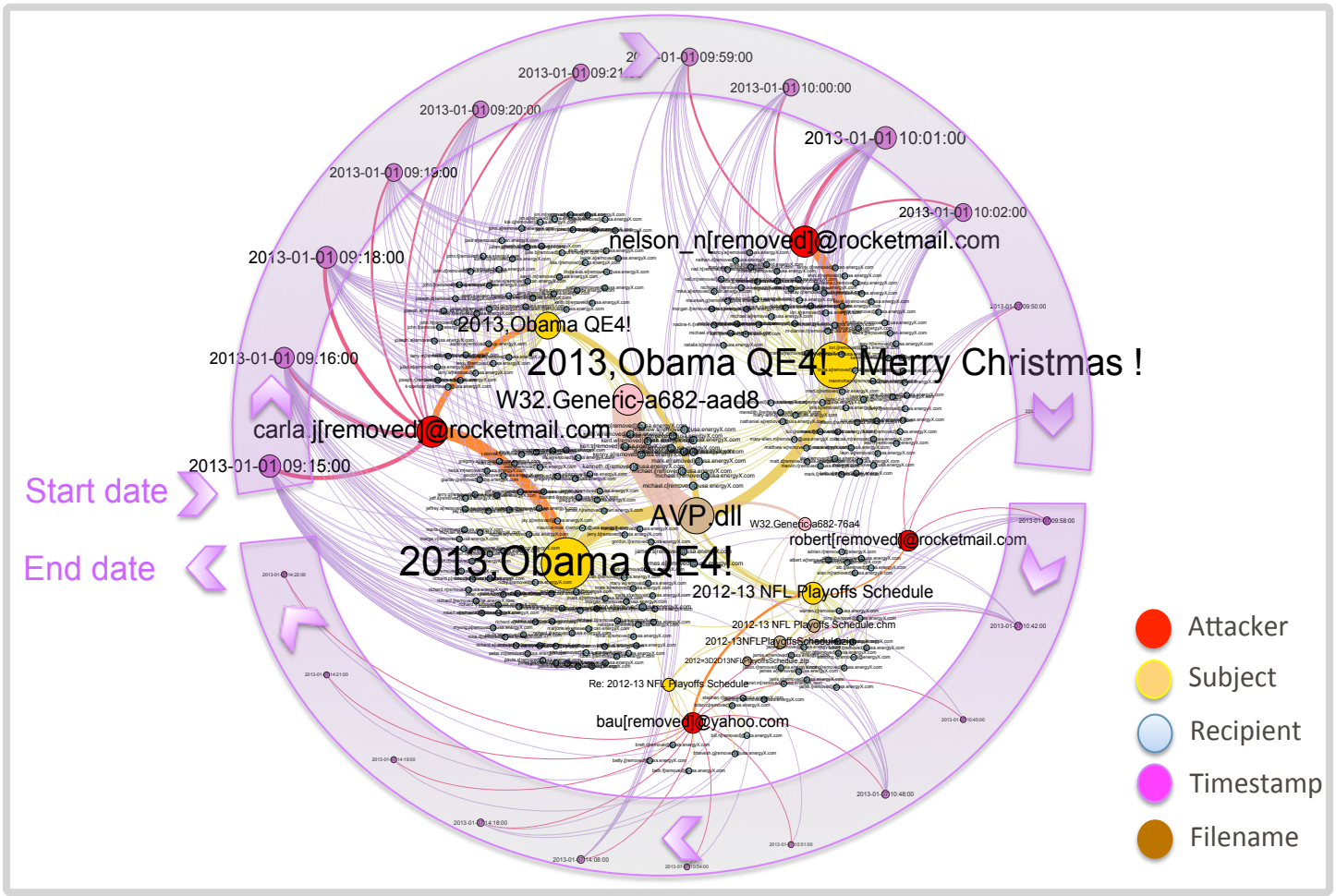


Fig. B.15 The New Year campaign, targeting a large energy research company (zoom for detail)

The Miniduke Campaign – February 20-21, 2013

Another good example of a highly focused attack campaign consisted of a series of targeted attacks launched in February 2013 against governments, which was dubbed "Miniduke" by security experts. The Miniduke campaign targeted dozens of computer systems at government agencies across Europe, in a series of attacks that exploited an Adobe Reader zero-day exploit (subsequently identified as CVE-2013-0640) which was used to drop a previously unknown, advanced piece of malware. An in-depth analysis revealed that this downloader was unique in that every compromised system contained a customized backdoor written in Assembler, suggesting that the authors possessed advanced technical skills. At system boot, the downloader then generated a unique fingerprint on every compromised computer, which was used later to uniquely encrypt the communications with the attacker's servers. An advanced C2 infrastructure had been set up by Miniduke creators, by which all communications between the malware and the C2 servers were initially proxied via Twitter accounts using encoded tweets (or Google searches as a fall-back mechanism); probably as an attempt to fly under the radar, but also to ensure the resilience of their C&C infrastructure.

To compromise their victims, attackers used extremely effective social engineering techniques that involved sending malicious PDF documents with highly relevant topics and well-crafted content informing the victims about a human rights seminar (ASEM), Ukraine's foreign policy, EU-Armenia relationships and NATO membership plans. A sample of email subjects and associated documents and MD5s used in this series of attacks are shown in Figure B.16.

The origins of the attacks (email senders) were identified as being mainly from Armenia, Ukraine, and Korea. Figure B.17 depicts graphically the Miniduke campaign as identified by Symantec's TRIAGE technology. About 208 spear-phishing emails were grouped together and identified as

Fig. B.16

Miniduke Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
Emb of RSA: The 13th Informal ASEM Seminar on Human Rights	ASEM_Seminar.pdf	6945e1fbef586468a6d4f0c4f184af8b ae52908370dcdf6c150b6e2ad3d8b11b 86cc193d9a47fd6a039453159ff35628 a7c89d433f737b3fdc45b9ffbc947c4d
State administration Ukraine: Meeting of the NATO-Ukraine commission	action_plan.pdf	ef90f2927421d61875751a7fe3c7a131 3668b018b4bb080d1875aee346e3650a 151add98eec006f532c635ea3fc205ce ef90f2927421d61875751a7fe3c7a131
MFA of the Republic of Armenia: EU-Armenia Partnership	EUAG_report.pdf	3f301758aa3d5d123a9ddbad1890853b cf5a5239ada9b43592757c0d7bf66169
Armenian MFA: 2013 Economic Meeting in Armenia	The 2013 Armenian Economic Association.pdf	668aaf324ebe42b18e507234281aa772 9c572606a22a756a1fcc76924570e92a cb633268f82f7047c9afa05d1e7f9b19 5ada55c4a39e3280e320b7b6703492dc

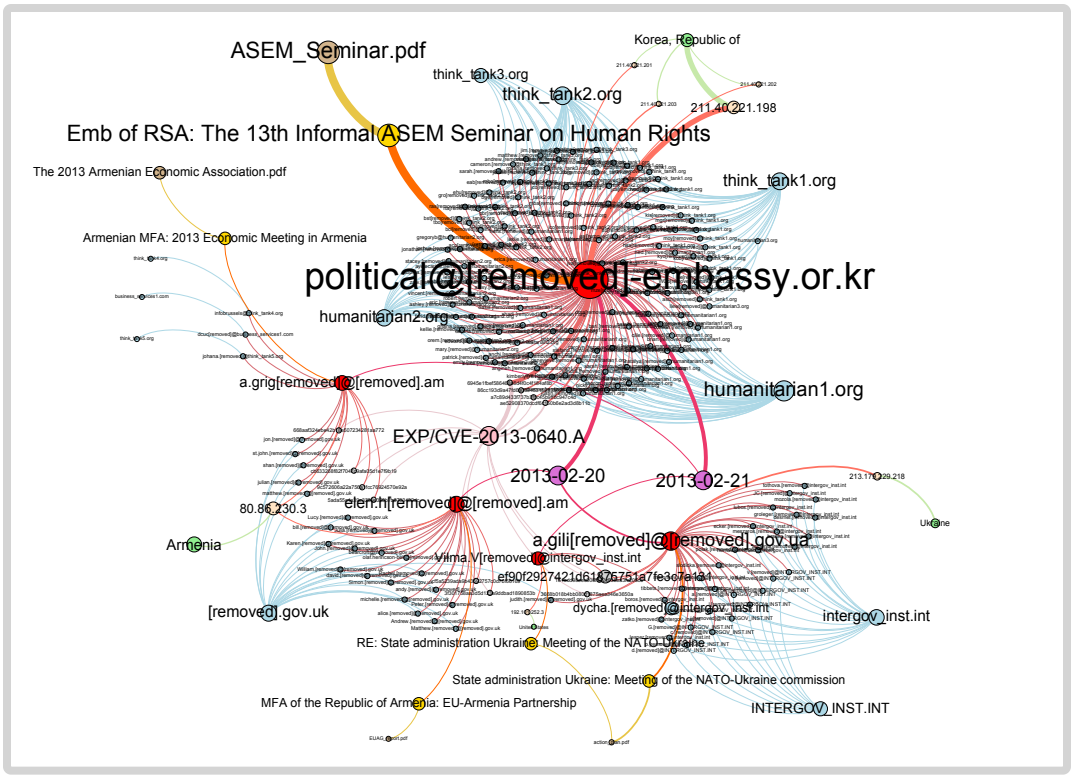


Fig. B.17 The Miniduke campaign (zoom for detail)

being associated with Miniduke. The diagram clearly shows that the bulk of the campaign was sent from a fake email account political@***-embassy.or.kr (whose IP address was mapped to Republic of Korea), targeting 3 different think-tanks and a humanitarian organization using a pdf document containing information on the ASEM human rights seminar.

At least 4 other email accounts (usually spoofed sender addresses) were used by the same group of attackers to target international and governmental institutions on the very same dates (Feb 20-21), this time from IP addresses located in Ukraine and Armenia and using other PDF documents discussing NATO-Ukraine and EU-Armenia political relations.

While we have no visibility into the attacker's ultimate goal, the Miniduke malware was quite likely designed for cyber-espionage and information stealing, just like many other targeted attacks of this kind. However, the sophistication of this cyber attack (in particular the customized malware written in Assembler, and the use of Twitter accounts and Google searches as part of the C2 infrastructure) makes it unusual and quite unique, indicating a type of threat actor that was not observed recently and shows technical traces reminiscent of old-school hackers from the late 1990s. While we can only speculate at this stage regarding the real identity of the authors, the technical indicators[14] and sophistication level of this cyber-attack could very well reflect the involvement, or at least sponsorship, of a nation-state.

As far as we know, Symantec customers have been fully protected from this fairly advanced malware campaign, as the spear-phishing emails sent by Miniduke attackers have been blocked between reaching the mailboxes of their targets.

The Elderwood Campaign: "Focused" does not Always Mean "Small" in Size

While highly targeted cyber-attack campaigns are usually focusing on a limited number of targets, it does not always mean that such campaigns are small in terms of the number of compromise attempts or spear-phishing emails sent by attackers. Unveiled by Symantec in April 2012, the Elderwood project was a good example of an advanced threat group that was capable of launching highly focused, yet large and persistent campaigns. In April 2012, we observed nearly 2,000 spear-phishing emails being sent by the Elderwood attackers within the same campaign to a large number of recipients who were employees of two major defense industries.

The "Elderwood Project"[15] was the name given to the group of attackers behind these targeted attacks, and comes from the exploit communication platform used in some of the attacks. The attack platform developed by this gang also enables them to quickly deploy zero-day exploits.

We have been monitoring the activities of the threat group behind the Elderwood platform for a few years now, which dates back as far as 2009 with the high profile attacks associated with the Hydraq[16] (Aurora) Trojan horse. The Elderwood attackers have consistently targeted a number of industries, and systematically used a number of zero-day exploits against not just the intended target organization, but also on the supply chain manufacturers that service the company in their cross-hairs. The attacking methodology has always used spear-phishing emails, but since 2012 we have observed an increased adoption of watering-hole attacks (compromising certain websites likely to be visited by individuals associated with the target organization) used in combination with spear-phishing emails as additional attack vectors used by the same attackers probably to maximize their success rate.

Serious zero-day vulnerabilities which are exploited in the wild and affect a widely used piece of software are relatively rare. However, the Elderwood attackers were able to exploit no less than four such zero-day vulnerabilities within the same cyber-attack campaign. Although there are other threat groups utilizing zero-day exploits (for example, the Miniduke, Sykipot,[17] Nitro,[18] or even Stuxnet[19] attacks), we have seen no other group use so many. The number of zero-day exploits used indicates access to a high level of technical capability.

Figure B.19 illustrates visually the Elderwood spear-phishing campaign identified by Symantec's advanced TRIAGE technology, which was blocked by Symantec in April 2012. In this campaign, a large number of email accounts (depicted with red nodes) were used by the attackers to send about 1,800 spear-phishing emails (whose subjects are depicted with yellow nodes) to the same amount of employees of two different organizations involved in the defense industry (represented with blue nodes). Only a few different MD5s were used as email attachments to try to compromise the targets, but all documents were dropping the same backdoor connecting to the same C&C servers (denoted with green nodes in the diagram). Interestingly, a large proportion of emails were sent apparently from the same mailer software (Foxmail 6). All email subjects (yellow nodes laid out on the external side of the visualization) were customized to every recipient (by adding his/her user name). The overall patterns visualized in Figure B.19 strongly suggest that attackers were able to automate the sending process of this series of cyber attacks. A sample of email subjects and associated documents and MD5s used in this Elderwood campaign are shown below in Figure B.18.

Fig. B.18

Elderwood Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
Wage Data 2012	page 1-2.doc	c0c83fe9f21560c3be8dd13876c11098
London 2012 Medal Top-Ten	MedalTop10.doc	919708b75b1087f863b6b49a71eb133d
Message from Anne regarding *** Organizational Announcement!	Message_from_PerInge.doc	8b47310c168f22c72a263437f2d246d0
The *** is in the unpromising situation after acquisition by ***	create.doc	4525759c6452f2855ca815277f519684
Hi, [REM]. I heard about the consolidation of ***, is that true?	Consolidation Schedule.doc	78c3d73e2e2bba6d8811c5dc39edd600
Invitation Letter to LED Industry Summit 2012.	[REM] Invitation Letter to LED Industry Summit 2012.doc	4525759c6452f2855ca815277f519684 84a1405c9e96c037a9d332def39f2d29

A few striking elements are standing out in Figure B.19, where we can identify some less volatile email features, such as:

- Mailer software used by attackers (which in most cases was Foxmail 6, 14, 103, 30 [cn], but also in a limited number of attacks, KooMail 5.41 [En] was also used to send emails).
- Domain name and IP address used as part of the C&C infrastructure (green nodes in the center).
- Limited number of email accounts (webmail1.com[20]) used to send attack emails in separate batches to subsets of recipients.

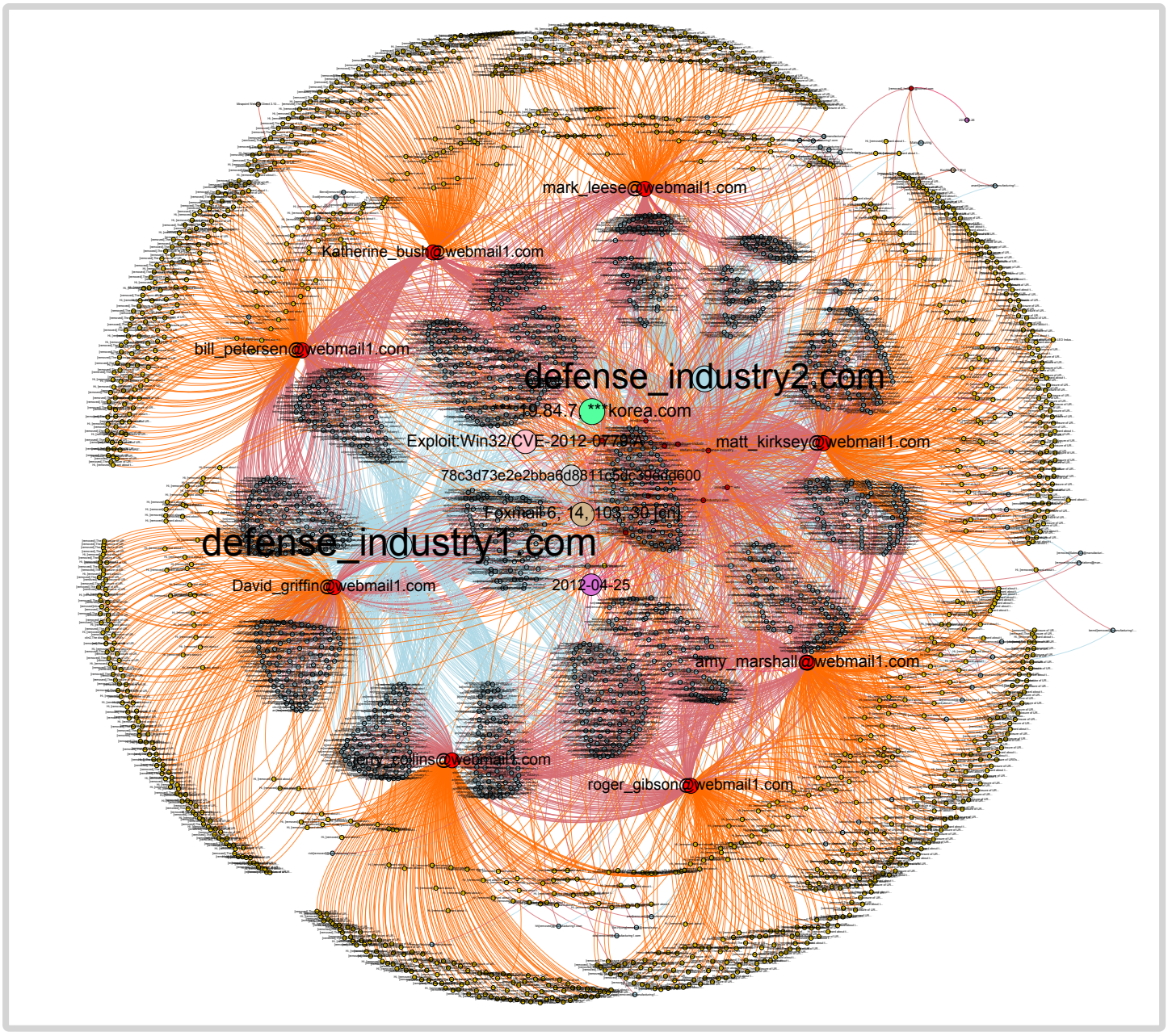


Fig. B.19 The Elderwood campaign: A highly focused campaign but large in size and likely automated (zoom for detail)

Type 2 – Mass-scale Organizational Targeted Attacks (MOTA)

One third of targeted attacks are organized on a larger-scale and fit the profile of what we call a Mass-scale Organizationally Targeted Attack (MOTA): they target a large number of people in multiple organizations working in different sectors over multiple days. As described earlier, we used a threshold of five different companies, active in five completely different sectors to classify attack campaigns and label them as "Mass-scale" (MOTA) versus "highly focused". Most of the large-scale campaigns are very well resourced, with up to four different exploits used during the same campaign.

One example of attacker group that is typically responsible for organizing MOTA-like campaigns is APT1, also known as "CommentCrew". An example of a campaign attributed to CommentCrew is visualized in Figure B.20. During this campaign, about 1,200 attack emails were sent from 44 email accounts (red nodes) to 191 different recipients (blue nodes) who are employees working in more than 20 different companies, active mainly in sectors such as Aerospace, Defense, Engineering, Satellite communications and Governmental organizations. Attack emails were sent on 10 different dates, however the whole campaign lasted for more than two months in April/May 2012. During this timeframe CommentCrew attackers were able to craft a significant number of very diverse phishing emails, all of them containing malicious documents exploiting various vulnerabilities in MS Office or Adobe software, in attempts to compromise their victims. A sample of email subjects and associated documents and MD5s used in this series of attacks are shown below in Figure B.21.

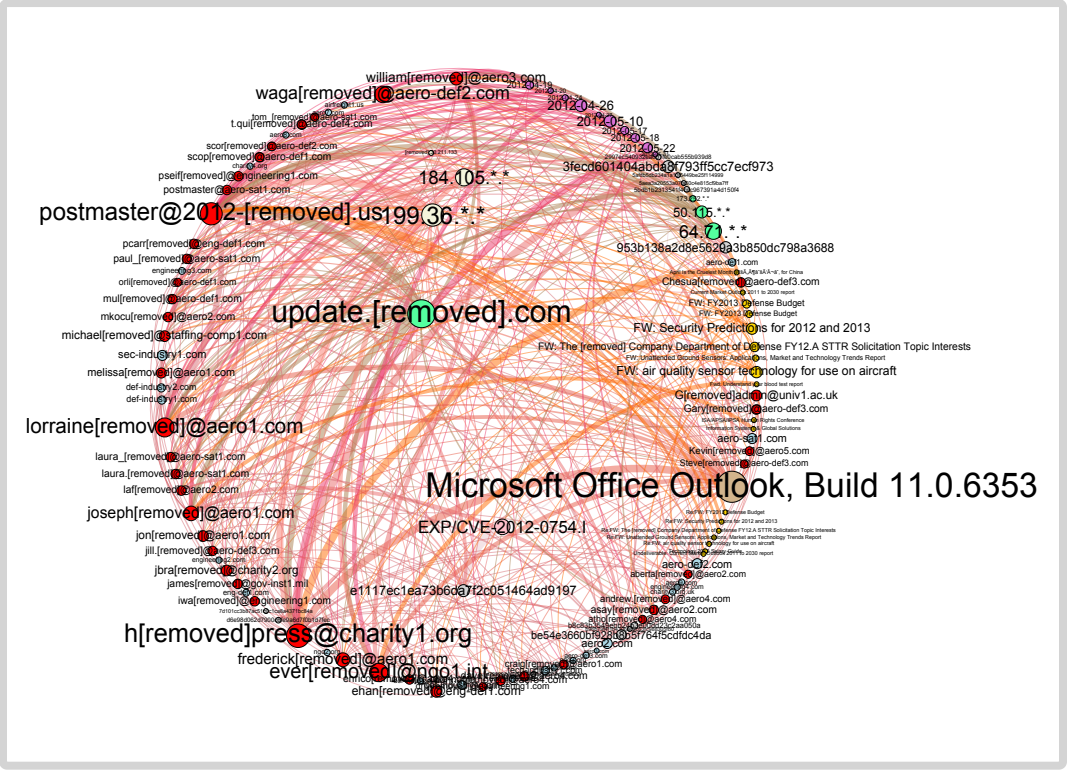


Fig. B.20 A campaign of attacks attributed to the CommentCrew group (April-May 2012) (zoom for detail)

Fig. B.21

APT1 Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
April Is the Cruelest Month … for China	April Is the Cruelest Month.pdf	5afdb5db234a1a13f5449be25f114999 2997ec540932ea6b1fe0cab555b939d8
FW: air quality sensor technology for use on aircraft	sensor environments.doc	3fecd601404abda8f793ff5cc7ecf973
FW: Security Predictions for 2012 and 2013	Security Predictions for 2012 and 2013.pdf	e1117ec1ea73b6da7f2c051464ad9197 d795292ea23217480ad92939daf6dd22
FW: FY2013 Defense Budget	FY2013_Budget_Request_Overview_Book.pdf	953b138a2d8e5629a3b850dc798a3688
Fwd: Understand your blood test report	Understand your blood test report.pdf	5aea3a20553a07fa50c4e815cf9ba7ff
Information Systems & Global Solutions	Schedule_list.pdf	b96b79f4f1b4306ac2c63fc988305fb0
FW: The *** Company Department of Defense FY12.A STTR Solicitation Topic Interests	Dept of Defense FY12 A STTR Solicitation Topics of Interest to <aerospace comp>.pdf	be54e3660bf928b8b5f764f5cdfdc4da
Current Market Outlook 2011 to 2030 report	[REM]_Current_Market_Outlook_2011_to_2030.pdf	d6e98d062d7900c6fe9a6d7f0b1d7fec
Technology 2012 Salary Guide	RHT_SalaryGuide_2012.pdf	5bdb1b2313541f4cdc967391a4d150f4
ISA/APSA/IPSA Human Rights Conference	HR 2012 Conference Program .doc	7d101cc3b87ac51c0c1ca8a4371bc84a
Re:FW: air quality sensor technology for use on aircraft	sensor environments.doc	3fecd601404abda8f793ff5cc7ecf973

Symantec's TRIAGE technology also identified another spear-phishing campaign attributed to CommentCrew, which took place on January 16, 2013, and is illustrated in Figure B.22. This attack campaign occurred a few weeks before the release by Mandiant of a report exposing Comment-Crew's multi-year, enterprise-scale computer espionage campaigns, in which they investigated computer security breaches made by the CommentCrew group at hundreds of organizations around the world. According to many experts, CommentCrew is one of the most prolific cyber-espionage groups in terms of the sheer quantity of information stolen.

Although our visibility of CommentCrew's activities is likely to be incomplete, we could analyze a number of intrusions that this threat group conducted against more than 30 companies just in the last 2 years. Figure B.22 shows one of the last series of targeted attacks performed by the group that we could observe just before the publication of Mandiant's report on their espionage activities. About 77 victims working in 16 different companies were targeted using the very same document (*Global_A&D_outlook_2012.pdf - 578de4091ed0b2752012668d59828fe2*) and similar email topics (*FW:2012 Global aerospace and defense industry outlook*). However, CommentCrew attackers have used different fake email accounts to conduct their attacks, as shown in the diagram in Figure B.22.

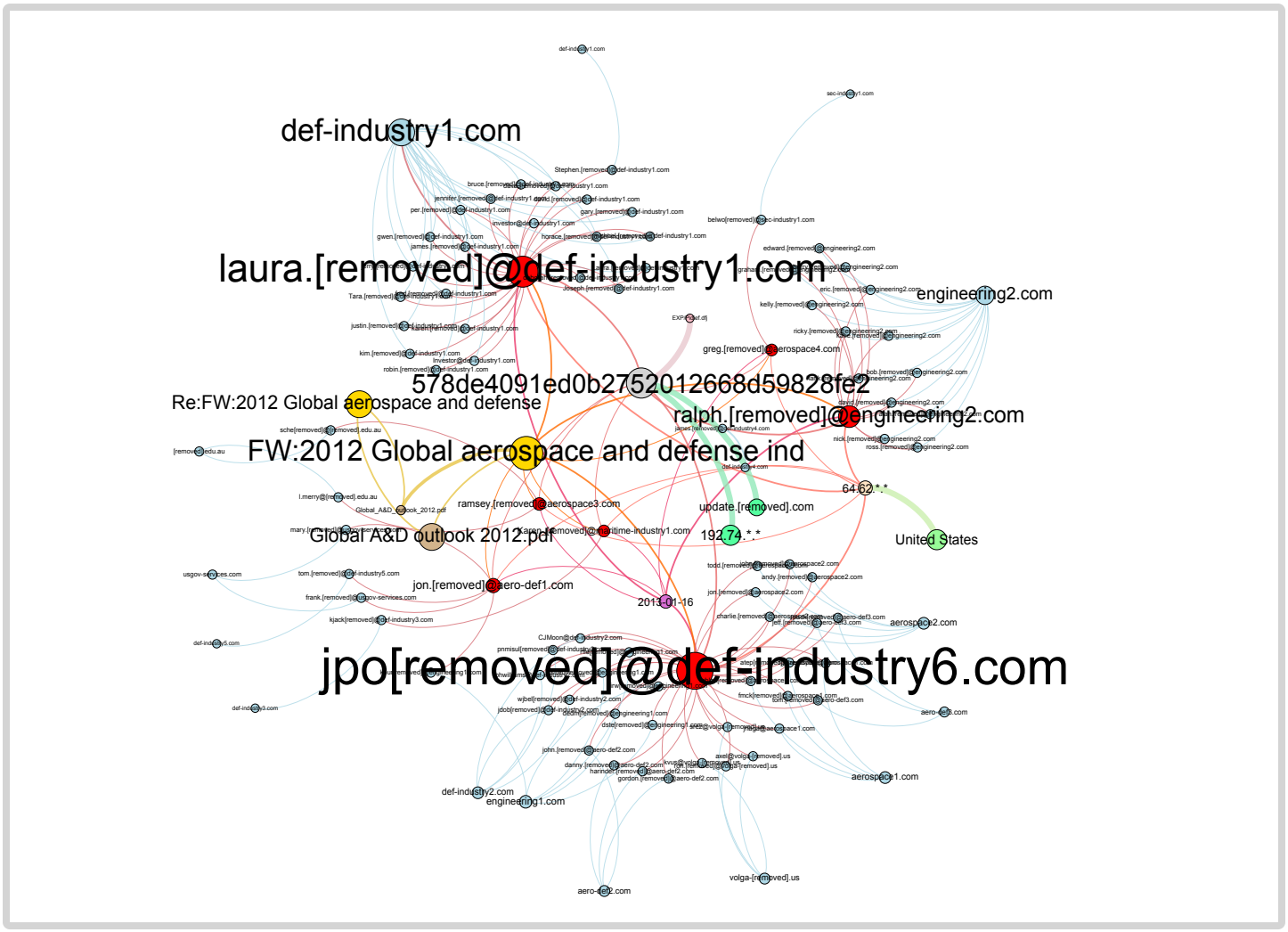


Fig. B.22 CommentCrew campaign identified in January 2013. (zoom for detail)

Footnotes

01 http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99

02 http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99

03 http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

04 CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.

05 Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

06 Developed by Symantec in the context of the European funded WOMBAT research project (http://www.wombat-project.eu), TRIAGE is a novel attack attribution method based on a multi-criteria decision algorithm. TRIAGE is currently improved and enriched with Visual Analytics technologies in the context of another European funded research project named VIS-SENSE (http://www.vis-sense.eu), in which Symantec collaborates with five other partners.

07 http://www.vis-sense.eu

08 Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. An analysis of rogue AV campaigns. In Proc. of the 13th International Conference on Recent Advances in Intrusion Detection (RAID), 2010.

09 O.Thonnard, M.Dacier. A Strategic Analysis of Spam Botnets Operations. CEAS'11, Perth, WA, Australia, Sep 2011.

10 Jelena Isacenkova, Olivier Thonnard, Andrei Costin, Davide Balzarotti, Aurelien Francillon. Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. International Workshop on Cyber Crime (IWCC 2013), IEEE S&P Workshops, 2013.

11 Olivier Thonnard, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, Martin Lee. Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat. In Proc. Of the 15th International conference on Research in Attacks, Intrusions, and Defenses (RAID), 2012.

12 Symantec Internet Security Threat Report (ISTR), Volume 17, April 2012.

13 Targeted recipients and domains were mapped to industry sectors based on the SIC taxonomy. This allows us to collect statistics on the prevalence of targeted attacks in various industry sectors.

14 http://www.symantec.com/security_response/writeup.jsp?docid=2013-030119-2820-99

15 http://www.symantec.com/connect/blogs/elderwood-project

16 http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99

17 http://www.symantec.com/security_response/writeup.jsp?docid=2010-031015-0224-99

18 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

19 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

20 Domain names have been anonymized or obfuscated for privacy reasons.

APPENDIX :: C
SPAM + FRAUD ACTIVITY TRENDS

Spam and Fraud Activity Trends

This section covers phishing and spam trends. It also discusses activities observed on underground economy-type servers as this is where much of the profit is made from phishing and spam attacks.

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they can then use to commit fraudulent acts. Phishing generally requires victims to provide their credentials, often by duping them into filling out an online form. This is one of the characteristics that distinguish phishing from spam-based scams (such as the widely disseminated "419 scam"[1] and other social engineering scams).

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver Trojans, viruses, and phishing attacks. Spam can also include URLs that link to malicious sites that, without the user being aware of it, attack a user's system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email services.

This section includes the following metrics:

- Analysis of Spam Activity Trends
- Analysis of Spam Activity by Geography, Industry Sector, and Company Size
- Analysis of Spam Delivered by Botnets
- Significant Spam Tactics
- Analysis of Spam by Categorization
- Phishing Activity Trends
- Analysis of Phishing Activity by Geography, Industry Sector, and Company Size
- New Spam Trend: BGP Hijacking

Analysis of Spam Activity Trends

Background

This section discusses the patterns and trends relating to spam message volumes and the proportion of email traffic identified as spam during 2013.

Methodology

The analysis for this section is based on global spam and overall email volumes for 2013. Global values are determined based on the statistically representative sample provided by Symantec Messaging Gateway[2] operations, and the spam rates include spam blocked by Symantec.cloud.

Commentary

- There were approximately 29 billion spam emails in circulation worldwide each day in 2013, compared with 30 billion in 2012; a decrease of 3.3 percent in global spam volume.
- Overall for 2013, 66.4 percent of email traffic was identified as spam, compared with 68.5 percent in 2012; a decrease of 1.9 percentage points.

Fig. C.1

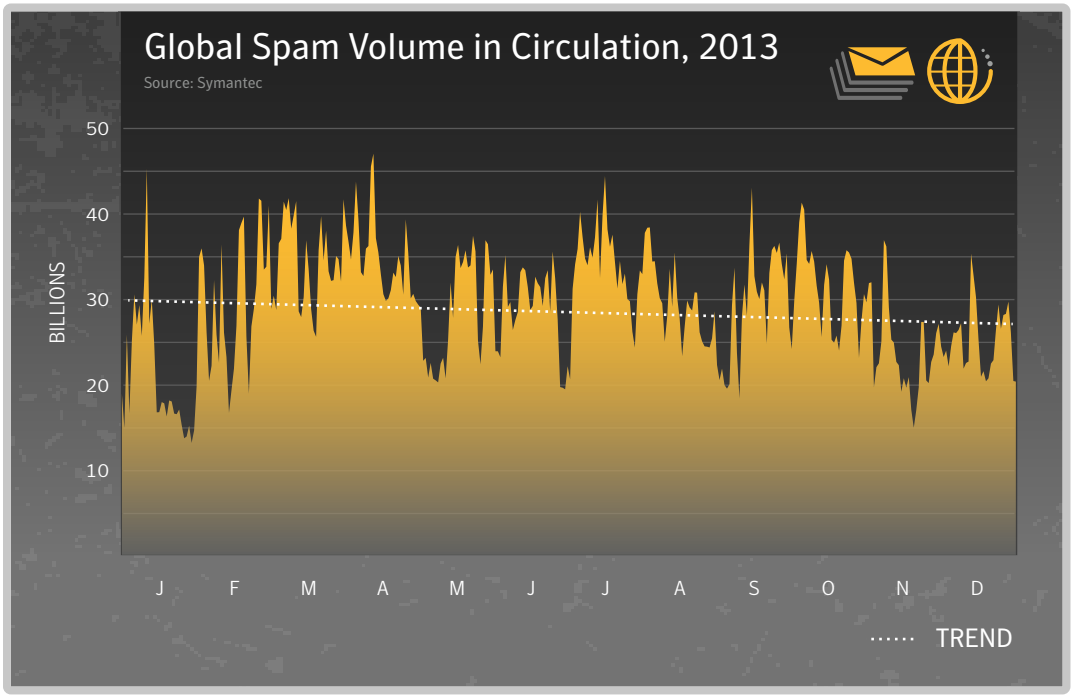
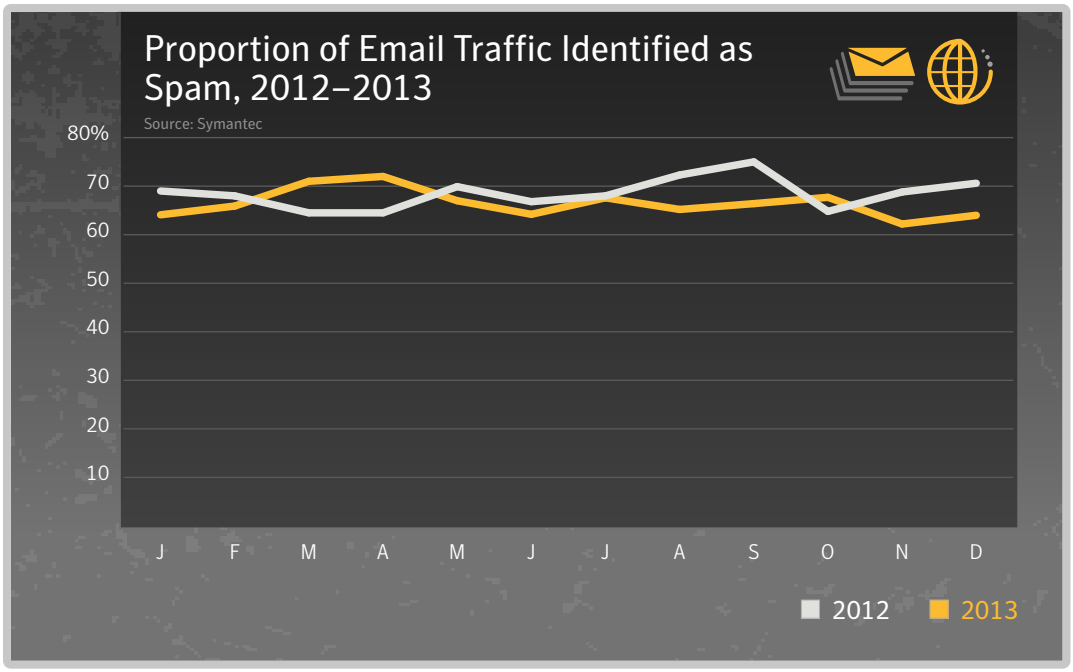


Fig. C.2


Proportion of Email Traffic Identified as Spam, 2012–2013
Source: Symantec
80%
70
60
50
40
30
20
10
J
F
M
A
M
J
J
A
S
O
N
D
2012
2013

Analysis of Spam Activity by Geography, Industry Sector, and Company Size

Background

Spam activity trends can also reveal patterns that may be associated with particular geographical locations, or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace that can drive down prices, increasing adoption rates. There may also be other factors at work, based on the local economic conditions that present different risk factors. Similarly the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat, by the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a spam attack because they are perceived to be a softer target than larger organizations. They are likely to have less-stringent security countermeasures than larger organizations, which are more likely to apply greater resources to their anti-spam and security countermeasures.

Methodology

Analysis of spam activity based on geography, industry and size is determined from the patterns of spam activity for Symantec. cloud clients for threats during 2013.

Fig. C.3

Proportion of Email Traffic Identified as Spam by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013 Spam	2012 Spam
Finance	73.0%	67.8%
Education	67.4%	70.5%
Chem/Pharm	66.5%	68.5%
Non-Profit	66.4%	69.6%
Manufacturing	66.0%	69.1%
Marketing/Media	65.9%	69.3%
Accom/Catering	65.9%	68.7%
Recreation	65.7%	69.0%
Gov/Public Sector	65.5%	68.9%
Agriculture	65.4%	68.9%

Fig. C.4

Proportion of Email Traffic Identified as Spam by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013 Spam	2012 Spam
1-250	70.4%	68.4%
251-500	65.4%	68.2%
501-1000	65.2%	68.3%
1001-1500	65.6%	68.8%
1501-2500	65.6%	68.9%
2501+	65.6%	68.4%

Fig. C.5

Proportion of Email Traffic Identified as Spam by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013 Spam	2012 Spam
Saudi Arabia	78.2%	79.1%
Sri Lanka	75.7%	73.1%
China	71.3%	73.3%
Hungary	71.1%	74.2%
Qatar	69.9%	72.6%
Brazil	69.7%	72.5%
Ecuador	69.6%	71.2%
Greece	68.9%	67.7%
Poland	68.6%	71.2%
India	68.5%	70.4%

Commentary

- The spam rate decreased across all top-ten geographies in 2013. The highest rate of spam is for organizations in Saudi Arabia, with an overall average spam rate of 78.2 percent. In 2012 the highest rate was also in Saudi Arabia, with an overall average spam rate of 79.1 percent.
- The spam rate decreased across all top-ten industry sectors in 2013 except for Finance, in which organizations were subjected to the highest spam rate of 73.0 percent. In 2012, the Marketing/Media sector had the highest spam rate of 69.3 percent.
- The spam rate decreased for all sizes of organization in 2013, except for small to medium-sized businesses with 1-250 employees. These organizations accounted for 70.4 percent of spam compared to 68.4 percent in 2012.
- 65.6 percent of emails sent to large enterprises with more than 2,500 employees in 2013 were identified as spam, compared with 68.4 percent in 2012.

Analysis of Spam Delivered by Botnets

Background

This section discusses botnets and their use in sending spam. Similar to how ballistic analysis can reveal the gun used to fire a bullet, botnets can be identified by common features within the structure of email headers and corresponding patterns during the SMTP[3] transactions. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis only reviews botnets involved in sending spam, and does not look at botnets used for other purposes such as financial fraud or DDoS attacks.

Methodology

Symantec.cloud spam honeypots collected approximately 15 million spam emails each day during 2013. These were classified according to a series of heuristic rules applied to the SMTP conversation and the email header information.

A variety of internal and external IP reputation lists were also used in order to classify known botnet traffic based on the source IP address of the sending machine. Information is shared with other security experts to ensure the data is up-to-date and accurate.

Fig. C.6

Top Sources of Botnet Spam by Location, 2013

Source: Symantec.cloud

Location of Botnet Activity	Percentage of Botnet Spam
India	6.6%
United States	5.9%
Spain	5.2%
Argentina	5.1%
Peru	4.4%
Italy	3.9%
Iran	3.1%
Russia	2.9%
Colombia	2.9%
Vietnam	2.7%

Fig. C.7

Analysis of Spam-Sending Botnet Activity at the End of 2013

Source: Symantec.cloud

Botnet Name	Percentage of Botnet Spam	Est. Spam Per Day	Top Sources of Spam From Botnet		
KELIHOS	46.90%	10.41BN	Spain 8.4%	United States 7.2%	India 6.6%
CUTWAIL	36.33%	8.06BN	India 7.7%	Peru 7.5%	Argentina 4.8%
DARKMAILER	7.21%	1.60BN	Russia 12.4%	Poland 8.3%	United States 8.1%
MAAZBEN	2.70%	598.12M	China 23.6%	United States 8.2%	Russia 4.8%
DARKMAILER3	2.58%	573.33M	United States 18.2%	France 10.4%	Poland 7.5%
UNCLASSIFIED[4]	1.17%	259.03M	China 35.1%	United States 10.0%	Russia 7.5%
FESTI	0.81%	178.89M	China 21.9%	Russia 5.8%	Ukraine 4.7%
DARKMAILER2	0.72%	158.73M	United States 12.6%	Belarus 8.3%	Poland 6.6%
GRUM	0.53%	118.00M	Russia 14.5%	Argentina 6.9%	India 6.9%
GHEG	0.35%	76.81M	Poland 17.4%	Vietnam 12.1%	India 11.5%

Commentary

- In 2013, approximately 76 percent of spam email was distributed by spam-sending botnets, compared with 79 percent in 2012. Ongoing actions to disrupt a number of botnet activities during the year helped to contribute to this gradual decline.
- The takedown of ZeroAccess Botnet resulted in the disruption of over half a million bots controlled by the botmaster.[5]
- The top two spam botnets, Kelihos and Cutwail were responsible for more than 83 percent of spam, generating an estimated 10 billion and 8 billion spam emails each day, respectively.
- India was top of the spam-sending botnet table in 2013, and was the source of approximately 6.6 percent of global botnet spam, 0.7 percentage points higher than the United States.

Significant Spam Tactics

Background

This section discusses significant spam tactics used throughout 2013, including the size of spam messages and the languages used in spam emails.

Fig. C.8

Frequency of Spam Messages by Size, 2013

Source: Symantec

Size	<5KB	5KB-10KB	10KB-50kb	50KB-100KB	>100KB
Percentage of Spam	32.8%	29.5%	27.0%	0.8%	1.0%

Fig. C.9

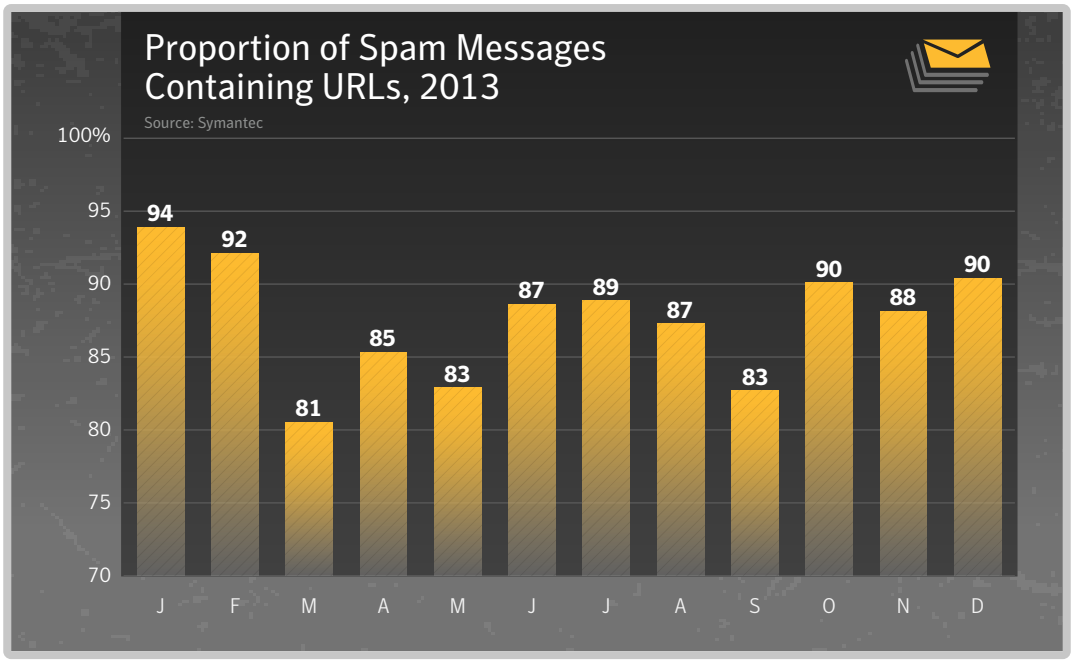


Fig. C.10

Analysis of Top-Level Domains Used in Spam URLs, 2013

Source: Symantec

Domains	Spam Percentage
.com	33.3%
.ru	22.9%
.pl	35.5%
.info	10.2%
.net	6.5%

Commentary

- In 2013, 32.8 percent of spam messages were less than 5KB in size. For spammers, smaller file sizes mean more messages can be sent using the same resources.
- Increased sizes are often associated with malicious activity, where email attachments contain malicious executable code.
- In 2013, 87.3 percent of spam messages contained at least one URL hyperlink, compared with 86.1 percent in 2012.
- In 2013, 35.5 percent of spam URLs were domains registered in the .pl top-level domain (TLD).
- The second most frequently used TLD was .com, which accounted for approximately 33.3 percent of all spam URL domains.
- The third most frequently used TLD was .ru, which is the top-level country code domain for Russia and accounted for approximately 22.9 percent of all spam URL domains.

Analysis of Spam by Categorization

Background

Spam is created in a variety of different styles and complexities. Some spam is plain text with a URL, while others are cluttered with images and/or attachments. Some are constructed with very little in terms of text, perhaps only a URL. And, of course, spam is distributed in a variety of different languages. It is also common for spam to contain "Bayes poison" – random text added to messages that has been haphazardly scraped from websites, with the purpose of "polluting" the spam with words bearing no relation to the intent of the spam message itself. Bayes poison is used to thwart spam filters that typically try to deduce spam based on a database of words that are frequently repeated in spam messages.

Any automated process to classify spam into categories needs to overcome this randomness issue. For example, the word "watch" may appear in the random text included in a pharmaceutical spam message, posing a challenge whether to classify the message as pharmaceutical spam or in the watches/jewelry category. Another challenge occurs when a pharmaceutical spam contains no words with an obvious relation to pharmaceuticals, but instead only contain an image and a URL.

Spammers attempt to get their messages through to recipients without revealing too many clues that the message is spam. Clues found in the plain text content of the email can be examined using automated anti-spam techniques. A common way to overcome automated techniques is by using random text. An equally effective way is to include very little in the way of extra text in the spam, instead including a URL in the body of the message.

Spam detection services often resist classifying spam into different categories because it is difficult to do (for the reasons above), and because the purpose of spam detection is to determine whether the message is spam and to block it rather than to identify its subject matter. In order to overcome the ambiguity faced by using automated techniques to classify spam, the most accurate way to do it is to have someone classify unknown spam manually. While time-consuming, this process provides much more accurate results. An analyst can read the message, understand the context of the email, view images, follow URLs, and visit websites in order to gather the bigger picture around the spam message.

Methodology

Once per month, several thousand random spam samples are collected and classified by Symantec.cloud using a combination of electronic and human analysis into one of the following categories:

- Casino/Gambling
- Degrees/Diplomas
- Diet/Weight Loss
- Jobs/Money Mules
- Malware
- Mobile Phones
- Pharmaceutical
- Phishing
- Scams/Fraud/419s
- Sexual/Dating
- Software
- Unknown/Other
- Unsolicited Newsletters
- Watches/Jewelry

Fig. C.11

Spam by Category, 2013

Source: Symantec.cloud

Category	2013	2012	Change (percentage points)
Pharmaceutical	17.7%	21.1%	-3.4
Watches/Jewelry	2.8%	9.2%	-6.4
Sexual/Dating	69.7%	54.6%	+15.1
Unsolicited Newsletters	0.1%	7.4%	-7.3
Casino/Gambling	0.6%	1.6%	-1.0
Diet/Weight Loss	1.1%	1.0%	+0.1
Malware	0.1%	1.9%	-1.8
Unknown/Other	1.0%	2.4%	-1.4%
Scams/Fraud/419s	0.2%	0.4%	-0.2
Software	0.9%	2.1%	-1.2
Jobs/Money Mules	6.2%	4.4%	+1.8
Degrees/Diplomas	0.1%	0.3%	-0.1
Mobile Phones	0.4%	0.6%	-0.2
Phishing	0.2%	0.4%	-0.2

Commentary

- Adult Spam dominated in 2013, with more than two-thirds (69.7 percent) of all spam related to adult spam, an increase of 15.1 percentage points compared with 2012. These are often email messages inviting the recipient to connect to the scammer through instant messaging, or a URL hyperlink where they are then typically invited to a pay-per-view adult-content webcam site. Often any IM conversation would be handled by a bot responder, or a person working in a low-pay, offshore call center.
- A category with a low percentage still means millions of spam messages. Although it is difficult to be certain what the true volume of spam in circulation is at any given time, Symantec estimates that approximately 29 billion spam emails were sent globally each day in 2013. Where some of the categories listed earlier represent 0.4 percent of spam, this figure equates to more than 120 million spam emails in a single day.
- Spam related to Watches/Jewelry, Casino/Gambling, Unsolicited Newsletters and Scams/Fraud all decreased.

Phishing Activity Trends

Background

This section discusses the proportion of malicious email activity that is categorized as phishing attacks and looks more closely at emerging trends, particularly social engineering techniques and how attackers can automate the use of RSS news feeds to incorporate news and current affairs stories into their scams.

Methodology

The data for this section is based on the analysis of email traffic collected from Symantec.cloud global honeypots, and from the analysis of malicious and unwanted email traffic data collected from customers worldwide. The analysis of phishing trends is based on emails processed by Symantec.cloud Skeptic™ technology[6] and emails collected in spam honeypots. Symantec.cloud spam honeypots collected approximately 15 million spam emails each day during 2013.

Fig. C.12

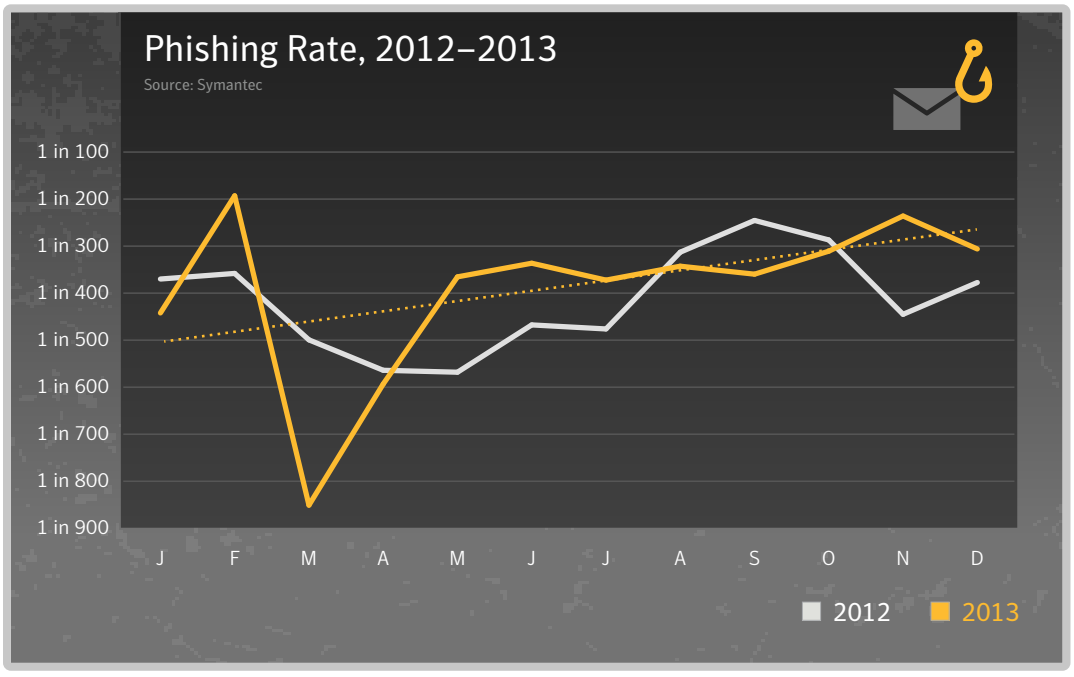


Fig. C.13

Phishing Category Types, Top 200 Organizations, 2013

Source: Symantec.cloud

Sectors	Phishing Percentage
Financial	71.7%
Information Services	21.0%
Others	7.0%
Government	0.2%

Others	Phishing Percentage
Telecommunications	5.2%
Retail	47.0%
Communications	10.7%
Retail Trade	0.6%
Security	0.1%
ISP	0.4%
Insurance	0.4%
Aviation	0.1%
Computer Software	25.5%
Entertainment	6.4%
Electronics	0.0%
Energy	3.3%

Fig. C.14

Tactics of Phishing Distribution, 2013

Source: Symantec.cloud

Attack Type	Phishing Percentage
Typosquatting	1.1%
Free Web Hosting Sites	3.7%
IP Address Domains	4.9%
Other Unique Domains	41.0%
Automated Toolkits	49.3%

Commentary

- Overall for 2013, 1 in 392.4 emails was identified and blocked as a phishing attack, compared with 1 in 414.3 in 2012.
- 70.9 percent of phishing attacks in 2013 related to spoofed financial organizations, compared with 67.3 percent in 2012
- Phishing attacks on organizations in the Information Services sector accounted for 21.8 percent of phishing attacks in 2013
- Phishing URLs spoofing banks attempt to steal a wide variety of information that can be used for identity theft and fraud. Attackers seek information such as names, government-issued identification numbers, bank account information, and credit card numbers. Cybercriminals are more focused on stealing financial information that can make them large amounts of money quickly versus goods that require a larger time investment, such as scams.
- 49.3 percent of phishing attacks were conducted through the use of phishing toolkits.
- In 2013 there was an increase in phishing activity spoofing energy companies, and mimicking vendors of online loyalty point schemes such as those collected whilst travelling long-haul flights. The reported increase in phishing activity against energy companies was relatively new, and was not reflected in the detailed analysis above. However, this will present a worrying trend if it continues to rise, since some energy companies may incentivize its customers to switch to paperless billing, and a successful phishing attack against an online account may then provide the attacker with enough information to open a false finance account using an online energy bill as proof of identity.

Analysis of Phishing Activity by Geography, Industry Sector, and Company Size

Background

Phishing activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots, for example the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a spam attack because SMBs are perceived to be a softer target as they are less likely to have the same levels of defense-in-depth as a larger organization, who tend to have greater budgetary expenditure applied to anti-spam and security countermeasures.

Methodology

Analysis of phishing activity based on geography, industry and size is determined from the patterns of spam activity for Symantec.cloud clients for threats during 2013.

Fig. C.15

Proportion of Email Traffic Identified as Phishing by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013	2012
Public Sector	1 in 216.4	1 in 95.4
Education	1 in 568.8	1 in 222.8
Accom/Catering	1 in 594.5	1 in 297.4
Marketing/Media	1 in 752.1	1 in 355.2
Finance	1 in 767.7	1 in 211.1
Non-Profit	1 in 780.6	1 in 362.3
Estate Agents	1 in 977.9	1 in 448.6
Prof Services	1 in 1,155.4	1 in 510.9
Agriculture	1 in 1,173.6	1 in 450.8
General Services	1 in 1,185.0	1 in 397.7

Fig. C.16

Proportion of Email Traffic Identified as Phishing by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013	2012
1-250	1 in 689.5	1 in 293.8
251-500	1 in 1,075.9	1 in 500.8
501-1000	1 in 1,574.6	1 in 671.1
1001-1500	1 in 1,309.8	1 in 607.0
1501-2500	1 in 1,709.3	1 in 739.1
2501+	1 in 844.7	1 in 346.0

Fig. C.17

Proportion of Email Traffic Identified as Phishing by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013	2012
South Africa	1 in 419.8	1 in 176.6
United Kingdom	1 in 454.1	1 in 190.6
Italy	1 in 873.5	1 in 520.0
Australia	1 in 906.4	1 in 426.0
Austria	1 in 1,049.0	1 in 611.6
Canada	1 in 1,059.3	1 in 400.2
Netherlands	1 in 1,115.9	1 in 123.1
Brazil	1 in 1,761.3	1 in 735.2
Denmark	1 in 1,768.6	1 in 374.3
New Zealand	1 in 1,784.7	1 in 740.0

Commentary

- The phishing rate has significantly decreased for all of the top-ten geographies in 2013. The highest average rate for phishing activity in 2013 was for organizations in South Africa, with an overall average phishing rate of 1 in 419.8. In 2012, the highest rate was for Netherlands, with an overall average phishing rate of 1 in 123.1.
- The phishing rate has decreased across all of the top-ten industry sectors in 2013. Organizations in the Government and Public Sector were subjected to the highest level of phishing activity in 2013, with 1 in 216.4 emails identified and blocked as phishing attacks. In 2012 the sector with the highest average phishing rate was also the Government and Public Sector, with a phishing rate of 1 in 95.4.
- The phishing rate has decreased for all sizes of organization in 2013. 1 in 844.7 emails sent to large enterprises with more than 2,500 employees in 2013 were identified and blocked as phishing attacks, compared with 1 in 346.0 in 2012.
- 1 in 689.5 emails sent to businesses with up to 250 employees in 2013 were identified and blocked as phishing attacks, compared with 1 in 293.8 in 2012.

New Spam Trend: BGP Hijacking

Background

The Internet is divided into thousands of smaller networks called Autonomous Systems (ASes), each of them belonging a single entity (e.g., an Internet Service Provider, a company, a university). Routing between ASes is achieved using the Border Gateway Protocol (BGP), which allows ASes to advertise to others the addresses of their network and receive the routes to reach the other ASes.

Each AS implicitly trusts the peer ASes it exchanges routing information with. BGP hijacking is an attack against the routing protocol that consists in taking control of blocks of IP addresses owned by a given organization without its authorization. This enables the attacker to perform other malicious activities (e.g. spamming, phishing, malware hosting) using hijacked IP addresses belonging to somebody else.

In the Symantec Internet Security Threat Report 2012[7] we introduced a new phenomenon where so-called "fly-by spammers" temporarily steal (or hijack) blocks of network IP addresses and use them to send spam and hinder their traceability. We presented a real-world case study involving a very sophisticated spammer who hijacked someone else's network for several months in 2011 before the victim network owner eventually noticed and regained control over his network. Although at that time we presented only one confirmed case of spammers behaving this way, we envisioned that such phenomenon would become more prevalent.

It is important to detect such malicious BGP hijacks. First, such attacks can lead to misattributing other attacks, such as denial of service attacks, launched from hijacked networks due to hijackers stealing IP identity. Correctly attributing attacks is critical when responding with possible legal action. Second, spam filters heavily rely on IP reputation systems, such as spam sender blacklists, to filter out emails coming from known spam networks. Sending spam from a hijacked network with a good reputation can thus defeat such protections.

Methodology

Studying fly-by spammers' operations involves (1) identifying spam-emitting networks and (2) determining whether these networks have been stolen (or hijacked) from their legitimate owner. A tool called SpamTracer has been developed within Symantec Research Labs to track and study fly-by spammers. SpamTracer monitors the routes towards spam networks identified by Symantec.cloud, to detect when spammers manipulate the Internet routing to steal (or hijack) network IP addresses and launch spam campaigns using those addresses.

Commentary

A detailed analysis of data collected by SpamTracer between January and July 2013 led to identification of 29 hijacked network IP address blocks. We further examined these cases and uncovered a common *modus operandi* used by spammers to hijack the networks.

Fly-by spammers ***modus operandi*****:** Spammers hijacked dormant network IP address blocks, i.e. by the time the networks were hijacked they had been left idle by their owner. This situation can result, for example, from an organization going out of business without properly returning its assigned network addresses leaving them in a dormant state. Spammers also advertised the hijacked IP address blocks in BGP using the AS of their legitimate owner in an effort not to raise suspicion and to remain stealthy. Finally, hijacks were short-lived, lasting from several minutes to a few days.

We can see through this *modus operandi* that fly-by spammers really try not to raise suspicion, remaining stealthy. First, they hijack dormant networks allowing them to avoid any disruption that would result from hijacking a network actively used by its owner. Second, they advertise the hijacked networks in BGP in a way that appears to be advertised by their legitimate owner. Finally, they hijack networks for a short period of time to send spam using the stolen addresses and quickly disappear afterwards.

Below we describe in more details some key characteristics of fly-by spammers.

Duration of hijacks: Figure C.18 depicts the duration of the identified hijacks. The minimum duration is 30 minutes and the maximum duration is 20 days. Most hijacks (20 out of 29) lasted at most 4 days. Overall fly-by spammers appear to perform short-lived hijacks, likely in an effort to remain stealthy. Such hijacks really contrast with the hijack case study we presented in our Internet Security Threat Report 2012, which lasted five months. As shown later in this document, short-lived hijacks are very effective at defeating known spam protections, such as spam sender blacklists.

Duration of network idle period: Figure C.19 depicts the duration of the period during which networks were left idle/dormant before being hijacked. Fly-by spammers appear to hijack more networks (23 out of 29) that have been dormant for a very long time, i.e. more than one year, possibly to ensure their owner has permanently left them idle.

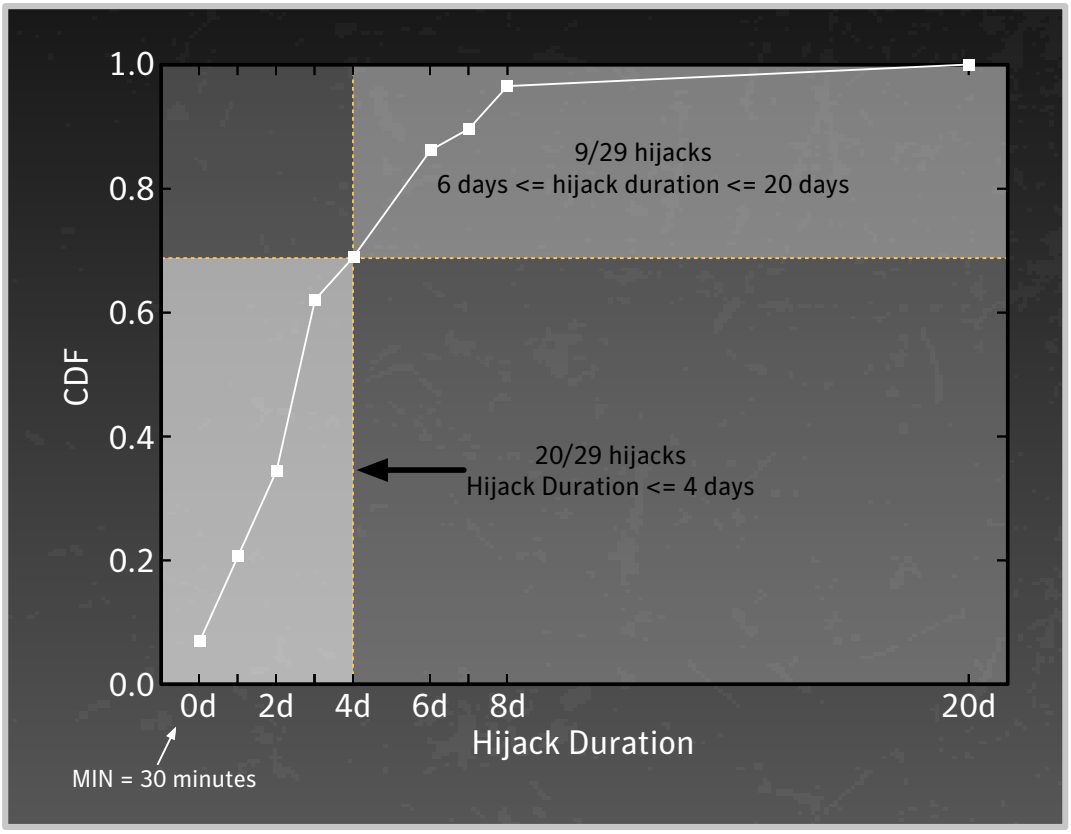


Fig. C.18 Duration of hijacks

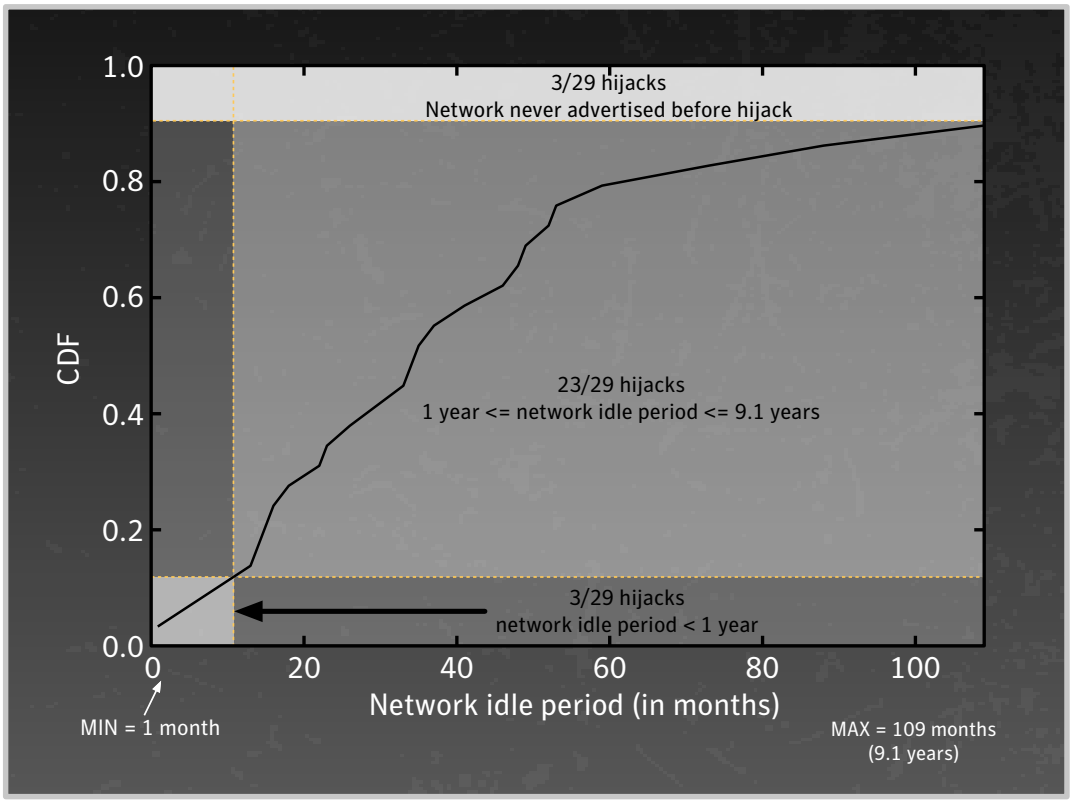


Fig. C.19 Duration of network Idle period

Routing and spamming behavior: To further illustrate the routing and spamming behavior of fly-by spammers, we consider some case studies. Figure C.20 shows the temporal correlation between the BGP advertisements for network IP address blocks and spam received from those networks at Symantec.cloud spamtraps. For example, the address block on the top of the figure was advertised in BGP (and hijacked) for only one day during which about 2,000 spam emails were received from it. The figure really highlights the strong temporal correlation between BGP advertisements and spam and the short-lived nature of the hijacks.

In order to assess the impact of spam from short-lived hijacks on spam sender blacklists, we extracted records for the hijacked networks in the Uceprotect[8], Manitu[9] and Spamhaus SBL and DROP[10] blacklists. Figure C.20 shows that out of the ten address blocks considered in these case studies only two had spam sources listed in those blacklists.

Finally, we also observed that a lot of scam websites advertised in the received spam emails were hosted on the hijacked networks, indicating that spammers took full advantage of the address blocks under their control.

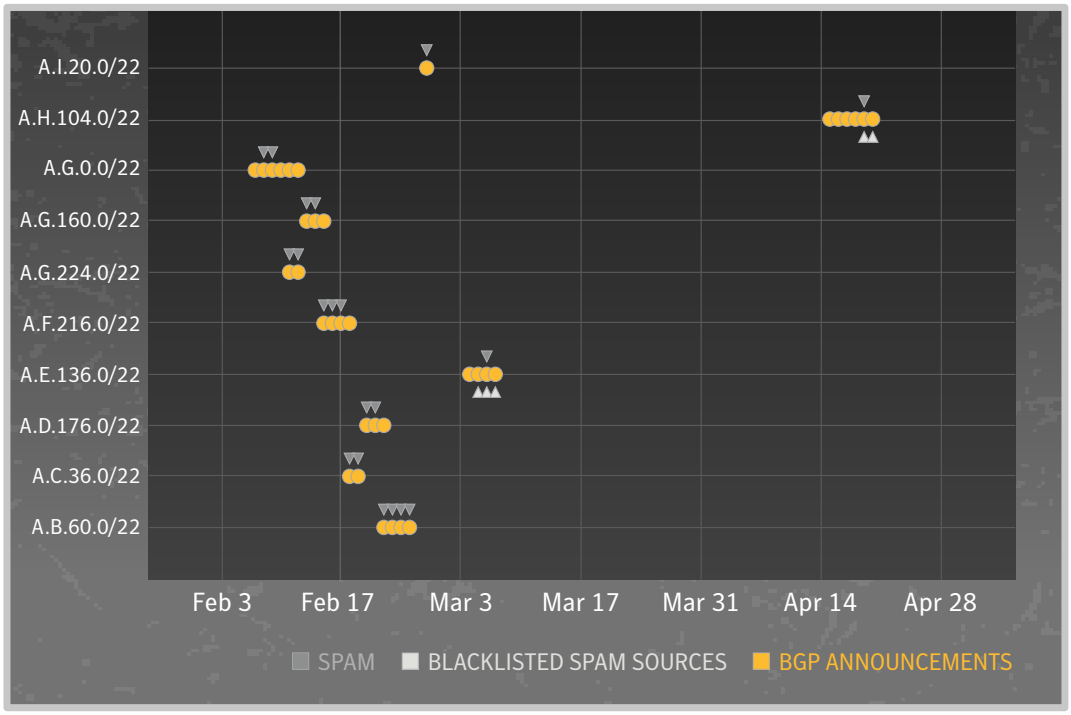


Fig. C.20 Temporal correlation between BGP advertisements and spam for hijacked networks

Effectiveness of fly-by spammers' spamming technique: Of the 29 hijacked network address blocks we observed only 13 (45 percent) of them were blacklisted either in Uceprotect, Manitu or Spamhaus SBL and DROP. Interestingly, Spamhaus' DROP (Don't Route Or Peer) is supposed to list hijacked networks, but little is known about how this list is actually built. Spam sent from short-lived hijacked networks thus appear to be very effective at defeating spam sender blacklists.

It is also noteworthy that none of the 29 hijacks were reported on any specialized mailing list, such as the North American Network Operators' Group mailing list, or published elsewhere. Finally, spammers never hijacked the same network twice showing that they not only perform short-lived hijacks but they also never reuse previously hijacked networks, likely in an effort to remain stealthy.

From these observations, fly-by spammers seem able to remain under the radar.

Networks targeted by fly-by spammers: We further looked at the organizations whose network address blocks were hijacked and found that:

- All hijacked address blocks were properly registered to an organization at the time they were hijacked. Moreover, they all belonged to different organizations.
- Of the 29 organizations, 12 of them were no longer in business while the remaining 17 were likely still in business.

These observations lead us to the conclusion that fly-by spammers seem to simply target dormant network IP address blocks regardless of their owner still being in business or not.

How to prevent fly-by spammers: BGP relies on the concept of trust among interconnect ASes exchanging routing information. This makes BGP insecure by design. An architecture[11] for securing BGP by relying on cryptography to ensure the authenticity and integrity of the routing information exchanged has been in development for many years now and is the most promising solution. However, the current state of the deployment of this architecture does not fully secure BGP and can consequently not prevent fly-by spammers using the *modus operandi* we presented. As a result, the only solution to prevent fly-by spammers for now is to use tools to detect such spammers and mitigate their effect, for example, by leveraging identified hijacked networks in spam filters to block emails that originate there.

Conclusion: Using SpamTracer, a system developed within Symantec Research Labs, we identified several confirmed attack cases where fly-by spammers temporarily stole (or hijacked) blocks of IP address and used them to send spam. We demonstrated that this technique for sending spam is very effective at defeating known protections, such as spam sender IP-based blacklisting. Finally we provided some insight into the *modus operandi* of these sophisticated spammers. This analysis confirms the first observations of fly-by spammers reported in our Internet Security Threat Report 2012 and shows the increasing prevalence of this phenomenon. By identifying confirmed cases of spammers performing BGP hijacks to send spam from stolen networks we also witnessed how spammers managed to evolve and become even more sophisticated, allowing them to send spam while remaining stealthy and hindering their traceability. Finally, this demonstrates the importance of securing the routing infrastructure of the Internet and studying the constantly evolving behavior of attackers to help improve current protections.

Footnotes

01 http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam
02 http://www.symantec.com/security_response/landing/spam
03 SMTP – Simple Mail Transfer Protocol
04 An as-yet unnamed spam-sending botnet.
05 http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet
06 http://www.symanteccloud.com/sv/se/globalthreats/learning_center/what_is_skeptic
07 http://www.symantec.com/threatreport/topic.jsp?id=spam_fraud_activity_trends&aid=future_spam_trends
08 http://www.uceprotect.net
09 http://www.dnsbl.manitu.net
10 http://www.spamhaus.org
11 http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-2/142_bgp.html

APPENDIX :: D
VULNERABILITY TRENDS

Vulnerability Trends

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security.

Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities being identified in the threat landscape because early detection and patching will minimize the chances of being exploited. This section discusses selected vulnerability trends, providing analysis and discussion of the trends indicated by the data.

The following metrics are included:

- Total Number of Vulnerabilities
- Zero-Day Vulnerabilities
- Web Browser Vulnerabilities
- Web Browser Plug-In Vulnerabilities
- Web Attack Toolkits
- SCADA Vulnerabilities

Total Number of Vulnerabilities

Background

The total number of vulnerabilities for 2013 is based on research from independent security experts and vendors of affected products. The yearly total also includes zero-day vulnerabilities that attackers uncovered and were subsequently identified post-exploitation. Symantec's DeepSight vulnerability database tracks vulnerabilities reported in major well-known applications that are in common business use and applications that customers have specifically requested to be tracked. For example, DeepSight does not track vulnerabilities in all open source projects or in all consumer products such as video games.

Symantec gathers information on all the aforementioned vulnerabilities as part of its DeepSight vulnerability database and alerting services. Examining these trends also provides further insight into other topics discussed in this report. Calculating the total number of vulnerabilities provides insight into vulnerability research being conducted in the threat landscape. There are many motivations for conducting vulnerability research, including security, academic, promotional, software quality assurance, and of course the malicious motivations that drive attackers.

Discovering vulnerabilities can be advantageous to both sides of the security equation: legitimate researchers may learn how better to defend against attacks by analyzing the work of attackers who uncover vulnerabilities; conversely, cybercriminals can capitalize on the published work of legitimate researchers to advance their attack capabilities. The vast majority of vulnerabilities that are exploited by attack toolkits are publicly known by the time they are exploited.

Methodology

Information about vulnerabilities is made public through a number of sources. These include mailing lists, vendor advisories, and detection in the wild. Symantec gathers this information and analyzes various characteristics of the vulnerabilities, including technical information and ratings in order to determine the severity and impact of the vulnerabilities. This information is stored in the DeepSight vulnerability database, which houses approximately 60,000 distinct vulnerabilities spanning a period of over 20 years. As part of the data gathering process, Symantec scores the vulnerabilities according to version 2.0 of the community-based CVSS (Common Vulnerability Scoring System[1]). Symantec adopted version 2.0 of the scoring system in 2008. The total number of vulnerabilities is determined by counting all of the vulnerabilities published during the reporting period.

All vulnerabilities are included, regardless of severity or whether or not the vendor who produced the vulnerable product confirmed them.

Fig. D.1

Total Vulnerabilities Identified 2006–2013

Source: Symantec

Year	Total Number of Vulnerabilities
2013	6,787
2012	5,291
2011	4,989
2010	6,253
2009	4,814
2008	5,562
2007	4,644
2006	4,842

Fig. D.2

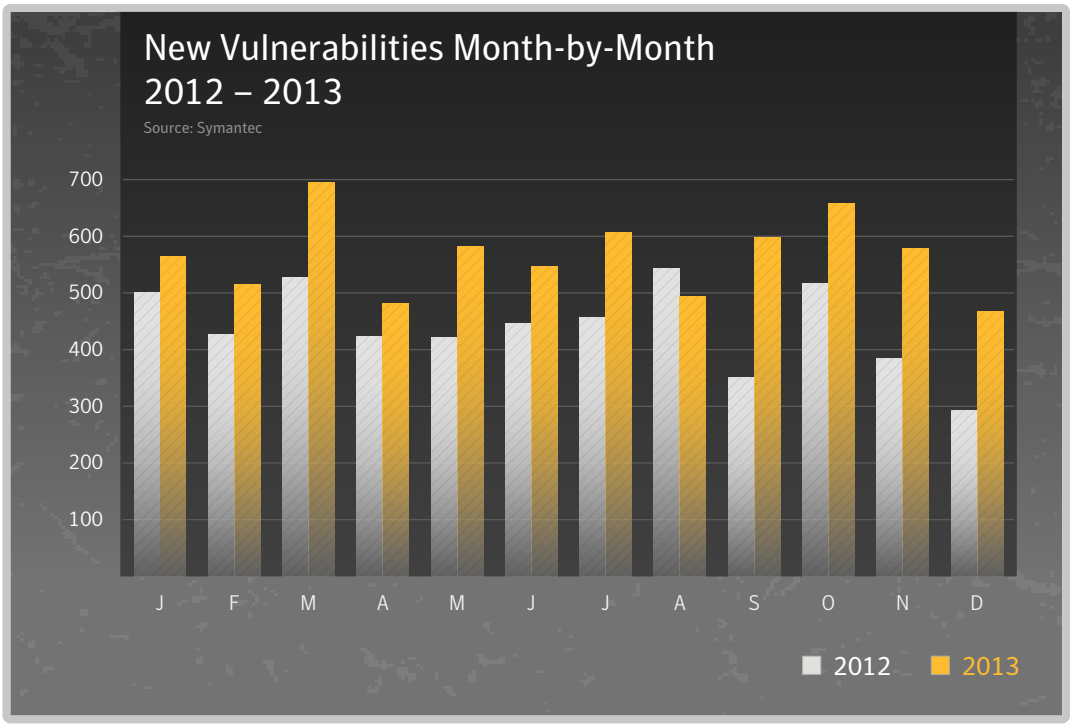


Fig. D.3

Most Frequently Attacked Vulnerabilities, 2013

Source: Symantec

BID	Number of Detections	Title
BID 31874	54,451,440	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
BID 8234	3,829,870	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
BID 10127	3,829,357	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
BID 6005	3,829,356	Microsoft Windows RPC Service Denial of Service Vulnerability
BID 10121	3,829,356	Microsoft Windows Object Identity Network Communication Vulnerability

Commentary

- **Actual number of new vulnerabilities reported is up, and trend is still upwards:** The total number of new vulnerabilities reported in 2013 stood at 6,787. This figure amounts to approximately 131 new vulnerabilities each week. Compared with the 5,291 new vulnerabilities reported in 2012, it represents an increase of 22 percent and the overall trend is still on an upward trajectory.
- **The most often exploited vulnerabilities are not the newest:** From observation of in-field telemetry, we can see that the most frequently used vulnerability in attacks is not the newest. Our data shows that the most commonly attacked component by a wide margin is the Microsoft Windows RPC component. The attacks against this component are mostly using the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874[2]). This vulnerability was first reported back in October 2008 and Symantec blocked 54.5 million attempts to exploit it in 2013. This figure represents 18 times the volume of the second most exploited vulnerability, the Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability (BID 8234[3]), from July 2003.
- The next two most often used vulnerabilities are the Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability (BID 10127[4]), dating from April 2004 and the Microsoft Windows RPC Service Denial of Service Vulnerability (BID 6005[5]), from October 2002.
- Finally the fifth most exploited vulnerability is the Microsoft Windows Object Identity Network Communication Vulnerability (BID 10121[6]), reported in April 2004.
- **All of the top five vulnerabilities are several years old with patches available:** So why are they used so often even several years after patches are available? There are several reasons why this is the case:
    - Trading of vulnerabilities[7] either through legitimate or clandestine channels has given exploitable vulnerabilities a significant monetary value. Because of the restricted information available on some of these new vulnerabilities, criminals may not be able to take advantage of them unless they are willing to pay the often substantial asking prices. If they are unable or unwilling to pay, they may resort to existing, widely available vulnerabilities that are tried and tested to achieve their goals, even if it may potentially be less effective.
    - For those willing to pay, they will want to ensure maximum return on their investment. This could mean they will use it discretely and selectively rather than making a big splash and arousing the attention of security vendors and other criminal groups looking for new vulnerabilities to use.
    - Older vulnerabilities have a more established malware user base, and so account for a greater amount of traffic. For example, widespread and well-established malware threats, such as W32.Downadup[8] and its variants, use the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), which continues to register over 150,000 hits each day. Because these threats use vulnerabilities to spread in an automated fashion, the number of attacks they can launch would generally be far higher than for targeted attacks.
    - For various reasons, not all of the user population apply security patches quickly or at all. This means older vulnerabilities can often still be effective, even years after patches are available. Because of this, there will always be a window of opportunity for criminals to exploit, and they are all too aware of this.
- One thing to note, websites hosting malicious toolkits often contain multiple exploits that can be tried against the visitor. In some cases, the kit will attempt to use all exploits at its disposal in a non-intelligent fashion whereas in more modern advanced kits, the website code will attempt to fingerprint the software installed on the computer before deciding which exploit(s) to send to maximize the success rate.

Zero-Day Vulnerabilities

Background

Zero-day vulnerabilities are vulnerabilities against which no vendor has released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases these threats can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

Methodology

Zero-day vulnerabilities are a sub-set of the total number of vulnerabilities documented over the reporting period. A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the affected vendor prior to exploitation and, at the time of the exploit activity, the vendor had not released a patch. The data for this section consists of the vulnerabilities that Symantec has identified that meet the above criteria.

Fig. D.4

Volume of Zero-Day Vulnerabilities, 2006–2013

Source: Symantec

Year	Count
2006	13
2007	15
2008	9
2009	12
2010	14
2011	8
2012	14
2013	23

Fig. D.5

Zero-Day Vulnerabilities Identified, 2013

Source: Symantec

CVE Identifier	Description
CVE-2013-0422	Oracle Java Runtime Environment CVE-2013-0422 Multiple Remote Code Execution Vulnerabilities
CVE-2012-3174	Oracle Java Runtime Environment CVE-2012-3174 Remote Code Execution Vulnerability
CVE-2013-0634	Adobe Flash Player CVE-2013-0634 Remote Memory Corruption Vulnerability
CVE-2013-0633	Adobe Flash Player CVE-2013-0633 Buffer Overflow Vulnerability
CVE-2013-0640	Adobe Acrobat And Reader CVE-2013-0640 Remote Code Execution Vulnerability
CVE-2013-0641	Adobe Acrobat And Reader CVE-2013-0641 Remote Code Execution Vulnerability
CVE-2013-0643	Adobe Flash Player CVE-2013-0643 Unspecified Security Vulnerability
CVE-2013-0648	Adobe Flash Player CVE-2013-0648 Remote Code Execution Vulnerability
CVE-2013-1493	Oracle Java SE CVE-2013-1493 Remote Code Execution Vulnerability
CVE-2013-2423	Oracle Java Runtime Environment CVE-2013-2423 Security Bypass Vulnerability
CVE-2013-1347	Microsoft Internet Explorer CVE-2013-1347 Use-After-Free Remote Code Execution Vulnerability
CVE-2013-1331	Microsoft Office PNG File CVE-2013-1331 Buffer Overflow Vulnerability
CVE-2013-3163	Microsoft Internet Explorer CVE-2013-3163 Memory Corruption Vulnerability
CVE-MAP-NOMATCH	vBulletin '/install/upgrade.php' Security Bypass Vulnerability
CVE-2013-3893	Microsoft Internet Explorer CVE-2013-3893 Memory Corruption Vulnerability
CVE-2013-3897	Microsoft Internet Explorer CVE-2013-3897 Memory Corruption Vulnerability
CVE-2013-3906	Multiple Microsoft Products CVE-2013-3906 Remote Code Execution Vulnerability
CVE-2013-3918	Microsoft Windows 'icardie.dll' ActiveX Control CVE-2013-3918 Remote Code Execution Vulnerability
CVE-MAP-NOMATCH	vBulletin Unspecified Security Vulnerability
CVE-MAP-NOMATCH	Microsoft Windows Kernel 'NDProxy.sys' Local Privilege Escalation Vulnerability
CVE-MAP-NOMATCH	Adobe Flash Player and AIR Type Confusion Remote Code Execution Vulnerability
CVE-2013-2463	Oracle Java SE CVE-2013-2463 Remote Code Execution Vulnerability
CVE-2013-3660	Microsoft Windows Kernel 'Win32k.sys' CVE-2013-3660 Local Privilege Escalation Vulnerability

Commentary

- 2013 saw an increase in number of zero-day vulnerabilities compared to 2012. There was a 39 percent increase in vulnerabilities in 2013 compared with 2012. However the number of vulnerabilities from 2013 was inflated due to Microsoft Oracle vulnerabilities, while in 2013 there were seven Adobe vulnerabilities, compared with only three in 2012.
- While the overall number of zero-day vulnerabilities is up, attacks using these vulnerabilities continue to be successful. Some of these vulnerabilities are leveraged in targeted attacks. Adobe Flash Player and Microsoft Windows ActiveX Control vulnerabilities are widely used in targeted attacks and Microsoft technologies accounted for almost a third of the zero-day vulnerabilities seen in 2013.
- Most of the attack scenarios are planned in such a way that an attacker crafts a malicious webpage to exploit the issue, and uses email or other means to distribute the page and entices an unsuspecting user to view it. When the victim views the page, the attacker-supplied code is run.

Web Browser Vulnerabilities

Background

Web browsers are ever-present components for computing for both enterprise and individual users on desktop and on mobile devices. Web browser vulnerabilities are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and adware. In addition, web browsers are exposed to a greater amount of potentially untrusted or hostile content than most other applications and are particularly targeted by multi-exploit attack kits.

Web-based attacks can originate from malicious websites as well as from legitimate websites that have been compromised to serve malicious content. Some content, such as media files or documents are often presented in browsers via browser plug-in technologies. While browser functionality is often extended by the inclusion of various plug-ins, the addition of a plug-in component also results in a wider potential attack surface for client-side attacks.

Methodology

Browser vulnerabilities are a sub-set of the total number of vulnerabilities cataloged by Symantec throughout the year. To determine the number of vulnerabilities affecting browsers, Symantec considers all vulnerabilities that have been publicly reported, regardless of whether they have been confirmed by the vendor. While vendors do confirm the majority of browser vulnerabilities that are published, not all vulnerabilities may have been confirmed at the time of writing. Vulnerabilities that are not confirmed by a vendor may still pose a threat to browser users and are therefore included in this study.

Commentary

- This metric examines the total number of vulnerabilities affecting the following web browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Opera
- All vulnerabilities decreased in 2013, except Microsoft Internet Explorer which saw an increase of 59 percent, compared to 2012.
- These five browsers had 591 reported vulnerabilities in total in 2013, which is a significant decrease from 891 in 2012. This drop is due to a dramatic reduction in vulnerabilities seen in Safari, Chrome and Firefox.

Fig. D.6

Browser Vulnerabilities, 2011–2013

Source: Symantec

	Apple Safari	Google Chrome	Microsoft Internet Explorer	Mozilla Firefox	Opera	Total
2013	54	219	148	157	13	591
2012	343	268	60	186	34	891
2011	117	62	48	98	26	351

Web Browser Plug-in Vulnerabilities

Background

This metric examines the number of vulnerabilities affecting plug-ins for web browsers. Browser plug-ins are technologies that run inside the web browser and extend its features, such as allowing additional multimedia content from web pages to be rendered. Although this is often run inside the browser, some vendors have started to use sandbox containers to execute plug-ins in order to limit the potential harm of vulnerabilities. Unfortunately, web browser plug-ins continue to be one of the most exploited vectors for web-based attacks and drive-by downloads silently infecting consumer and enterprise users.

Many browsers now include various plug-ins in their default installation and also provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of web browsers and are often required in order to use many commercial sites. Vulnerabilities affecting plug-ins are an increasingly favored vector for a range of client-side attacks, and the exploits targeting these vulnerabilities are commonly included in attack kits. Web attack kits can exploit up to 25 different browser and browser plug-in vulnerabilities at one time, enabling full access to download any malware to the endpoint system.

Some plug-in technologies include automatic update mechanisms that are designed to keep software up-to-date, which may aid in limiting exposure to certain vulnerabilities. Enterprises that choose to disable these updating mechanisms, or continue to use vulnerable out-of-date versions, will continue to put their enterprises at considerable risk of silent infection and exploitation. Through a variety of drive-by web attacks, exploits against browser plug-in vulnerabilities continue to be a favored infection vector for hackers and malware authors to breach enterprises and consumer systems. To help mitigate the risk, some browsers have started to check for the version of installed third party plug-ins and inform the user if there are any updates available for install. Enterprises should also check if every browser plug-in is needed and consider removing or disabling potentially vulnerable software.

Methodology

Web browser plug-in vulnerabilities comprise a sub-set of the total number of vulnerabilities cataloged by Symantec over the reporting period. The vulnerabilities in this section cover the entire range of possible severity ratings and include vulnerabilities that are both unconfirmed and confirmed by the vendor of the affected product. Confirmed vulnerabilities consist of security issues that the vendor has publicly acknowledged, by either releasing an advisory or otherwise making a public statement to concur that the vulnerability exists. Unconfirmed vulnerabilities are vulnerabilities that are reported by third parties, usually security researchers, which have not been publicly confirmed by the vendor. That a vulnerability is unconfirmed does not mean that the vulnerability report is not legitimate; only that the vendor has not released a public statement to confirm the existence of the vulnerability.

Fig. D.7

Browser Plug-In Vulnerabilities, 2012–2013

Source: Symantec

	Adobe Acrobat Reader	Adobe Flash	Active X	Apple Quicktime	Firefox Extension	Oracle Sun Java	Total
2012	32	70	118	28	0	64	312
2013	68	56	54	13	0	184	375

Commentary

- Symantec identified the following plug-in technologies as having the most reported vulnerabilities in 2013:
  - Adobe Reader
  - Adobe Flash Player
  - Apple QuickTime
  - Microsoft ActiveX
  - Mozilla Firefox extensions
  - Oracle Sun Java Platform Standard Edition (Java SE)
- In 2012, 375 vulnerabilities affecting browser plug-ins were documented by Symantec, an increase compared to the 312 vulnerabilities affecting browser plug-ins in 2012.
- ActiveX vulnerabilities decreased in 2013.
- Java vulnerabilities increased in 2013. This trend was already visible in 2012 and grew again. This is also reflected in the vulnerability usage in attack toolkits which have focused around Adobe Flash Player, Adobe PDF Reader and Java in 2013.

Web Attack Toolkits

Web attack toolkits are a collection of scripts, often PHP or JavaScript files, which are used to create malicious websites that exploit vulnerabilities in order to infect visitors. There are a few dozen known families used in the wild. Many toolkits are traded or sold on underground forums for USD$100-$1000.

Some are actively developed with new vulnerabilities added over time, and some web attack toolkits employ a subscription model that operates rather like a Software-as-a-Service (SaaS) model. The exploit code is kept away from the criminals who are renting the toolkit, so that they may not steal the toolkit author's intellectual property. However, the attacker will include code that links to the actual toolkit. This may be further hidden behind fast-flux DNS in order to further obfuscate the attack code.

Since many toolkits regularly use the same exploits, it is often difficult to identify the specific attack toolkit behind each infection attempt. An attack toolkit may contain many different exploits, each focusing on a variety of browser-independent plug-in vulnerabilities. In general, older exploits are not removed from the toolkits, since some systems may still be unpatched and these may often be tried first, in order to keep the newer attacks below the radar. This is perhaps why many of the toolkits still contain an exploit for the old Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability (BID 17462) from 2006. The malicious script will test all possible exploits in sequence until one succeeds. This may magnify the attack numbers seen for older vulnerabilities, even if they were unsuccessful.

For more information on Web attack toolkits, please read Appendix A: Threat Activity Trends - Analysis of Malicious Web Activity by Attack Toolkits.

SCADA Vulnerabilities

Background

This metric will examine the SCADA (Supervisory Control and Data Acquisition) security threat landscape. SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes, but is not limited to, power generation, manufacturing, oil and gas, water treatment, and waste management. The security of SCADA technologies and protocols is a concern related to national security because the disruption of related services can result in, among other things, the failure of infrastructure and potential loss of life.

Methodology

This discussion is based on data surrounding publicly known vulnerabilities affecting SCADA technologies. The purpose of the metric is to provide insight into the state of security research in relation to SCADA systems. To a lesser degree, this may provide insight into the overall state of SCADA security. Vulnerabilities affecting SCADA systems may present a threat to critical infrastructure that relies on these systems. Due to the potential for disruption of critical services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks. This is a concern for both governments and enterprises involved in the critical infrastructure sector. While this metric provides insight into public SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure it is likely that private security research is conducted by SCADA technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

Fig. D.8

SCADA Vulnerabilities Identified, 2013

Source: Symantec

BugTraq#	Description	Published
57438	Rockwell Automation ControlLogix CVE-2012-6442 Denial of Service Vulnerability	11 January 2013
57309	Rockwell Automation ControlLogix CVE-2012-6436 Remote Denial of Service Vulnerability	11 January 2013
57651	Rockwell Automation ControlLogix CVE-2012-6437 Security Bypass Vulnerability	11 January 2013
57311	Rockwell Automation ControlLogix CVE-2012-6435 Denial of Service Vulnerability	11 January 2013
58917	Rockwell Automation ControlLogix CVE-2012-6439 Denial of Service Vulnerability	11 January 2013
57435	Rockwell Automation ControlLogix CVE-2012-6440 Replay Security Bypass Vulnerability	11 January 2013
59703	Rockwell Automation ControlLogix CVE-2012-6438 Remote Denial of Service Vulnerability	11 January 2013
59709	Rockwell Automation ControlLogix CVE-2012-6441 Information Disclosure Vulnerability	14 January 2013
62936	Schneider Electric Software Update Remote Arbitrary Code Execution Vulnerability	16 January 2013
62635	Schneider Electric Products Multiple Security Vulnerabilities	16 January 2013
57317	Schneider Electric Accutech Manager Heap Buffer Overflow Vulnerability	21 January 2013
64351	Schneider Electric Ethernet Modules CVE-2013-2761 Denial of Service Vulnerability	23 January 2013
59708	Ecava IntegraXor CVE-2012-4700 ActiveX Control Remote Buffer Overflow Vulnerability	05 February 2013

Fig. D.8

SCADA Vulnerabilities Identified, 2013 (cont.)

Source: Symantec

BugTraq#	Description	Published
62419	WellinTech KingView CVE-2012-4711 Memory Corruption Vulnerability	12 February 2013
57909	Multiple Schneider Electric Products 'ModbusDrv.exe' Local Buffer Overflow Vulnerability	11 March 2013
61598	Mitsubishi MX Component ActiveX Control 'ActUWzd.dll' Remote Buffer Overflow Vulnerability	25 March 2013
57306	RSLinx Enterprise 'Logger.dll' CVE-2012-4695 Denial of Service Vulnerability	05 April 2013
58950	Invensys Wonderware Information Server CVE-2013-0688 Cross Site Scripting Vulnerability	07 May 2013
62878	Invensys Wonderware Information Server CVE-2013-0685 Denial of Service Vulnerability	07 May 2013
57308	Invensys Wonderware Information Server CVE-2013-0686 Information Disclosure Vulnerability	07 May 2013
57767	Invensys Wonderware Information Server CVE-2013-0684 SQL Injection Vulnerability	07 May 2013
64684	Multiple Schneider Electric Products XML External Entity Information Disclosure Vulnerability	16 July 2013
62880	ClearSCADA Web Requests Remote Denial of Service Vulnerability	01 August 2013
61968	Schneider Electric Multiple Trio J-Series Radio Devices CVE-2013-2782 Security Bypass Vulnerability	22 August 2013
57315	WellinTech KingView ActiveX Controls Multiple Insecure Method Vulnerabilities	04 September 2013
57307	Invensys Wonderware InTouch XML External Entities Information Disclosure Vulnerability	20 September 2013
62879	RSLinx Enterprise 'LogReceiver.exe' Integer Overflow Denial of Service Vulnerability	07 October 2013
59704	RSLinx Enterprise 'LogReceiver.exe' Integer Overflow Denial of Service Vulnerability	07 October 2013
57310	RSLinx Enterprise 'LogReceiver.exe' Out-of-bounds Remote Denial of Service Vulnerability	07 October 2013
62660	InduSoft Thin Client 'novapi7.dll' ActiveX Control Buffer Overflow Vulnerability	08 October 2013
58999	Ecava IntegraXor Project Directory Information Disclosure Vulnerability	15 December 2013
58692	Schneider Electric Accutech Manager RFManagerService SQL Injection Vulnerablity	18 December 2013

Commentary

- The number of SCADA vulnerabilities decreased in 2013: In 2013, there were 32 public SCADA vulnerabilities, a decrease compared with the 52 vulnerabilities disclosed in 2012

Footnotes

01 http://www.first.org/cvss/cvss-guide.html
02 http://www.securityfocus.com/bid/31874
03 http://www.securityfocus.com/bid/8234
04 http://www.securityfocus.com/bid/10127
05 http://www.securityfocus.com/bid/6005
06 http://www.securityfocus.com/bid/10121
07 http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/231900575/more-exploits-for-sale-means-better-security.html
08 http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99

APPENDIX :: E GOVERNMENT THREAT ACTIVITY TRENDS

Government Threat Activity Trends

The following section of the Symantec Internet Security Threat Report for Government provides an analysis of threat activity trends relating to government and Critical Infrastructure Protection (CIP), including malicious activity that Symantec observed in 2013.

Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Critical Infrastructure Sector
- Sources of Origin For Government-Targeted Attacks
- Attacks by Type-Notable Critical Infrastructure Sectors

Malicious Activity by Critical Infrastructure Sector

Background

This metric indicates the level to which government and critical infrastructure organizations may have been compromised and are being used by attackers as launching pads for malicious activity. These attacks could potentially expose sensitive and confidential information, which could have serious ramifications for government and critical infrastructure organizations. Such information could be used for strategic purposes in the case of state- or group-sponsored attacks, especially since attackers who use compromised computers for malicious activity can mask their actual location.

Methodology

This metric evaluates the amount of malicious activity originating from computers and networks that are known to belong to government and critical infrastructure sectors. To measure this, Symantec cross-referenced the IP addresses of known malicious computers with standard industrial classification (SIC[1]) codes that are assigned to each industry and provided by a third-party service[2]. Symantec has compiled data on numerous malicious activities that were detected originating from the IP address space of these organizations. These activities include bot-infected computers, phishing hosts, spam zombies, and network attack origins.

Fig. E.1

Malicious Activity by Critical Infrastructure Sector

Source: Symantec

Industry Sector	Percentage of CIP Source Activity	Percentage of CIP Source IP Addresses
Financial Services	48.3%	2.4%
Manufacturing	42.4%	95.5%
Biotech / Pharmaceutical	4.9%	0.9%
Government	1.5%	0.2%
Government - State	1.4%	0.1%
Internet Service Provider	0.7%	0.7%
Aerospace	0.2%	0.1%
Transportation	0.2%	0.001%
Utilities / Energy	0.1%	0.03%
Telecommunications	0.1%	0.02%
Government - National	0.1%	0.1%
Health Care	0.02%	0.01%
Government - Local	0.00001%	0.0001%

Commentary

- Financial Services was the top sector for malicious activity: The Financial Services sector was the origin for the most malicious activity in 2013, accounting for 48.3 percent of attacks and 2.4 percent of source IP addresses originating from CIP networks.

Sources of Origin for Government-Targeted Attacks

Background

Attacks targeting government organizations may serve as a means of expressing disagreement with policies and programs that the government has developed and implemented. Such attacks are likely to be carried out for a variety of reasons, including blocking access to government internet-based resources, gaining access to potentially sensitive information, and discrediting the government itself. In addition, attacks may be motivated by espionage and attempts to steal government-classified information. These attacks may result in the disruption of critical services, as with Denial-of-Service (DoS) attacks, or the exposure of highly sensitive information. An attack that disrupts the availability of a high-profile government organization website will get much wider notice than one that takes a single user offline. In addition, malicious code attacks targeting governments can be motivated by profit because governments store considerable amounts of personal identification data that could be used for fraudulent purposes, such as identity theft. Personal data can include names, addresses, government-issued identification numbers, and bank account credentials, all of which can be effectively exploited for fraud by attackers. Government databases also store information that could attract politically motivated attacks, including critical infrastructure information and other sensitive intelligence.

Methodology

This metric will assess the top sources of origin for government-targeted attacks by determining the location of computers from which the attack occurred. It should be noted that attackers often attempt to obscure their tracks by redirecting attacks through one or more servers that may be located anywhere in the world; thus, the attacker may be located somewhere other than from where the attacks appear to originate.

Fig. E.2

Sources of Origin for Government-Targeted Attacks

Source: Symantec

Country/Region	Percent of Source Activity	Percent of Source IP Addresses
United States	80.21%	18.58%
China	7.88%	59.23%
Netherlands	4.23%	4.13%
United Kingdom	1.34%	1.90%
Germany	1.27%	1.87%
Taiwan	1.11%	3.47%
Russia	1.07%	4.52%
Japan	1.04%	3.10%
France	0.98%	1.23%
Korea, South	0.87%	1.96%

Commentary

- The United States and China were the top two sources of origin for attacks that targeted the government sector in 2013.
- The high ranking in this metric of these two countries reflects the fact that they were also the top two ranking sources of origin for all internet-wide network attacks globally, with the highest populations of Internet-connected users worldwide.

Attacks by Type – Notable Critical Infrastructure Sectors

Background

This section of the Symantec Internet Security Threat Report for Government focuses on the types of attacks detected by sensors deployed in notable critical infrastructure sectors. Government and critical infrastructure organizations are the target of a wide variety of attack types. The ability to identify attacks by type assists security administrators in evaluating which assets may be targeted and may assist them in ensuring that assets receiving a disproportionate number of attacks are made secure.

The following sectors will be discussed in detail:

- Government
- Biotech/Pharmaceutical
- Healthcare
- Financial Services
- Transportation
- Telecommunications
- Utilities

Methodology

The following types of attacks are considered for this metric:

Attacks on Web Servers: Web servers facilitate a variety of services for government and critical infrastructure sectors, such as hosting publicly available information, customer support portals, and online stores. Some web servers also host remotely accessible interfaces that employees use to perform routine, job-related tasks from remote locations. Furthermore, a web server may be a portal to an organization's internal network and database systems.

Attacks on Web Browsers: Web browsers are exposed to a greater amount of potentially untrusted or hostile content than most other applications. As the internet has become commonplace among business and leisure activities, there is an increased reliance on browsers and their plug-ins. Attacks on web browsers can originate from malicious websites as well as legitimate websites that have been compromised to serve malicious content. Browsers can also facilitate client-side attacks because of their use of plug-ins and other applications in handling potentially malicious content served from the web, such as compromised documents and media files.

Attacks on SMTP (Simple Mail Transfer Protocol): SMTP is designed to facilitate the delivery of email messages across the Internet. Email servers using SMTP as a service are likely to be targeted by attackers because external access is required to deliver email. While most services can be blocked by a firewall to protect against external attacks and allow access only to trusted users and entities, for email to function effectively for organizations, it has to be available both internally and externally to other email servers. The necessity of allowing both internal and external access increases the probability that a successful attack will improve attackers' chances of gaining access to the network.

Denial-of-Service (DoS) Attacks: DoS attacks are a threat to government and critical infrastructures because the purpose of such attacks is to disrupt the availability of high-profile websites or other network services and make them inaccessible to users and employees. A successful DoS attack could result in the disruption of internal and external communications, making it practically impossible for employees and users to access potentially critical information. Because these attacks often receive greater exposure than those that take a single user offline, especially for high-profile government websites, they could also result in damage to the organization's reputation. A successful DoS attack on a government network could also severely undermine confidence in government competence and impair the defense and protection of government networks.

Backscatter: Generally, backscatter is considered to be a type of internet background noise, which is typically ignored. While not a direct attack, backscatter is evidence that a DoS attack against another server on the internet is taking place and is making use of spoofed IP addresses. When one of these spoofed IP addresses matches the address of a Symantec sensor, any error messages that the attacked server sends to the spoofed address will be detected by a Symantec sensor as backscatter.

Shellcode/Exploit attacks: Shellcode is a small piece of code used as the payload in the exploitation of a vulnerability. An attacker can exploit a vulnerability to gain access to a system, inject this code, and use a command shell to take control of a compromised machine. By remotely controlling a compromised system, an attacker can gain access to an organization's network and, from there, perpetrate additional attacks. Moreover, this type of attack can monopolize valuable resources that may be critical to government operations.

Fig. E.3

Attacks by Type: Overall Government and Critical Infrastructure Organizations

Source: Symantec

Top-Ten Attacks	Percentage
Web (server)	95.3%
Denial of Service	0.7%
Shellcode/Exploit	0.4%
Peer-to-Peer	2.6%
Web (browser)	0.8%
SMTP (Email)	0.2%
DNS	0.01%
Miscellaneous	0.004%
Bruteforce	0.01%

Commentary

- Web server attacks were the most common type of attack for government and critical infrastructure: In 2013, the most common attack type seen by all sensors in the government and critical infrastructure sectors related to attacks on web servers and accounted for 95.3 percent of all attacks.
- Peer to Peer (P2P) attacks were the second-most common type of attack for government and critical infrastructure, accounting for 2.6 percent of attacks. P2P attacks comprise of general ones such as DoS, man-in-the-middle and worm propagation attacks, and specific ones such as rational attacks, file poisoning, and so on.
- DoS attacks are often associated with social and political protests, since they are intended to render a site inaccessible to legitimate users of those services. Man-in-the-middle attacks are where the attacker inserts himself undetected between two nodes. He can then choose to stay undetected and spy on the communication, or more actively manipulate the communication.
- Worms already pose one of the biggest threats to the internet. Previously, worms such as Code Red or Nimda were capable of infecting hundreds of thousands of hosts within hours. There is no doubt that better engineered worms will be able to achieve the same result in a matter of seconds. Worms propagating through P2P applications would be disastrous; it is probably the most serious threat.

Fig. E.4

Attacks by Type: Notable Critical Infrastructure Sectors

Source: Symantec

Top Attacks	Percentage
Government	
SMTP (Email)	25.3%
Web (server)	27.7%
Shellcode/Exploit	32.5%
Denial of Service	6.2%
Web (browser)	6.1%
Biotech/Pharmaceutical	
Peer-to-Peer	41.18%
Denial of Service	58.69%
Shellcode/Exploit	0.01%
Web (server)	0.01%
SMTP (Email)	0.10%
Financial Services	
Web (server)	3.7%
Peer-to-Peer	46.0%
Shellcode/Exploit	7.2%
Web (browser)	37.4%
SMTP (Email)	3.0%
Healthcare	
Shellcode/Exploit	35.7%
Web (server)	23.7%
Denial of Service	4.1%
Bruteforce	36.5%
Transportation	
Denial of Service	6.5%
Shellcode/Exploit	2.6%
Bruteforce	45.8%
Web (server)	45.2%

Top Attacks	Percentage
Telecommunications	
Denial of Service	49.7%
Shellcode/Exploit	17.0%
Web (browser)	0.1%
Web (server)	33.1%
Utilities	
Denial of Service	66.5%
Shellcode/Exploit	15.5%
Web (browser)	14.8%
Web (server)	1.5%
SMTP (Email)	1.4%

Commentary

- The Financial Services sector was predominantly targeted by P2P attacks followed by Shellcode/Exploit attacks, whereas Transportation sectors were primarily targeted by web server and bruteforce attacks in 2013.
- Shellcode/Exploit attacks have become the most common for the Government sector and Healthcare. A shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability. It is called Shellcode because it typically starts a command shell from which the attacker can control the compromised machine. Shellcode can either be local or remote, depending on whether it gives an attacker control over the machine it runs on (local) or over another machine through a network (remote).
- DoS attacks dominate Biotech, Telecommunications and Utilities sectors, attempting to disrupt services and communications within them.

Footnotes

01 SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more on this, please see http://www.sec.gov

02 http://www.digitalenvoy.net

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Security Response Publications: http://www.symantec.com/security_response/publications/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

For specific country offices and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

04/14 21284431-5