Symantec

2013 Trends, Volume 19, Published April 2014

ISTR

INTERNET SECURITY THREAT REPORT ✦ 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

In 2013 much attention was focused on cyber-espionage, threats to privacy and the acts of malicious insiders. However the end of 2013 provided a painful reminder that cybercrime remains prevalent and that damaging threats from cybercriminals continue to loom over businesses and consumers. Eight breaches in 2013 each exposed greater than 10 million identities, targeted attacks increased and end-user attitudes towards social media and mobile devices resulted in wild scams and laid a foundation for major problems for end-users and businesses as these devices come to dominate our lives.

This year's ISTR once again covers the wide-ranging threat landscape, with data collected and analyzed by Symantec's security experts. In this summary, we call out seven areas that deserve special attention.

The most important trends in 2013 were:

2013 Was The Year of Mega Breach

Our Internet Security Threat Report 17 reported 2011 as the Year of the Data Breach. The year was extraordinary because in addition to increased cybercrime-driven breaches, Anonymous in acts of hactivism breached dozens of companies. With Anonymous less active, breach numbers returned to more predictable growth in 2012. And then came 2013. If 2011 was the year of the breach, then 2013 can best be described as the Year of the Mega Breach.

The total number of breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches. It was also larger than the 208 breaches in 2011. But even a 62 percent increase does not truly reflect the scale of the breaches in 2013. Eight of the breaches in 2013 exposed more than 10 million identities each. In 2012 only one breach exposed over 10 million identities. In 2011, only five were of that size.

2011 saw 232 million identities exposed, half of the number exposed in 2013. In total over 552 million identities were breached in 2013, putting consumer's credit card information, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, login, passwords, and other personal information into the criminal underground.

Targeted Attacks Grow and Evolve

While targeted attacks continue to rise, Symantec observed an interesting evolution in these attacks. As first reported in last year's Internet Security Threat Report, attackers added watering-hole attacks to their arsenal. But reports of the death of spear phishing are greatly exaggerated. While the total number of emails used per campaign has decreased and the number of those targeted has also decreased, the number of spear-phishing campaigns themselves saw a dramatic 91 percent rise in 2013.

This "low and slow" approach (campaigns also run three times longer than those in 2012) are a sign that user awareness and protection technologies have driven spear phishers to tighten their targeting and sharpen their social engineering. We have also observed the addition of real world social engineering, combining virtual and real world attacks, being employed to increase the odds of success.

This year's Internet Security Threat Report also introduces a new calculation. Using epidemiology concepts commonly applied to public health issues, we have estimated the risk industries and users face of being targeted for attack. It sends a warning to some industries that may view the volume of attacks against them as no cause for concern. For instance, while the most targeted attacks in 2013 were against Governments and the Services industry, the industries at most risk of attack were Mining, Governments and then Manufacturing. Their odds of being attacked are 1 in 2.7, 1 in 3.1 and 1 in 3.2 respectively.

Executive Summary

Zero-day Vulnerabilities and Unpatched Websites Facilitated Watering-Hole Attacks

More zero-day vulnerabilities were discovered in 2013 than any other year Symantec has tracked. The 23 zero-day vulnerabilities discovered represent a 61 percent increase over 2012 and are more than the two previous years combined.

Zero-day vulnerabilities are coveted because they give attackers the means to silently infect their victim without depending on social engineering. And by applying these exploits in a watering-hole attack they avoid the possibility of anti-phishing technology stopping them. Unfortunately legitimate web sites with poor patch management practices have facilitated the adoption of watering hole attacks. 77 percent of legitimate websites had exploitable vulnerabilities and 1-in-8 of all websites had a critical vulnerability. This gives attackers plenty of choices in websites to place their malware and entrap their victims.

Typically cutting-edge attackers stop using a vulnerability once it is made public. But this does not bring an end to their use. Common cybercriminals rapidly incorporate zero-day vulnerabilities to threaten all of us. Even though the top five zero-day vulnerabilities were patched on average within four days, Symantec detected a total of 174,651 attacks within 30 days of these top five becoming known.

Ransomware attacks grew by 500 percent in 2013 and turned vicious

Scammers continued to leverage profitable ransomware scams – where the attacker pretends to be local law enforcement, demanding a fake fine of between $100 to $500. First appearing in 2012 these threats escalated in 2013, and grew by 500 percent over the course of the year.

These attacks are highly profitable and attackers have adapted them to ensure they remain profitable. The next step in this evolution was Ransomcrypt, commonly known as Cryptolocker. This is the most prominent of these threats and turns ransomware vicious by dropping all pretence of being law enforcement and is designed to encrypt a user's files and request a ransom for the files to be unencrypted. This threat causes even more damage to businesses where not only the victims' files are encrypted but also files on shared or attached network drives.

Holding encrypted files for ransom is not entirely new, but getting the ransom paid has previously proven problematic for the crooks. With the appearance of online payment methods ransomcrypt is poised for growth in 2014. Small businesses and consumers are most at risk from losing data, files or memories. Prevention and backup are critical to protecting users from this type of attack.

Social Media Scams and Malware Flourish on Mobile

While the prevalence of mobile malware is still comparatively low, 2013 showed that the environment for an explosive growth of scams and malware attacks is here. Our Norton Report, a global survey of end-users, showed that 38 percent of mobile users had already experienced mobile cybercrime. Lost or stolen devices remain the biggest risk, but mobile users are behaving in ways that leave themselves open to other problems.

Mobile users are storing sensitive files online (52 percent), store work and personal information in the same online storage accounts (24 percent) and sharing logins and passwords with families (21 percent) and friends (18 percent), putting their data and their employers' data at risk.

Yet only 50 percent of these users take even basic security precautions.

The number of brand new malware families created slowed as malware authors worked to perfect existing malware. In 2012 each mobile malware family had an average of 38 variants. In 2013 each family had 58. However several events in 2013 showed that mobile users are highly susceptible to scams via mobile apps. It might be said that mobile malware has not yet exploded because the bad guys have not needed it to get what they want.

Executive Summary

Prevalence of Scams Fail to Change User Behaviour on Social Media

Surrounded by their friends, users continue to fall for scams on social media sites. Fake offers such as free cell phone minutes accounted for the largest number of attacks of Facebook users in 2013 – 81 percent in 2013 compared to 56 percent in 2012. And while twelve percent of social media users say someone has hacked into their social network account and pretended to be them, a quarter continue to shared their social media passwords with others and a third connect with people they don't know.

As social media becomes more and more of an activity done on mobile devices these bad behaviours are likely to have worse consequences.

Attackers are turning to the Internet of Things

Baby monitors, as well as security cameras and routers, were famously hacked in 2013. Furthermore, security researchers demonstrated attacks against smart televisions, automobiles and medical equipment. This gives us a preview of the security challenge presented by the rapid adoption of the Internet of Things (IoT).

The benefit to attackers of compromising these devices may not yet be clear, and some suspect claims about hacked devices (refrigerators for instance) are to be expected. But the risk is real. IoT devices will become access points for targeted attackers and become bots for cybercriminals.

Of immediate concern are attacks against consumer routers. Computer worms like Linux.Darlloz are making a comeback as attackers target devices without users to social engineer, but with unpatched vulnerabilities they can remotely exploit. Control of these devices can prove profitable for attackers, using DNS redirection to push victims to fake websites, usually to steal financial details.

Today the burden of preventing attacks against IoT devices falls on the user; however this is not a viable long-term strategy. Manufacturers are not prioritizing security – they need to make the right security investments now. The risk gets even higher with the proliferation of data being generated from these devices. Big data is big money and unless the right security steps are taken it's all available for an enterprising cybercriminal.

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.Exprespam 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

1 — 2012

+700%

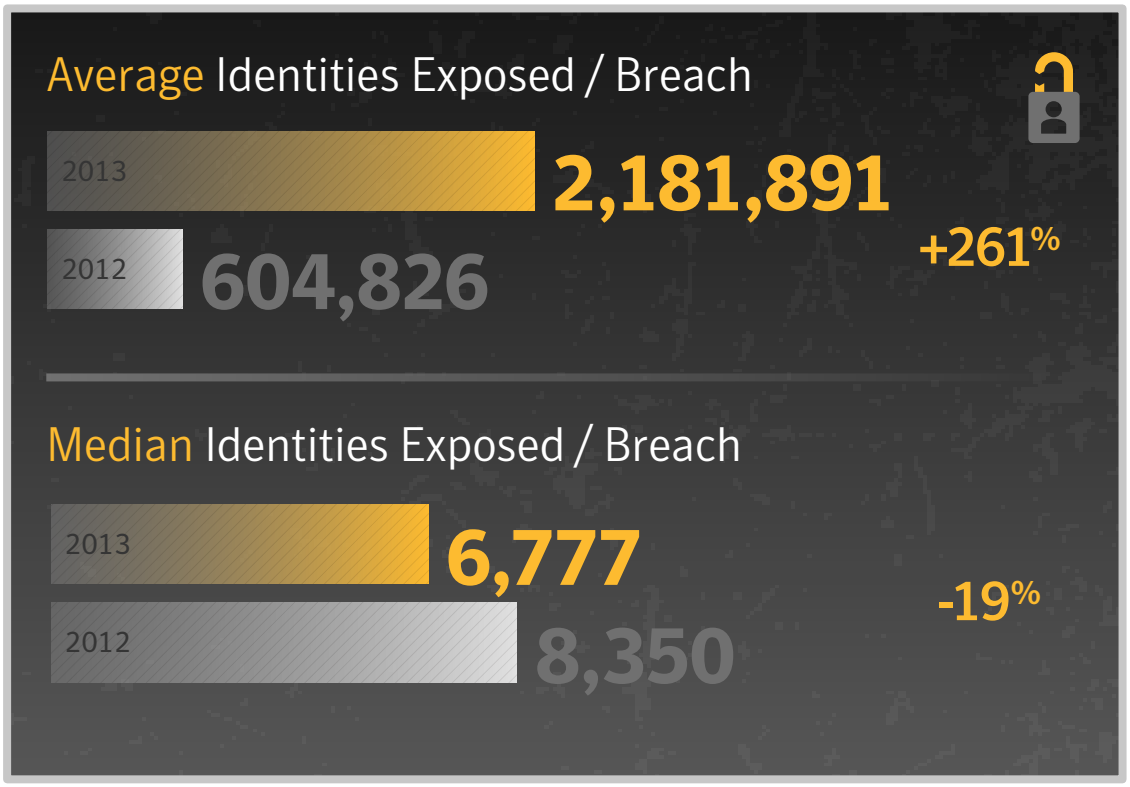
8 — 2013

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

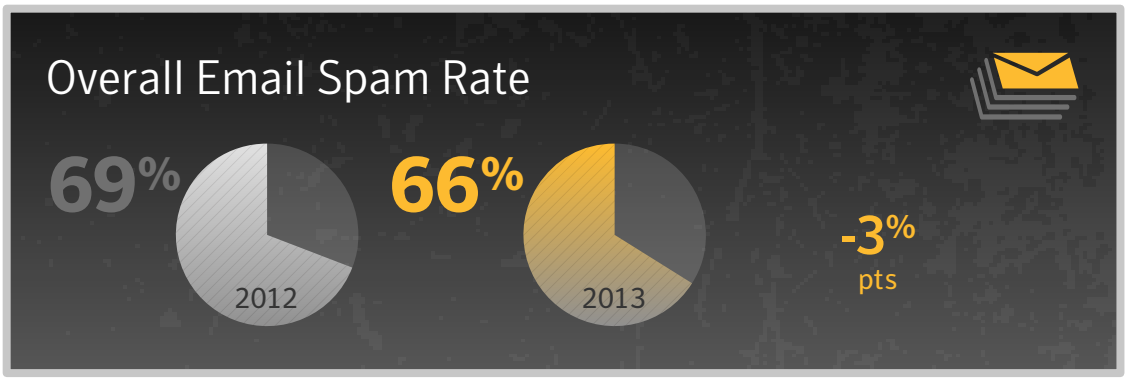
- *Mega Breaches were data breach incidents that resulted in the personal details of at least 10 million identities being exposed in an individual incident. There were eight in 2013, compared with only one in 2012.*

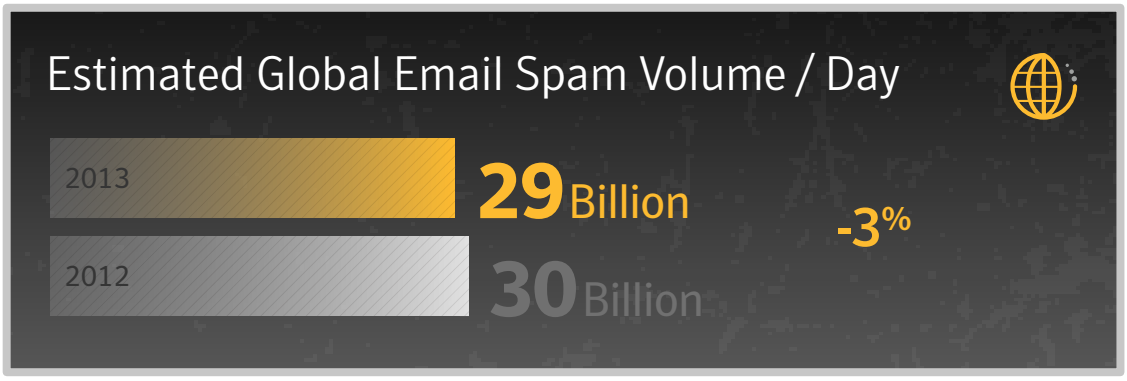
Breaches

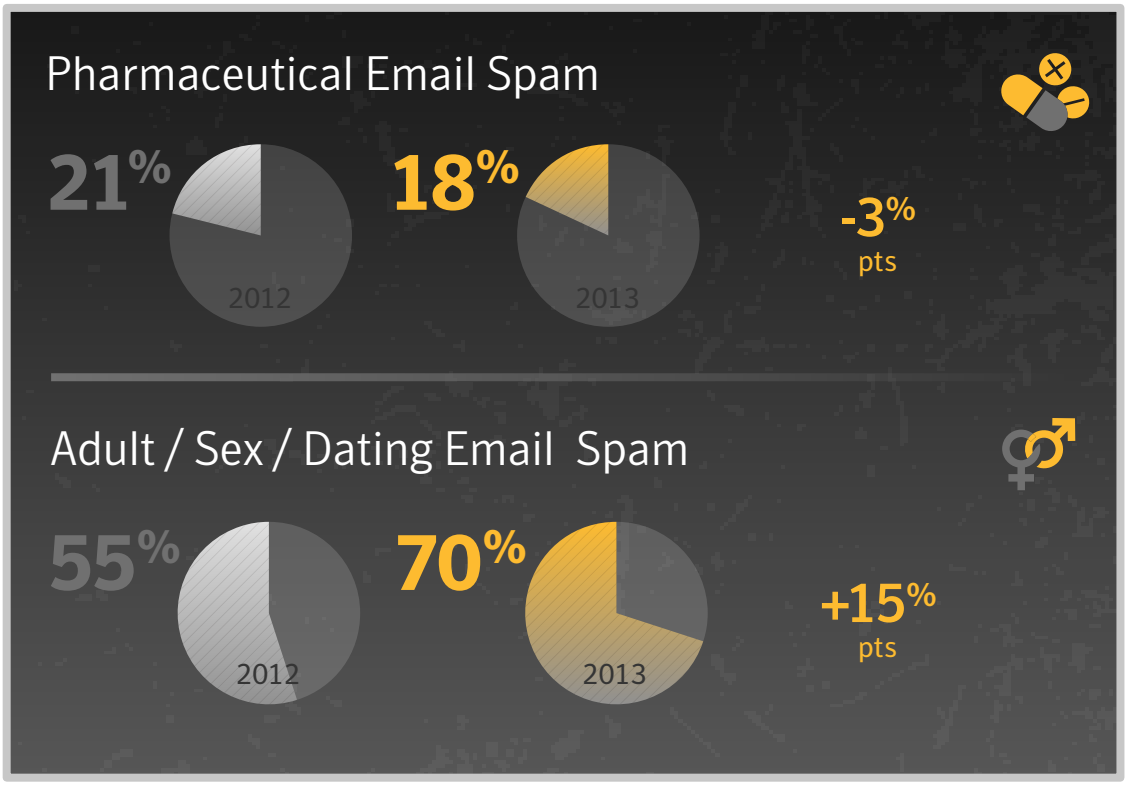


- *Hacking continued to be the primary cause of data breaches in 2013. Hacking can undermine institutional confidence in a company, exposing its attitude to security and the loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 34 percent 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

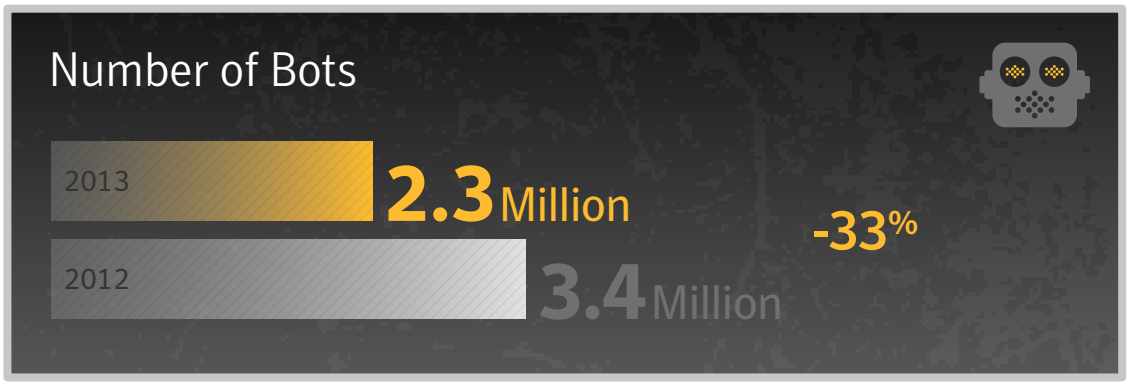


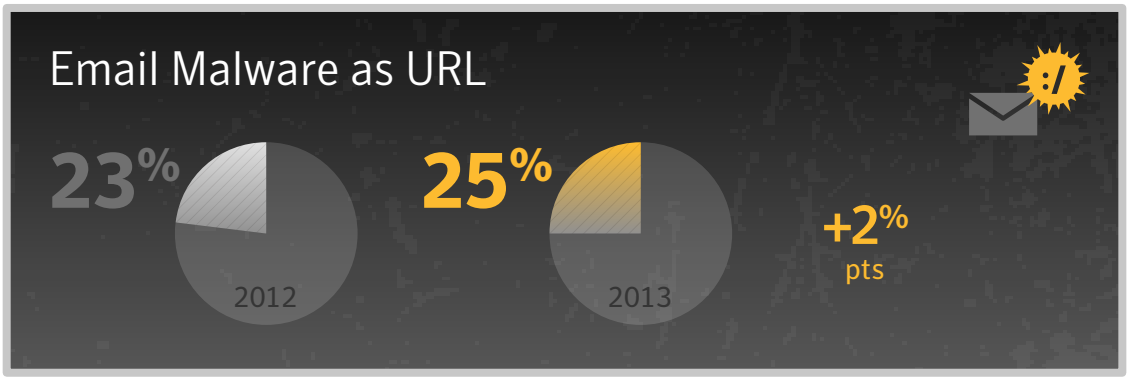


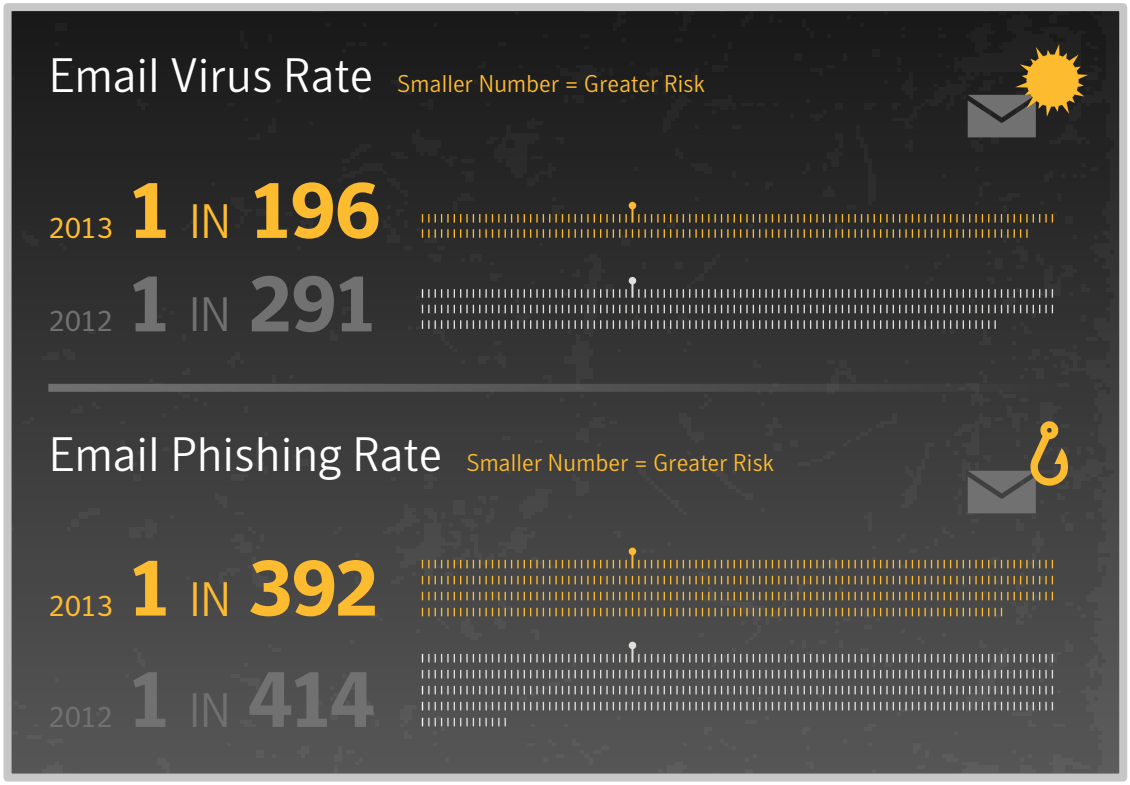


- *Approximately 76 percent of spam email was distributed by spam-sending botnets, compared with 79 percent in 2012. Ongoing actions to disrupt a number of botnet activities during the year have helped to contribute to this gradual decline.*
- *In 2013, 87 percent of spam messages contained at least 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%

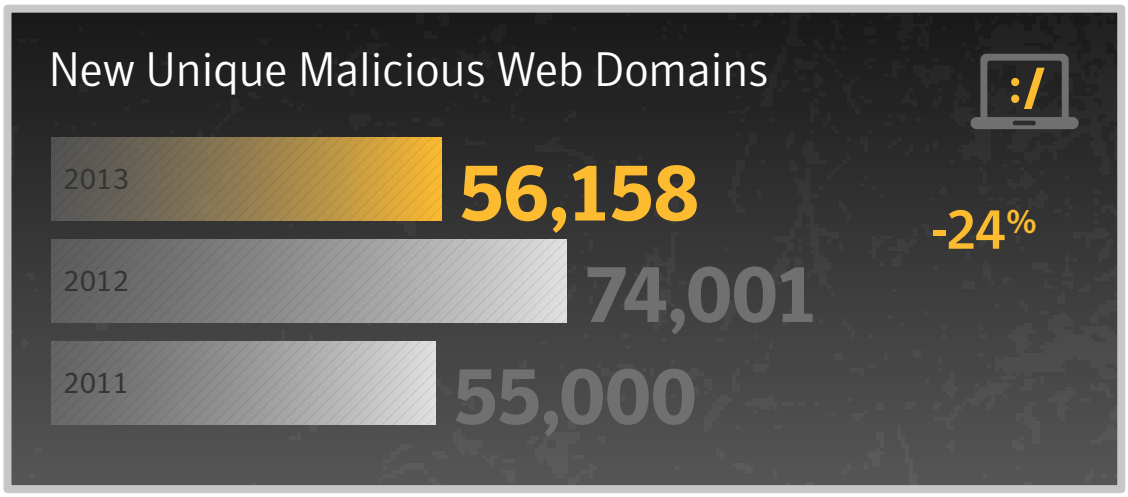
Mobile Vulnerabilities

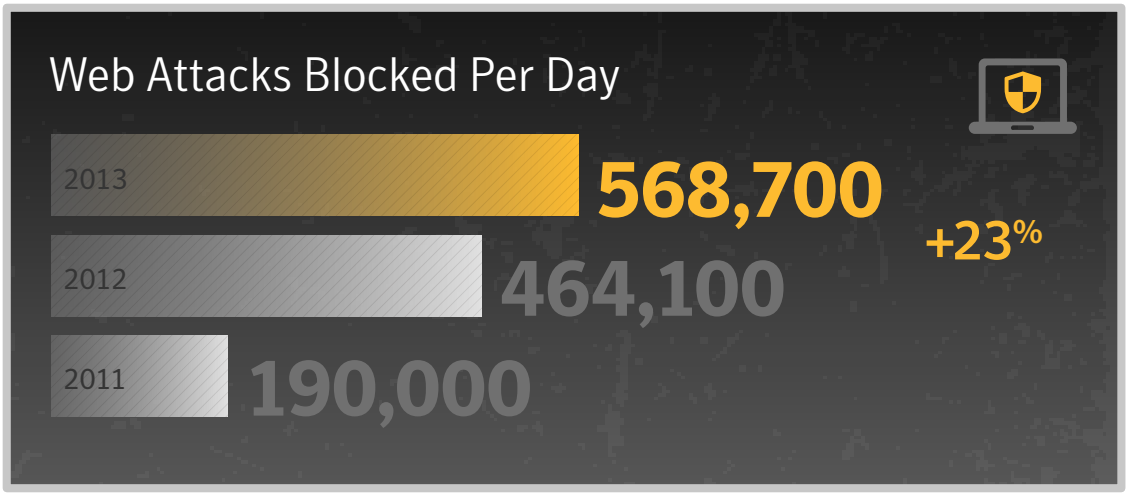
2013	127
2012	416

-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

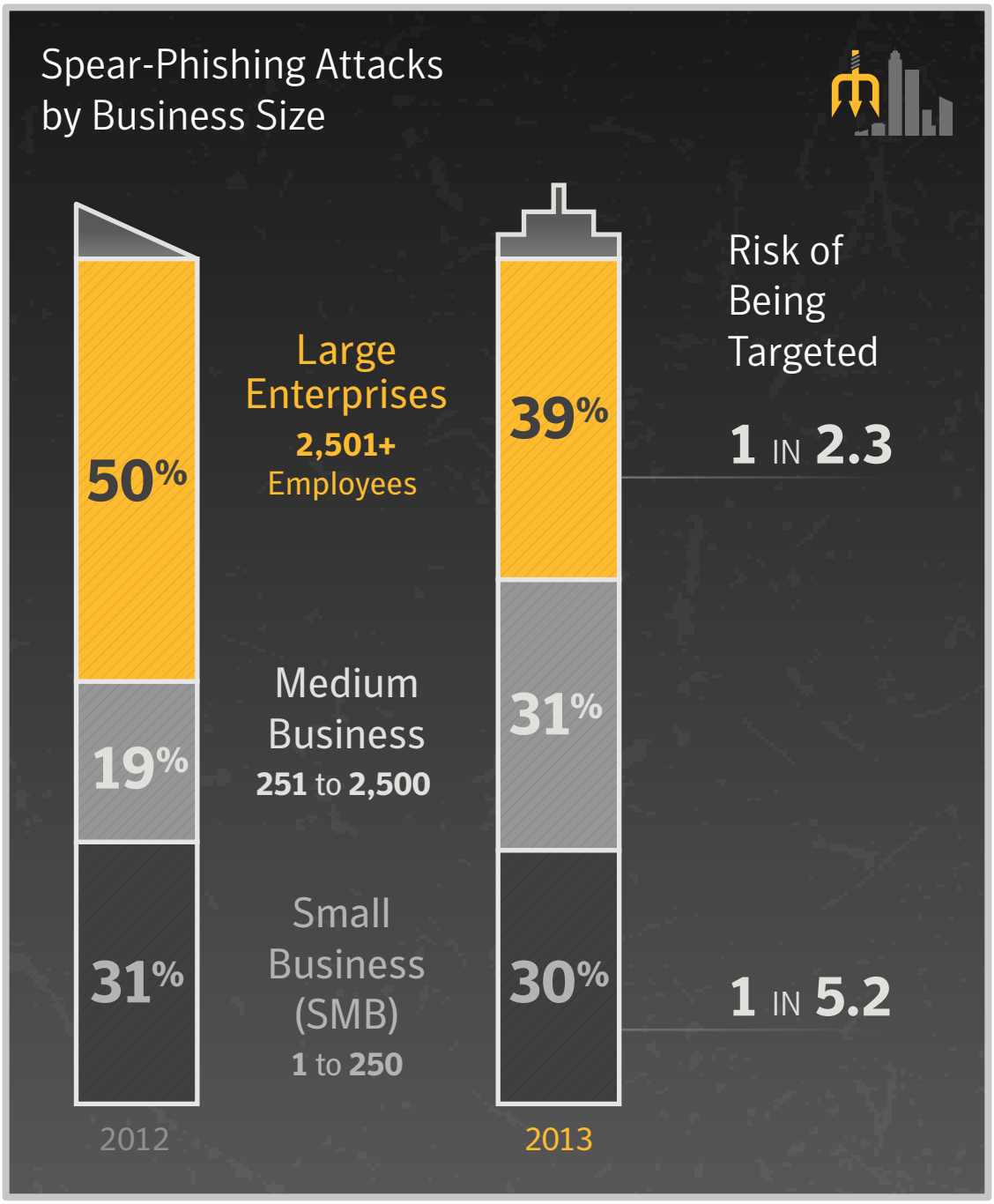




- *Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites.*
- *10 percent of malicious website activity was classified in the Technology category, 7 percent were classified in the Business category and 5 percent were classified as Hosting.*
- *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.*

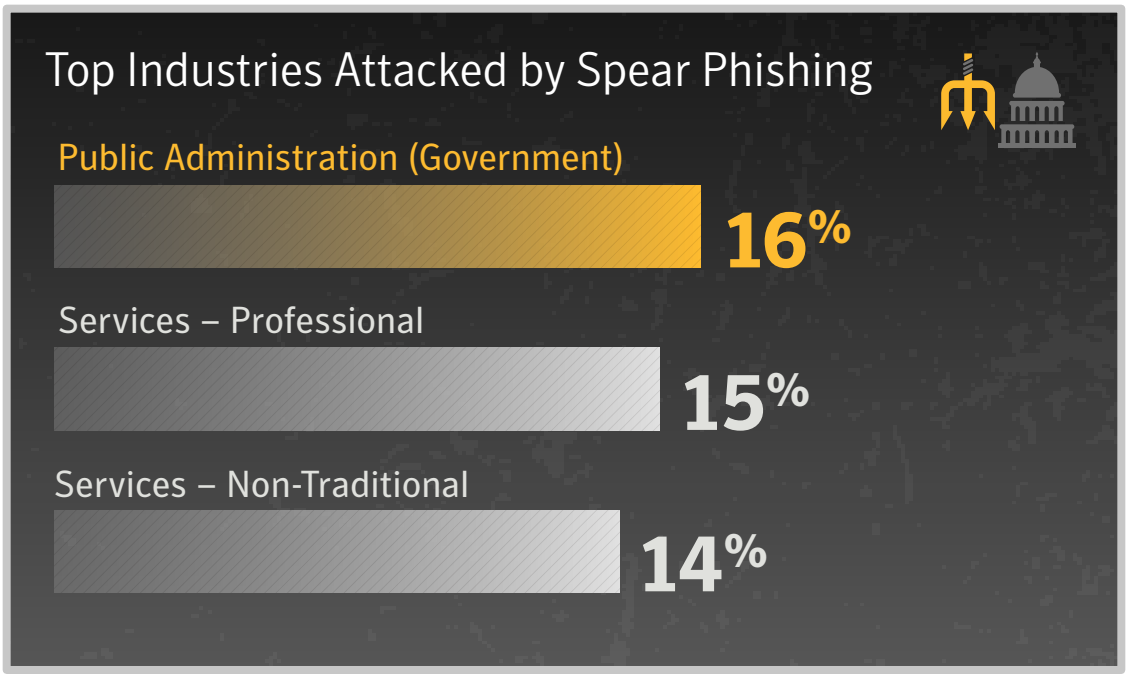
Targeted Attacks – Spear Phishing

TARGETED ATTACKS
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

Spear-Phishing Emails Per Day

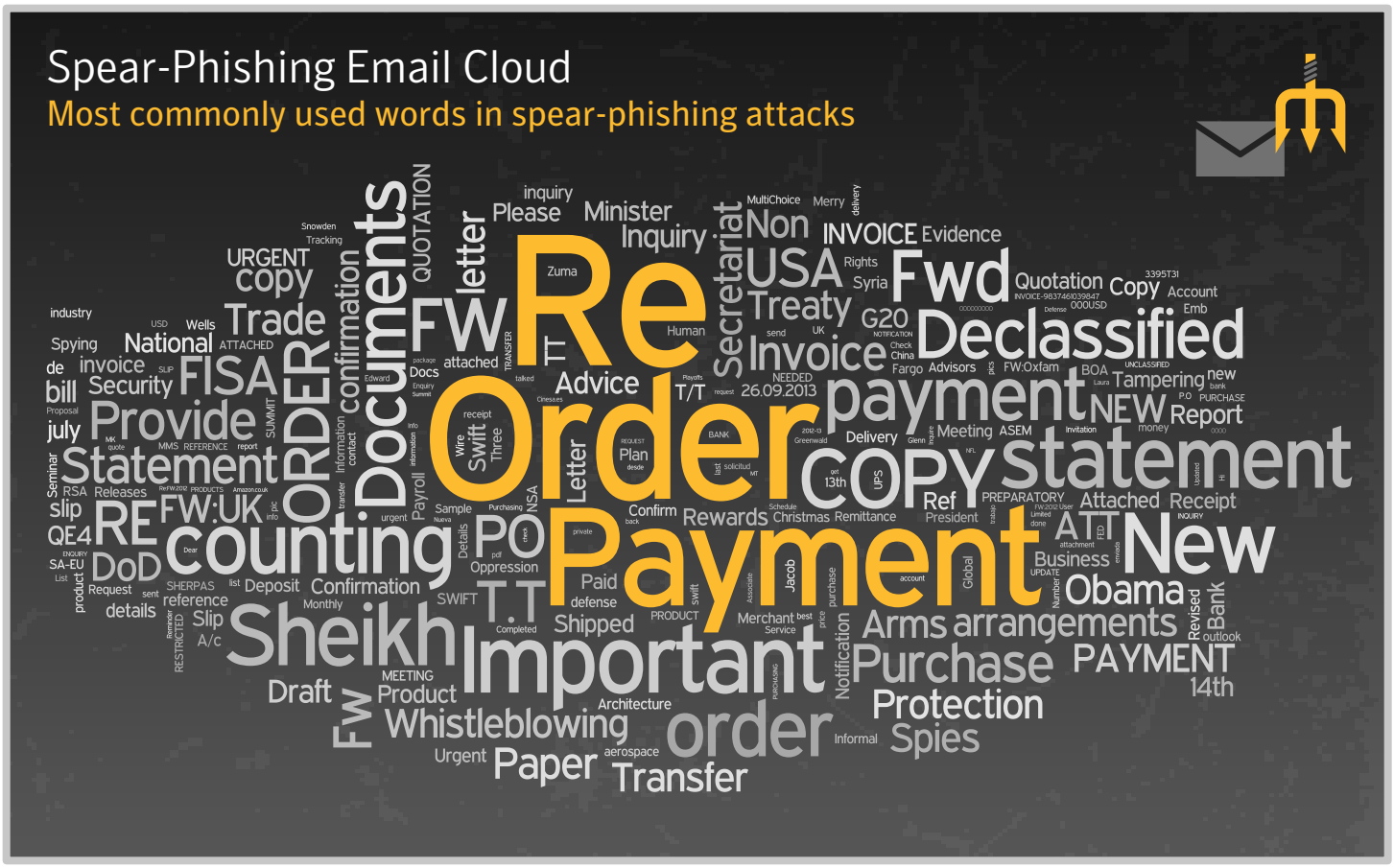
2012		2013
116	-28%	83

Spear-Phishing Email Campaigns

Campaigns in 2013	+91%	779
Recipients Per Campaign	-79%	23
Attacks Per Campaign	-76%	29
Average Time of Campaign	3x longer than 2012	Days 8

- *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


Spear-Phishing Email Cloud
Most commonly used words in spear-phishing attacks
Re
Order
Payment
Important
Sheikh
counting
Statement
Documents
Fwd
Declassified
payment
statement
New
Invoice
Secretariat
USA
Treaty
Non
INVOICE
Evidence
Please
Minister
Inquiry
inquiry
letter
FW
Trade
copy
URGENT
QUOTATION
confirmation
ORDER
FISA
Provide
National
Security
invoice
bill
Spying
Advice
T/T
TT
Letter
COPY
NEW
Report
Tampering
Quotation
Copy
Account
G20
Fargo
Advisors
FW:Oxfam
BOA
Delivery
Meeting
ASEM
Ref
PREPARATORY
Attached
Receipt
ATT
Business
Obama
Arms
arrangements
Purchase
PAYMENT
14th
Protection
Spies
Informal
Notification
Merchant
Shipped
Paid
defense
Rewards
Confirm
Christmas
Remittance
President
Oppression
PO
T.T
SWIFT
Deposit
Confirmation
Monthly
Slip
A/c
reference
details
Request
DoD
QE4
SA-EU
RE
FW:UK
slip
RSA
Releases
Seminar
July
Payroll
Sample
NSA
Swift
Three
Plan
Docs
attached
Edward
Human
Zuma
send
UK
NEEDED
26.09.2013
13th
UPS
Jacob
Global
Revised
Bank
outlook
Draft
MEETING
Product
Whistleblowing
Urgent
Paper
Transfer
order
Architecture
aerospace
FW
Multichoice
Merry
delivery
Rights
Syria
Check
China
Emb
3395T3I
000USD
Defense
Laura
UNCLASSIFIED
new
bank
PURCHASE
money
invitation
Greenwald
Glenn
NFL
Service
price
purchase
account
Associate
PURCHASING
Number
UPDATE
attachment
FED
envelope
INQUIRY
Limited
done
FW:2012 User
Schedule
Purchasing
Nueva
pdf
private
back
Dear
ENQUIRY
SHERPAS
list
sent
product
RESTRICTED
Reminder
Snowden
Tracking
USD
Wells
ATTACHED
SUMMIT
MMS
REFERENCE
report
quote
MK
Ref.W.2012
PRODUCTS
Amazon.co.uk
pic
info
transfer
urgent
Cinesaes
Playoffs
request
BANK
solicitud
desde
REQUEST
receipt
Wire
Enquiry
Summit
Payoffs
talked
PRODUCT
best
Completed
Greenwald
Laura
PO
PURCHASE
Proposal
Seminar
Releases
Amazon.co.uk
Dear
List
Request
sent
Slip
A/c
Monthly
Deposit
Confirmation
Oppression
Shipped
Paid
defense
Merchant
Service
Rewards
Confirm
Christmas
Remittance
President
Ref
PREPARATORY
Attached
Receipt
ATT
Business
Obama
Arms
arrangements
Purchase
PAYMENT
14th
Protection
Spies
Informal
Notification
Merchant
Revised
Bank
outlook
Draft
MEETING
Product
Whistleblowing
Urgent
Paper
Transfer
order
Architecture
aerospace
FW
Jacob
Global
UPS
13th
Plan
Letter
Swift
Three
Payroll
Sample
NSA
Docs
attached
Edward
Human
Zuma
send
UK
NEEDED
26.09.2013
Playoffs
request
BANK
solicitud
desde
REQUEST
receipt
Wire
Enquiry
Summit
Cinesaes
talked
TRANSFER
package
Check
China
Fargo
Advisors
FW:Oxfam
BOA
UNCLASSIFIED
Laura

Targeted Attacks – Web-Based

TARGETED ATTACKS
WEB-BASED

Scanned Websites With Vulnerabilities ...

53% 2012

77% 2013

+25% pts

... % of Which Were Critical

24% 2012

16% 2013

-8% pts

1 IN **8** sites had critical unpatched vulnerabilities

New Vulnerabilities

2013 **6,787**

2012 **5,291**

+28%

SSL and **TLS** protocol renogotiation vulnerabilities were most commonly exploited

- *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

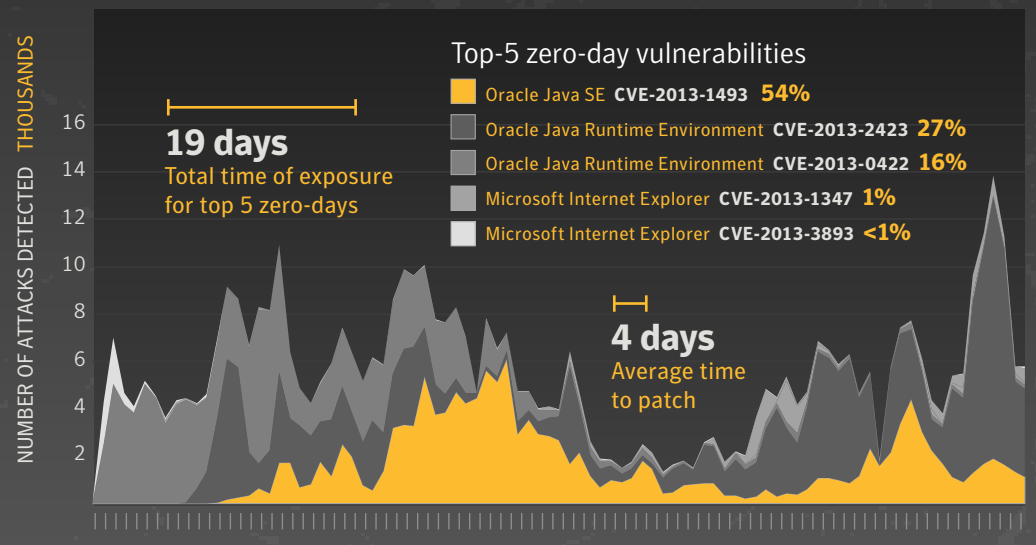
14
2012

+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.

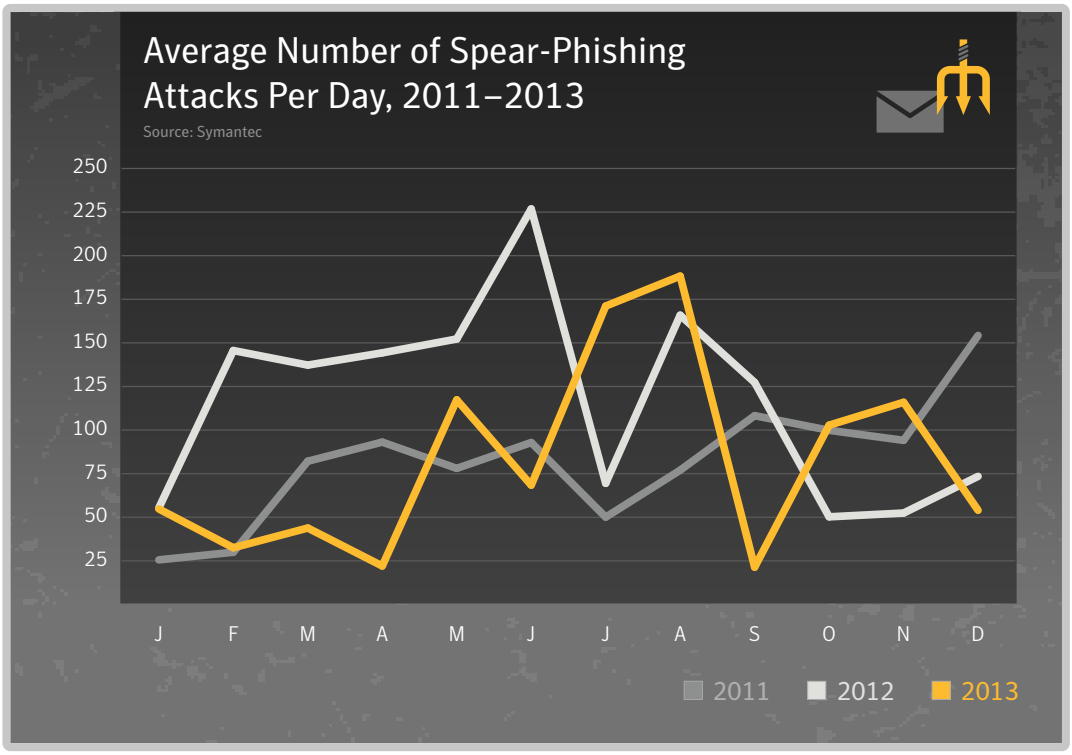
The number of recipients of spear-phishing emails during a campaign is also lower, at 23 recipients per campaign, down from 111 in 2012 and 61 in 2011. In contrast, these campaigns are lasting longer. The average duration of a campaign is 8.2 days, compared to 3 days in 2012 and 4 days in 2011. This 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

EMAIL CAMPAIGNS

2011 – 2013

Source: Symantec

	2013	2012	2013 vs 2012	2011	2013 vs 2011
SUBJ: Campaigns	779	408	+91%	165	+472%
Average Number of Email Attacks Per Campagn	29	122	-76%	78	-62%
Recipients per Campaign	23	111	-81%	61	-62%
Average Duration of a Campaign (in days)	8.2	3	+173%	4	+105%

- *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

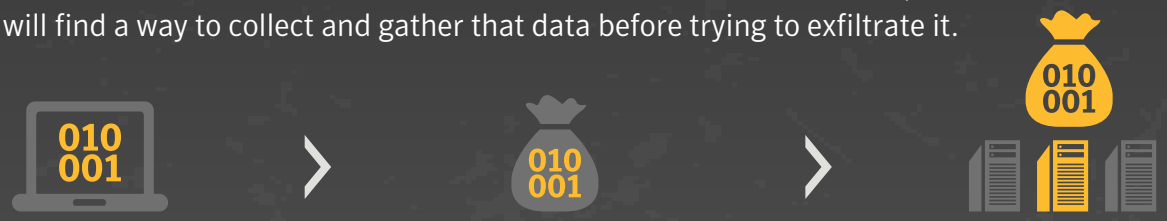
KEY STAGES

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.

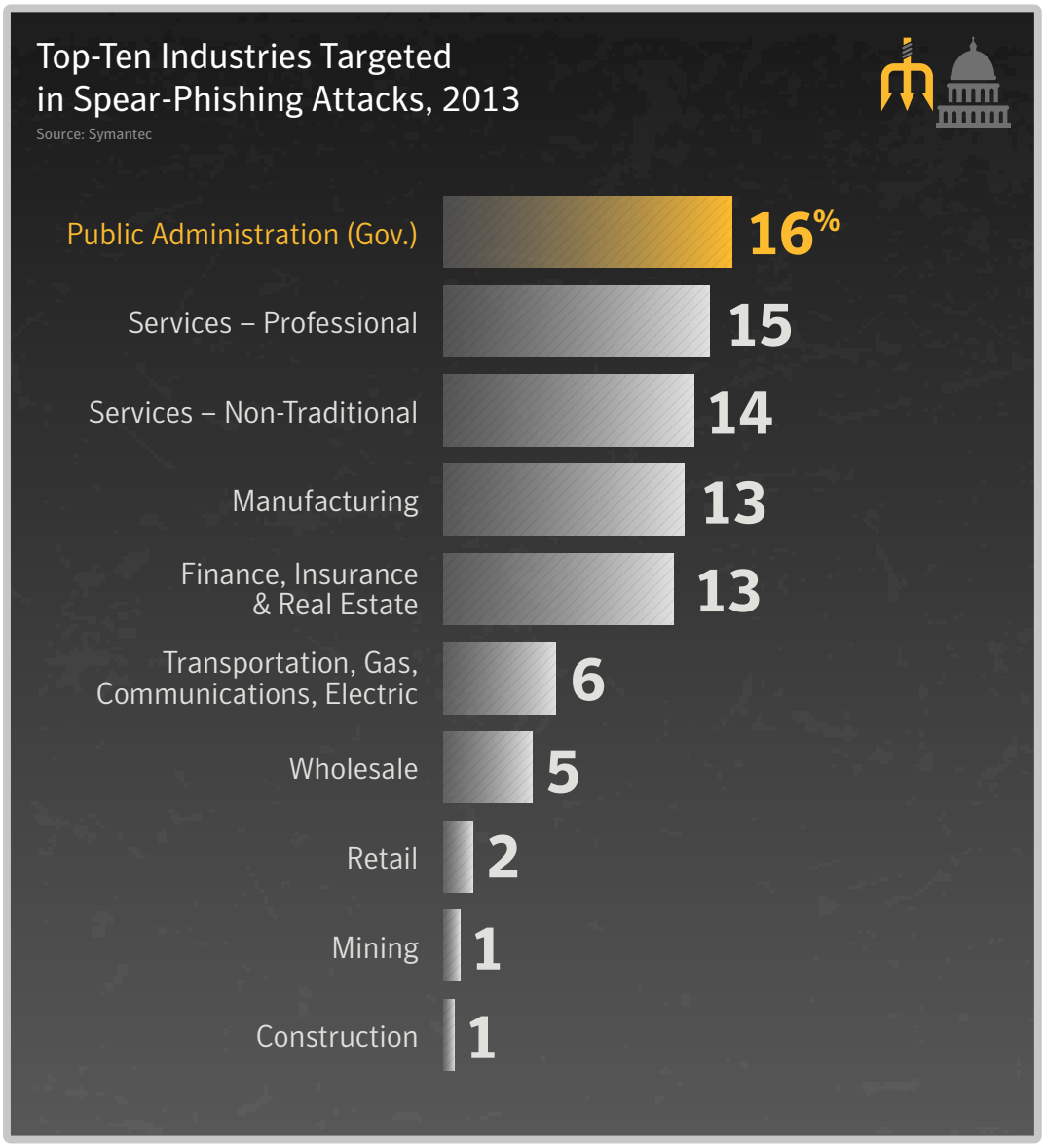
03 CAPTURE Once the valuable data has been discovered and identified, the attacker will find a way to collect and gather that data before trying to exfiltrate it.



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

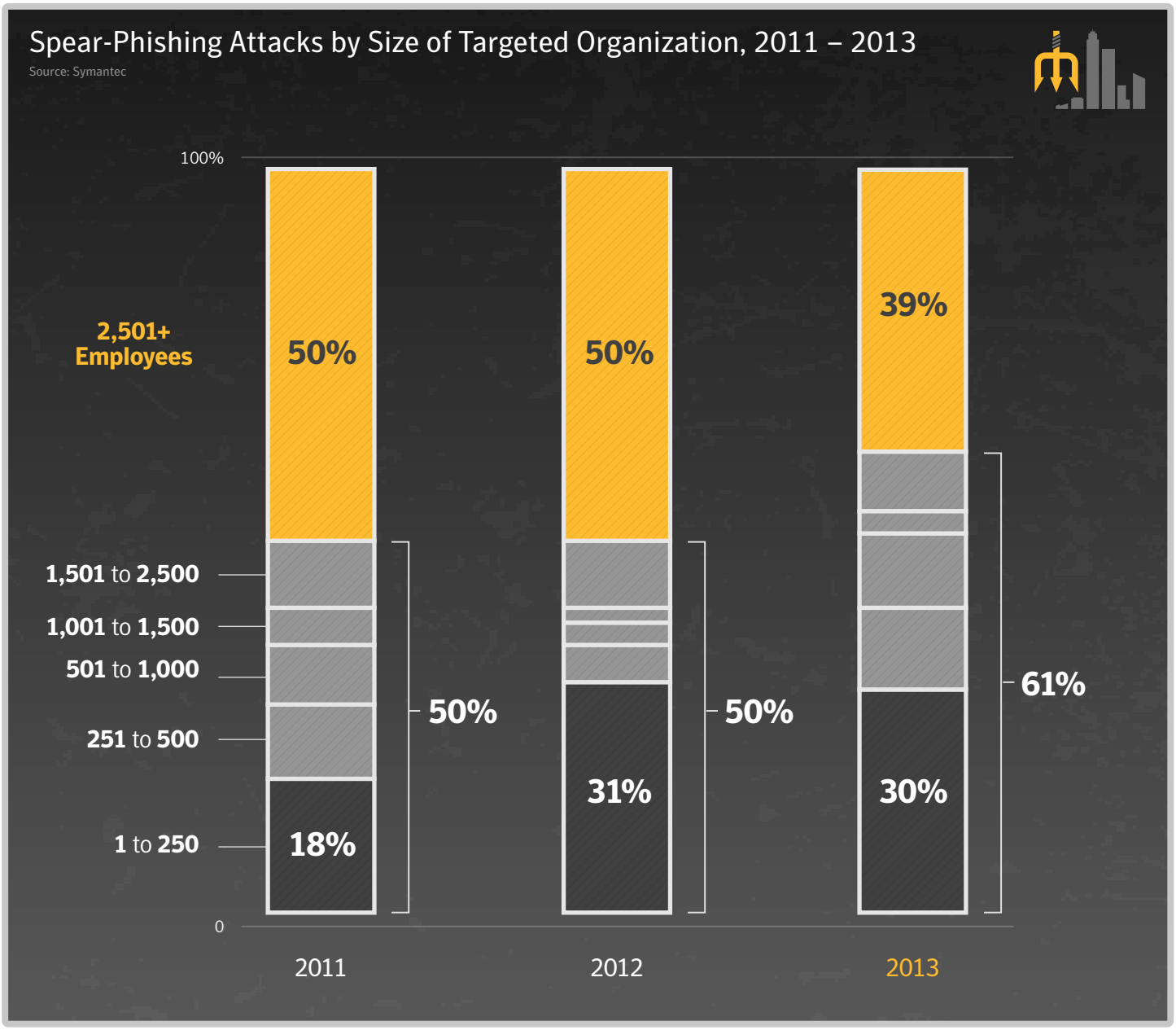


Politics and Targeted Attacks

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,

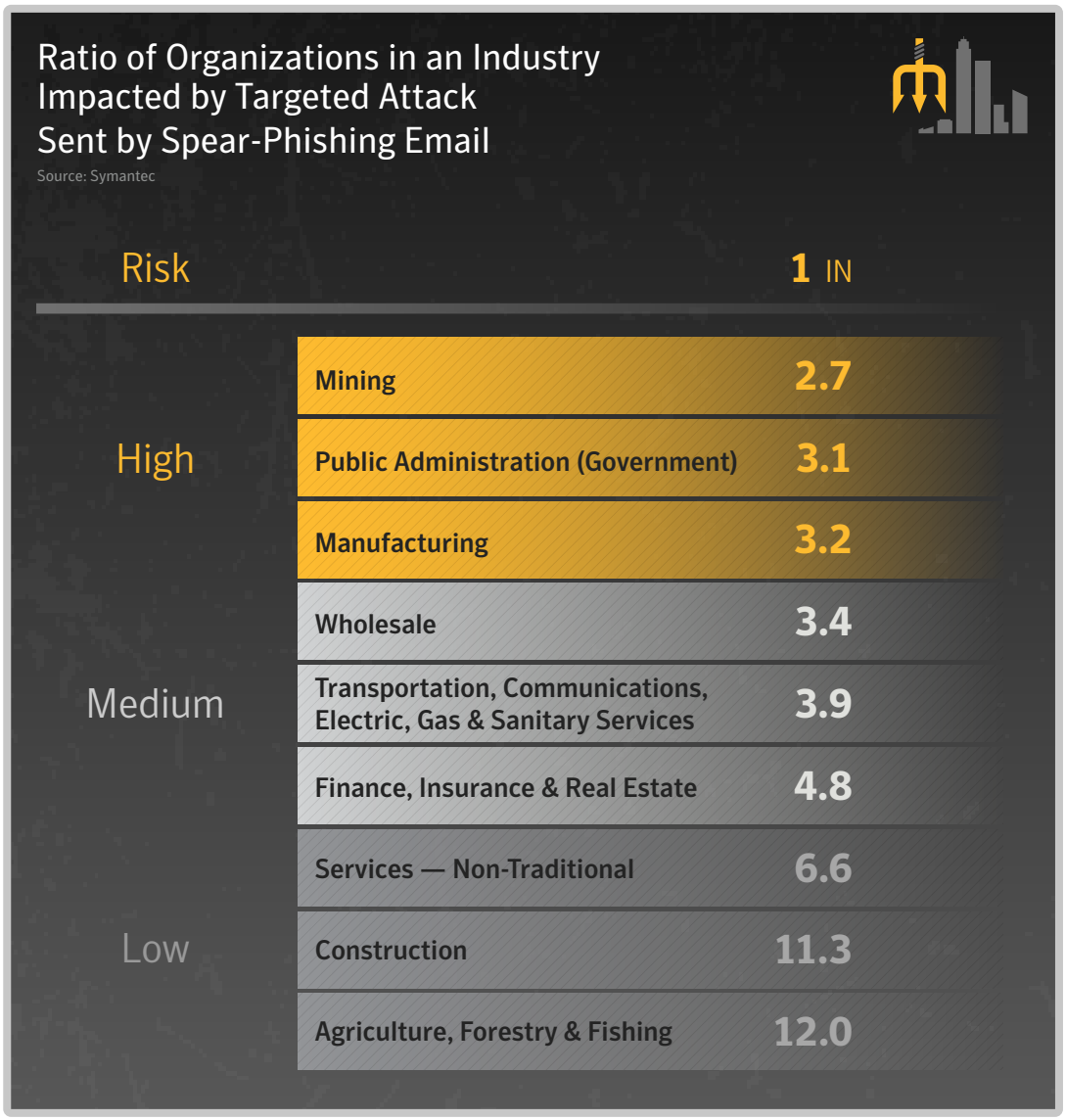
Fig. 6

- *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

Ratio of Organizations Targeted by Industry Size Sent by Spear-Phishing Email[07]

Source: Symantec

Risk		1 IN
High	2,500+	2.3
	1,501–2,500	2.9
	1,001–1,500	2.9
Medium	501–1,000	3.8
	251–500	4.3
	1–250	5.2

- *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

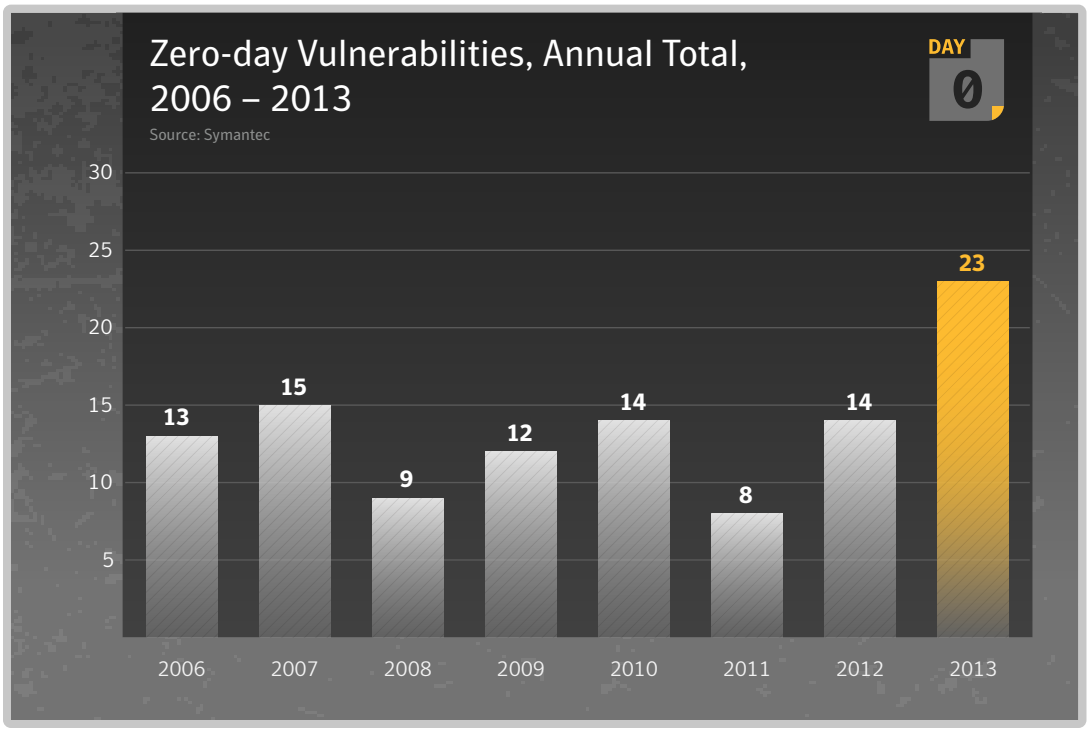
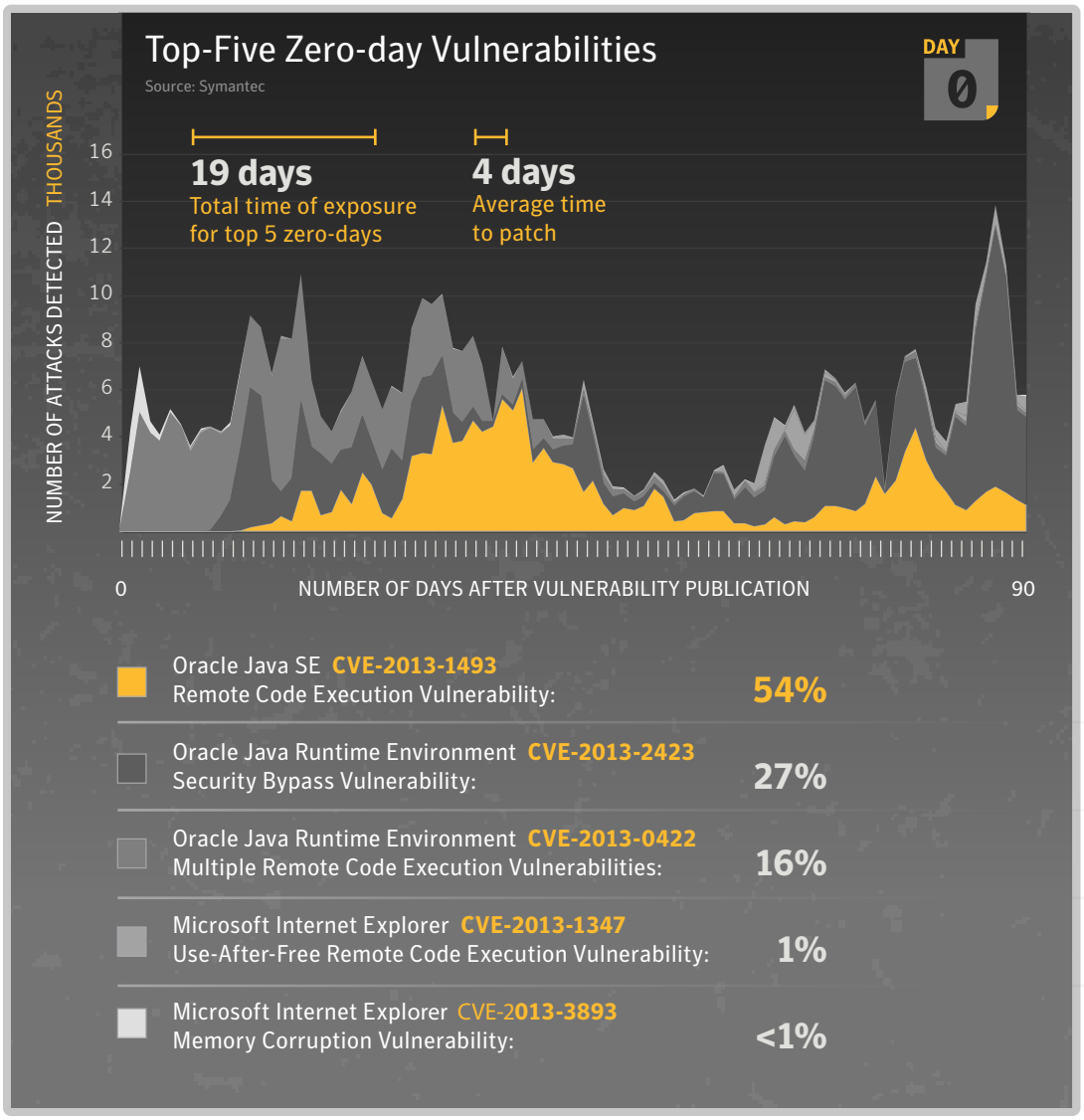


Fig. 11



- *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.

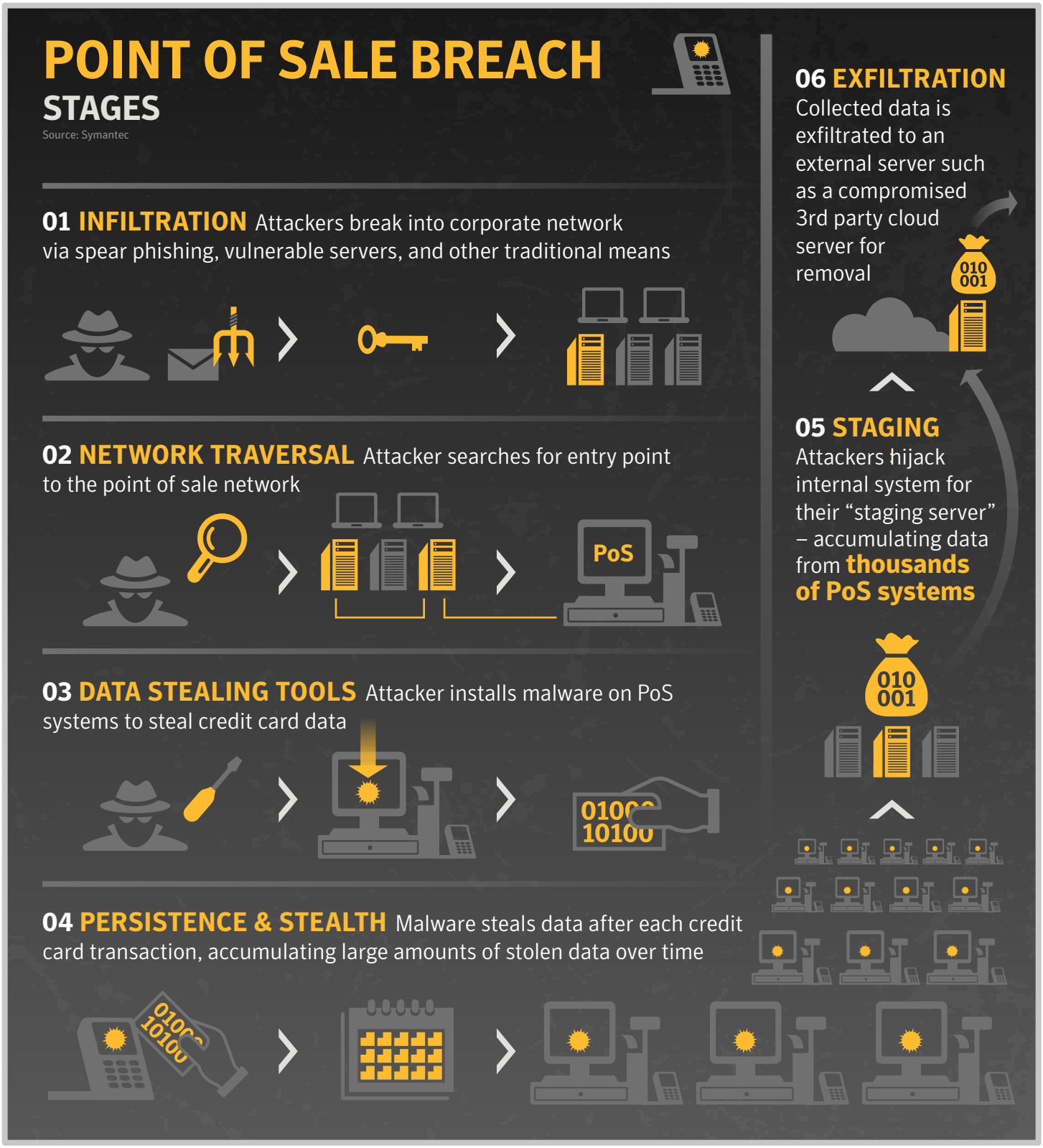
02 Once the attacker has established a beachhead into the network, they will need to get to their targeted systems. To achieve this, the attacker needs to either attempt to exploit vulnerabilities using brute-force attacks or steal privileged credentials from an employee through an information-stealing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

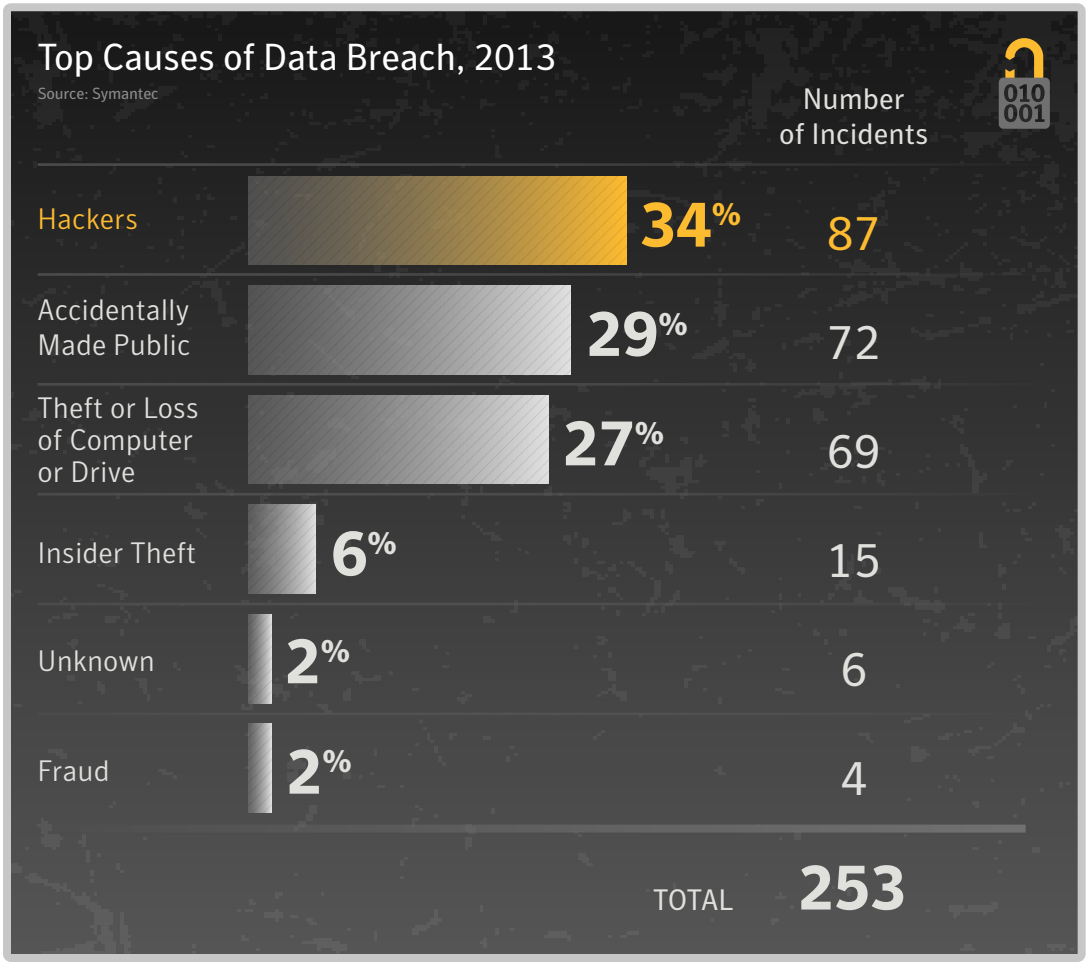
Data Breaches

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.

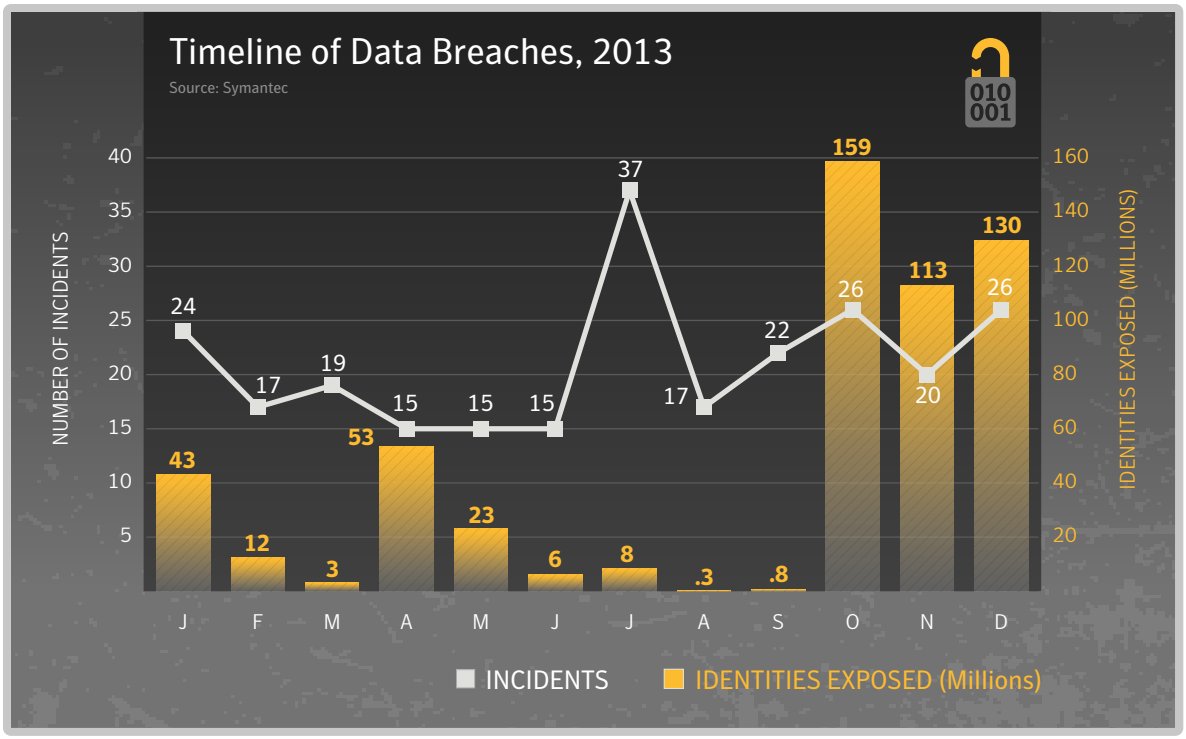
Alternatively system glitches may expose data to users who should not be able to see or share such material. For instance, users may be granted permissions on company storage resources that are higher than necessary, thus granting them too much access rather than just enough to do what they need. Privileged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

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."

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.

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.

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.

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.

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.

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

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

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

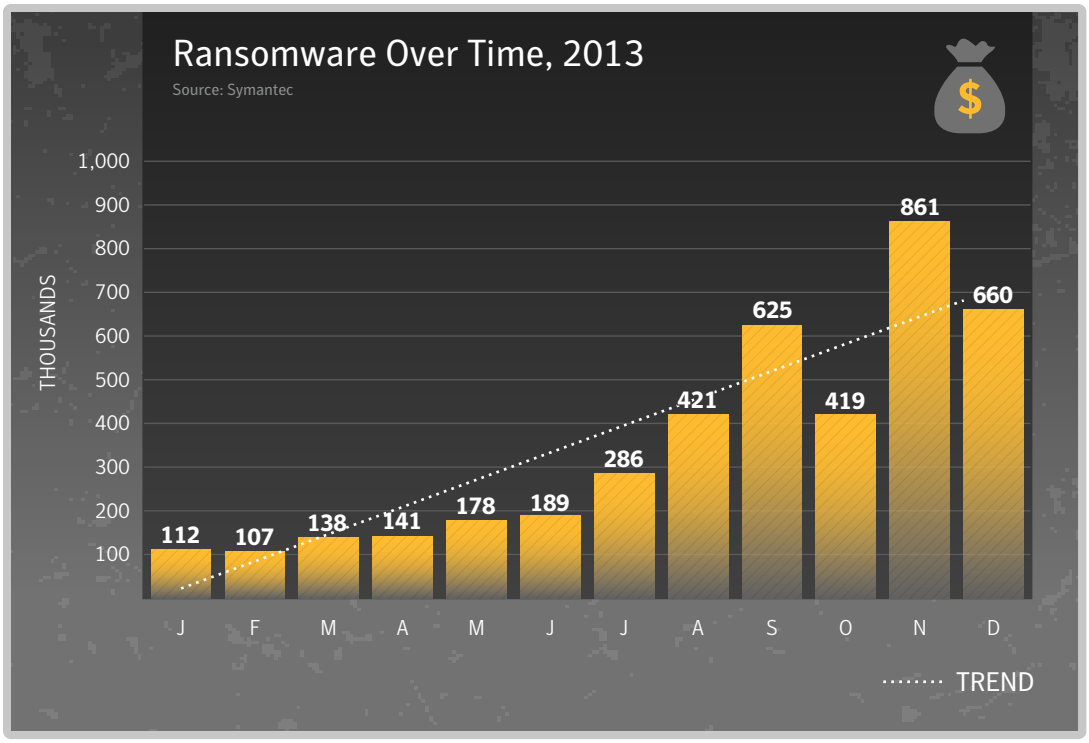
Top-Ten Botnets, 2013

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.

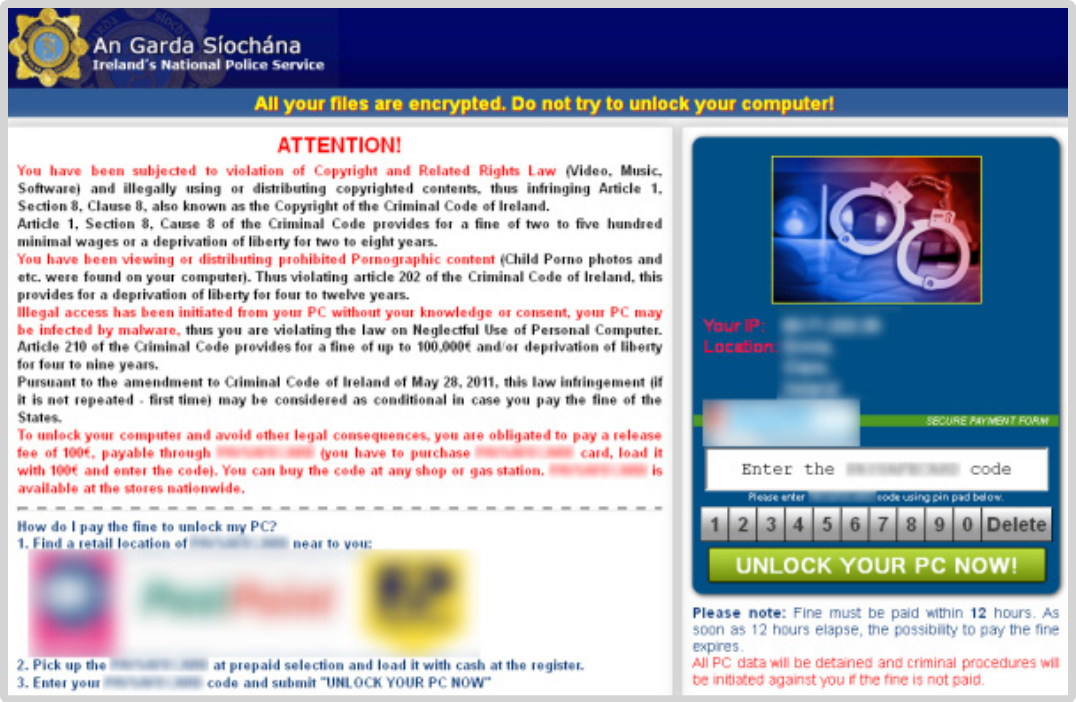


Fig. 4 *Browser-based ransomware threat, Browlock.*

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

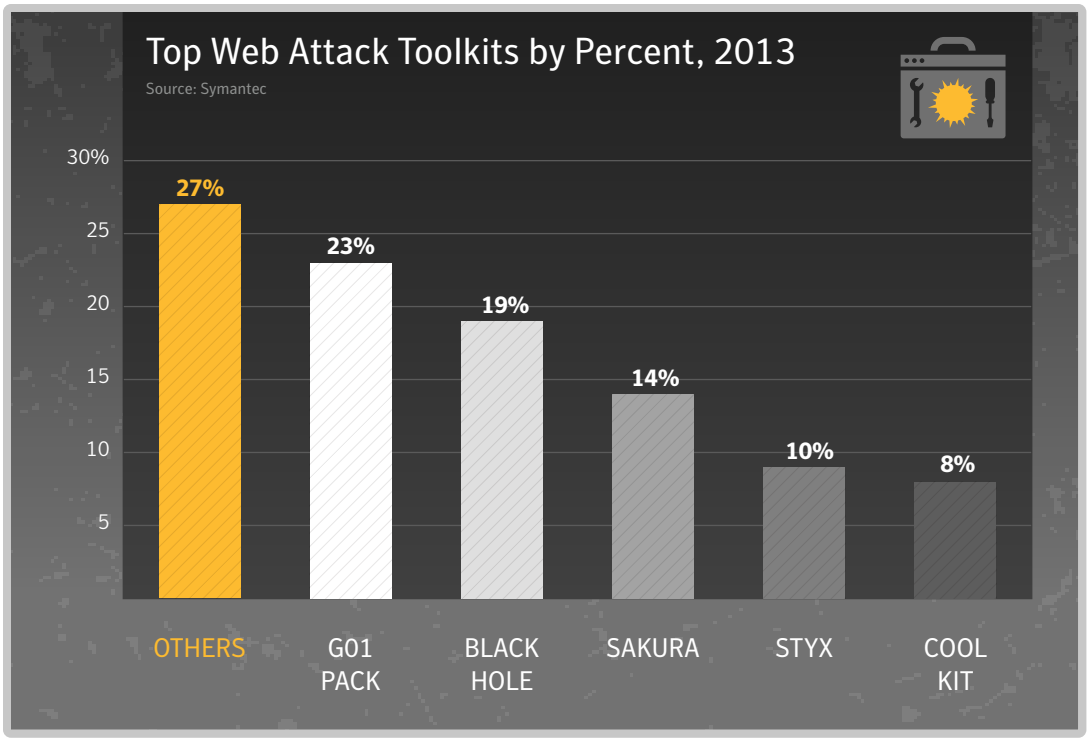
This sort of setup has allowed toolkit owners to experiment with different service offerings. This ranges from end-to-end coverage where the toolkit administrator sets everything up, to a less hands-on approach where tech support services are available to help the purchaser if they encounter configuration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

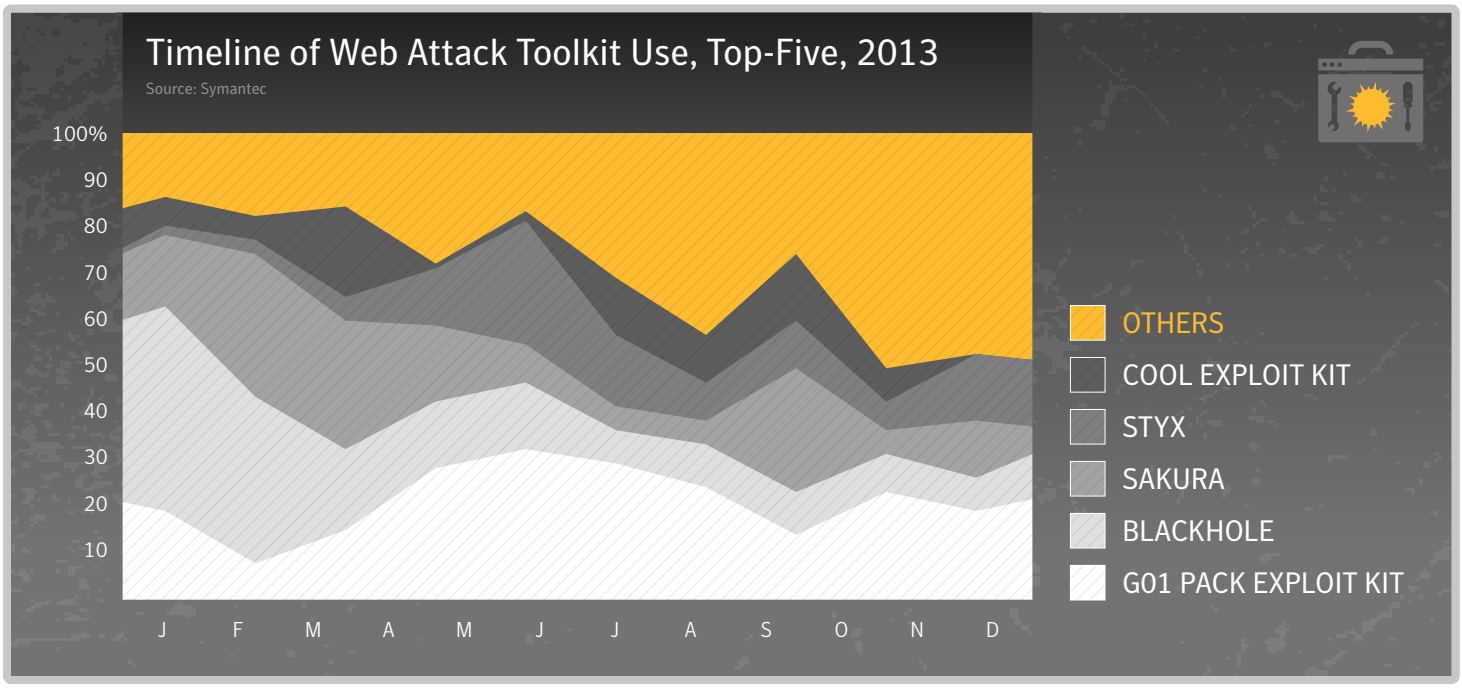
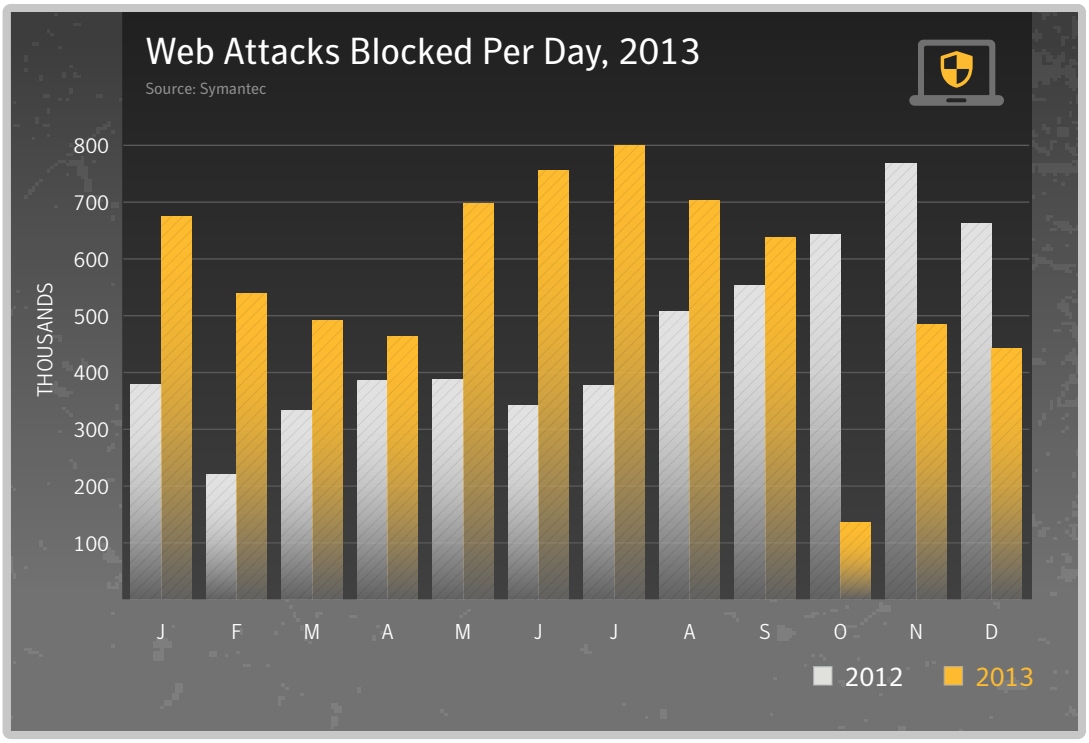


Fig. 8



- *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.

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.

Social Engineering Toolkits: From RATs to Creepware

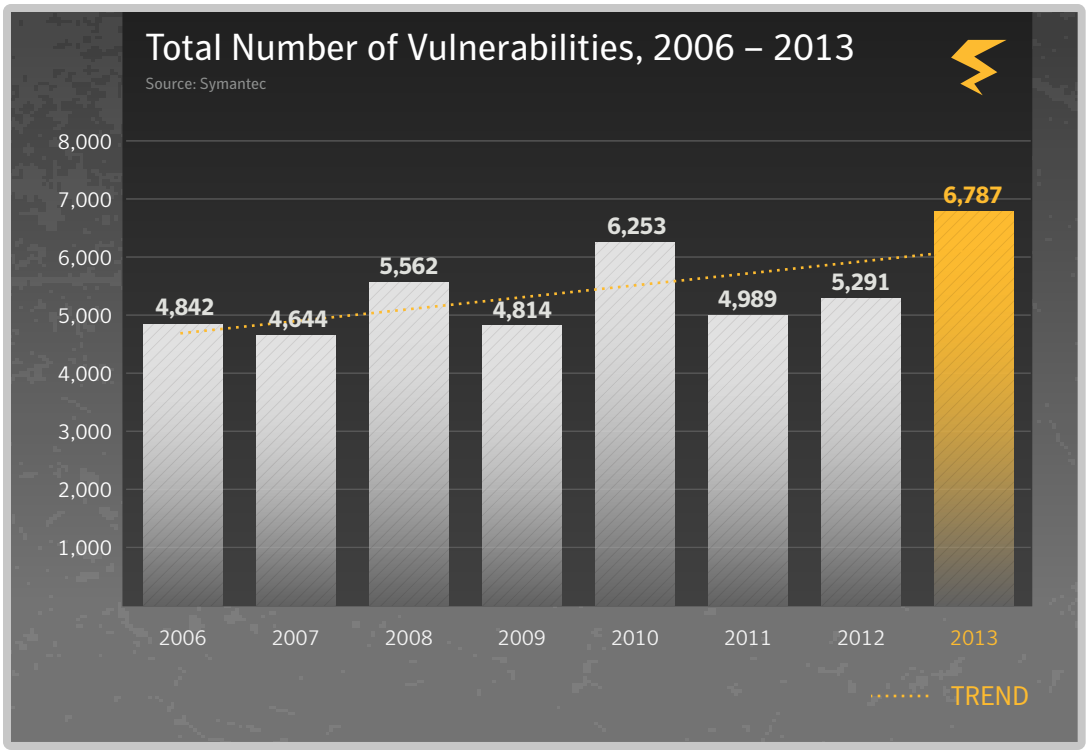
While web-attack toolkits tend to dominate the discussion in the threat landscape, they are not the only type of toolkits out there. There are also toolkits designed for penetration testing and detecting vulnerabilities that are open to exploits, often used legitimately by the whitehat community, but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

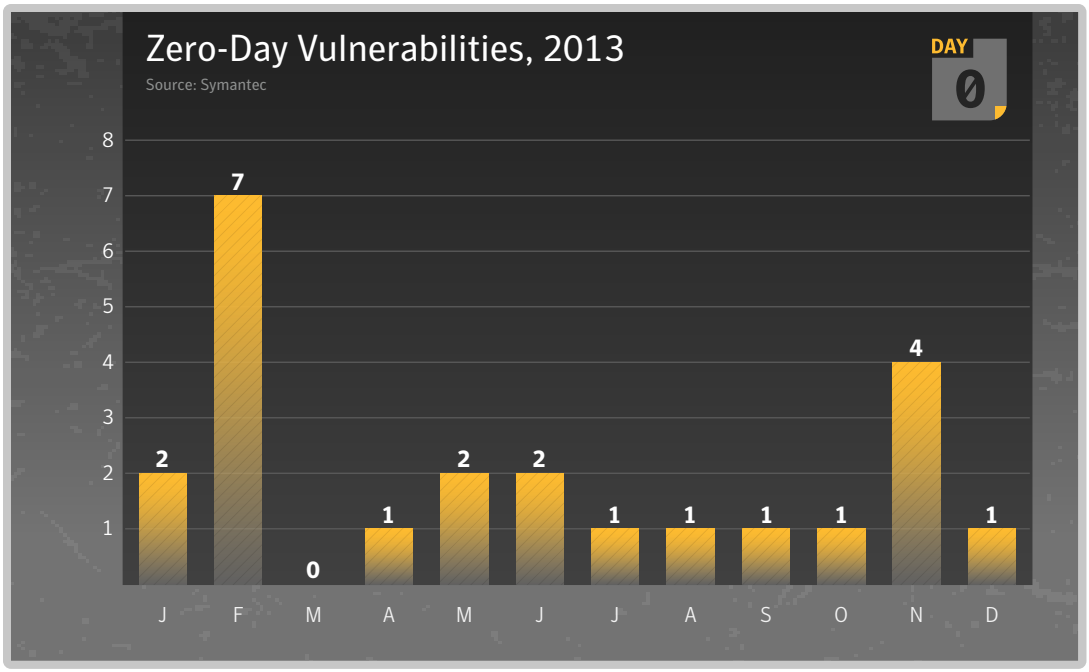
Creepware is a type of threat that uses toolkits. These threats are usually installed through social engineering and allow attackers to spy on the victims.[26] In many cases, the attackers administer their creepware by using toolkits that allow them to carry out various activities through the toolkit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

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

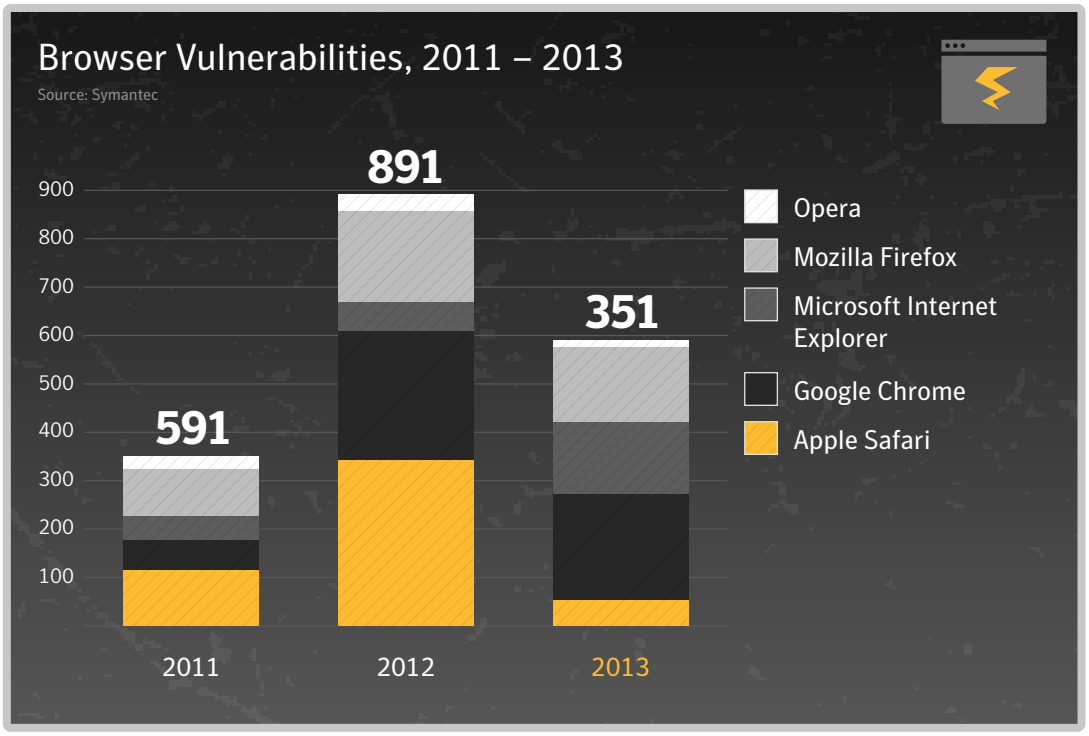
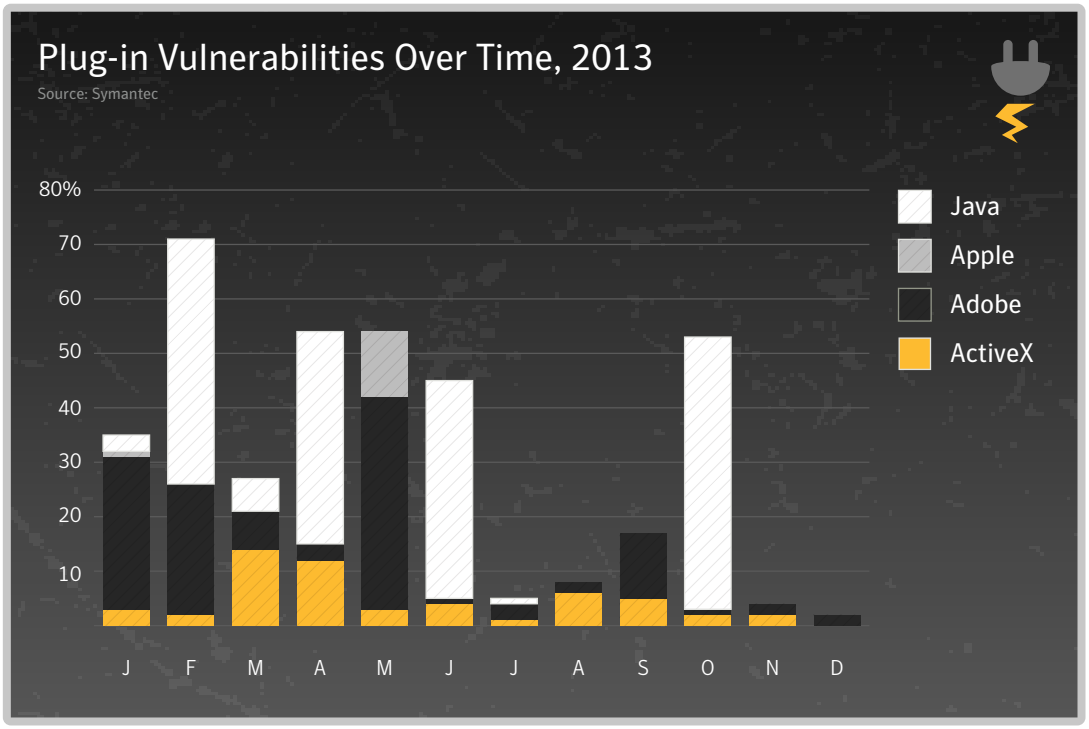
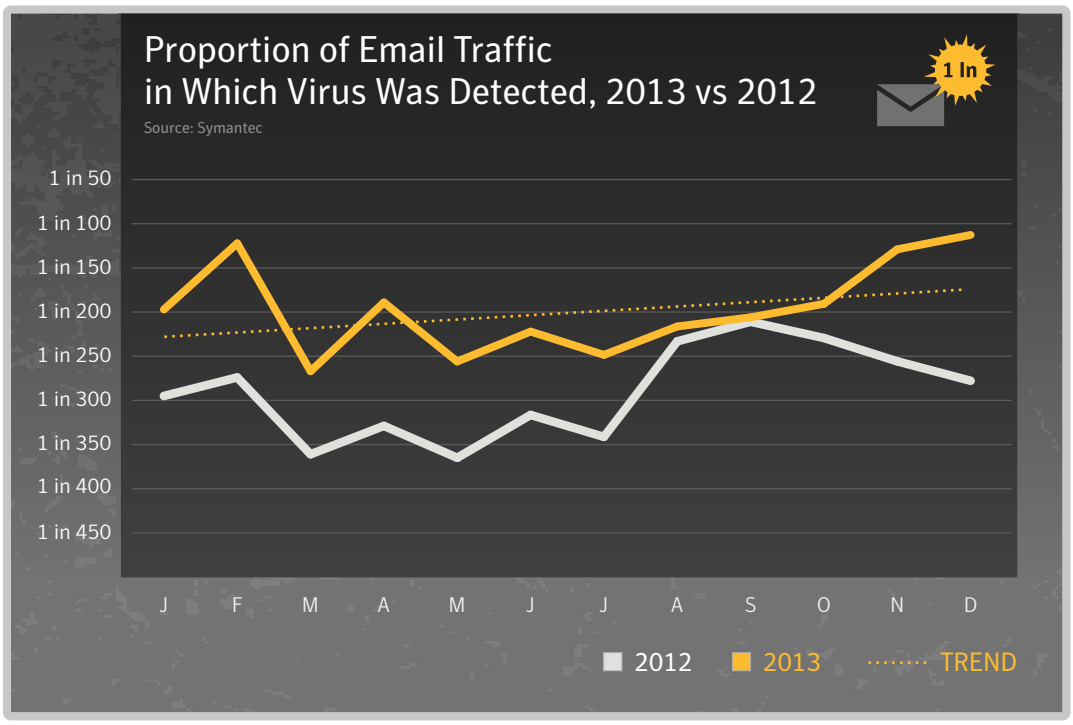


Fig. 13



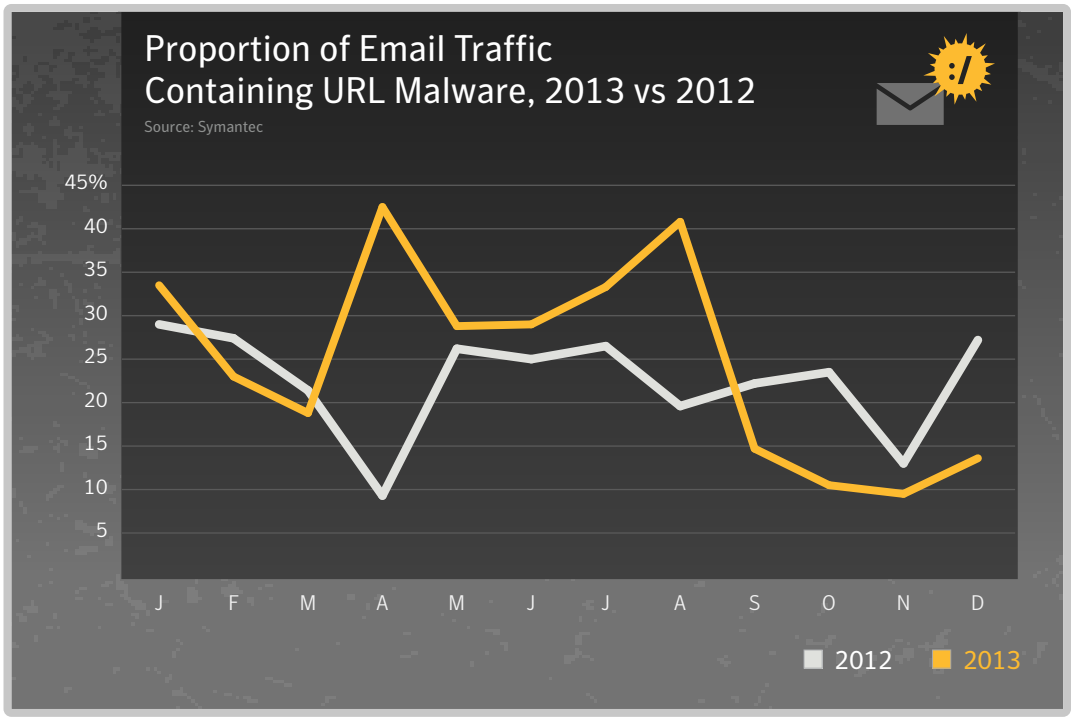
- *In 2013, 375 vulnerabilities affecting browser plug-ins were documented by Symantec, an increase compared to 312 vulnerabilities affecting browser plug-ins in 2012.*
- *ActiveX vulnerabilities decreased in 2013.*
- *Java vulnerabilities increased in 2013. This upward trend was already visible in 2012, 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

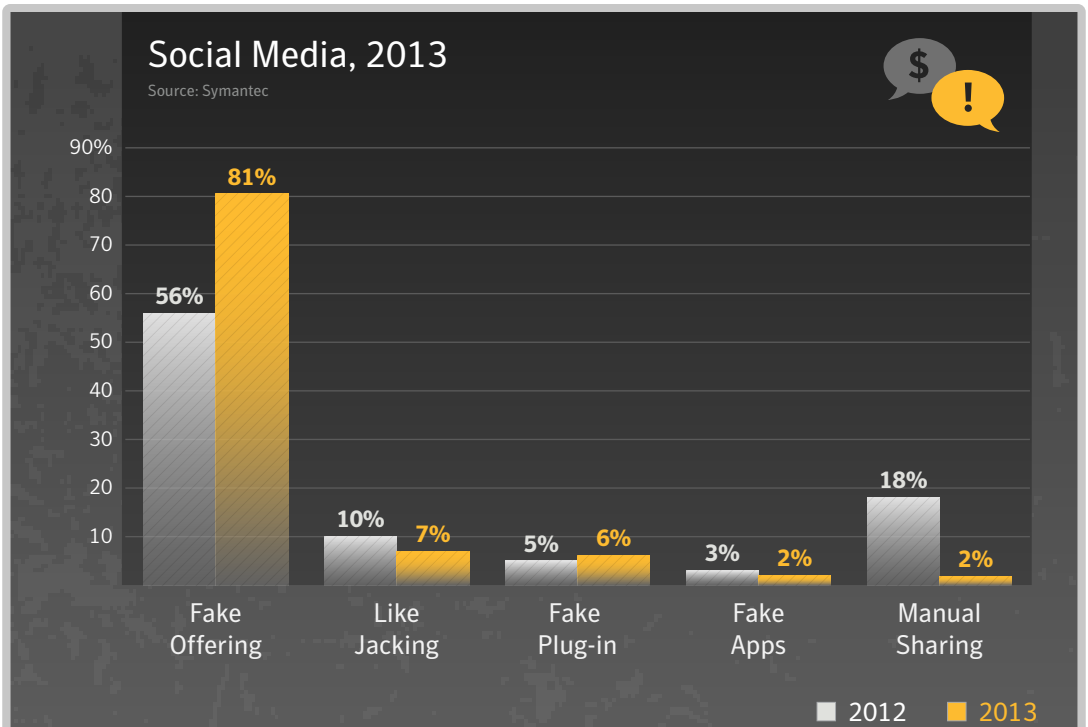
Phishing and spam is evolving, moving further away from email and into the social media landscape. These social media campaigns include the same lures that are seen in phishing and spam email. The types of material being offered remains similar to past years: gift cards, electronics, concert tickets, 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.*

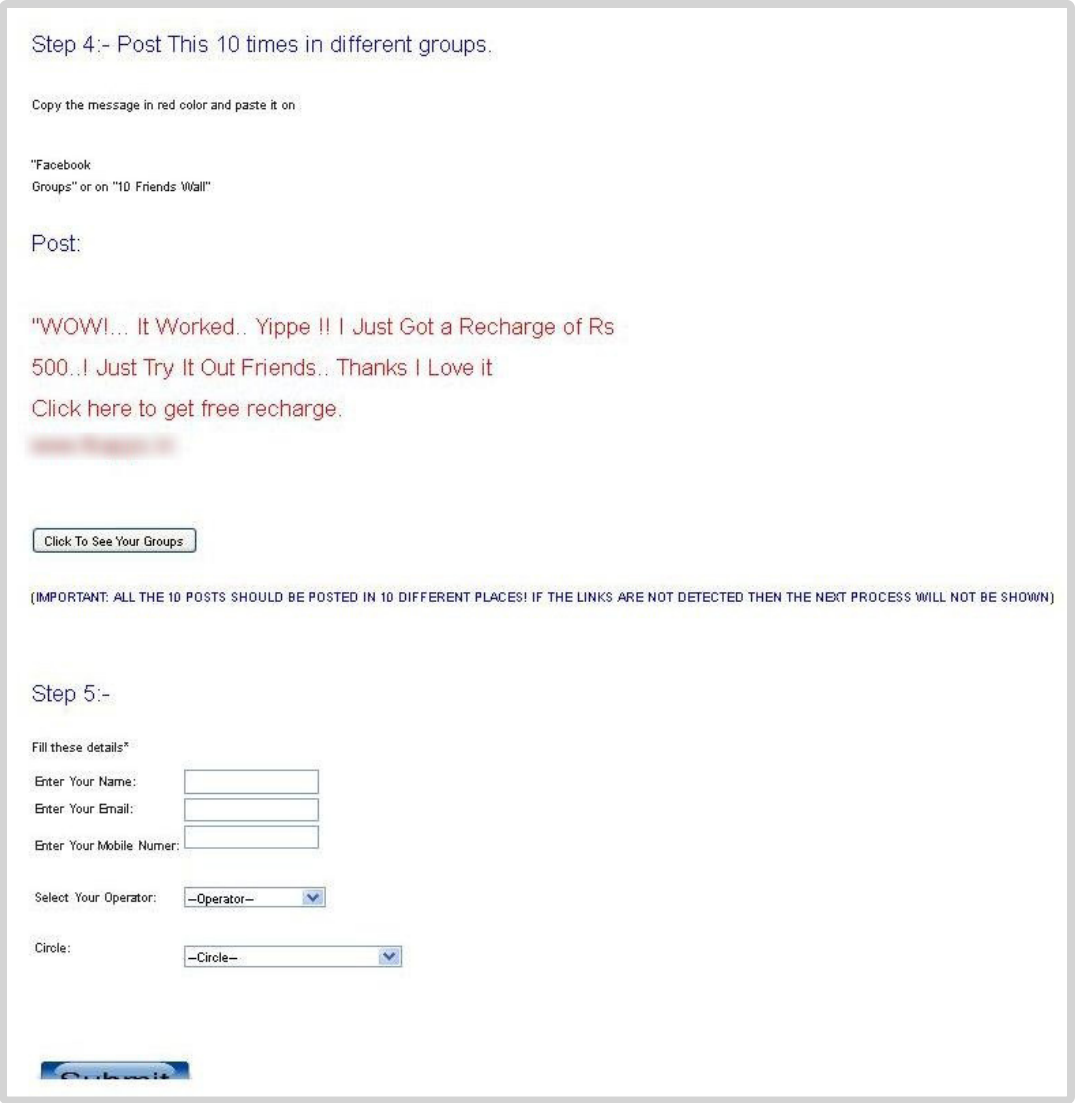


Fig. 2 *Social media scam offering free cell phone minutes.*

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

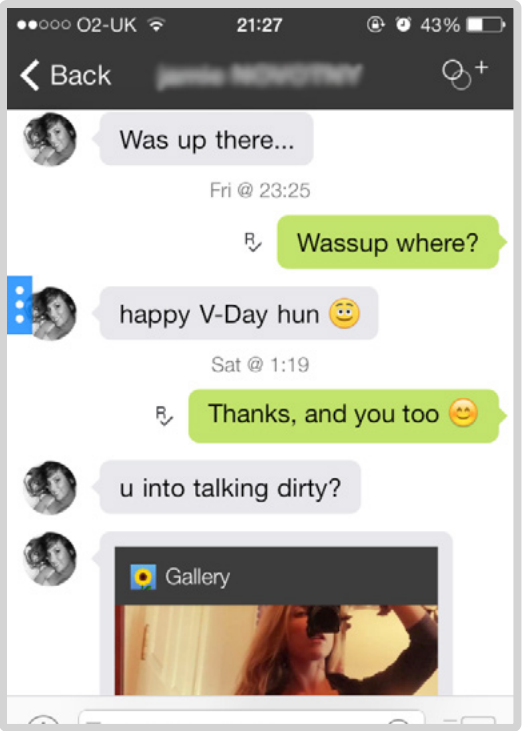


Fig. 3 Dating scam, where scammers send racy photos if the user agrees to install apps of their choosing.

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.

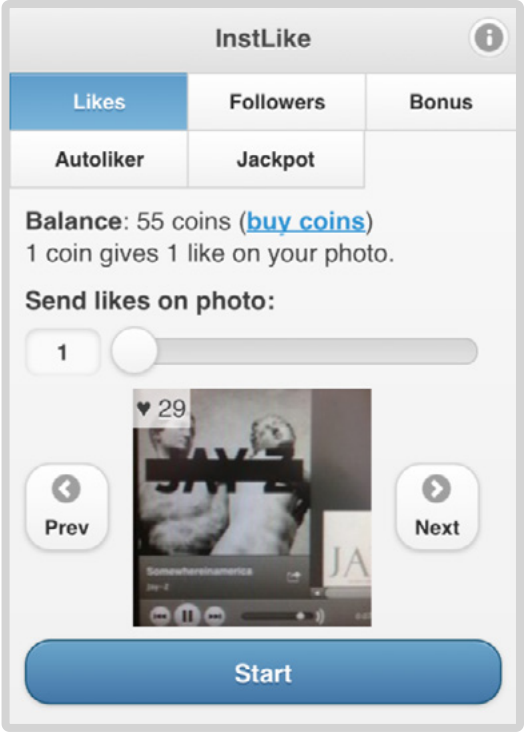


Fig. 4 *The InstLike application*

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.

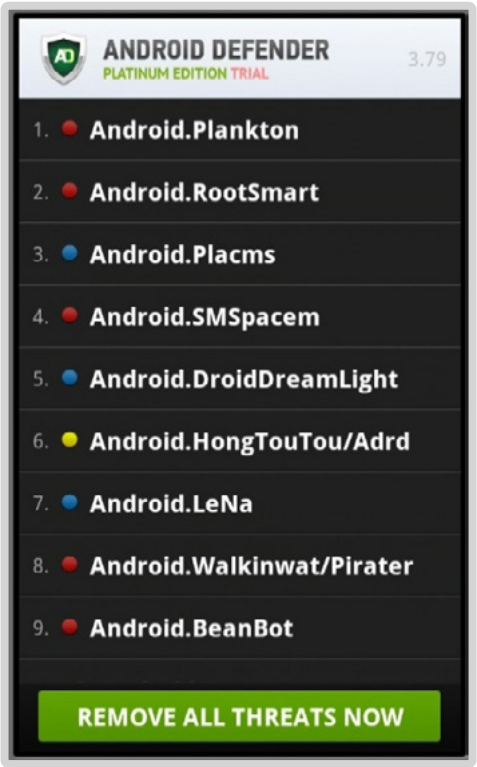


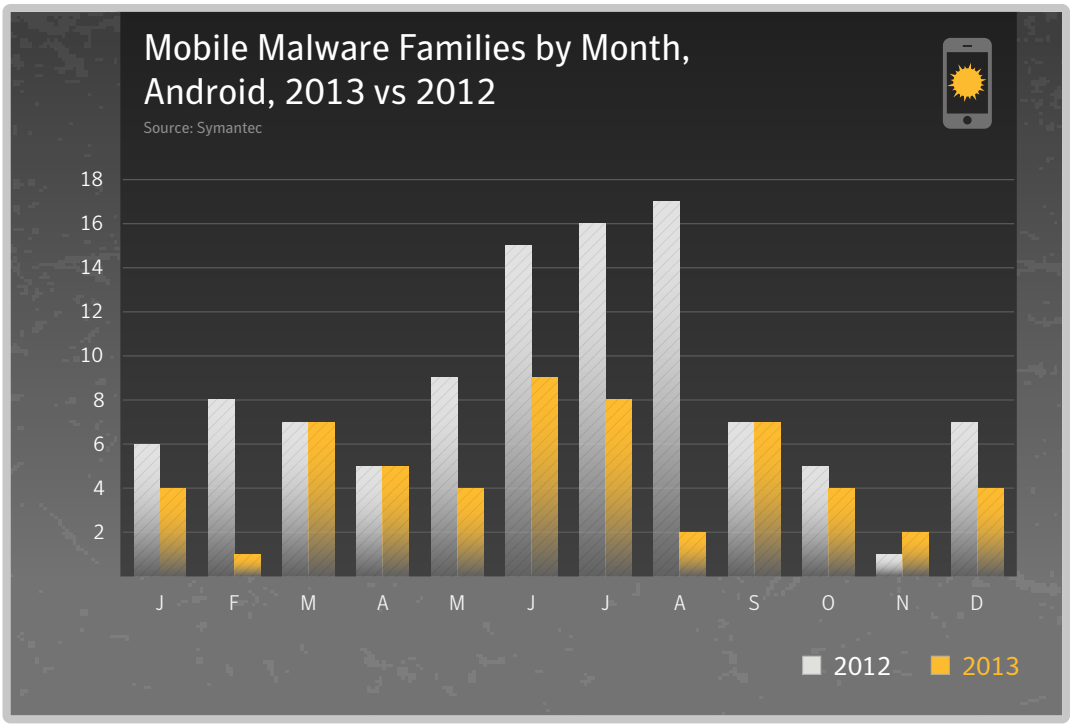
Fig. 5 Android.Fakedefender showing fake threats.

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

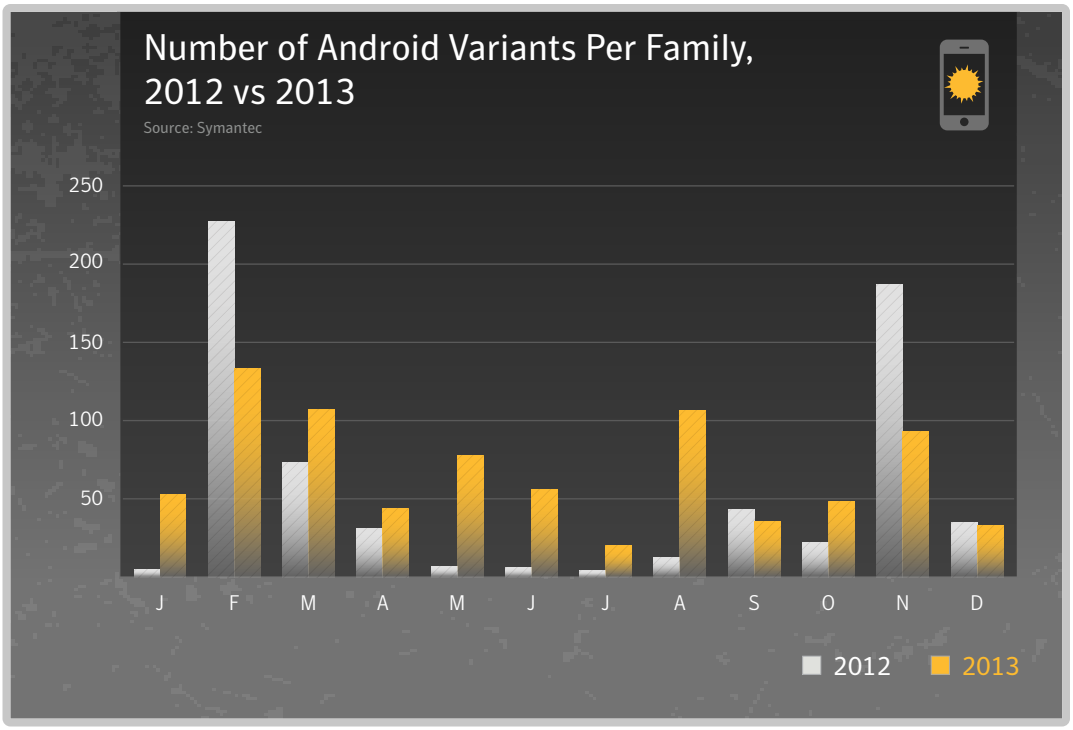
In 2012, Symantec's Norton Report showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger.

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.

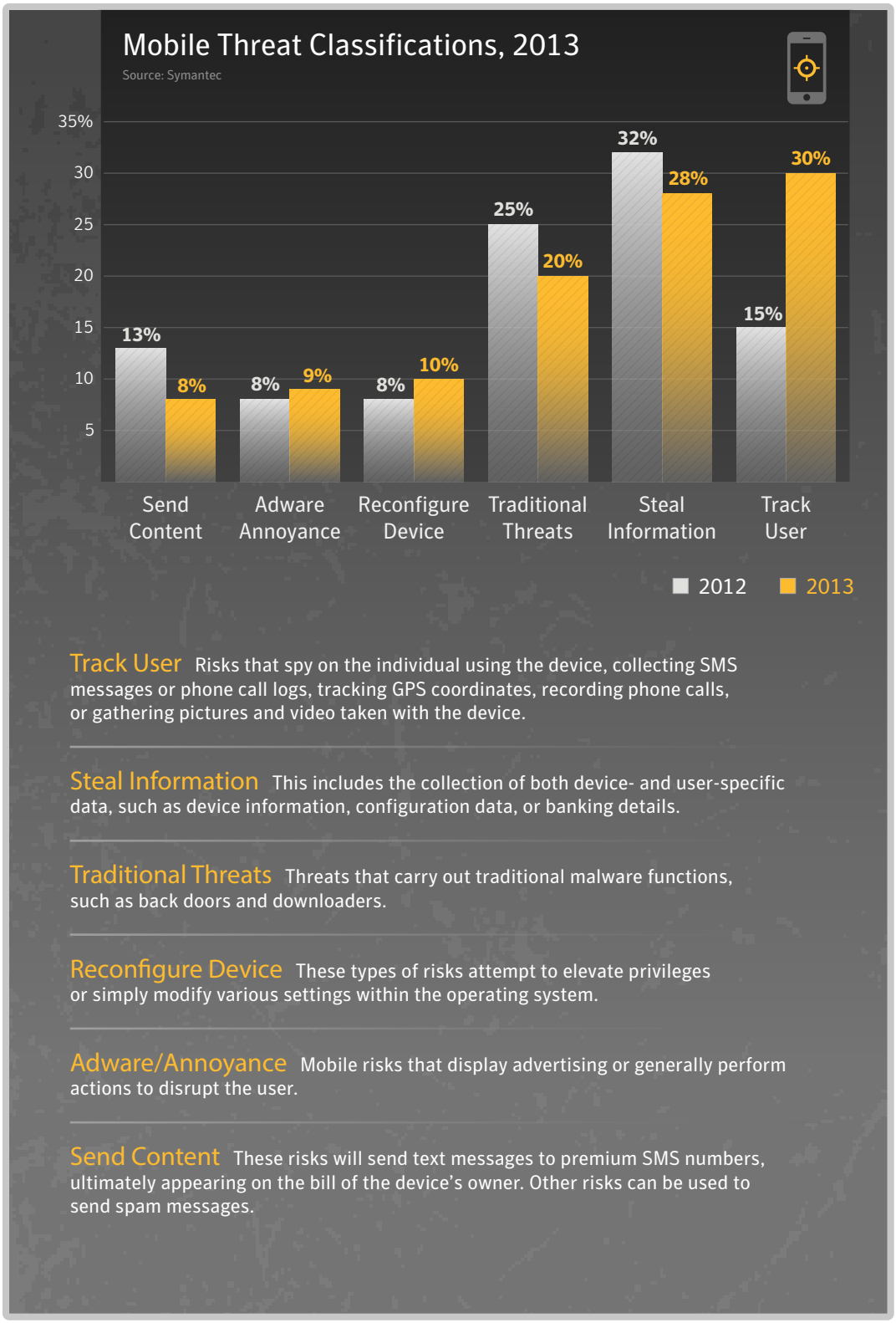
Also of note in 2013 is that mobile malware seemed almost exclusively focused on the Android platform. In fact only one new family was discovered outside this operating system—an information stealing Trojan for the Windows mobile platform.

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.

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.

Fig. 8



- *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.Exprespam.[35]

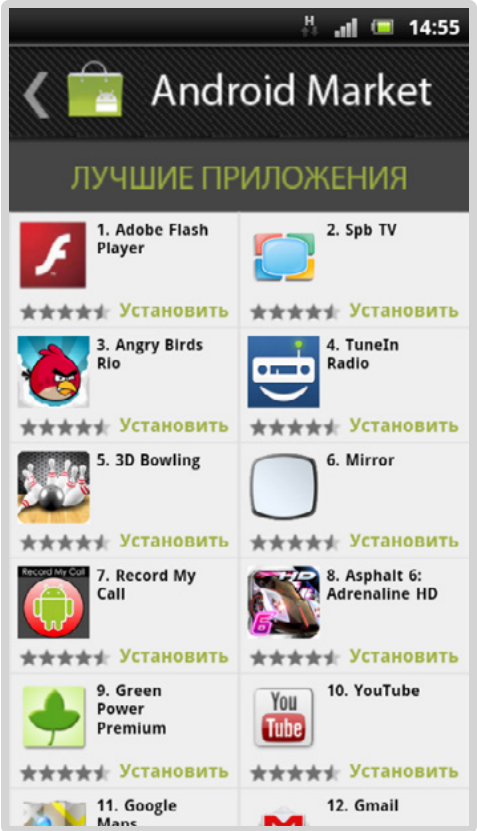


Fig. 10 A fake Russian app market, offering threats masked as popular apps.

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.

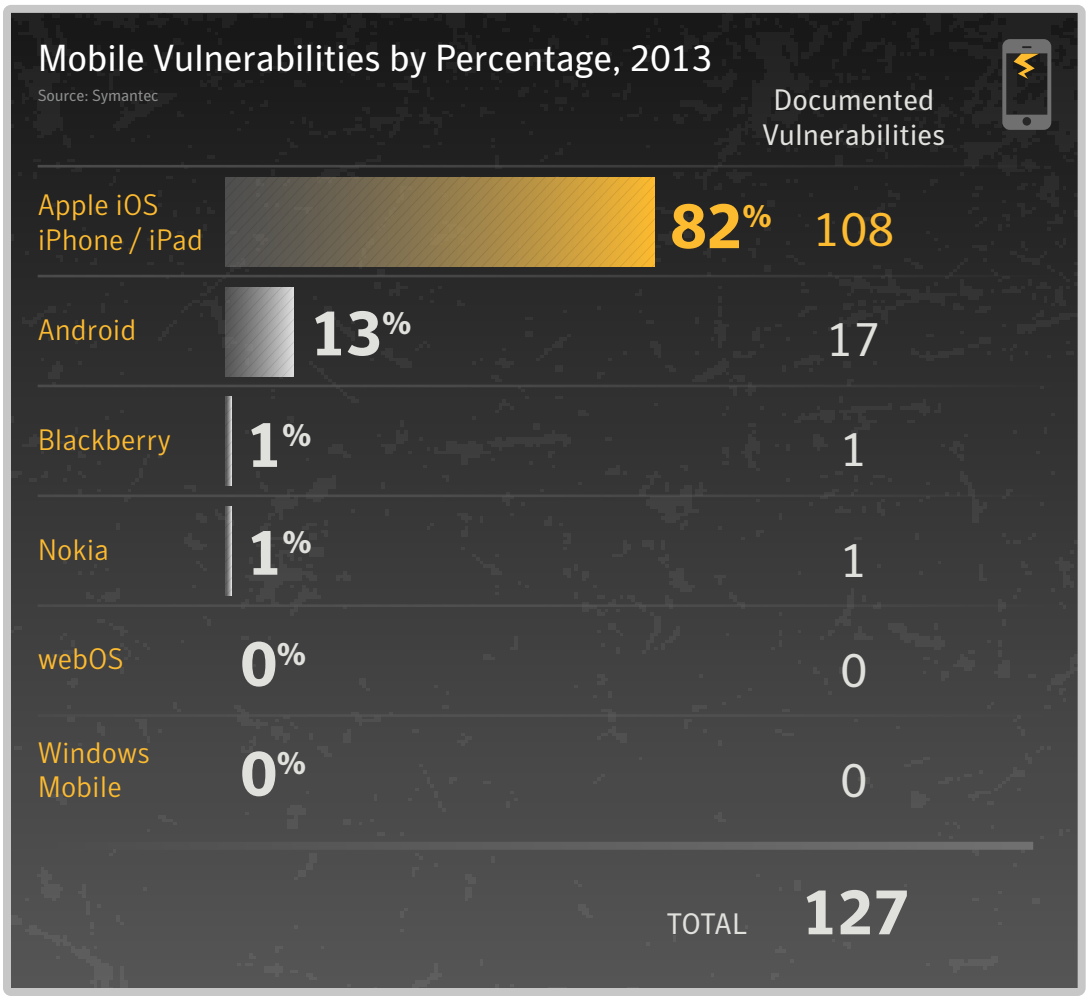
Vulnerabilities

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.*

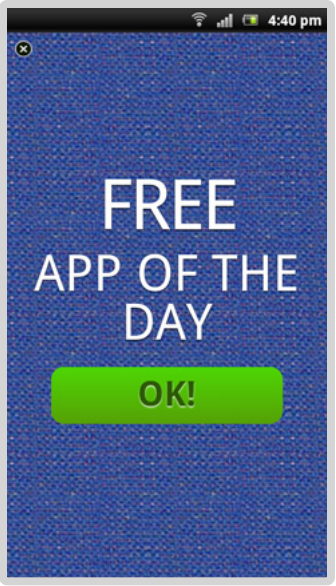


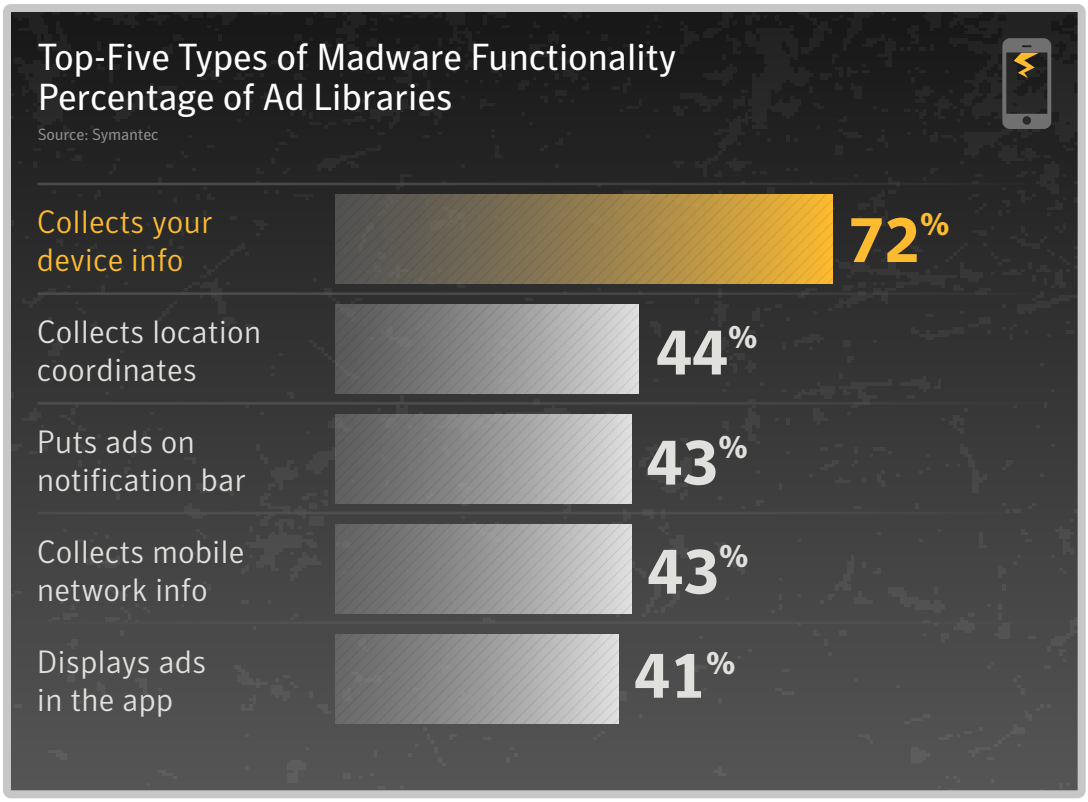
Fig. 12 Example madware pop-up advertisement.

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.

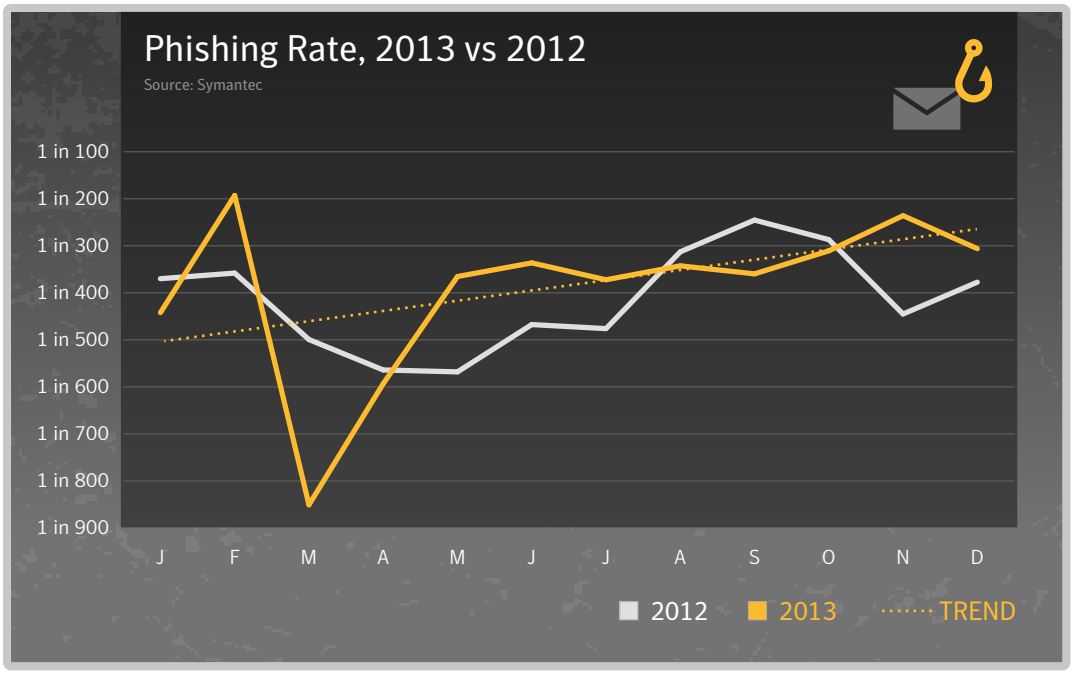
The phishing rate for the year has increased, from 1 in 414.3 emails per day, to 1 in 392.4. The busiest month of the year was February, where the rate rose to 1 in 193.0 emails.

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

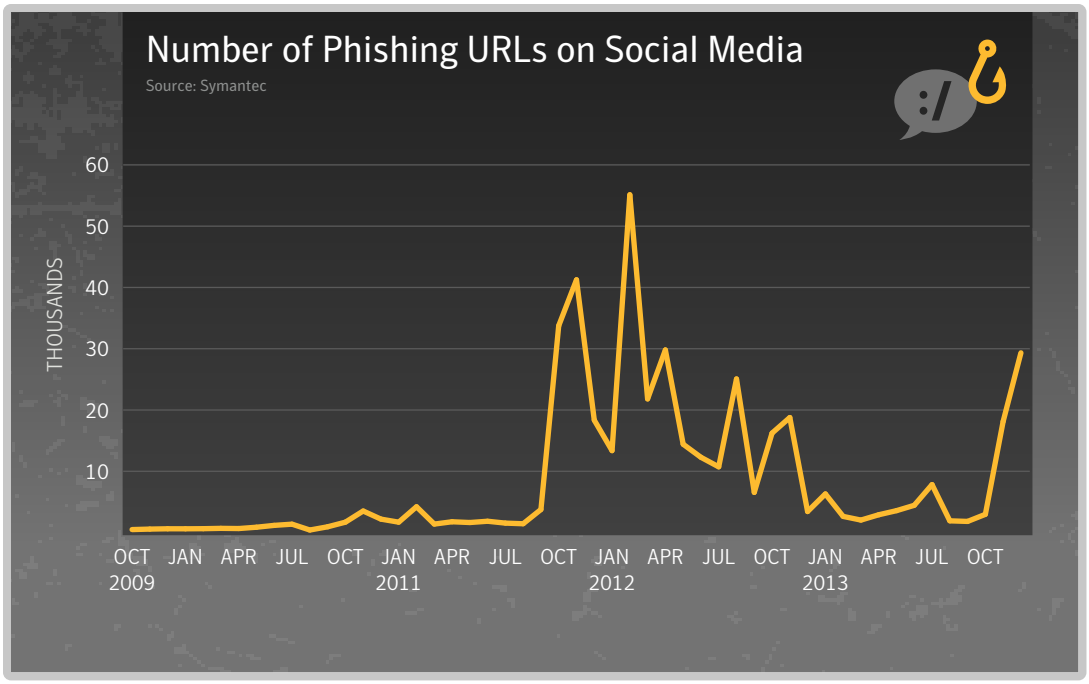
- *The phishing rate has increased in 2013, from 1 in 414 for 2012 to 1 in 392 in 2013.*
- *Login credentials for various accounts are the primary type of information sought by phishers.*
- *Spam rates are down 3 percentage points in 2013, making up 66 percent of email traffic.*
- *Scammers are working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

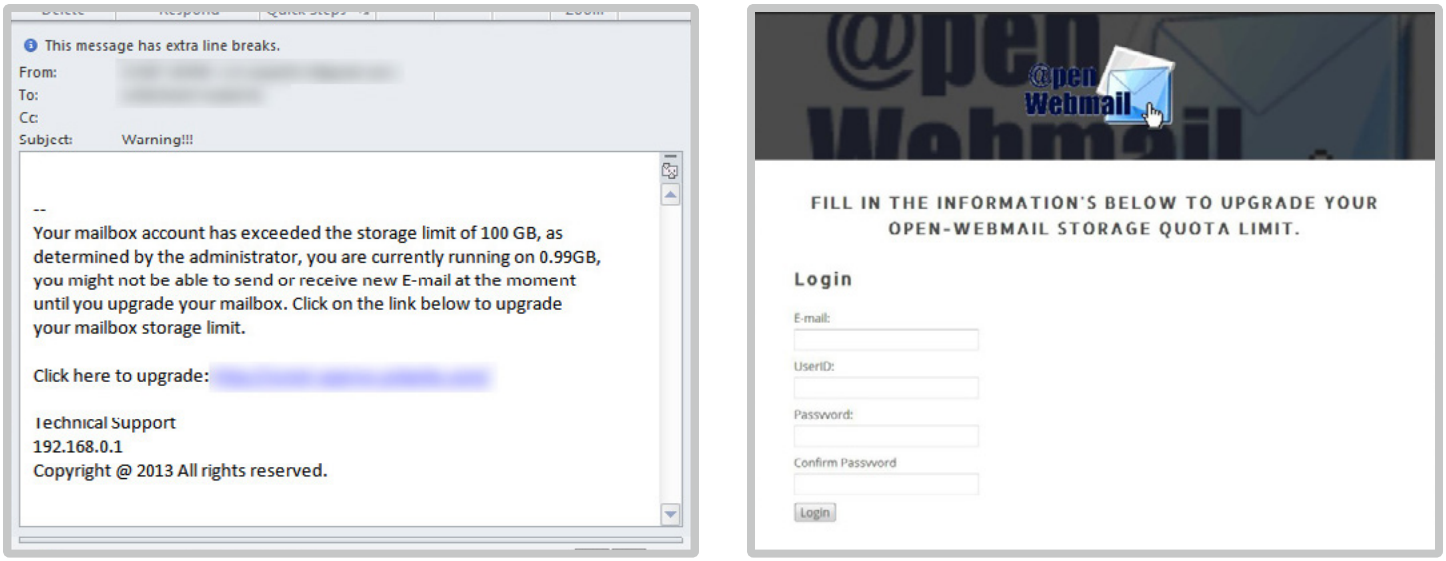


Fig. 3 Example quota phishing email and website.

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.

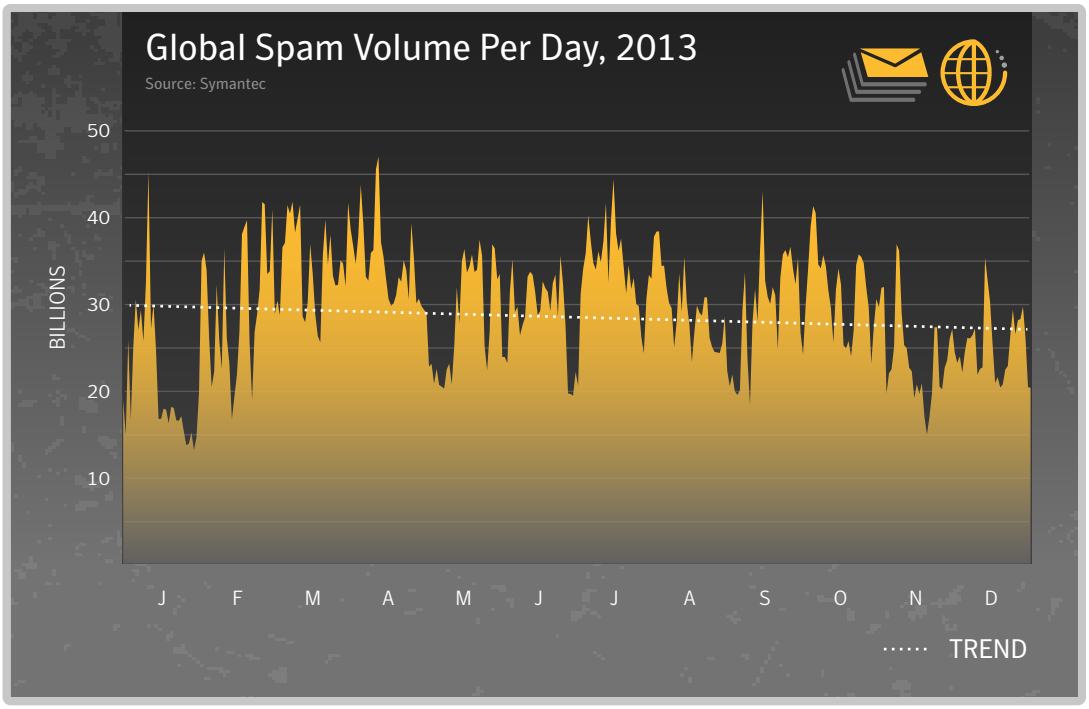
One of the latest findings from analysis of phishing activity in 2013 was the emergence of campaigns targeting information not usually associated with more traditional phishing activities. These include attempts to steal frequent flyer and loyalty card accounts, online credentials for utility accounts, 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.

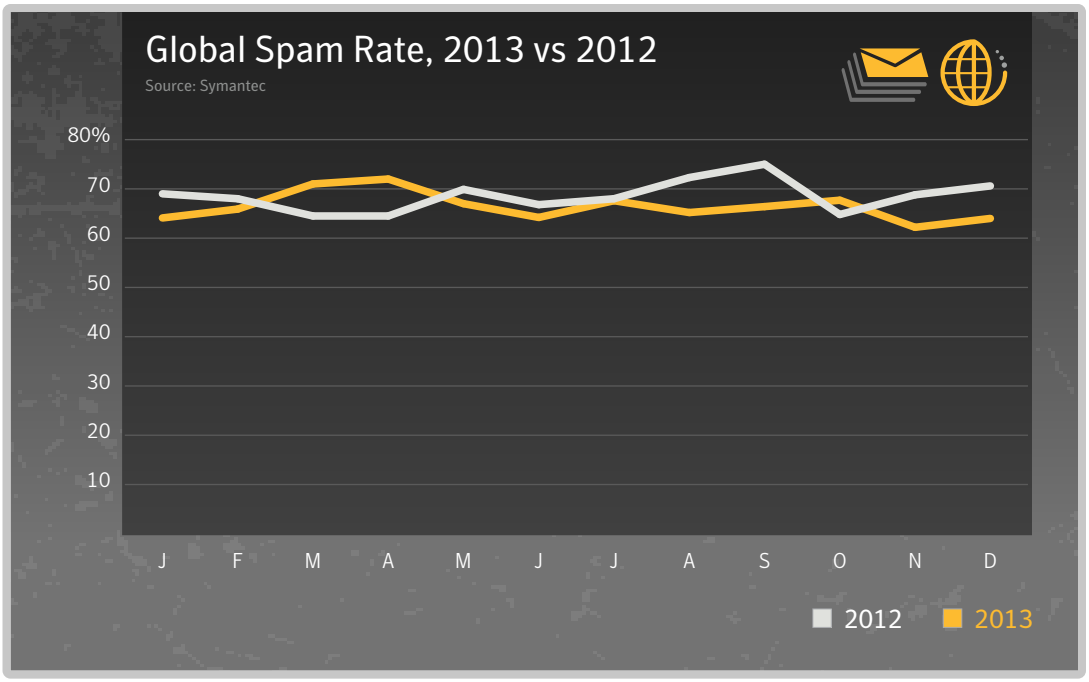
In terms of spam campaign strategies, some were quite blatant, clearly selling pills, whilst in other cases the message entirely unrelated topics - such as subject lines referencing replica watches, while the email body linked to pornographic sites.

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 wrist-watches 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 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

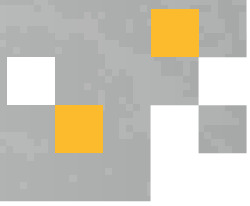
42 http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

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

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

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: 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

Copyright © 2014 Symantec Corporation.
All rights reserved. Symantec, the Symantec Logo,
and the Checkmark Logo are trademarks or registered
trademarks of Symantec Corporation or its affiliates in
the U.S. and other countries. Other names may
be trademarks of their respective owners

04/14 21284430-3