Symantec

SYMANTEC INTELLIGENCE REPORT

OCTOBER ⌖ 2013

CONTENTS

Executive Summary

Welcome to the October edition of the Symantec Intelligence report. Symantec Intelligence aims to provide the latest analysis of cyber security threats, trends, and insights concerning malware, spam, and other potentially harmful business risks.

This month we saw one of the largest data breaches in a number of years, where 150 million identities were exposed due to this one breach. This has more than doubled the number of identities exposed so far this year, when compared to our previous numbers through September.

October also saw an increase in the number of targeted attacks. These numbers are up fivefold compared to September, and even surpassing previous Octobers in 2011 and 2012, though still much lower than their peaks this summer. When comparing the size of the targeted organizations, we see that a majority of attack attempts are against large corporations with 2500-plus employees. However, when looking at the first time an organization registers a targeted attack attempt, this number is much higher for organizations with fewer than 250 employees. This indicates that more new attack attempts are being made across the smaller business spectrum, though larger organizations are more likely to be targeted continuously.

Also, the total number of mobile vulnerabilities disclosed dropped significantly in October. September's number was unusually high due to the release of a major update to a popular mobile operating system, which addressed a number of vulnerabilities in the software.

In other news, fake offerings continue to dominate Social Media attacks, disclosed vulnerability numbers are up 17 percent compared to the same period last year, and email spam rates have increased slightly over a three-month period, while phishing attempts and viruses attachments through email have decreased slightly.

We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

Ben Nahorney, Cyber Security Threat Analyst

symantec_intelligence@symantec.com

BIG NUMBERS

Overall Email Phishing Rate:

HIGHER NUMBER = LOWER RISK

Aug	1 in 626
Sep	1 in 1,056
Oct	1 in 1,135

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

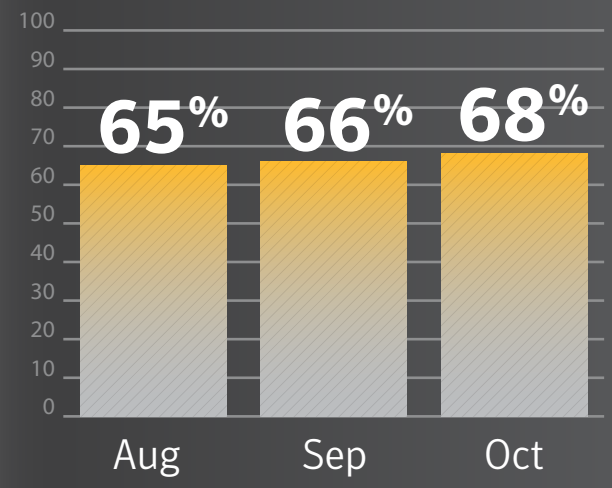
Aug	1 in 340
Sep	1 in 383
Oct	1 in 437

Mobile Vulnerabilities

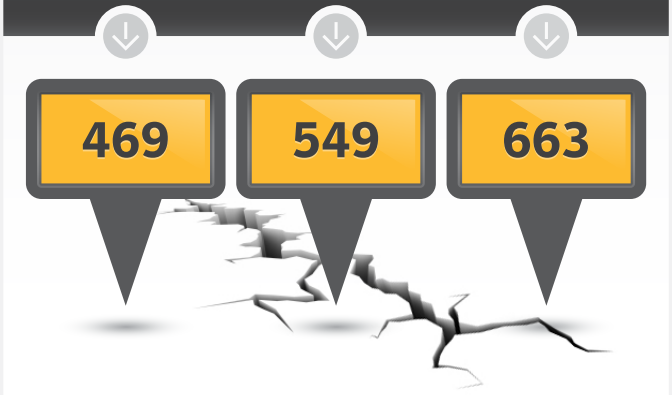
Aug	2
Sep	45
Oct	5

Estimated Global Email Spam Rate Per Day

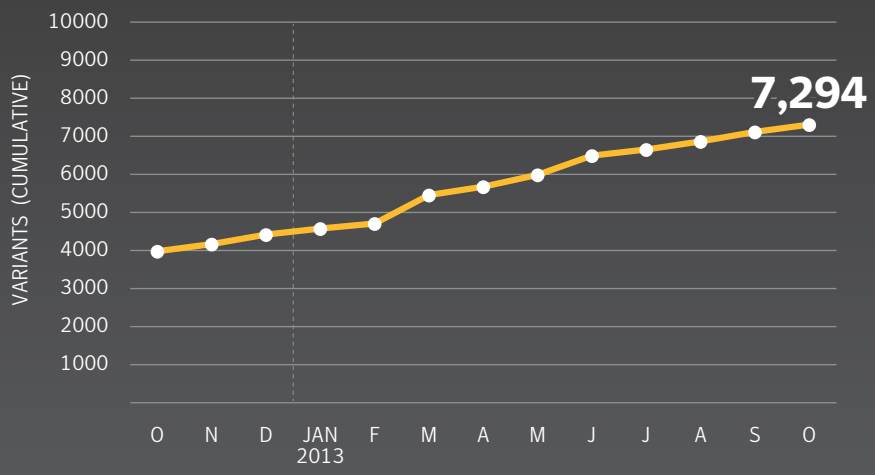
SPAM AS PERCENT OF ALL EMAIL

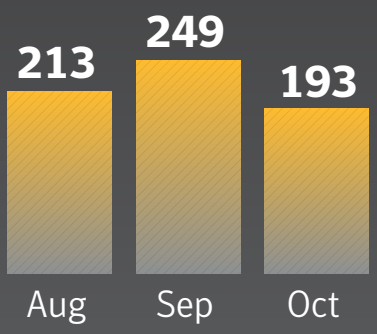


New Vulnerabilities



Mobile Malware Variants





Data Breaches

Number of Breaches (Year-to-Date)

165

Number of Identities Exposed (Year-to-Date)

248,282,045

TARGETED ATTACKS

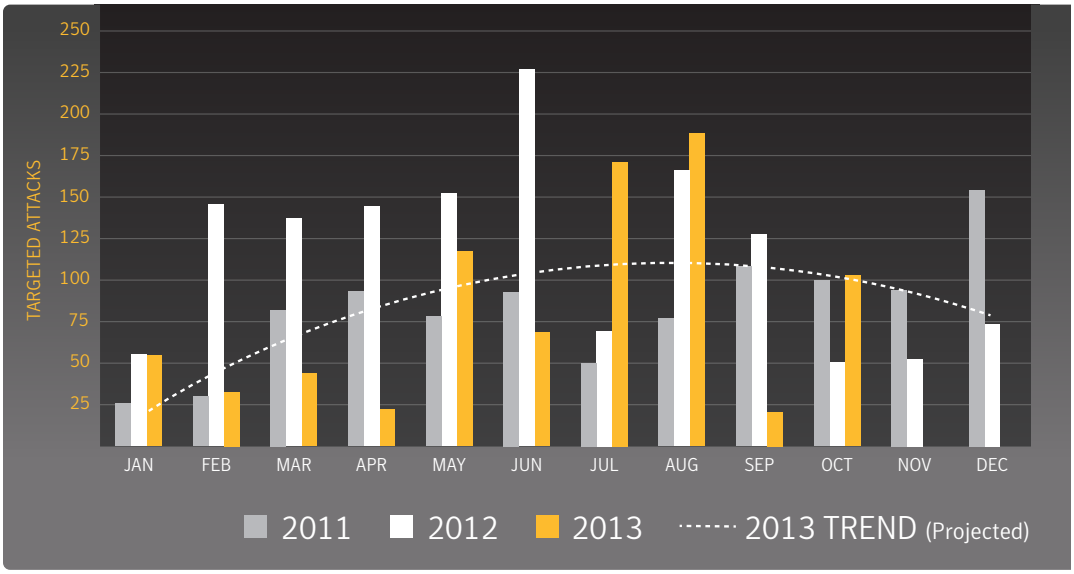
Targeted Attacks in 2013

At a Glance

- The number of targeted attacks in October were up since last month, even surpassing the number of attacks recorded in October of both 2011 and 2012.
- More companies logged their first targeted attack in October than previous months, making it the second largest month for new attacks this year.
- Large organizations of 2500+ continue to make up the lion's share of the total number of targeted attacks by organization size, though organizations with fewer than 250 employees are targeted more often, based on first attacks.

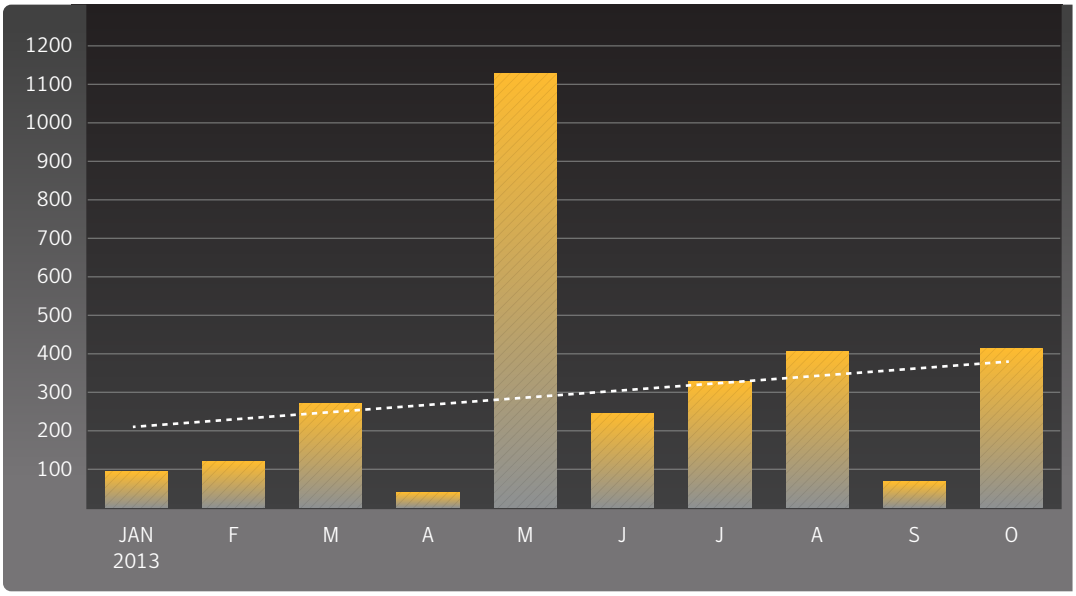
Targeted Attacks per Day

Source: Symantec



First Attacks Logged by Month

Source: Symantec



Attacks by Size of Targeted Organization

Source: Symantec

Company Size	Percent
1-250	26.1%
251-500	11.3%
501-1000	10.2%
1001-1500	3.1%
1501-2500	8.6%
2500+	40.8%

First Attacks Logged by Size

Source: Symantec

Company Size	Percent
1-250	50.2%
251-500	11.0%
501-1000	9.4%
1001-1500	5.1%
1501-2500	5.2%
2500+	19.0%

Top 10 Industries Attacked

Source: Symantec

Industry	Percent
Services - Professional	22.2%
Public Administration	19.2%
Services - Non-Traditional	14.8%
Finance, Insurance & Real Estate	13.0%
Transportation, Communications, Electric, & Gas	9.1%
Manufacturing	8.7%
Wholesale	4.2%
Logistics	2.1%
Retail	1.0%
Mining	1.0%

The “Professional” services category includes services such as Legal, Accounting, Health, and Education. “Non-Traditional” services include Hospitality, Recreational, and Repair services.

File Extensions of Attachments

Source: Symantec

File Extension	Percent
.exe	31.17%
.scr	20.52%
.doc	8.12%
.pdf	6.07%
.class	5.41%
.dmp	3.12%
.dll	2.09%
.jpg	1.64%
.xls	1.43%
.pif	1.24%

SOCIAL MEDIA

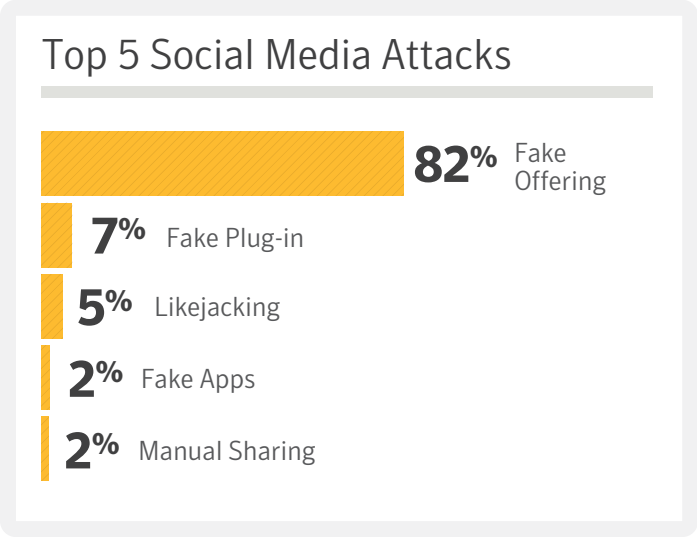
Social Media

At a Glance

- 82 percent of all social media attacks so far in 2013 have been fake offerings. This is up from 56 percent in 2012.
- Fake Plug-ins are the second-most common type of social media attacks at 7 percent, up from fifth place in 2012, at 5 percent.
- Fake Apps have risen overall in 2013, now making up 2 percent of social media attacks. In 2012, this category was ranked sixth.

Top 5 Social Media Attacks, 2013

Source: Symantec



Methodology

Fake Offering. 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.

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 can steal sensitive information from the infected machine.

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 Apps. Applications provided by attackers that appear to be legitimate apps; however, they contain a malicious payload. The attackers often take legitimate apps, bundle malware with them, and then re-release it as a free version of the app.

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

DATA BREACHES

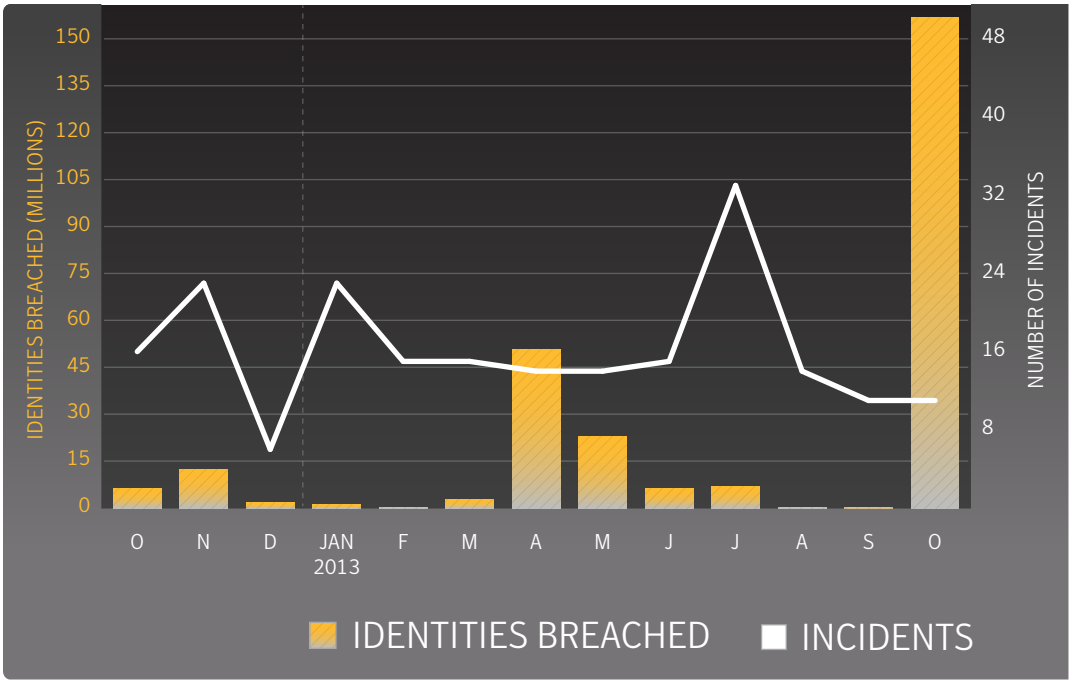
Data Breaches

At a Glance

- October saw the largest single breach in a number of years, with reports of 150 million identities exposed in a single breach.
- There were a number of breaches reported during October that occurred earlier in the year. This brings the total number of breaches to 165 for so far in 2013.
- Of the reported breaches so far in this year, the top three types of information exposed are a person's real name, government ID number (e.g. Social Security), and birth date.

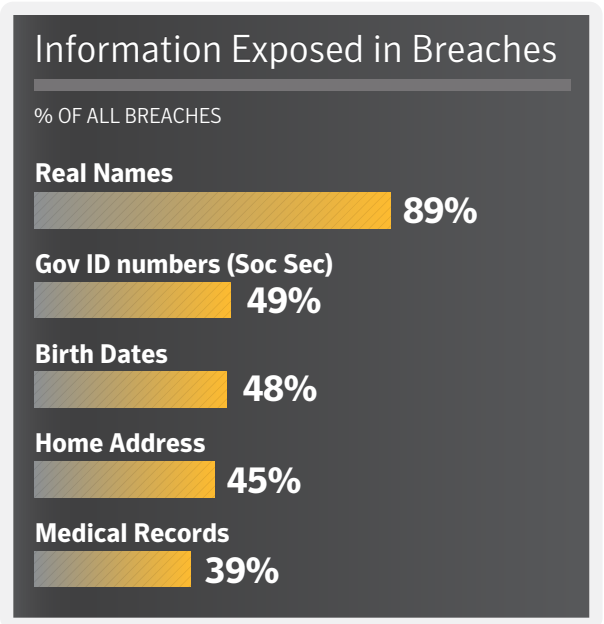
Timeline of Data Breaches, 2013

Source: Symantec



Top 5 Types of Information Exposed

Source: Symantec



Methodology

This data is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model that measures the levels of threats, including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information.

In some cases a data breach is not publicly reported during the same month the incident occurred, or an adjustment is made in the number of identities reportedly exposed. In these cases, the data in the Norton CCI is updated. This causes fluctuations in the numbers reported for previous months when a new report is released.

Norton Cybercrime Index
http://us.norton.com/protect-yourself

MOBILE

Mobile

At a Glance

- So far in 2013, 37 percent of mobile malware tracks users, up from 15 percent in 2012.
- Traditional threats, such as back doors and downloaders are present in 22 percent of all mobile malware threats.
- Risks that collect data, the most common risk in 2012, is down 11 percentage points to 21 percent of risks.
- Four new mobile malware families were discovered in October, along with 193 new variants.

Mobile Malware by Type

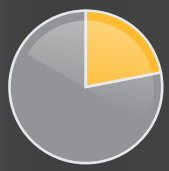
Source: Symantec

Track User

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

Collect Data

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

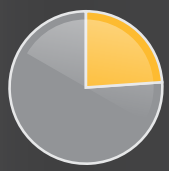


Traditional Threats

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

Change Settings

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



Adware/Annoyance

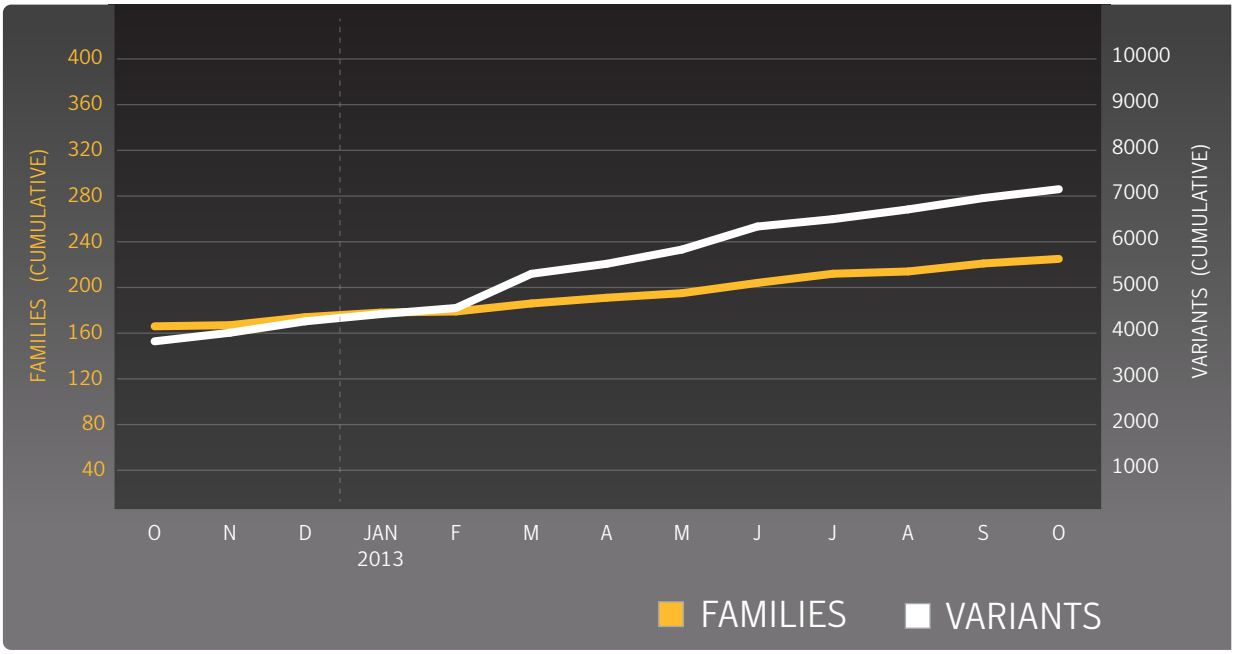
Mobile risks that display advertising or generally perform actions to disrupt the user.

Send Content

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

Cumulative Mobile Android Malware

Source: Symantec



VULNERABILITIES

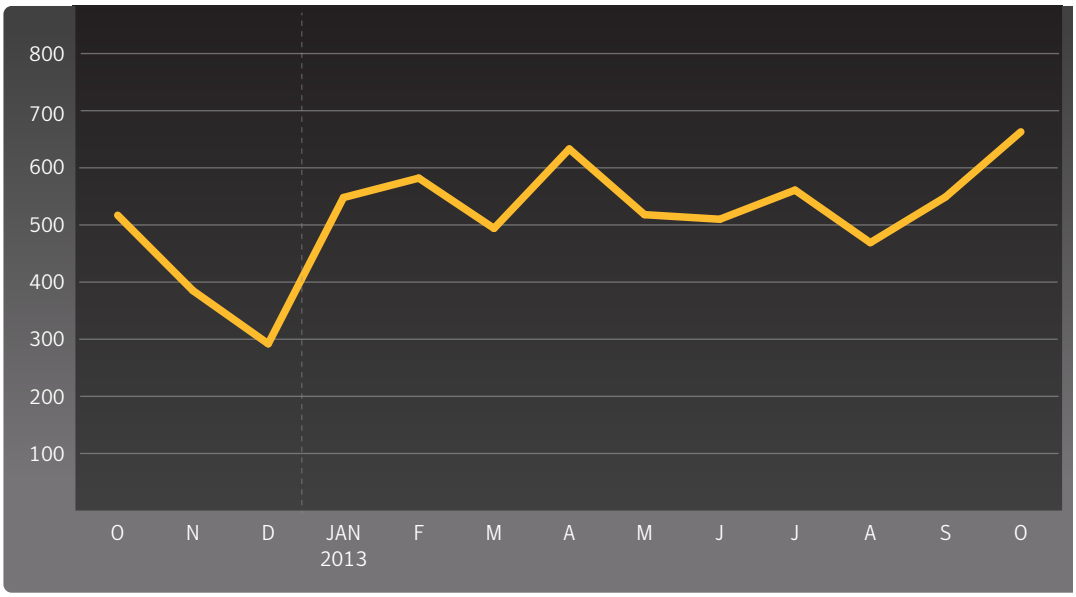
Vulnerabilities

At a Glance

- There were 663 new vulnerabilities discovered in October, bringing the total for the year up to 5527, a 17 percent increase compared to the same period in 2012.
- There were 5 vulnerabilities discovered in mobile operating systems during the month of October.
- Google's Chrome browser continues to lead in reporting browser vulnerabilities, while Oracle's Java leads in reported plug-in vulnerabilities.

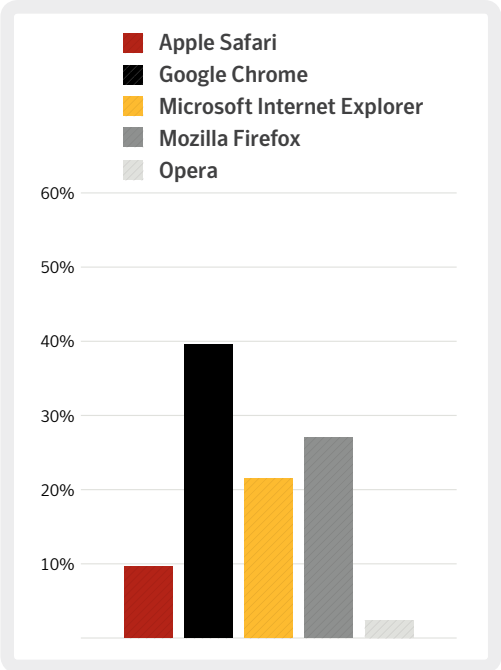
Total Vulnerabilities Disclosed by Month

Source: Symantec



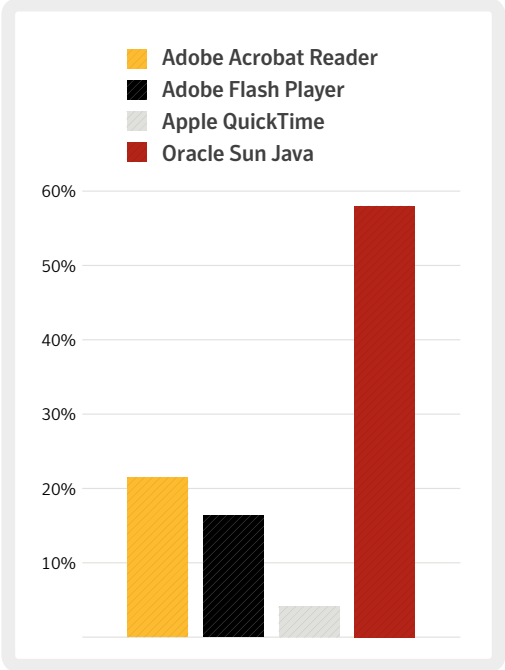
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

Spam

At a Glance

- The global spam rate increased 1.3 percentage points in October to 67.7 percent, up from 66.4 percent in September.
- Education was the most commonly targeted industry, knocking Pharmaceuticals from the top spot this month.
- The top-level domain (TLD) for Russia, .ru, continues to top the list of malicious TLDs in October.
- Pharmaceutical spam is the most common category, at 69.4 percent. Sex/Dating spam comes in second at 23.6 percent.

Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Sri Lanka	81.2%
Saudi Arabia	77.0%
Hungary	76.9%
China	72.5%
Egypt	72.4%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	68.8%
Chem/Pharm	68.6%
Non-Profit	68.3%
Marketing/Media	68.2%
Manufacturing	68.2%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
United States	6.90%
Finland	6.87%
India	5.96%
Peru	5.47%
Italy	5.39%
Spain	5.04%
Canada	4.95%
Brazil	4.88%
Argentina	4.25%
Iran	3.45%

Average Spam Message Size*

Source: Symantec

*Month	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Sep	19.6%	20.4%	60.0%
Aug	33.1%	34.1%	32.9%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	67.4%
251-500	67.9%
501-1000	67.6%
1001-1500	67.9%
1501-2500	67.6%
2501+	67.8%

Spam by Category

Source: Symantec

Category	Percent
Pharma	69.4%
Sex/Dating	23.6%
Jobs	3.9%
Watches	1.2%
Software	0.8%

Spam URL Distribution Based on Top Level Domain Name*

Source: Symantec

*Month	.ru	.com	.biz	.info
Sep	37.92%	30.82%	13.83%	4.2%

*Data lags one month

Phishing

At a Glance

- The global phishing rate is down in October, comprising one in 1 in 1,134.9 email messages. In September this rate was one in 1 in 1,055.7.
- Financial themes continue to be the most frequent subject matter, with 78.9 percent of phishing scams containing this theme.
- Australia has the highest rate in October, where one in 370.9 emails was a phishing scam.
- The United States tops the list of sources of phishing emails, responsible for distributing 32.8 percent of phishing scams.
- The Public Sector was the most targeted industry in October, with one in every 460.2 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	Percent
United States	31.84%
Germany	18.70%
United Kingdom	16.22%
South Africa	15.23%
Australia	6.26%
Sweden	3.80%
Brazil	2.11%
Hong Kong	0.88%
Netherlands	0.77%
Canada	0.63%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 763.6
251-500	1 in 1,383.8
501-1000	1 in 1,941.8
1001-1500	1 in 1,478.4
1501-2500	1 in 2,370.0
2501+	1 in 1,114.2

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 460.2
Finance	1 in 631.5
Education	1 in 651.7
Marketing/Media	1 in 739.5
Accom/Catering	1 in 825.5

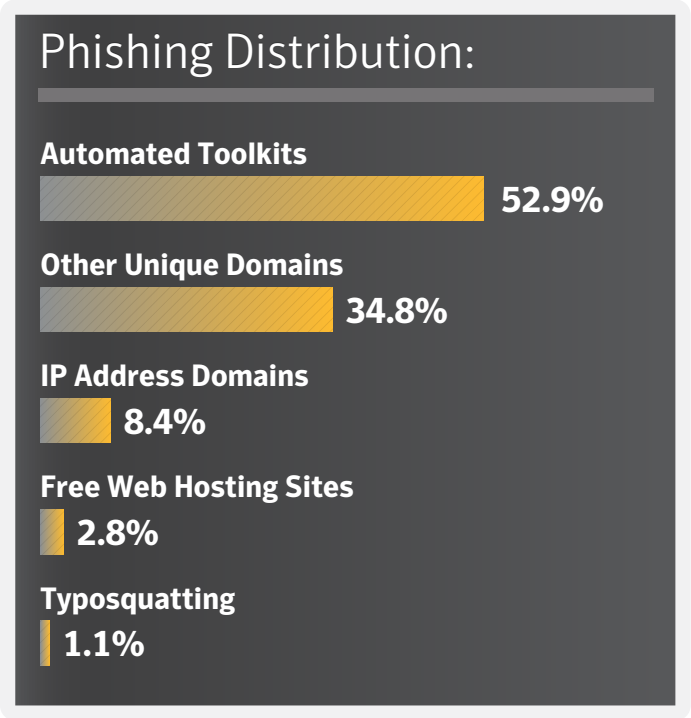
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
Australia	1 in 370.9
Monaco	1 in 486.3
South Africa	1 in 534.2
United Kingdom	1 in 726.7
Denmark	1 in 809.9

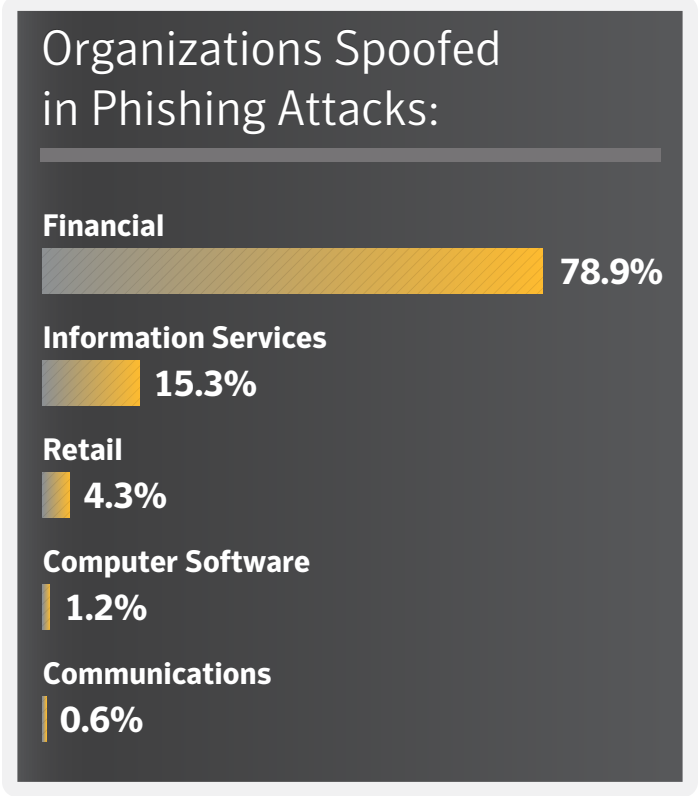
Phishing Distribution

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in October was one in 436.7 emails, compared to one in 383.1 in September.
- The United Kingdom topped the list of geographies, with one in 240.7 emails containing a virus.
- The United Kingdom was also the largest source of virus-laden emails, making up 38.2 percent of all email-based viruses.
- Small-to-medium size businesses with 1-250 employees were the most targeted company size, where one and 369.6 emails contained a virus.

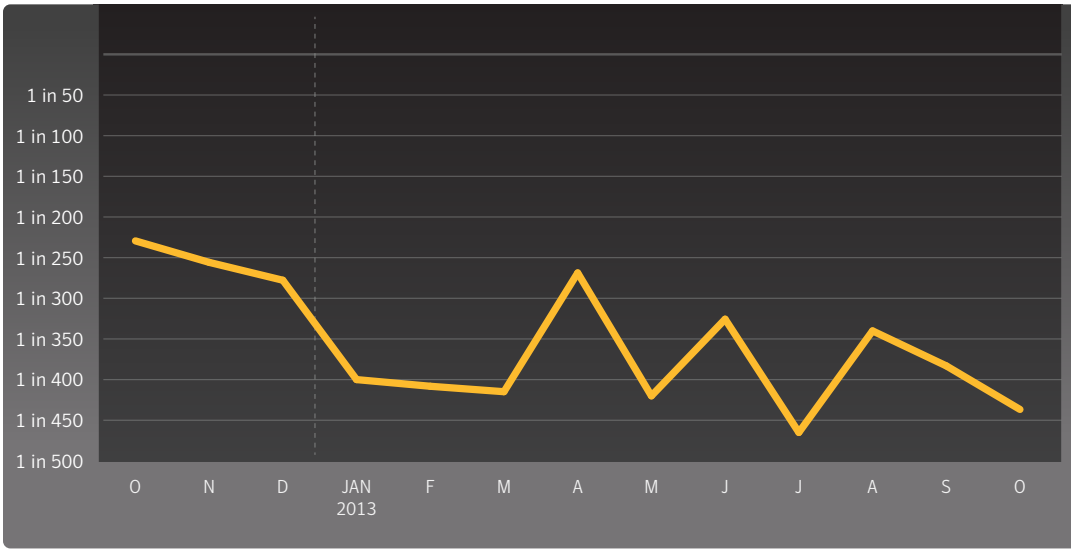
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United Kingdom	38.18%
United States	33.31%
Australia	6.17%
India	2.39%
Netherlands	2.33%
South Africa	2.30%
Japan	1.78%
Hong Kong	1.78%
Canada	1.70%
France	1.68%

Proportion of Email Traffic in Which Virus Was Detected

Source: Symantec



Top 5 Activity for Malware Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 179.4
Telecoms	1 in 186.2
Other	1 in 231.6
Transport/Util	1 in 303.9
Accom/Catering	1 in 317.9

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
United Kingdom	1 in 240.7
United Arab Emirates	1 in 278.1
Australia	1 in 297.5
Austria	1 in 325.7
Hungary	1 in 342.8

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 369.6
251-500	1 in 447.4
501-1000	1 in 601.9
1001-1500	1 in 469.5
1501-2500	1 in 718.6
2501+	1 in 413.8

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 13.7 percent of all malware blocked at the endpoint.
- In comparison, 6.7 percent of all malware were variants of W32.Sality.
- Approximately 40.5 percent of the most frequently blocked malware last month was identified and blocked using generic detection.

Top 10 Most Frequently Blocked Malware

Source: Symantec

Malware	Percent
W32.Sality.AE	5.96%
W32.Ramnit!html	5.34%
W32.Ramnit.B	4.62%
W32.Almanahe.B!inf	3.80%
W32.Downadup.B	3.60%
W32.Ramnit.B!inf	3.22%
Trojan.Malscript	2.22%
W32.Virut.CF	2.04%
Trojan.Zbot	1.55%
W32.SillyFDC	1.49%

Policy Based Filtering

At a Glance

- The most common trigger for policy-based filtering applied by Symantec Web Security .cloud for its business clients was for the "Social Networking" category, which accounted for 51.6 percent of blocked Web activity in October.
- "Advertisement & Popups" was the second-most common trigger, comprising 19.7 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	51.63%
Advertisement & Popups	19.67%
Streaming Media	3.86%
Hosting Sites	3.70%
Computing & Internet	3.21%
Chat	2.67%
Peer-To-Peer	2.49%
Search	2.13%
Gambling	0.94%
News	0.87%

About Symantec

Symantec protects the world's information and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

More Information

- Security Response Publications: http://www.symantec.com/security_response/publications/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec. Confidence in a connected world.

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