Symantec

SYMANTEC INTELLIGENCE REPORT

NOVEMBER ⌖ 2013

CONTENTS

Executive Summary

Welcome to the November 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.

November saw another increase in the number of targeted attacks. While these numbers are up slightly compared to October, they're almost double the number of targeted attacks during the same month in 2012, though still much lower than their peaks this summer.

This month we saw another large data breach reported, where 42 million identities were exposed as a result. However, the breach apparently took place in January, resulting in an increase in overall numbers for the beginning of this year.

It appears that the email virus rate increased in November, where one in 235 emails contained a malicious attachment. This is up from one in 437 emails last month, and the highest rate we've seen since November 2012. In terms of industries most likely to encounter malicious emails, the Public Sector tops the list at one in 62 emails. The United Kingdom tops both the source and destinations locations for the month.

In other news, spam rates dropped 5.5 percentage points to 62.2 percent of email, fake offerings still top the list of social media attacks at 82 percent, 36 percent of all malicious mobile apps track user activity, and 438 new vulnerabilities were disclosed during the month.

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

Sep	1 in 1,056
Oct	1 in 1,134
Nov	1 in 1,311

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

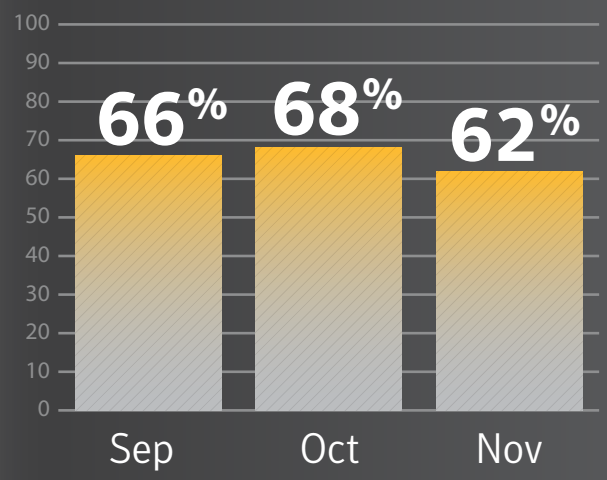
Sep	1 in 383
Oct	1 in 437
Nov	1 in 253

Mobile Vulnerabilities

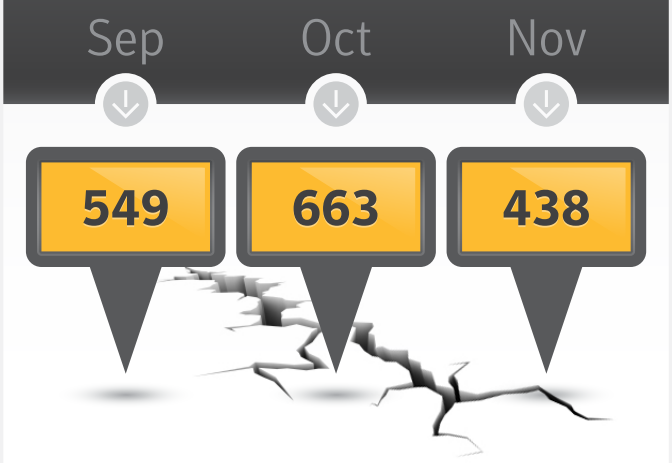
Sep	45
Oct	5
Nov	6

Estimated Global Email Spam Rate Per Day

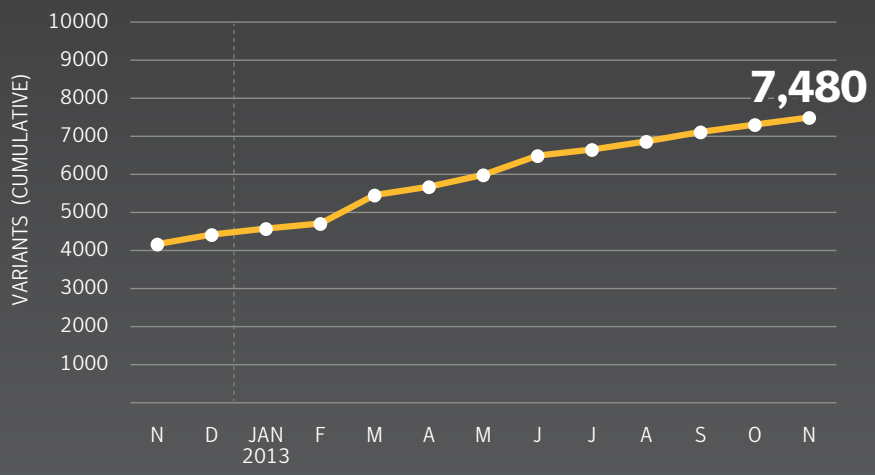
SPAM AS PERCENT OF ALL EMAIL

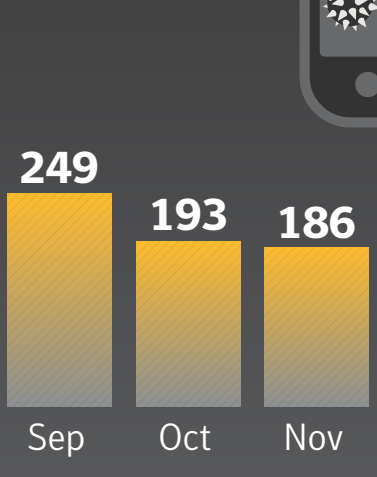


New Vulnerabilities



Mobile Malware Variants





Data Breaches

Number of Breaches (Year-to-Date)

186

Number of Identities Exposed (Year-to-Date)

296,422,090

TARGETED ATTACKS

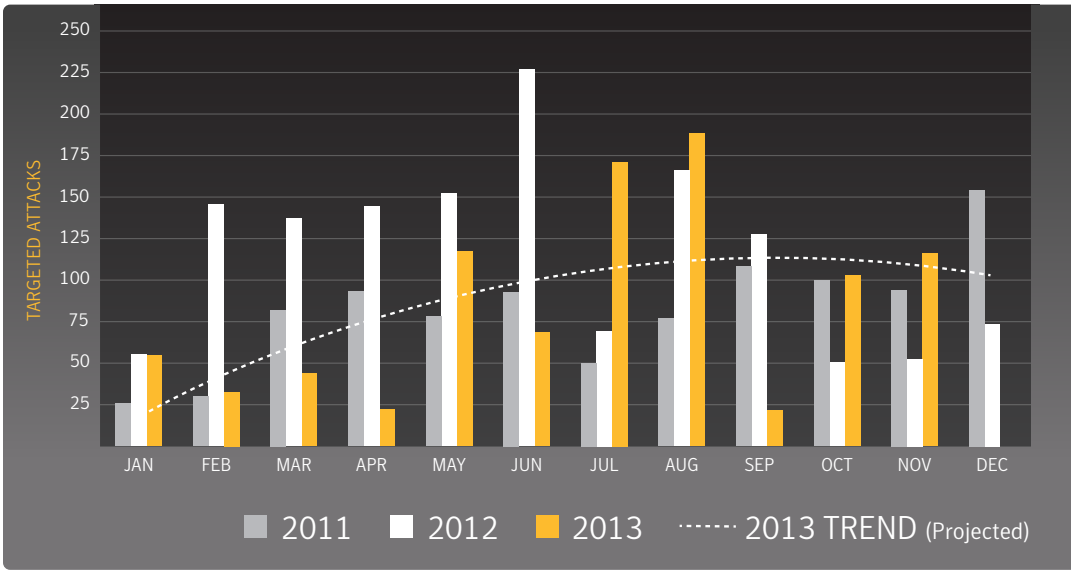
Targeted Attacks in 2013

At a Glance

- The number of targeted attacks in November were up since the previous month, even surpassing the number of attacks recorded in November of both 2011 and 2012.
- 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.
- The .exe file type was the most common attachment, making up 30.9% of email-based targeted attacks that included file attachments.

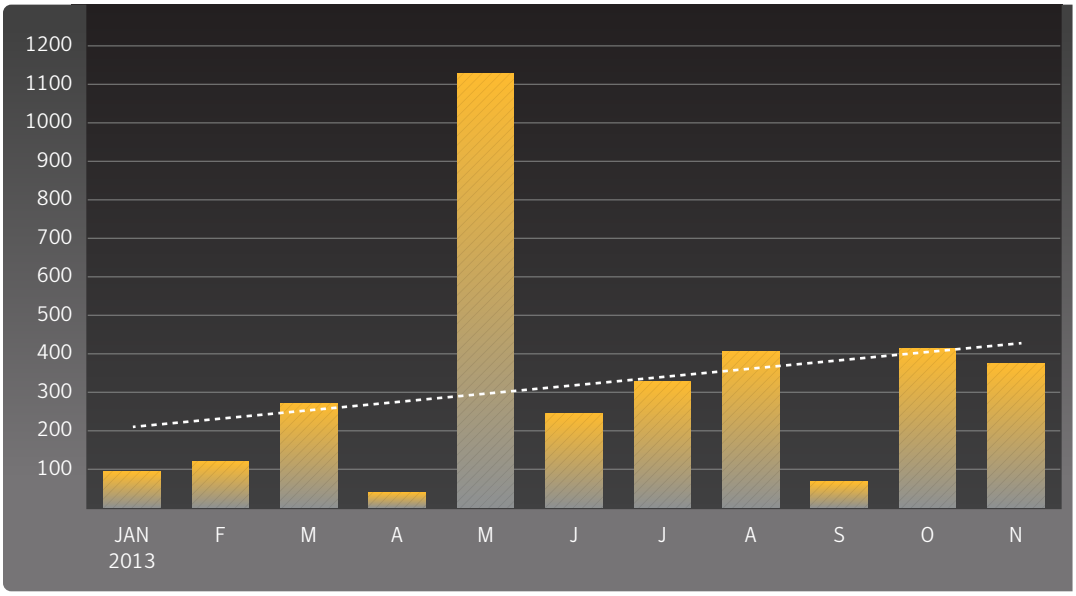
Targeted Attacks per Day

Source: Symantec



First Attacks Logged by Month

Source: Symantec



Attacks by Size of Targeted Organization

Source: Symantec

Company Size	Percent
1-250	29.6%
251-500	10.8%
501-1000	9.5%
1001-1500	3.2%
1501-2500	7.9%
2500+	39.0%

First Attacks Logged by Size

Source: Symantec

Company Size	Percent
1-250	51.5%
251-500	10.9%
501-1000	9.3%
1001-1500	5.3%
1501-2500	5.1%
2500+	17.9%

Top 10 Industries Attacked

Source: Symantec

Industry	Percent
Services - Professional	20.3%
Services - Non Traditional	18.8%
Public Administration	15.3%
Finance, insurance & Real Estate	13.2%
Manufacturing	10.3%
Transportation, communications, electric, gas & Sanitary Services	8.0%
Wholesale	5.0%
Retail	2.3%
Nonclassifiable Establishments	2.0%
Logistics	1.9%

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	30.9%
.scr	19.0%
.doc	8.0%
.pdf	5.5%
.class	5.0%
.jpg	4.0%
.dmp	2.8%
.dll	1.8%
.au3	1.4%
.xls	1.3%

SOCIAL MEDIA

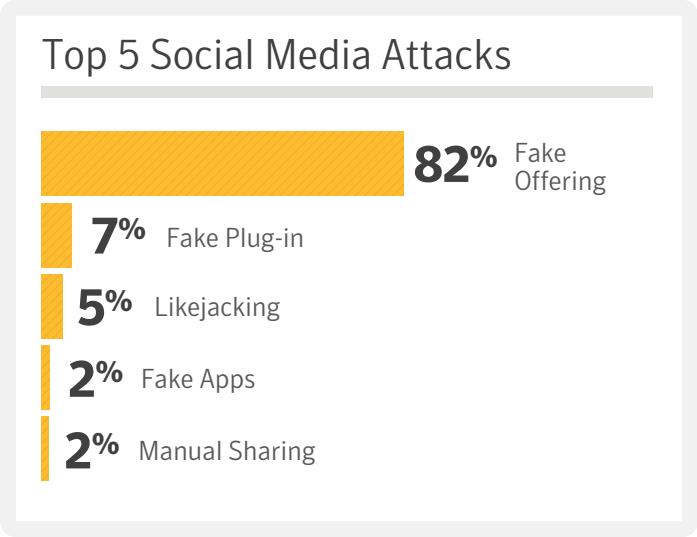
Social Media

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

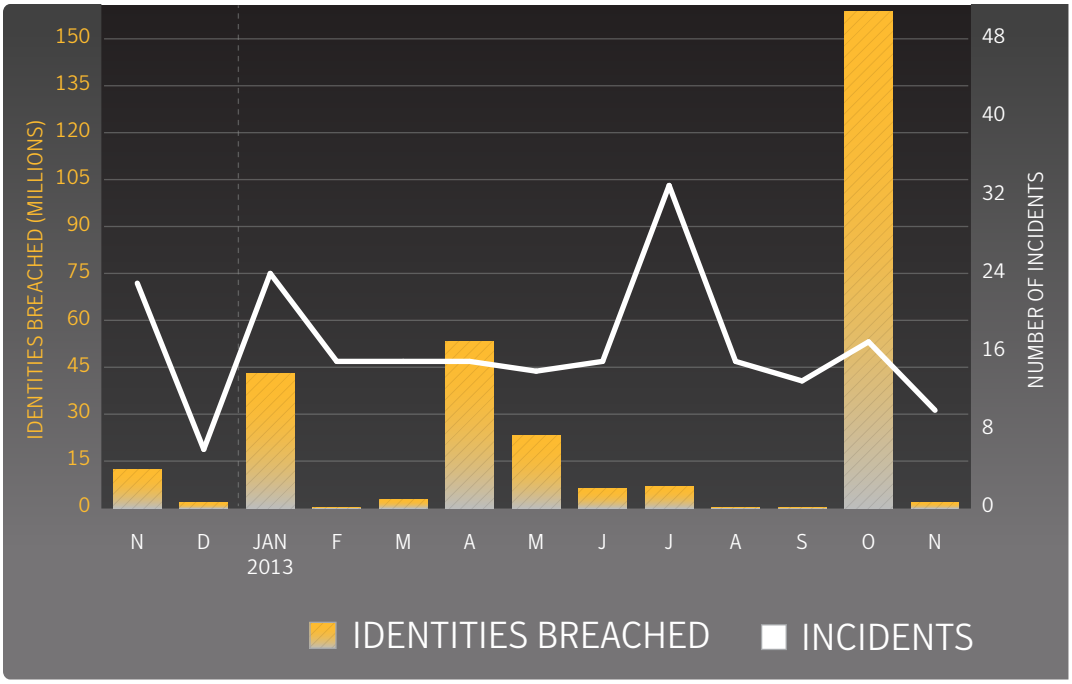
Data Breaches

At a Glance

- The largest breach that was reported in November actually occurred back in January, where 42 million identities were exposed.
- There were a number of breaches reported during November that occurred earlier in the year. This brings the total number of breaches to 186 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.

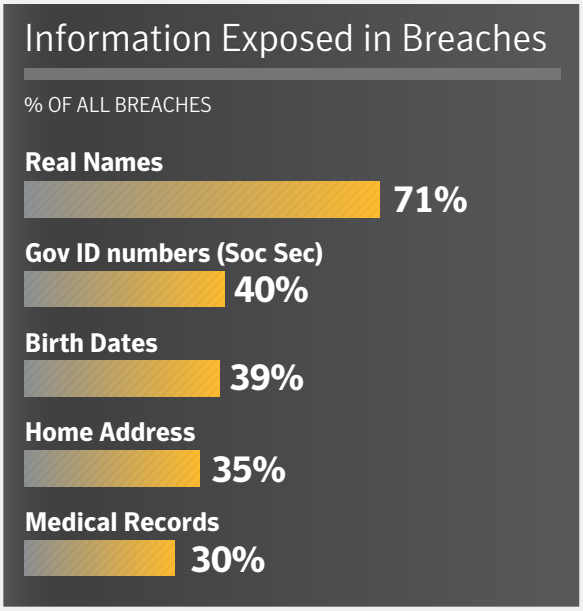
Timeline of Data Breaches, 2013

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, 36 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 9 percentage points to 23 percent of risks.
- Four new mobile malware families were discovered in November, along with 186 new variants.

Mobile Malware by Type

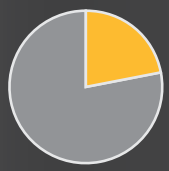
Source: Symantec

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.

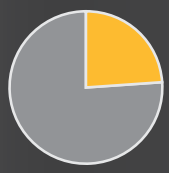


Traditional Threats

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

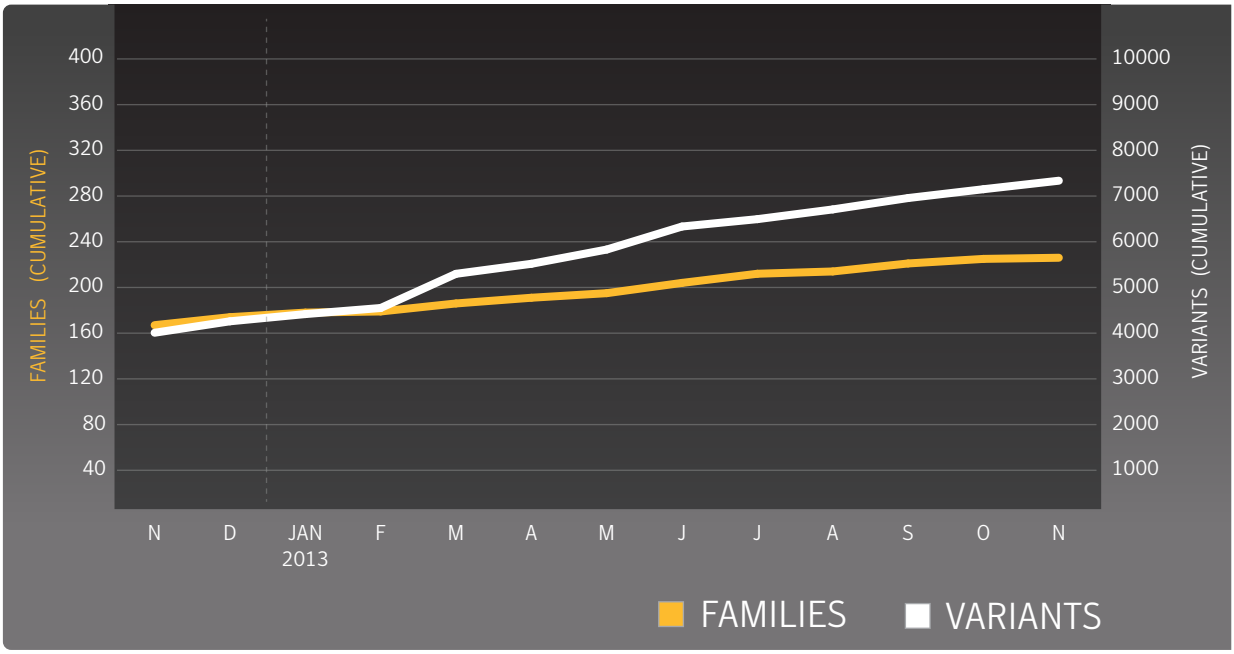
Mobile risks that display advertising or generally perform actions to disrupt the user.

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

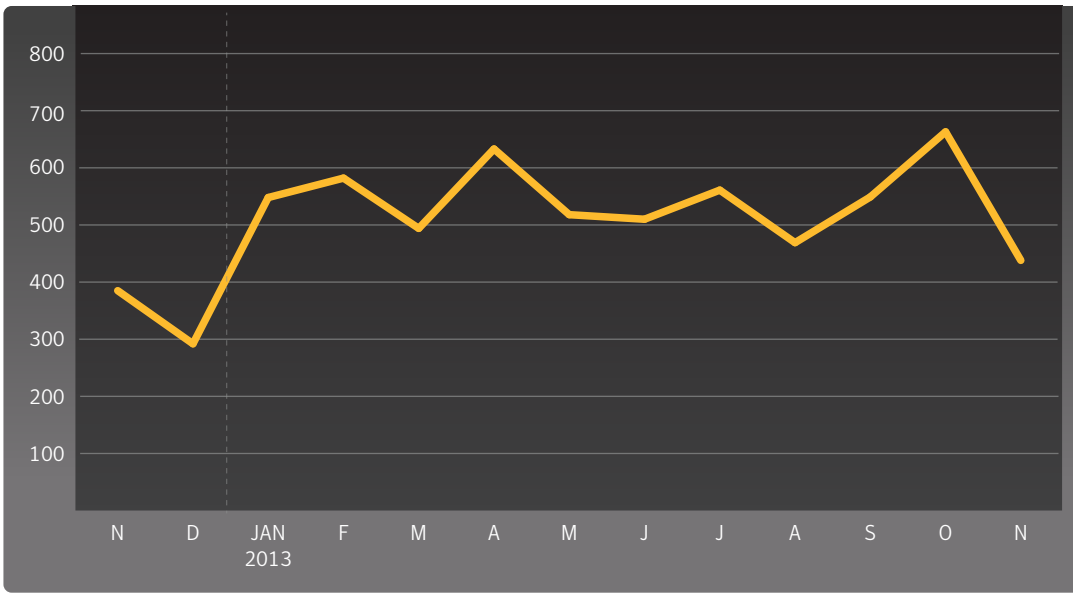
Vulnerabilities

At a Glance

- There were 438 new vulnerabilities discovered in November, bringing the total for the year up to 5965, a 16 percent increase compared to the same period in 2012.
- There were 6 vulnerabilities discovered in mobile operating systems during the month of November.
- Google's Chrome browser continues to lead in reporting browser vulnerabilities, while Oracle's Java leads in reported plug-in vulnerabilities.
- Two zero-day vulnerabilities were disclosed during the month of November.

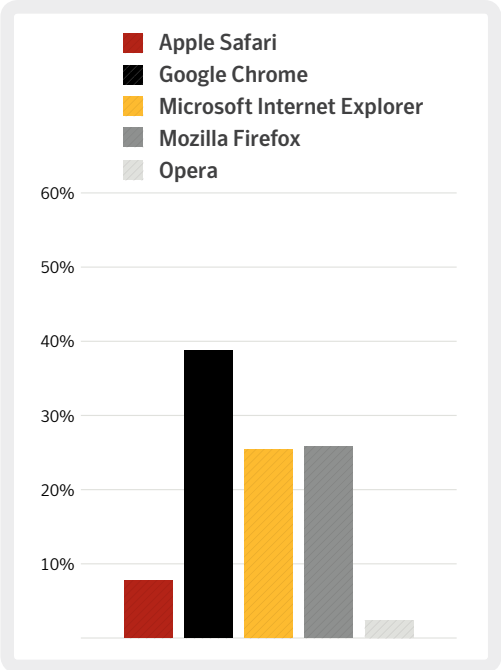
Total Vulnerabilities Disclosed by Month

Source: Symantec



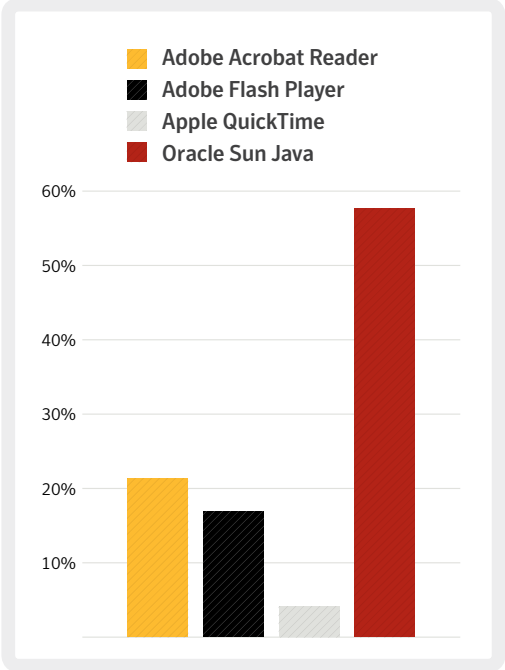
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

Spam

At a Glance

- The global spam rate decrease 5.5 percentage points in November to 62.2 percent, up from 67.7 percent in October.
- Education was the most commonly targeted industry, knocking Pharmaceuticals from the top spot this month.
- The .com top-level domain (TLD) was the most frequently used malicious TLD in November.
- Sex Dating spam is the most common category, at 71.2 percent. Job-related spam comes in second at 16.5 percent.

Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Sri Lanka	77.5%
Israel	68.7%
Greece	67.9%
Hungary	67.7%
Brazil	67.4%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	63.6%
Non-Profit	63.5%
Recreation	62.8%
Chem/Pharm	62.7%
Gov/Public Sector	62.7%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
United States	8.7%
Brazil	6.4%
Russian Federation	6.2%
India	5.5%
Canada	5.2%
Peru	4.8%
Argentina	3.9%
Spain	3.8%
Iran	3.3%
Italy	3.0%

Average Spam Message Size

Source: Symantec

Month*	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Oct	40.2%	26.0%	33.8%
Sep	19.6%	20.4%	60.0%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	62.0%
251-500	62.6%
501-1000	61.9%
1001-1500	62.3%
1501-2500	62.1%
2501+	62.3%

Spam by Category

Source: Symantec

Category	Percent
Sex/Dating	71.2%
Jobs	16.5%
Pharma	8.8%
Watches	1.4%
Software	1.2%

Spam URL Distribution Based on Top Level Domain Name

Source: Symantec

Month*	.com	.biz	.eu	.us
Oct	26.1%	17.7%	13.6%	11.8%
Sep	30.8%	13.8%	n/a	n/a

*Data lags one month

Phishing

At a Glance

- The global phishing rate is down in November, comprising one in 1 in 1,311 email messages. In October this rate was one in 1 in 1,135.
- Financial themes continue to be the most frequent subject matter, with 74.8 percent of phishing scams containing this theme.
- South Africa had the highest rate in November, where one in 486 emails was a phishing scam.
- The United States tops the list of sources of phishing emails, responsible for distributing 31.7 percent of phishing scams.
- The Public Sector was the most targeted industry in November, with one in every 435 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	Percent
United States	31.7%
United Kingdom	16.2%
Sweden	9.8%
Australia	8.7%
South Africa	8.3%
Germany	7.8%
Singapore	7.5%
Hong Kong	2.6%
Austria	2.2%
Netherlands	2.2%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 886
251-500	1 in 1,313
501-1000	1 in 1,886
1001-1500	1 in 1,667
1501-2500	1 in 2,266
2501+	1 in 1,368

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 435
Education	1 in 708
Accom/Catering	1 in 776
Marketing/Media	1 in 868
Non-Profit	1 in 1,007

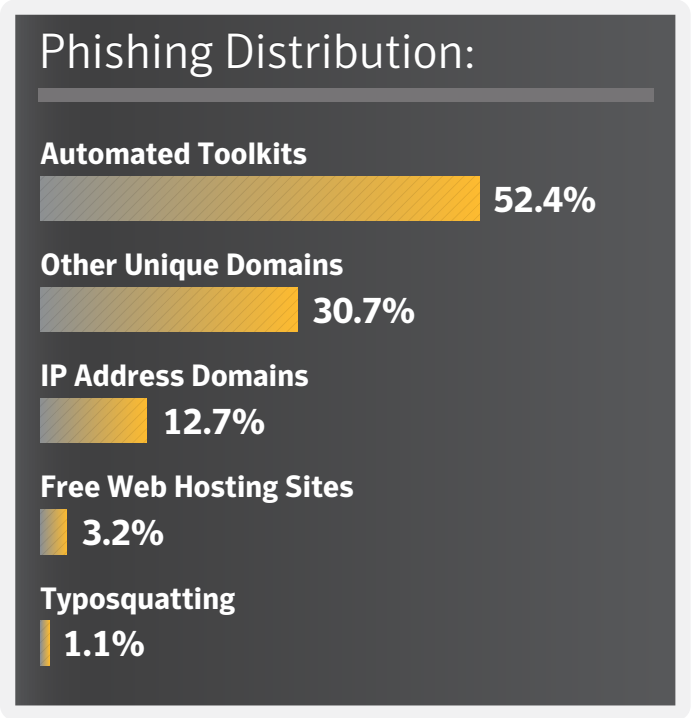
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
South Africa	1 in 486
United Kingdom	1 in 755
Austria	1 in 829
Italy	1 in 871
Netherlands	1 in 1,004

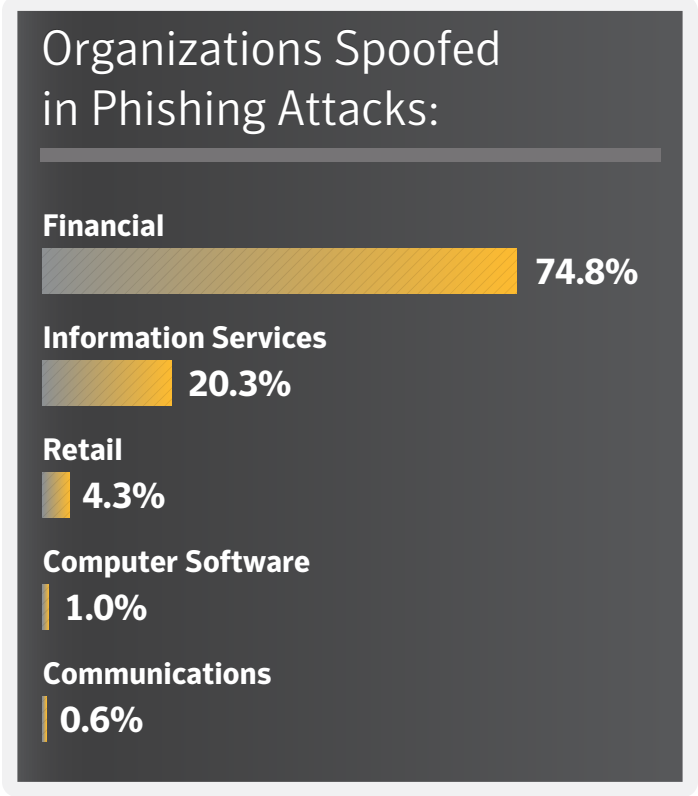
Phishing Distribution

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in November was one in 235 emails, compared to one in 437 in October.
- The United Kingdom topped the list of geographies, with one in 109 emails containing a virus.
- The United Kingdom was also the largest source of virus-laden emails, making up 54.9 percent of all email-based viruses.
- Small-to-medium size businesses with 1-250 employees were the most targeted company size, where one and 202 emails contained a virus.

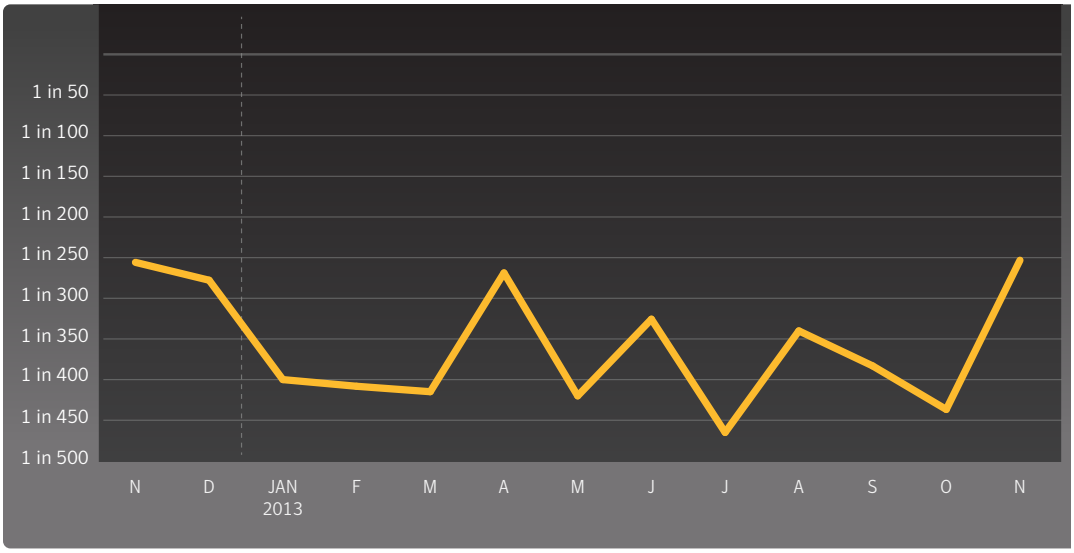
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United Kingdom	54.9%
United States	15.3%
Australia	9.1%
South Africa	3.6%
Hong Kong	2.2%
France	1.8%
Netherlands	1.8%
Japan	1.7%
India	1.4%
Canada	1.0%

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 62
Education	1 in 130
Accom/Catering	1 in 158
Marketing/Media	1 in 189
Recreation	1 in 191

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
United Kingdom	1 in 109
Austria	1 in 229
United Arab Emirates	1 in 254
Hungary	1 in 258
Ireland	1 in 272

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 202
251-500	1 in 244
501-1000	1 in 317
1001-1500	1 in 246
1501-2500	1 in 417
2501+	1 in 254

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 12.3 percent of all malware blocked at the endpoint.
- In comparison, 6.6 percent of all malware were variants of W32.Sality.
- Approximately 45.9 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	5.73%
W32.Ramnit!html	4.83%
W32.Ramnit.B	4.13%
W32.Almanahe.B!inf	3.61%
W32.Downadup.B	3.53%
W32.Ramnit.B!inf	2.88%
Trojan.Zbot	2.47%
W32.Virut.CF	1.87%
W32.SillyFDC	1.54%
W32.Mabezat.B!inf	1.01%

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 42.7 percent of blocked Web activity in November.
- "Advertisement & Popups" was the second-most common trigger, comprising 21.4 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	42.7%
Advertisement & Popups	21.4%
Streaming Media	4.5%
Hosting Sites	4.0%
Computing & Internet	3.4%
Chat	3.0%
Search	2.4%
Peer-To-Peer	1.7%
News	1.0%
Entertainment	0.9%

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