Symantec

SYMANTEC INTELLIGENCE REPORT

DECEMBER ⌖ 2013

CONTENTS

Executive Summary

Welcome to the December 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 see the email virus rate increase for the second month in a row, reaching an annual high of one in 164 emails.

Targeted attacks continue to focus on the Service-related industries, both in the professional and non-traditional realms. Two out of every five targeted attacks appear to be focused on these Service categories.

We also saw an increase in the overall number of data breaches reported in December, many of which occurred in previous months. Many of these disclosures from earlier in the year could be due to various regulations and/or laws requiring the disclosure of a breach during the year it occurred.

In other news, the number of mobile malware variants has declined for the third month in a row, and global spam rate has increased this month, after a two month decline.

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

Oct	1 in 1,134
Nov	1 in 1,311
Dec	1 in 1,053

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

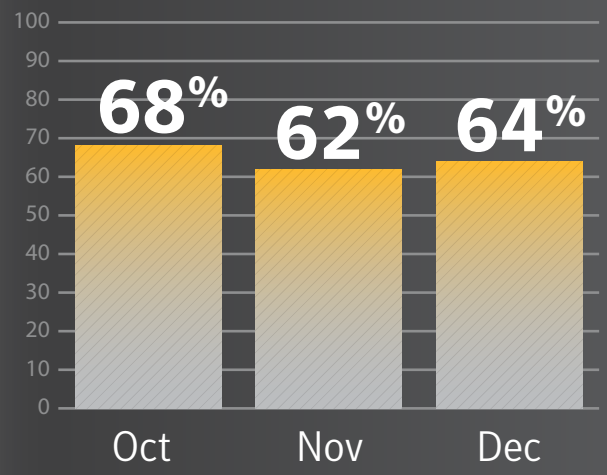
Oct	1 in 437
Nov	1 in 253
Dec	1 in 164

Mobile Vulnerabilities

Oct	5
Nov	6
Dec	1

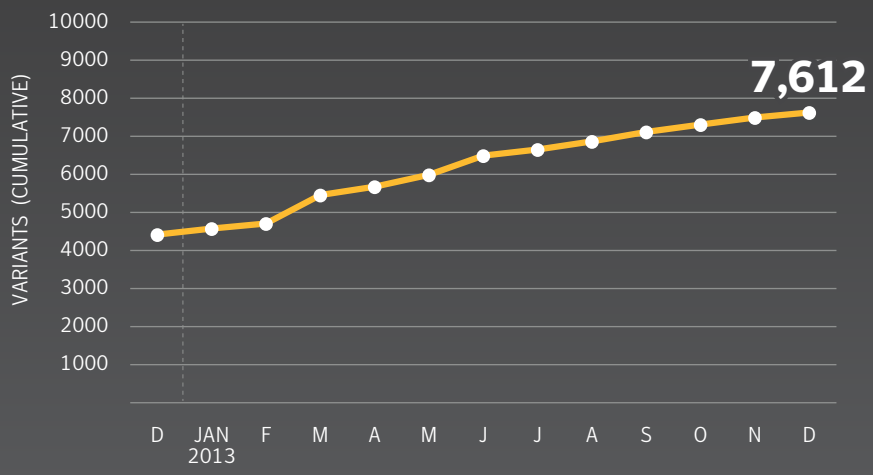
Estimated Global Email Spam Rate Per Day

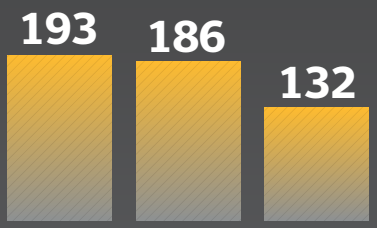
SPAM AS PERCENT OF ALL EMAIL



New Vulnerabilities

Mobile Malware Variants





Data Breaches

Number of Breaches (Year-to-Date)

215

Number of Identities Exposed (Year-to-Date)

342,794,556

TARGETED ATTACKS

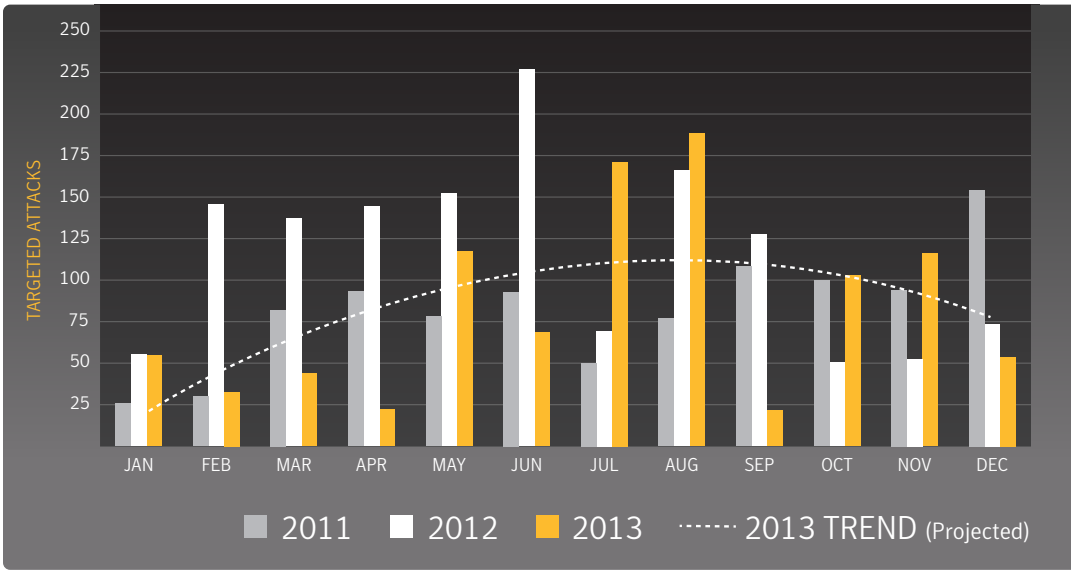
Targeted Attacks in 2013

At a Glance

- Targeted attacks were down in December, after above-average numbers in October and November.
- Large organizations of 2500+ are targeted in 39% of attacks, 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 31.3% of email-based targeted attacks that included file attachments.

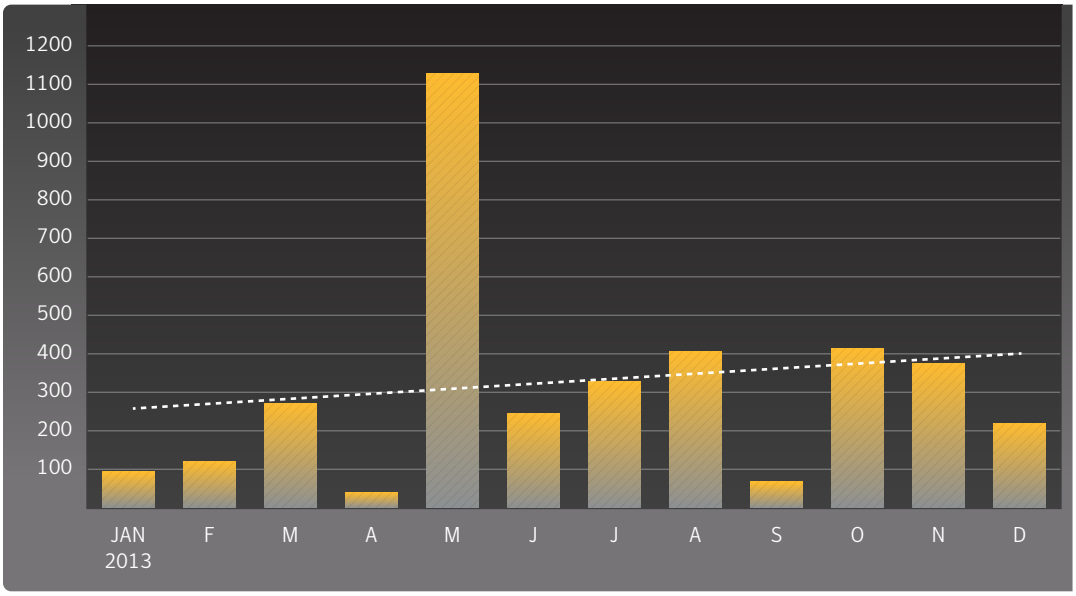
Targeted Attacks per Day

Source: Symantec



First Attacks Logged by Month

Source: Symantec



Attacks by Size of Targeted Organization

Source: Symantec

Company Size	Percent
1-250	29.8%
251-500	10.7%
501-1000	9.5%
1001-1500	3.3%
1501-2500	7.6%
2500+	39.0%

First Attacks Logged by Size

Source: Symantec

Company Size	Percent
1-250	52.5%
251-500	10.9%
501-1000	9.2%
1001-1500	5.1%
1501-2500	4.9%
2500+	17.4%

Top 10 Industries Attacked

Source: Symantec

Industry	Percent
Services - Professional	20.1%
Services - Non Traditional	18.5%
Public Administration	14.8%
Finance, insurance & Real Estate	13.4%
Manufacturing	11.1%
Transportation, communications, electric, gas & Sanitary Services	8.0%
Wholesale	5.2%
Retail	2.2%
Nonclassifiable Establishments	2.0%
Logistics	1.8%

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	31.3%
.scr	18.4%
.doc	7.9%
.pdf	5.3%
.class	4.7%
.jpg	3.8%
.dmp	2.7%
.dll	1.8%
.au3	1.7%
.xls	1.2%

SOCIAL MEDIA

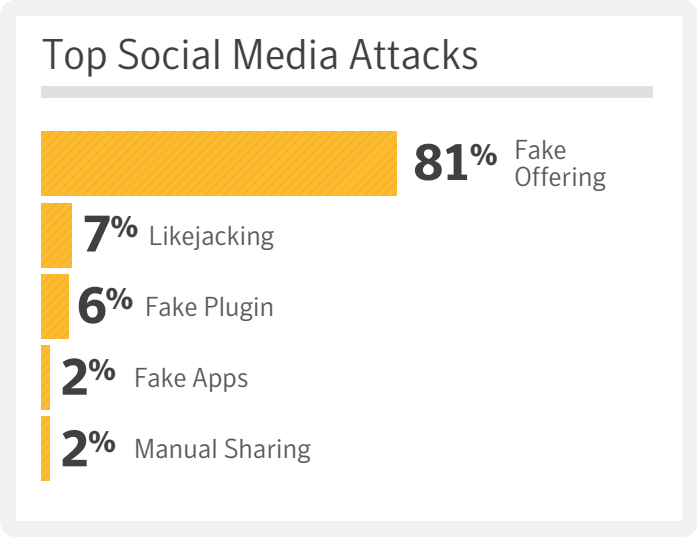
Social Media

At a Glance

- 81 percent of all social media attacks in 2013 where fake offerings. This is up from 56 percent in 2012.
- Likejacking is the second-most common type of social media attack at 7 percent, though it is down from 2012, when it made up 10 percent.
- Fake Apps have risen overall in 2013, 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

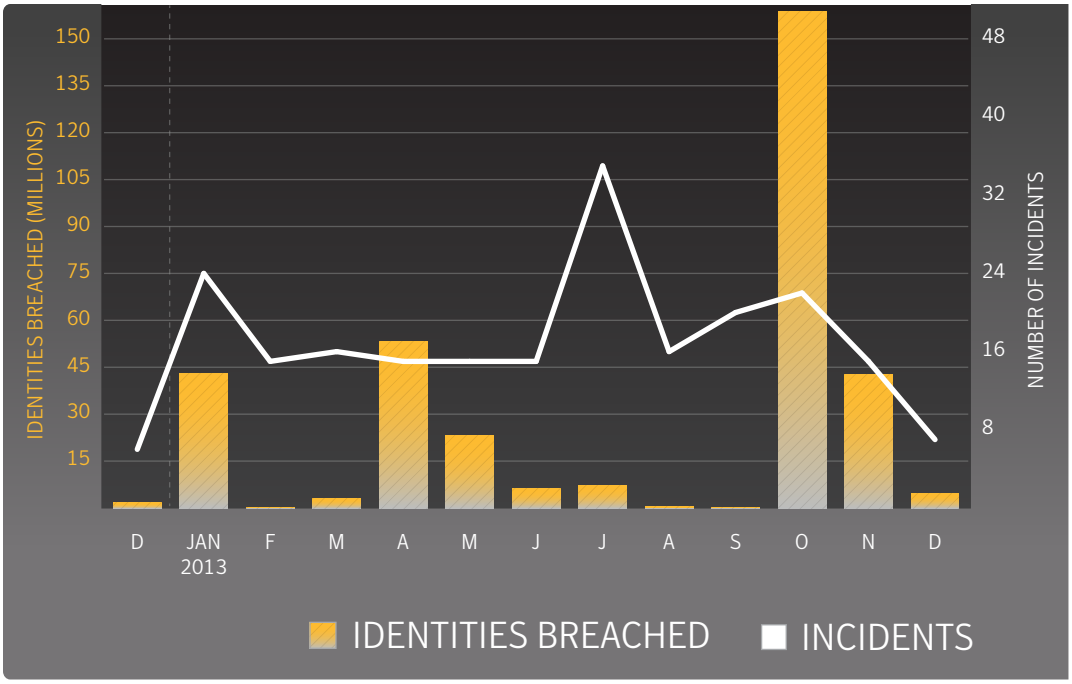
Data Breaches

At a Glance

- The largest breach that was reported in December actually occurred during November, where 40 million identities were exposed.
- There were a number of breaches reported during December that occurred earlier in the year. This brings the total number of reported breaches to 215 so far for 2013.
- Of the reported breaches so far, the top three types of information exposed are a person's real name, government ID number (e.g. Social Security), and birth date.

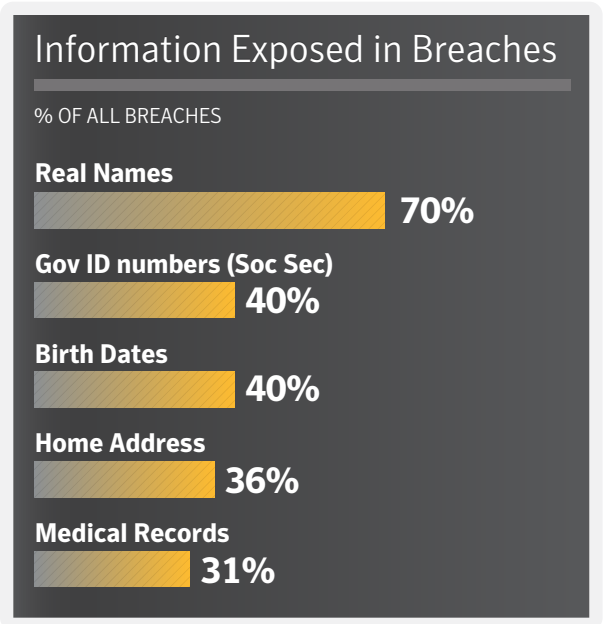
Timeline of Data Breaches, 2013

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

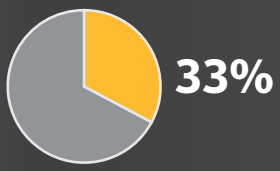
Mobile

At a Glance

- 33 percent of mobile malware tracks users in 2013, up from 15 percent in 2012.
- Traditional threats, such as back doors and downloaders are present in 20 percent of all mobile malware threats.
- Risks that collect data, the most common risk in 2012, is down 12 percentage points to 20 percent of risks.
- Four new mobile malware families were discovered in December, along with 132 new variants.

Mobile Malware by Type

Source: Symantec



33%

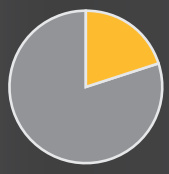
Track User

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.

21%

Adware/Annoyance

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



20%

Traditional Threats

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

20%

Collect Data

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

10%

Change Settings

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

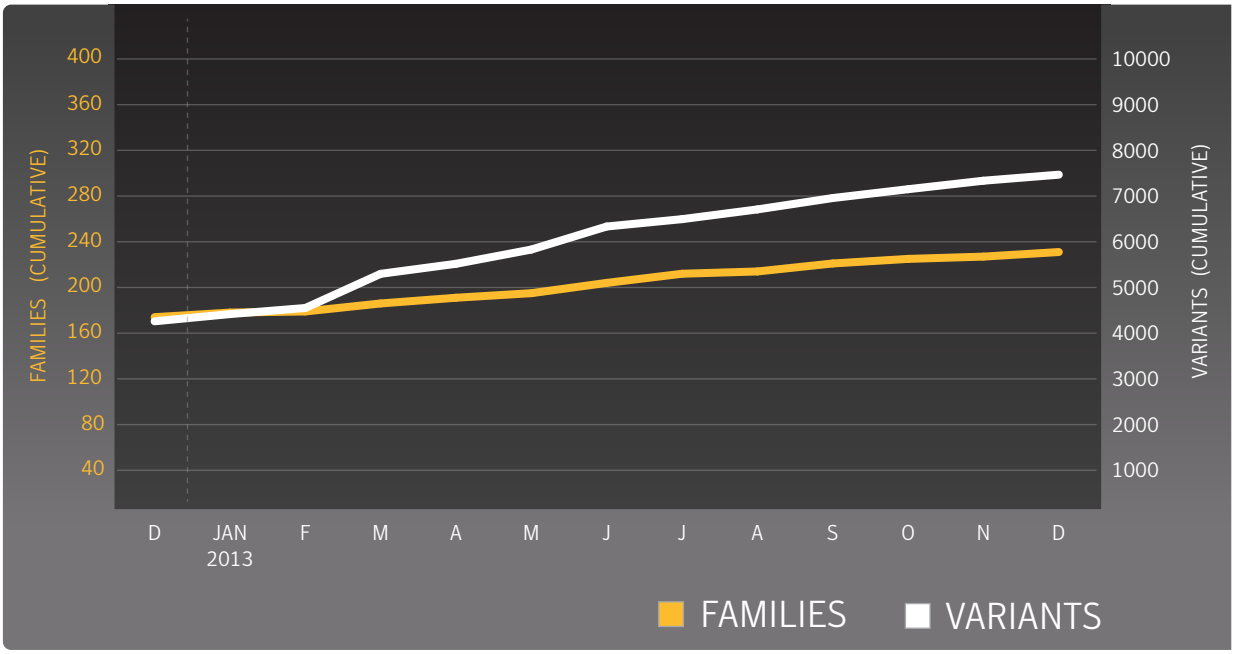
8%

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

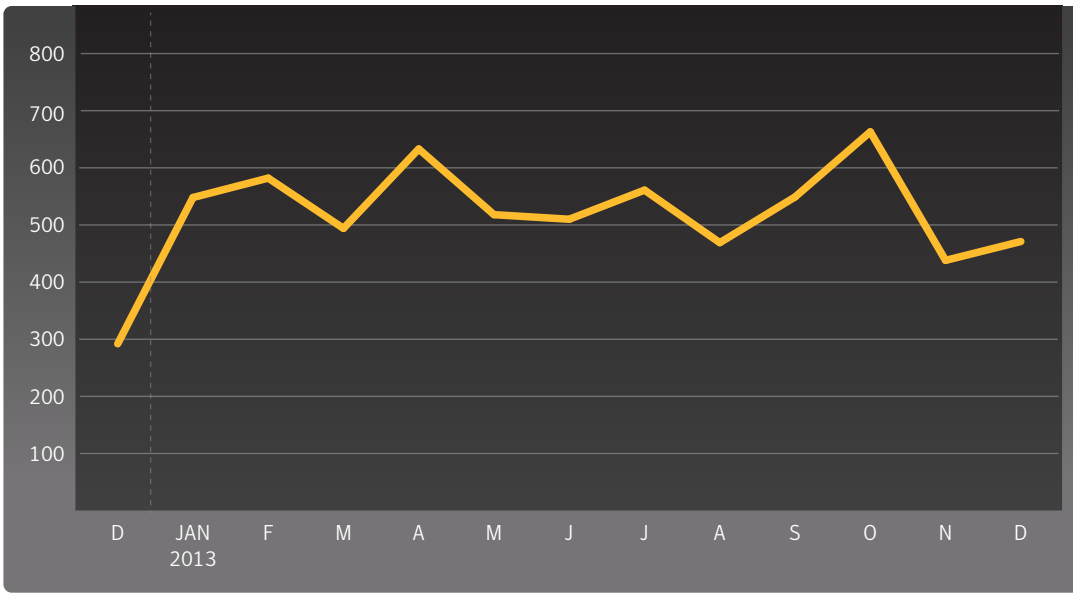
Vulnerabilities

At a Glance

- There were 471 new vulnerabilities discovered in December, bringing the total for the year up to 6436, a 18 percent increase compared to 2012.
- There was one vulnerability in mobile operating systems disclosed during the month of December.
- 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 December.

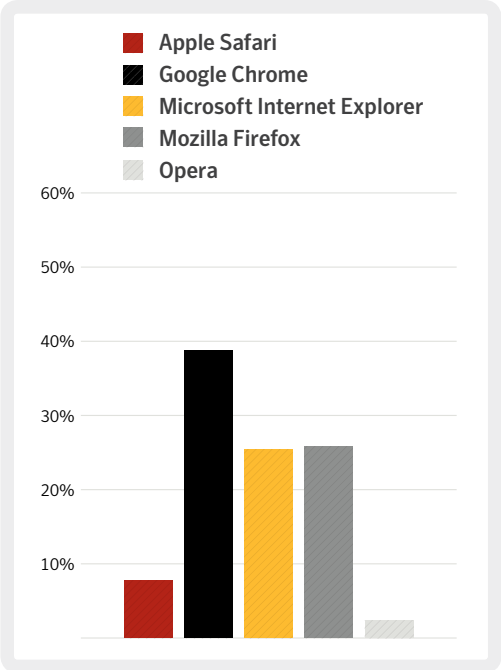
Total Vulnerabilities Disclosed by Month

Source: Symantec



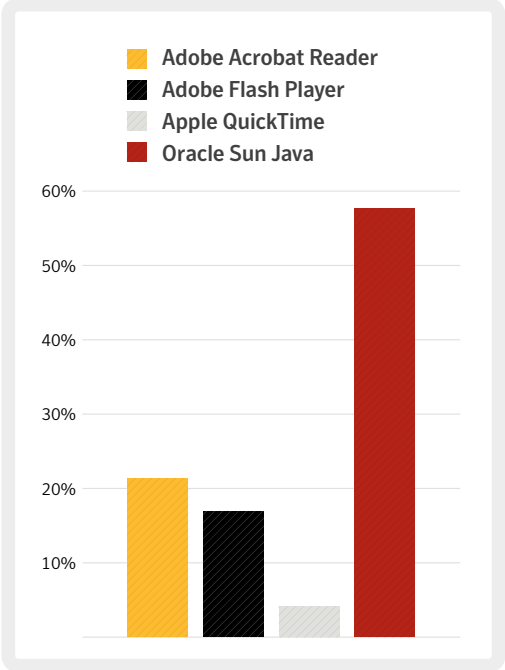
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

Spam

At a Glance

- The global spam rate increase 1.8 percentage points in December to 64 percent, up from 62.2 percent in November.
- Education was the most commonly targeted industry, taking the top spot for the second month in a row.
- The .com top-level domain (TLD) was again the most frequently used malicious TLD in December.
- Sex Dating spam is the most common category, at 76.3 percent. Pharmaceutical and Job-related spam tied for second at 9.2 percent each.

Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Sri Lanka	75.2%
Israel	71.6%
France	71.5%
Saudi Arabia	69.2%
China	69.1%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	65.9%
Gov/Public Sector	65.6%
Non-Profit	65.4%
Chem/Pharm	65.1%
IT Services	64.9%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
Spain	7.6%
United States	7.6%
Finland	6.4%
Argentina	5.1%
Italy	4.9%
India	4.1%
Canada	4.0%
Brazil	3.7%
Peru	3.5%
Romania	3.1%

Average Spam Message Size

Source: Symantec

Month*	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Nov	37.0%	24.7%	38.4%
Oct	40.2%	26.0%	33.8%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	63.7%
251-500	64.0%
501-1000	63.7%
1001-1500	64.1%
1501-2500	63.8%
2501+	64.2%

Spam by Category

Source: Symantec

Category	Percent
Sex/Dating	76.3%
Pharma	9.2%
Jobs	9.2%
Watches	1.8%
Software	1.3%

Spam URL Distribution Based on Top Level Domain Name

Source: Symantec

Month*	.com	.info	.us	.biz
Nov	36.7%	26.1%	10.1%	9.6%
Oct	26.1%	n/a	11.8%	17.7%

*Data lags one month

Phishing

At a Glance

- The global phishing rate is up in December, comprising one in 1 in 1,053 email messages. In November this rate was one in 1 in 1,311.
- Financial themes continue to be the most frequent subject matter, with 61.6 percent of phishing scams containing this theme.
- The United Kingdom had the highest rate in December, where one in 530 emails was a phishing scam.
- Australia tops the list of sources of phishing emails, responsible for distributing 35.9 percent of phishing scams.
- The Public Sector was the most targeted industry in December, with one in every 173 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	Percent
Australia	35.9%
New Zealand	29.3%
United States	18.8%
United Kingdom	6.0%
South Africa	3.5%
Sweden	2.1%
Chile	1.3%
Netherlands	0.5%
Canada	0.3%
Malaysia	0.3%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 862
251-500	1 in 944
501-1000	1 in 1,489
1001-1500	1 in 1,811
1501-2500	1 in 1,963
2501+	1 in 2,905

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 173
Finance	1 in 652
Education	1 in 803
Accom/Catering	1 in 834
Marketing/Media	1 in 1,016

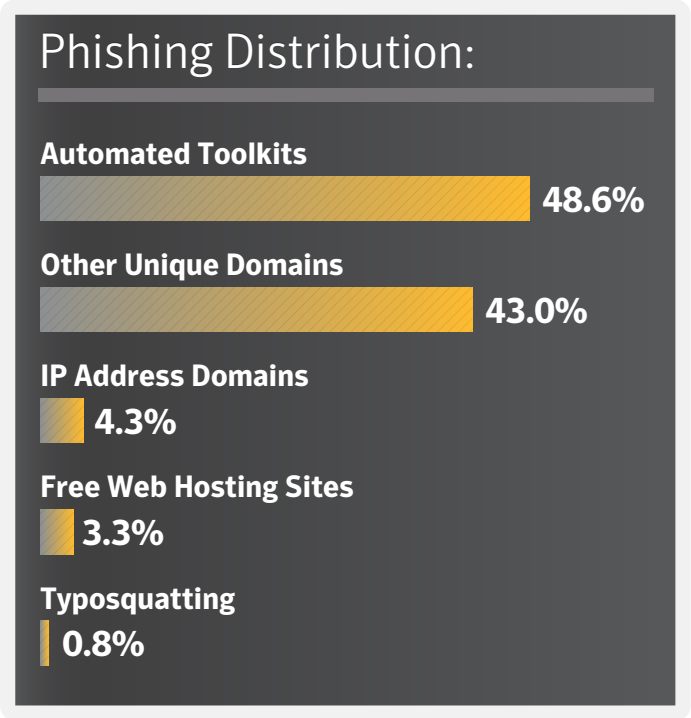
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
United Kingdom	1 in 530
Australia	1 in 734
Mexico	1 in 1,062
New Zealand	1 in 1,073
Italy	1 in 1,096

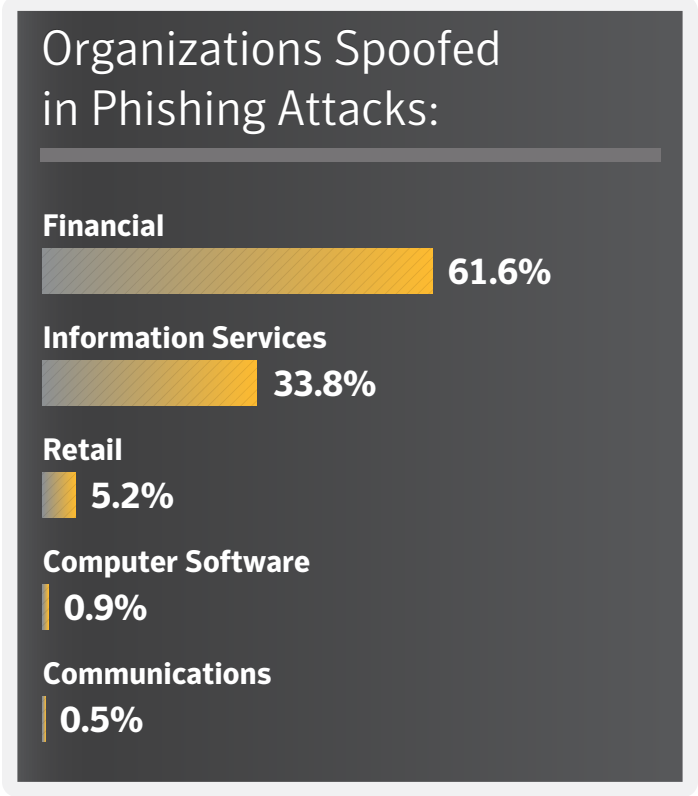
Phishing Distribution

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in December was one in 164 emails, compared to one in 253 in November.
- The United Kingdom topped the list of geographies, with one in 65 emails containing a virus.
- The United Kingdom was also the largest source of virus-laden emails, making up 60.7 percent of all email-based viruses.
- Small-to-medium size businesses with 1-250 employees were the most targeted company size, where one and 147 emails contained a virus.

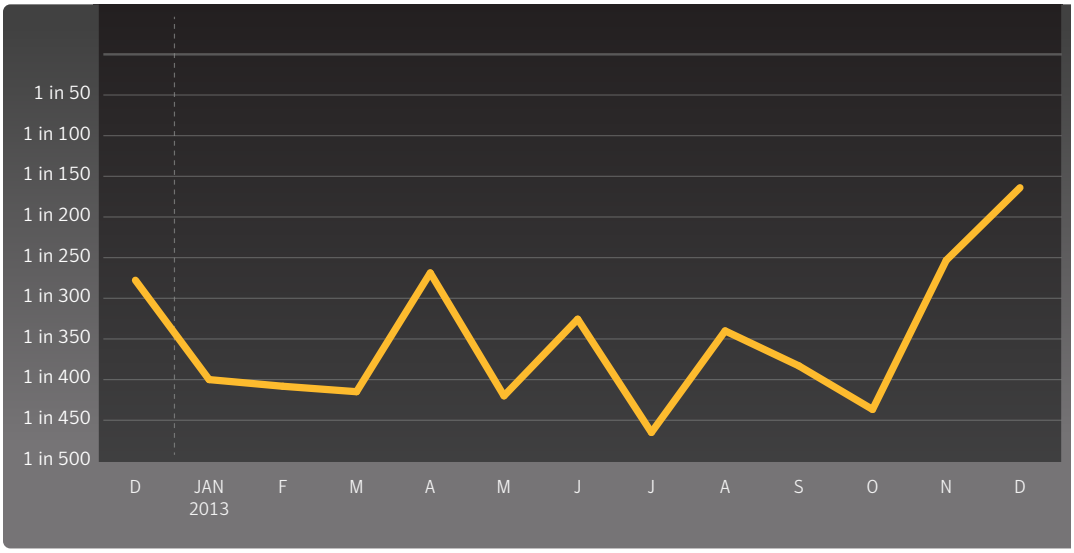
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United Kingdom	60.7%
Sri Lanka	14.0%
United States	13.9%
Australia	2.7%
France	0.9%
South Africa	0.9%
Japan	0.8%
Netherlands	0.7%
Singapore	0.5%
Hong Kong	0.5%

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 33
Education	1 in 76
Accom/Catering	1 in 122
Recreation	1 in 150
Prof Services	1 in 151

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
United Kingdom	1 in 65
Switzerland	1 in 128
Austria	1 in 200
Ireland	1 in 201
Hungary	1 in 256

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 147
251-500	1 in 150
501-1000	1 in 167
1001-1500	1 in 183
1501-2500	1 in 213
2501+	1 in 324

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 8.1 percent of all malware blocked at the endpoint.
- In comparison, 4.3 percent of all malware were variants of W32.Sality.
- Approximately 30.1 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	5.7%
W32.Ramnit!html	4.8%
W32.Ramnit.B	4.1%
W32.Almanahe.B!inf	3.6%
W32.Downadup.B	3.5%
W32.Ramnit.B!inf	2.9%
Trojan.Zbot	2.5%
W32.Virut.CF	1.9%
W32.SillyFDC	1.5%
W32.Mabezat.B!inf	1.0%

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 50.8 percent of blocked Web activity in December.
- "Advertisement & Popups" was the second-most common trigger, comprising 21.1 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	50.8%
Advertisement & Popups	21.1%
Streaming Media	4.9%
Hosting Sites	3.6%
Computing & Internet	3.4%
Search	1.8%
Chat	1.6%
Gambling	1.3%
News	1.1%
Entertainment	1.0%

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