Symantec

SYMANTEC INTELLIGENCE REPORT

JULY ⌖ 2013

CONTENTS

Executive Summary

Welcome to the July 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.

In this month's report we take a look at the latest trends in the threat landscape. In the realm of data breaches, July sees an increase in the number of breaches, with 21 reported so far during the month. We also note that 62 percent of all data breaches result in the exposure of real names, while 39 percent reveal either a person's birth day or a government identification number (such as a Social Security number).

Data breaches aren't the only location that identities and personal data are being compromised. Mobile malware in 2013 has also contributed significantly to data exposure, where 43 percent of mobile threats specifically attempt to steal information from the device. This is up significantly since 2012, where 15 percent of mobile threats behaved similarly.

In other news there were 561 new vulnerabilities discovered in July, a 17 percent increase compared to the same period in 2012. The global spam rate rose 3.4 percentage points in July to 67.6 percent and the top-level domain for Poland comprised almost 59% of spam-related domains in July. Finally, financial-themed phishing emails top the list of topics, comprising close to 70 percent of all phishing attempts blocked.

We've also provided a run-down on the biggest security stories for the month of July, recapping what happened and what that means to our readers.

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

May	1 in 562
Jun	1 in 464
Jul	1 in 736

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

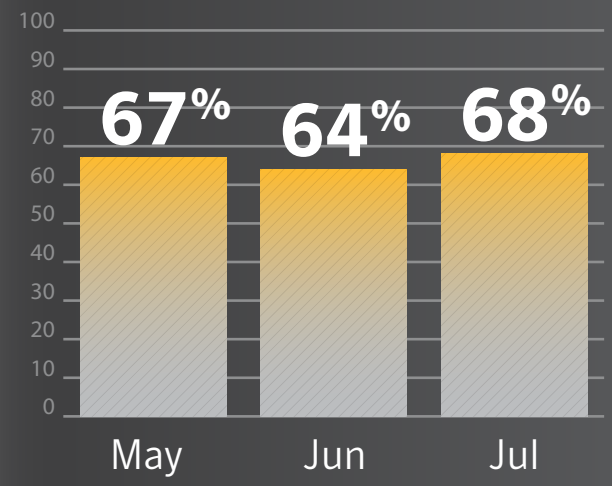
May	1 in 420
Jun	1 in 326
Jul	1 in 465

Mobile Vulnerabilities

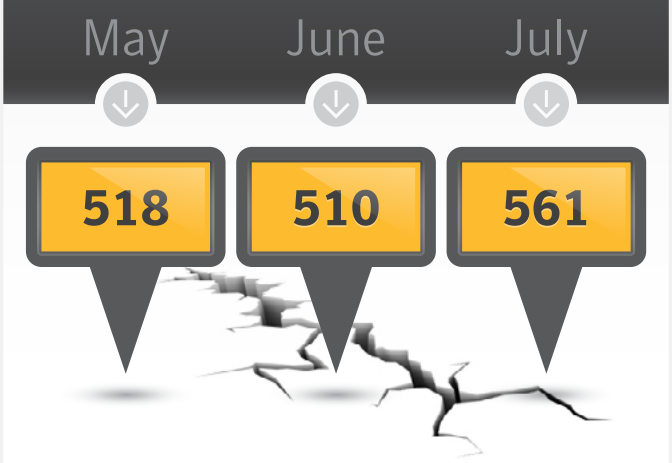
May	0
June	4
July	3

Estimated Global Email Spam Rate Per Day

SPAM AS PERCENT OF ALL EMAIL



New Vulnerabilities



Data Breaches

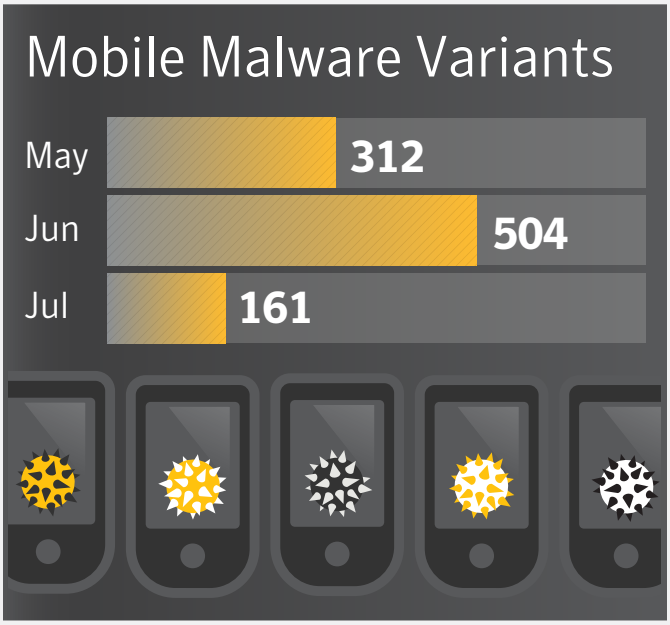
Number of Breaches (Year-to-Date)

109

Number of Identities Exposed (Year-to-Date)

86,901,952

Mobile Malware Variants



TIMELINE

July Security Timeline

July 01

A new crypto-currency was hit by malware in early July. The relatively new digital currency claims to offer quicker transaction speeds than its competitors, as well as an ability to mine currency on consumer-grade computers. The Trojan in question attempts to steal the victim's digital wallet and send it to an attacker.

July 08

It emerged for the first time in July that last year's London Olympics could have been subjected to a cyberattack that could have left the opening ceremony without light. According to Olympic CyberSecurity head Oliver Hoare, extensive precautions were put in place after attack tools and targeting information were discovered that were thought to be related to the Olympics.

Hoare received a phone call in the early hours of the morning before the opening ceremony and was told of the potential attack. Although a lot of attention and planning had revolved around the threat of a terrorist attack on the games, Hoare said that "extensive testing had still taken place for a range of different possibilities" including cyber attacks. The CyberSecurity team had run multiple tests dealing with an attack on the electricity infrastructure and, although time was against them, this planning with Olympic organizers and private sector electricity providers meant that they were well prepared.

July 10

A popular messaging platform that enables users to chat to groups of up to 30 friends on their mobile device became the target of a worm attack. The worm spread manually through the messaging service on certain devices, changing contact group names to "Priyanka". However, for anything malicious to occur to the device, users needed to accept and install a contact file, also named Priyanka. Deleting this contact and clearing the messaging service data should clean the device.

July 15

Attackers targeted and defaced the Pilipino website of a global technology news publication. The website displayed several pop-ups which said that there had been a security breach. The attackers appear to be part of Pinoy Vendetta, a hacking group based in the Philippines that undertakes acts of hacktivism, with the aim of finding weaknesses in websites based in the country. The page which users were redirected to claims that the group was "testing the security" of the website.

July 21

A forum for an online community surrounding a popular Linux distribution suffered a data breach, affecting 1.8 million of its members. The forum's operators said that attackers accessed "every user's local username, password, and email address" from the database, but emphasized that passwords were encrypted. Nonetheless, the operators have encouraged users to change their passwords on the forum and any other services where they may have used the same password. The company that backs the forum said that it is continuing to investigate how attackers gained access to this data and is working to address the issue.

July 22

A German cryptographer has released details on a way to hack SIM cards. Karsten Nohl and his team discovered an exploit that can crack update keys using over-the-air commands. An attacker can use the stolen key to sign and send malicious software to the device, potentially enabling the attacker "to send SMS, change voicemail numbers, and query the phone location," says Nohl. With an estimated one eighth of the world's SIMs at risk, Nohl recommends that carriers update the SIM cards of affected phones.

July 24

A popular call and messaging app became the latest high-profile hacking victim of the Syrian Electronic Army (SEA). The service's database was breached and its website defaced following a successful phishing attack against one its employees. The company released a statement to say that the phishing attack allowed access to a customer support panel and a support administration system, but that no sensitive user data was exposed.

July 25

Symantec took part in the successful takedown of a cyber-criminal gang in Tokyo. The takedown followed months of painstaking work monitoring and investigating the activities of a prolific Tokyo crime gang alongside Japanese law enforcement agencies. The end result was the arrest of nine of its members including a well-known figure in poker tournament circles with over US$1.5 million winnings to his name. This raid by the police is a major blow to the crime gang that was previously engaged in many forms of cyber-criminal activities including spamming, running a fake online dating site, fake antivirus, and information theft.

July 26

Four Russians and a Ukrainian were charged for their role in the largest hacking and data breach scheme in U.S. history to-date. The five conspired in a "worldwide scheme that targeted major corporate networks, stole more than 160 million credit card numbers and resulted in hundreds of millions of dollars in losses", according to attorney Paul Fishman. The charges include computer hacking conspiracy, wire fraud, conspiracy to commit wire fraud, and unauthorized computer access. The men worked with Albert Gonzalez, a hacker serving 20 years in prison and best known for masterminding the TJX hack in which he stole tens of millions of credit and debit card numbers.

DATA BREACHES

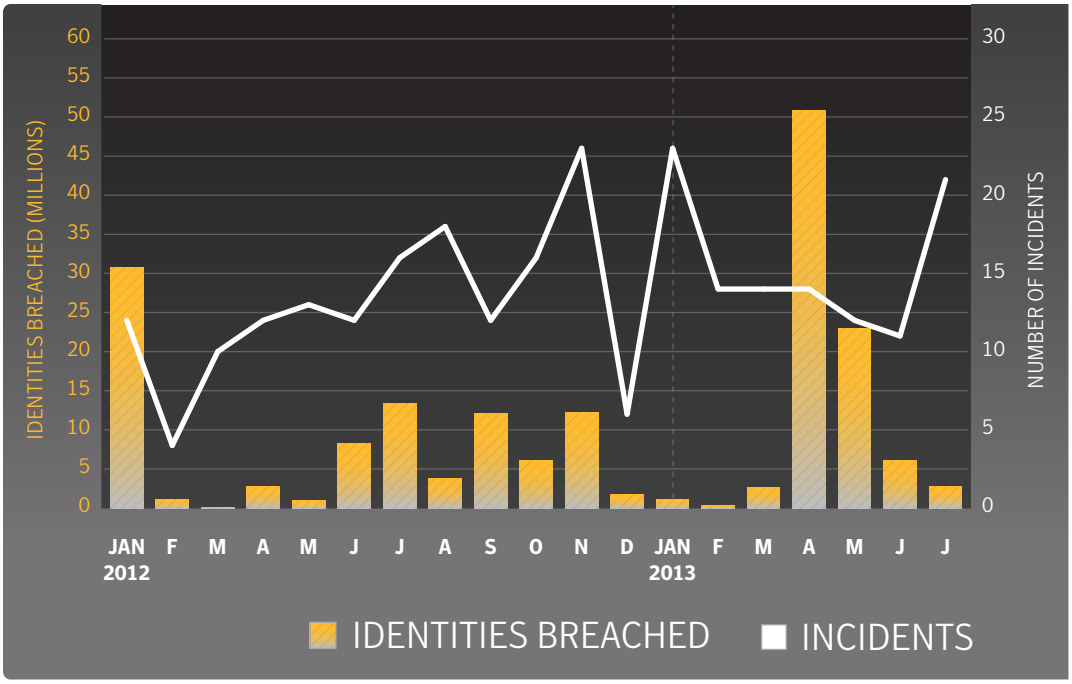
Data Breaches

At a Glance

- There were 21 data breaches recorded during the month of July, making it the second-highest month for the year behind January. So far there have been 109 data breaches recorded through July, up 16 percent over the same period in 2012.
- However, the number of identities stolen was the third-lowest for the year, at 2.7 million. This brings the total identities exposed to 86.9 million in 2013 so far.
- Of the data breaches reported so far in 2013, 62 percent contain a person's real name. Birth dates and government ID numbers (e.g. Social Security) numbers appear in 39 percent of breaches.

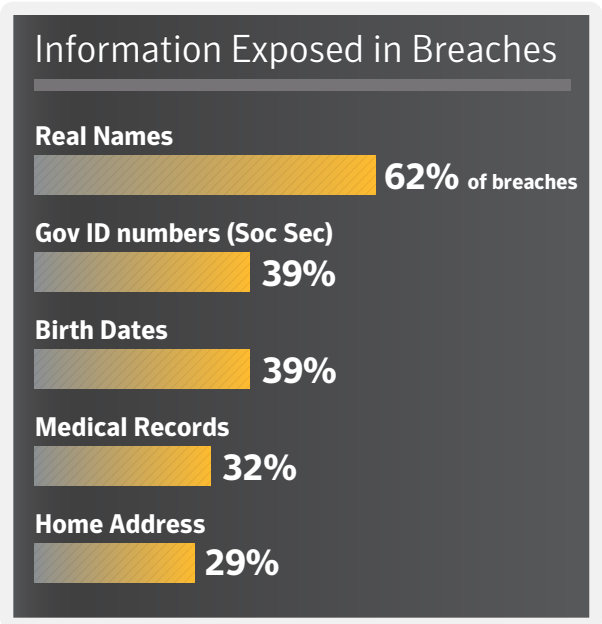
Timeline of Data Breaches, 2013

Source: Symantec



Top 5 Data Breaches by Type 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

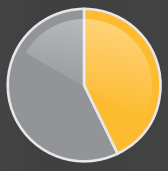
Mobile

At a Glance

- So far in 2013, 43 percent of mobile malware tracks users, up from 15 percent in 2012.
- Adware/Annoyance risks have also increased, from 8 percent in 2012 to 23 percent of mobile malware found so far this year.
- Risks that collect data, the most common risk in 2012, has dropped significantly, down 15 percentage points to 17 percent of risks.
- Eight new mobile malware families were discovered in July, along with 161 new variants.

Mobile Malware by Type

Source: Symantec



43%

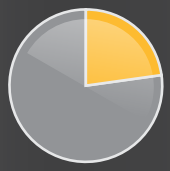
Track User

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.

17%

Collect Data

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



23%

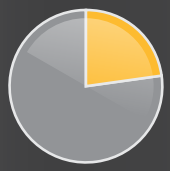
Traditional Threats

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

11%

Change Settings

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



23%

Adware/Annoyance

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

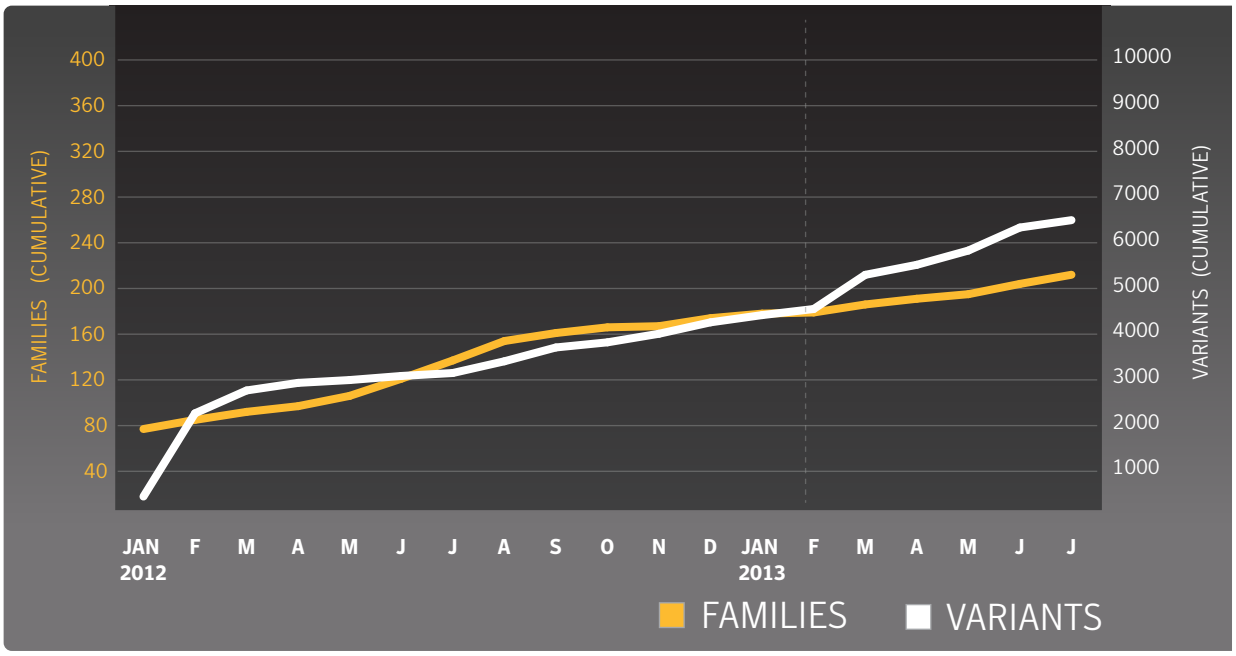
6%

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

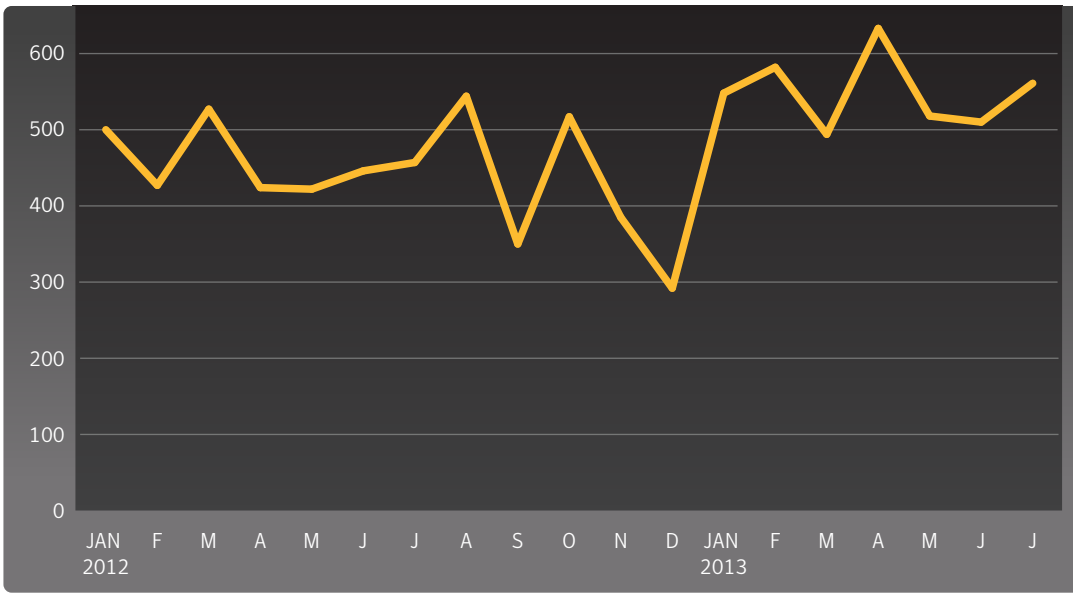
Vulnerabilities

At a Glance

- There were 561 new vulnerabilities discovered in July, bringing the total for the year up to 3846, a 17 percent increase compared to the same period in 2012.
- One zero-day vulnerability was disclosed in July, a vulnerability in Internet Explorer (CVE-2013-3163).
- Three vulnerabilities were discovered in mobile operating system during the month of July.
- Google's Chrome browser continues to lead in reporting browser vulnerabilities, which Oracle's Java leads in reported plug-in vulnerabilities.

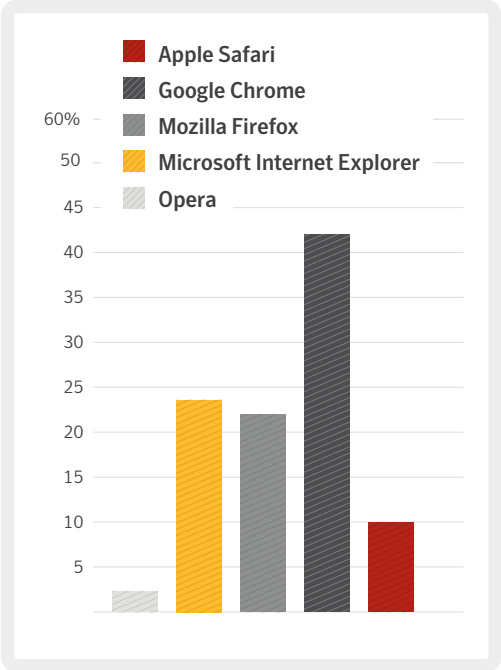
Total Vulnerabilities Disclosed by Month

Source: Symantec



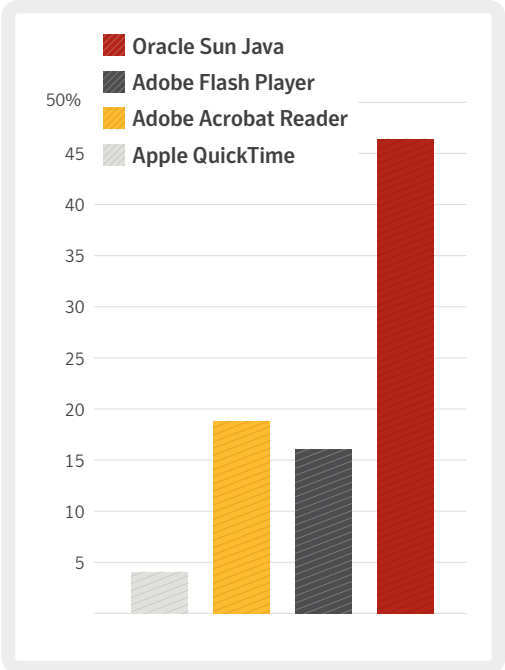
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

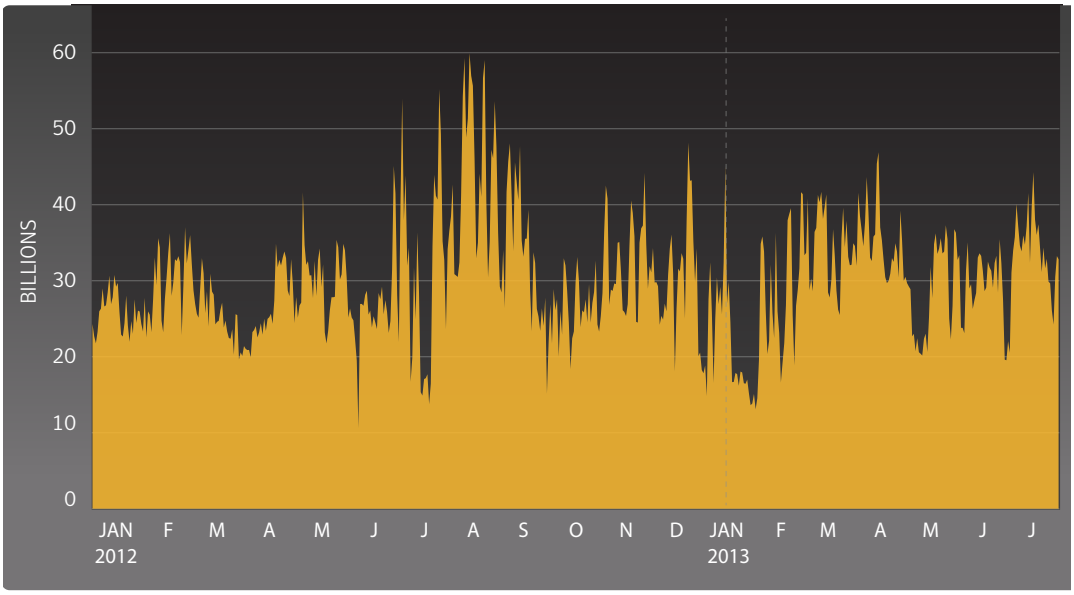
Spam

At a Glance

- The global spam rate rose 3.4 percentage points in July to 67.6 percent, up from 64.2 percent in June.
- Education continues to be the most commonly targeted industry, as was the case in June.
- The top-level domain (TLD) for Poland, .pl, has topped the list of malicious TLDs, comprising almost 59% of spam-related domains in July.
- Sex/Dating spam continues to be the most common category, at 60.7 percent. Pharmaceutical spam comes in second at 27.9 percent.

Global Spam Volume Per Day

Source: Symantec



Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Saudi Arabia	82.2%
Sri Lanka	76.8%
China	74.3%
Hungary	72.8%
Qatar	72.2%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	69.2%
Chem/Pharm	68.9%
Non-Profit	68.4%
Manufacturing	68.3%
Accom/Catering	68.0%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
United States	8.53%
Italy	7.56%
Spain	6.25%
Argentina	6.22%
India	5.07%
Brazil	4.64%
Finland	3.81%
Canada	3.60%
Germany	3.51%
Colombia	3.30%

Average Spam Message Size*

Source: Symantec

*Month	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Jun	22.2%	47.5%	30.3%
May	33.8%	40.1%	26.1%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	67.2%
251-500	67.8%
501-1000	67.6%
1001-1500	68.0%
1501-2500	67.3%
2501+	67.8%

Spam by Category

Source: Symantec

Category	June	May
Sex/Dating	60.7%	78.7%
Pharma	27.9%	11.1%
Jobs	8.8%	2.5%
Watches	1.8%	4.7%
Software	0.5%	0.8%

Spam URL Distribution Based on Top Level Domain Name*

Source: Symantec

*Month	.pl	.com	.net	.biz
Jun	58.9%	18.4%	8.7%	2.9%
May	8.7%	22%	N/A%	N/A

*Data lags one month

Phishing

At a Glance

- The global phishing rate is down in July, comprising one in every 736.5 email messages. In June this rate was one in 463.5.
- Financial themes continue to be the most frequent subject matter, with 69.8 percent of phishing scams containing this theme.
- The United Kingdom not only tops the most targeted geography, where one in 367.0 emails are phishing scams, but is also the top source in July, responsible for 36.9 percent of all phishing scams.
- The Public Sector was the most targeted industry in July, with one in every 193.1 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	July
United Kingdom	36.90%
United States	31.89%
Hong Kong	14.41%
South Africa	4.49%
Australia	2.93%
Brazil	1.77%
Netherlands	1.50%
Germany	1.31%
France	0.63%
Sweden	0.59%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 729.1
251-500	1 in 356.5
501-1000	1 in 1,595.9
1001-1500	1 in 1,413.3
1501-2500	1 in 1,981.0
2501+	1 in 675.6

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 193.1
Finance	1 in 262.1
Accom/Catering	1 in 462.1
Education	1 in 502.9
Non-Profit	1 in 714.6

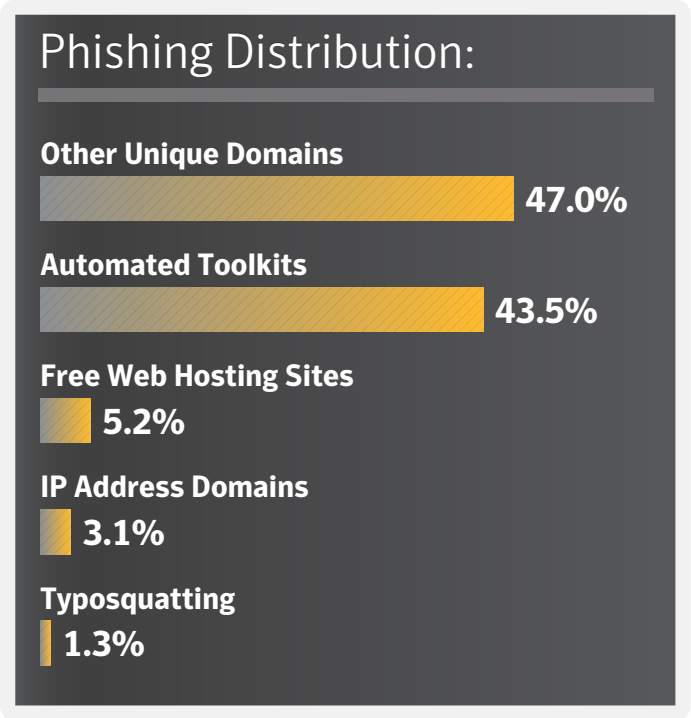
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
United Kingdom	1 in 367.0
South Africa	1 in 401.5
Belgium	1 in 467.3
Norway	1 in 724.9
Canada	1 in 1,026.3

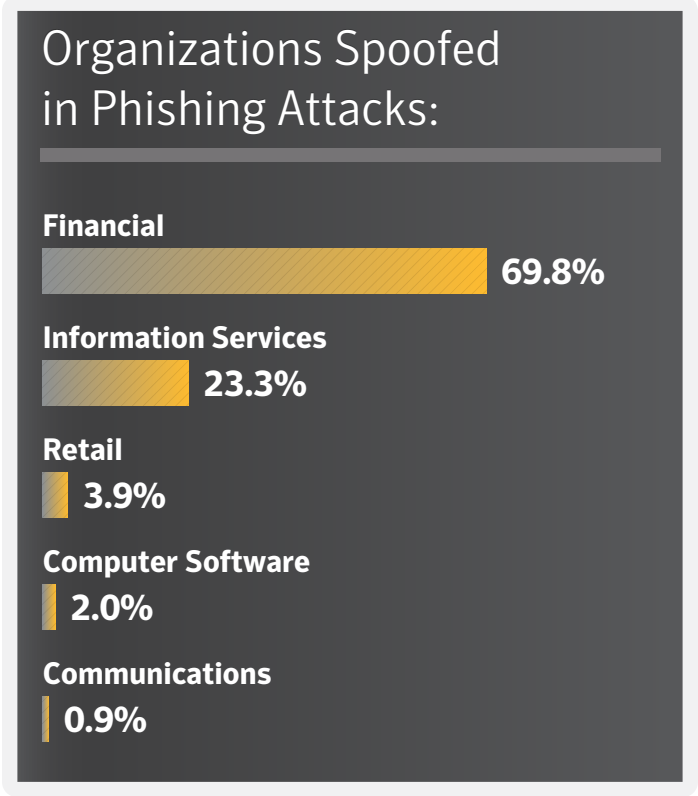
Phishing Distribution in July

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in July was one in 465.1 emails, compared to one in 325.7 in June.
- The United Kingdom topped the list of impacted geographies, with one in 258.4 emails containing a virus.
- The United States was the largest source of virus-laden emails, making up 44.2 percent of all email-based viruses.
- Businesses with 251-500 employees were the most targeted company size, where one and 325.8 emails contained a virus.

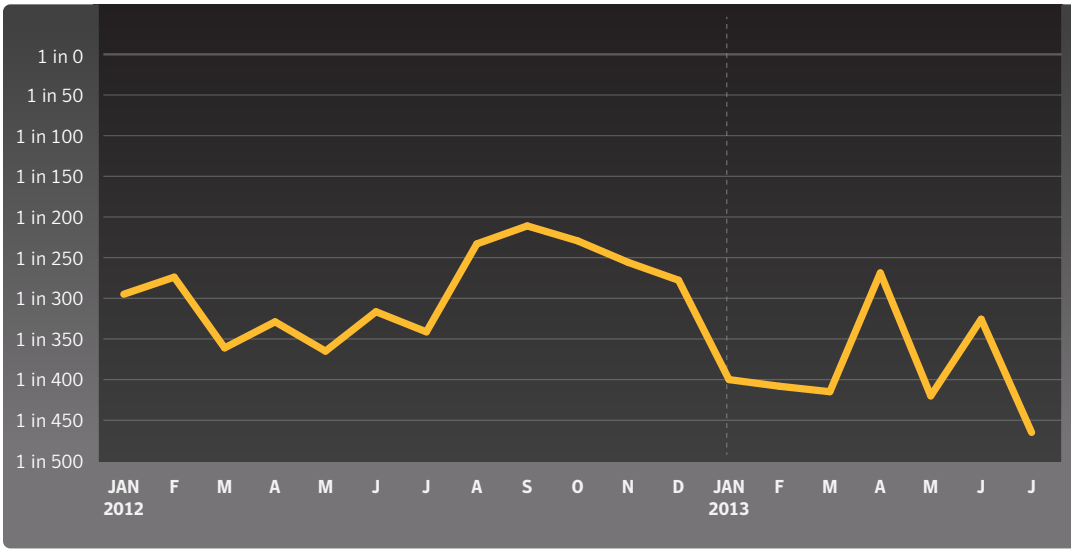
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United States	44.19%
United Kingdom	24.70%
Australia	6.37%
Canada	6.02%
India	3.93%
Netherlands	3.62%
South Africa	2.50%
Hong Kong	1.52%
Brazil	1.02%
Germany	0.69%

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 93.0
Education	1 in 298.3
Accom/Catering	1 in 345.1
Finance	1 in 385.4
Marketing/Media	1 in 427.4

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
United Kingdom	1 in 258.4
Hungary	1 in 369.2
South Africa	1 in 371.4
Belgium	1 in 386.5
Netherlands	1 in 419.8

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 529.8
251-500	1 in 325.8
501-1000	1 in 711.8
1001-1500	1 in 490.4
1501-2500	1 in 780.7
2501+	1 in 433.8

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 17.6 percent of all malware blocked at the endpoint.
- In comparison, 8.1 percent for all malware were variants of W32.Sality.
- Approximately 37.8 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	July
W32.Sality.AE	7.08%
W32.Ramnit!html	6.92%
W32.Ramnit.B	6.07%
W32.Ramnit.B!inf	4.32%
W32.Downadup.B	3.45%
W32.Almanahe.B!inf	3.29%
W32.Virut.CF	2.30%
Trojan.Zbot	2.07%
W32.SillyFDC.BDP!lnk	1.32%
W32.SillyFDC	1.20%

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 32.7 percent of blocked Web activity in July.
- "Advertisement & Popups" was the second-most common trigger, comprising 20.3 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	32.74%
Advertisement & Popups	20.32%
Search	4.73%
Streaming Media	3.33%
Computing & Internet	3.21%
Peer-To-Peer	2.88%
Chat	2.80%
Hosting Sites	1.74%
Games	1.27%
News	1.17%

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

- Symantec.cloud Global Threats: http://www.symanteccloud.com/en/gb/globalthreats/
- Symantec Security Response: http://www.symantec.com/security_response/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- 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