Symantec

SYMANTEC INTELLIGENCE REPORT

AUGUST ⌖ 2013

CONTENTS

Executive Summary

Welcome to the August 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 social media scams so far in 2013. What we have noticed is that fake offerings, such as bogus opportunities for discount purchases, has dominated the social landscape this year, making up 82 percent of all social media attacks.

In the realm of data breaches, August saw a decrease in the number of breaches, with seven reported during the month. However, there were a further nine breaches reported in August that had occurred earlier in the year, bringing the total to 125 breaches resulting in a total of 91 million identities being exposed in 2013 so far.

In other news, 213 new mobile malware variants were discovered this month, a modest increase since July, but nowhere near the numbers we saw in June. There were 469 new vulnerabilities discovered in August, a 13 percent increase compared to the total in August of 2012.

The global spam rate fell 2.4 percentage points from July to 65.2 percent. The top-level domain for Poland (i.e. .pl) comprised almost 48% of spam-related domains in August, topping the list two months in a row.

Finally, financial-themed phishing emails top the list of topics, comprising 66.8 percent of all phishing attempts blocked. Many of these phishing attempts appear to have come from Japan, which is responsible for 55 percent of phishing emails.

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

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

Jun	1 in 464
Jul	1 in 736
Aug	1 in 626

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

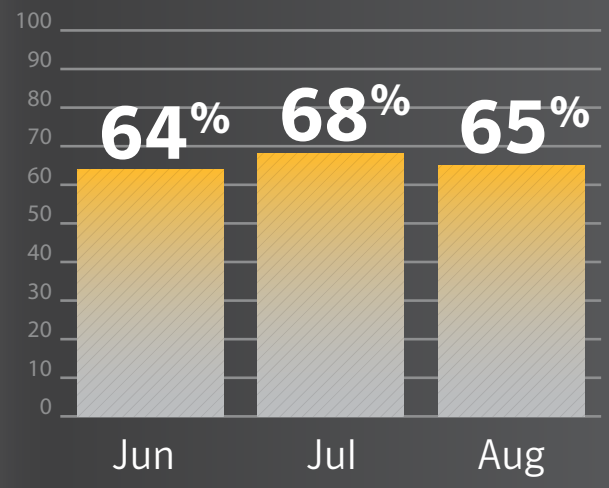
Jun	1 in 326
Jul	1 in 465
Aug	1 in 340

Mobile Vulnerabilities

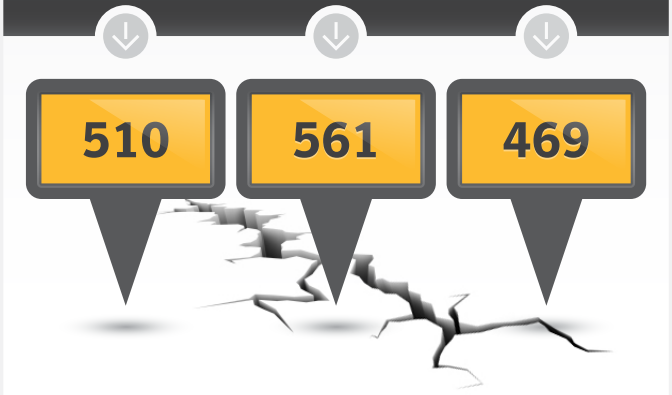
June	4
July	3
Aug	2

Estimated Global Email Spam Rate Per Day

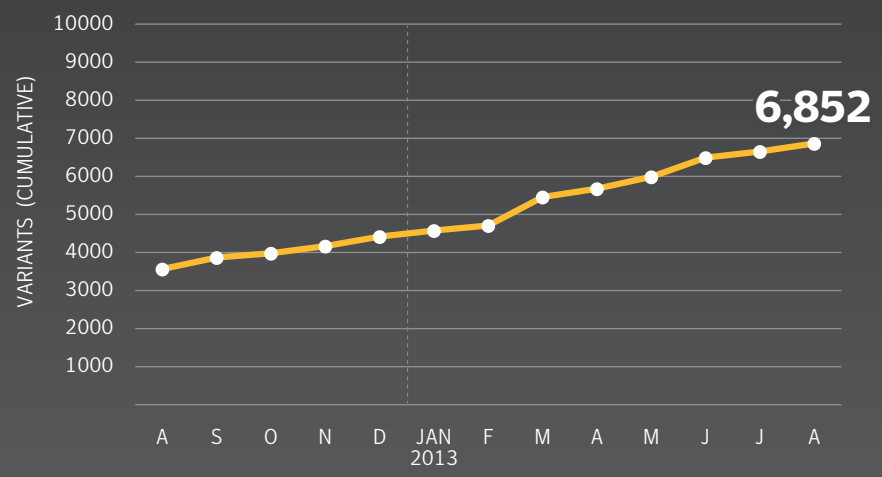
SPAM AS PERCENT OF ALL EMAIL

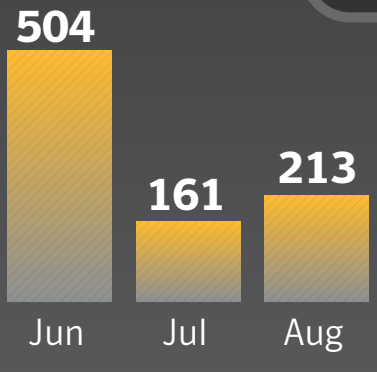


New Vulnerabilities



Mobile Malware Variants





Data Breaches

Number of Breaches (Year-to-Date)

125

Number of Identities Exposed (Year-to-Date)

91,068,940

TIMELINE

August Security Timeline

August 06

Attackers continued to target the 'Master Key' Android vulnerability, which allows them to inject malicious code into apps without invalidating the digital signatures. Security researchers have found that the flaw has been used to target the app of a South Korean bank. The attackers offered a malicious update for the banking app, as well as a Trojanized version of the full app, on a third-party app store. These malicious offerings take advantage of the vulnerability, allowing the infected app to keep the same cryptographic signature as the legitimate release. When the user opens the infected app, they are prompted to input their account information. If they do so, their data is sent to a remote server under the attacker's control.

August 11

Another critical vulnerability was found in Android, which could allow attackers to steal from the wallets of a well-known digital currency. Developers of the digital currency stated that any wallet that was generated by an Android app is vulnerable to theft due to a flaw within the mobile OS itself. The vulnerability involves a component which generates secure random numbers.

The developers recommended that users update their wallet app as soon as possible. They also told users to generate a new address with a repaired random number generator and send the money in the wallet back to themselves.

August 16

A computer glitch may have caused the opening of the doors in a maximum security wing at a Florida prison. The possible glitch set prisoners free, with gang members able to pursue an attack on a fellow inmate. However, a surveillance video released suggests that the doors may have been opened intentionally, possibly by a prison staff member, or remotely by someone else, by triggering a "group release" button in the computerized system.

The video raises the possibility that some prisoners knew in advance that the doors were going to open. It's the second time in two months that all of the doors in the maximum security wing opened at once. Part of the investigation into this latest incident will establish what vulnerabilities may exist within the software and whether it constituted a remote hack or not.

August 21

The company behind a popular video game suffered a data breach affecting a portion of its North American players of one of its most popular online games. The company has revealed that the breach was the result of nefarious work by hackers, and that passwords and credit card numbers stored in encrypted form were breached. In addition, user names, email addresses, and some real names were accessed.

The company has said they will contact affected users about the breach and will force players to change their passwords. It will also develop new security features for user accounts.

August 22

It has emerged that attackers compromised the wire payment switch at a number of US banks to steal millions of dollars over the past several months. The attackers conducted distributed denial-of-service (DDoS) attacks against at least three unnamed banks. While this was happening, the attackers hijacked the wire payment switch to make fraudulent wire transfers from multiple accounts.

Attackers often target a customer's bank account through malware that steals banking credentials. However, in this campaign, attackers could get access to numerous accounts at once by simply targeting the wire payment switch while the banks' resources were diverted elsewhere.

August 26

New European data regulations have come into effect, requiring telecom operators and Internet service providers (ISPs) to notify authorities of data breaches within 24 hours of detection. These organizations must tell authorities which pieces of information were compromised within one day of discovering the breach and what measures will be put in place to mitigate the damage. If full disclosure isn't possible during this time limit, the companies must provide an initial set of information and give further details within three days. If their customers' personal data is "adequately encrypted," the companies would not have to notify their customers as, according to the European Commission, a breach would "not actually reveal the subscriber's personal data."

While the laws aim to improve data protection in the EU, some have criticized the stricter time limit. The European Parliament is reportedly set to vote on whether the law will remain as it is in October, and if they vote to change it, the amended regulations will be put in place in May 2014.

August 27

The websites of several high-profile news and social media organizations were affected by a cyber attack undertaken by the Syrian Electronic Army (SEA) against the companies' domain name system (DNS) provider. According to the providers, the hacking group managed to access the login credentials of a reseller and used their account to modify the DNS records of several domain names. As a result, the SEA could redirect traffic from these websites to their own address. The provider said it has since changed the DNS records back, modified the affected reseller's login credentials, and has strengthened its own security.

August 28

New malware targeting users of a popular social network has been found. The malware not only steals everything stored in the victim's browser, but also blocks the victim's access to the browser settings to prevent them from removing the malware. An independent researcher has said that the malware appears as a link in an email or on the social network and tells users that they have been tagged in a post. When the user clicks on the link, they are directed to a Web page that asks them to download a plug-in in order to watch a video. However, this was found to be a malicious plug-in that allows an attacker to get access to everything stored on the victim's browser, such as online accounts with saved passwords. The malware can also block the user from accessing their browser settings to remove the threat and can block access to websites that offer antivirus software.

According to the researcher, the malware has been spreading at a rate of 40,000 attacks an hour and has already potentially affected more than 800,000 people using a well-known browser. The malware is spreading by hijacking victims' accounts and reaching out to people on their friends' lists. The social network said it was working to clear the malicious links from its website while the browser extensions involved have been disabled.

SOCIAL MEDIA

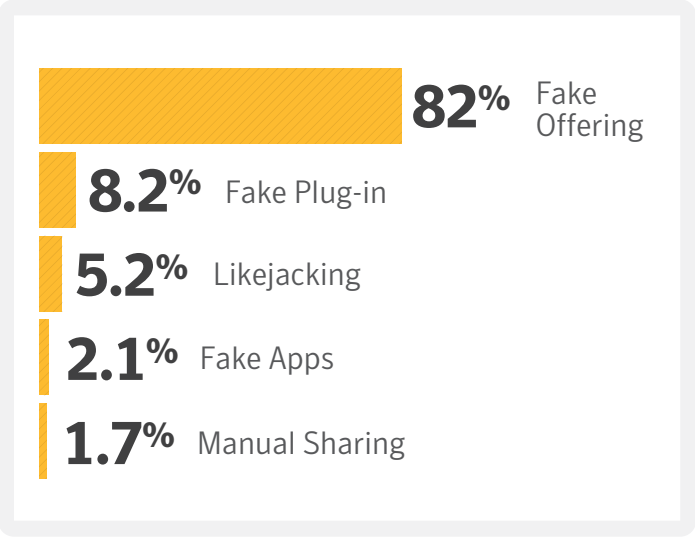
Social Media

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 8.2 percent, up from fifth place in 2012, at 5 percent.
- Fake Apps have risen overall in 2013, now making up 2.1 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

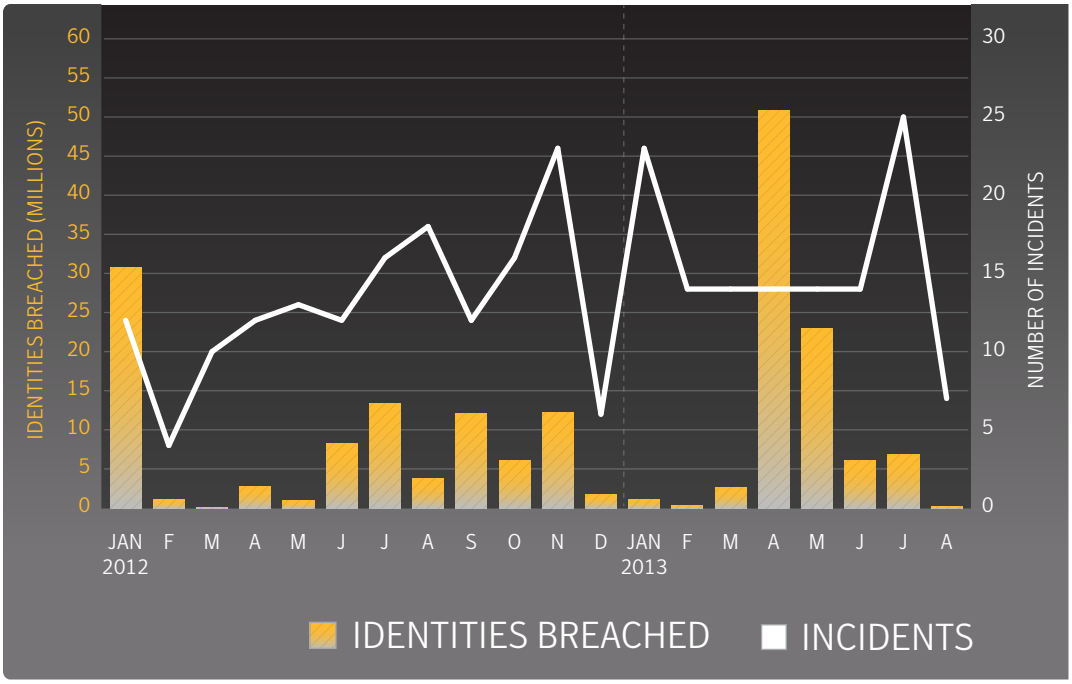
Data Breaches

At a Glance

- August appears to contain the least data breach activity this year, both in terms of the number of breaches and identities exposed. However, this number may change as further breaches are disclosed
- There were a number of breaches reported during August that occurred earlier in the year. This brings the total number of breaches to 125 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, birth date, and government ID number (e.g. Social Security).

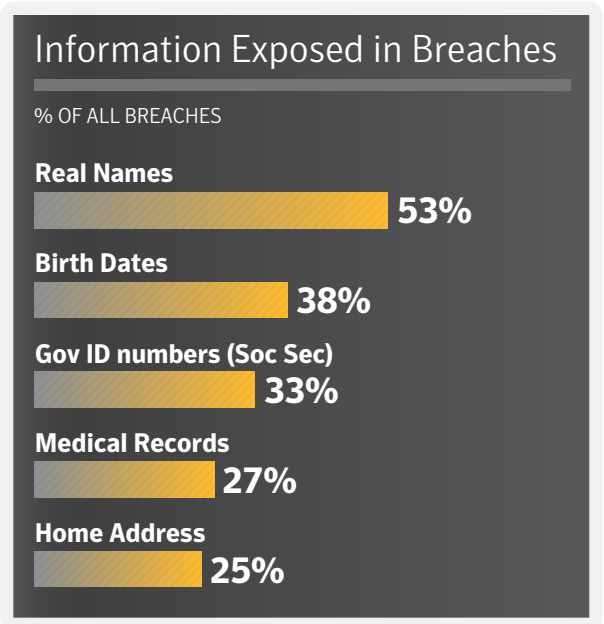
Timeline of Data Breaches, 2013

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, 40 percent of mobile malware tracks users, up from 15 percent in 2012.
- Traditional threats, such as back doors and downloaders are present in almost a quarter of all mobile malware threats.
- Risks that collect data, the most common risk in 2012, is down 15 percentage points to 17 percent of risks.
- Two new mobile malware families were discovered in August, along with 213 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

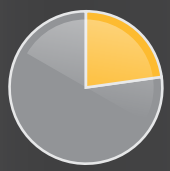
This includes the collection of both device- and user-specific data, such as device information, configuration data, or banking details.

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

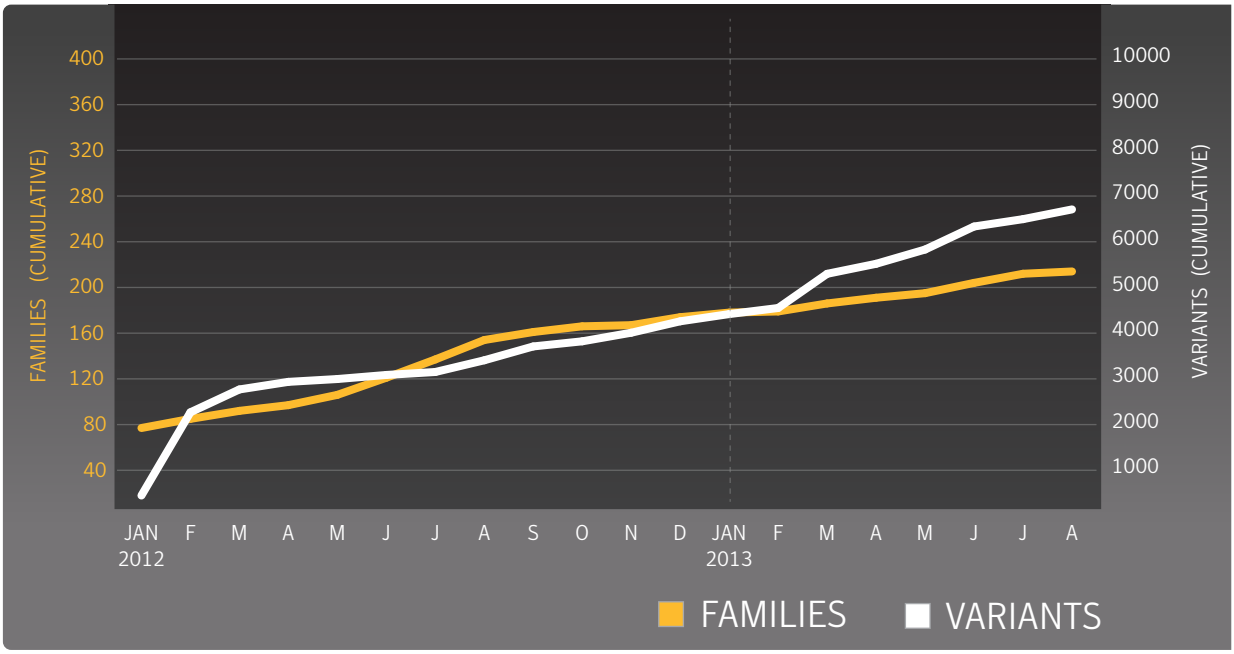
Mobile risks that display advertising or generally perform actions to disrupt the user.

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

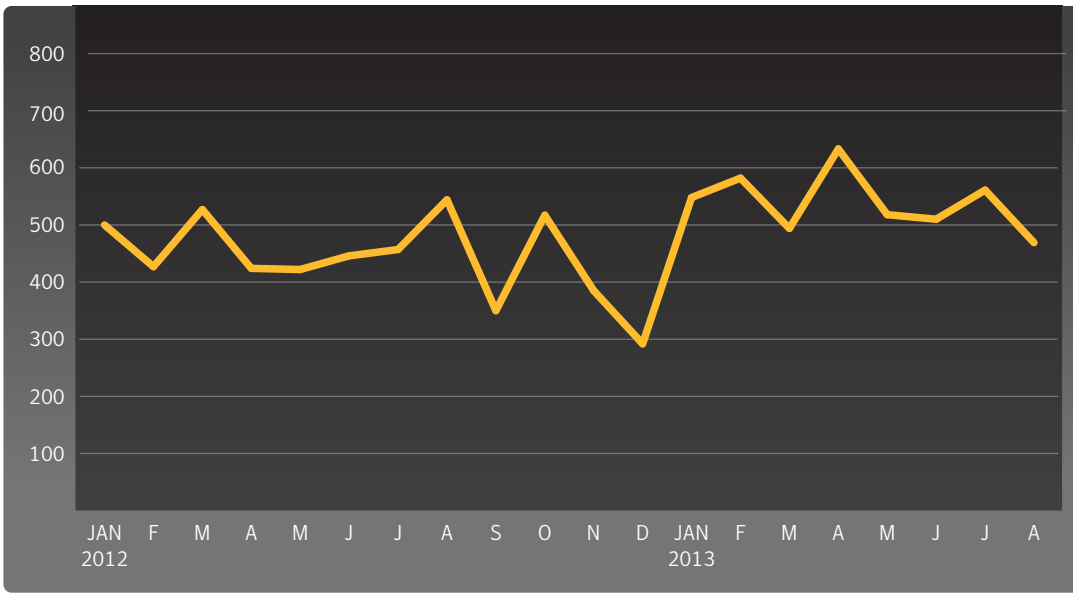
Vulnerabilities

At a Glance

- There were 469 new vulnerabilities discovered in August, bringing the total for the year up to 4315, a 13 percent increase compared to the same period in 2012.
- Two vulnerabilities were discovered in mobile operating systems during the month of August.
- Google's Chrome browser continues to lead in reporting browser vulnerabilities, while Oracle's Java leads in reported plug-in vulnerabilities.
- No zero-day vulnerabilities were disclosed during the month of August.

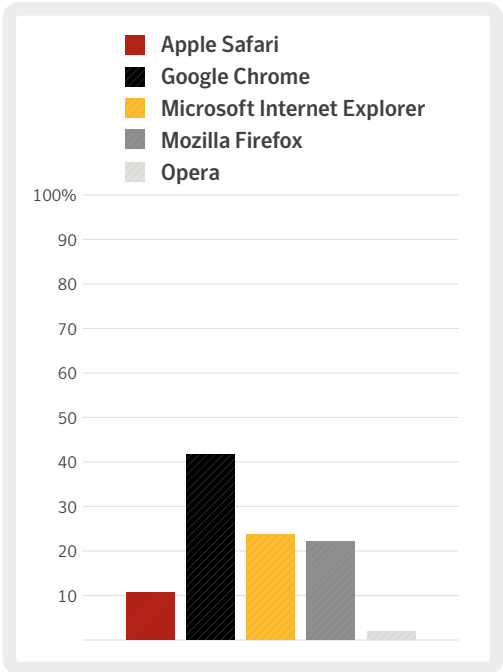
Total Vulnerabilities Disclosed by Month

Source: Symantec



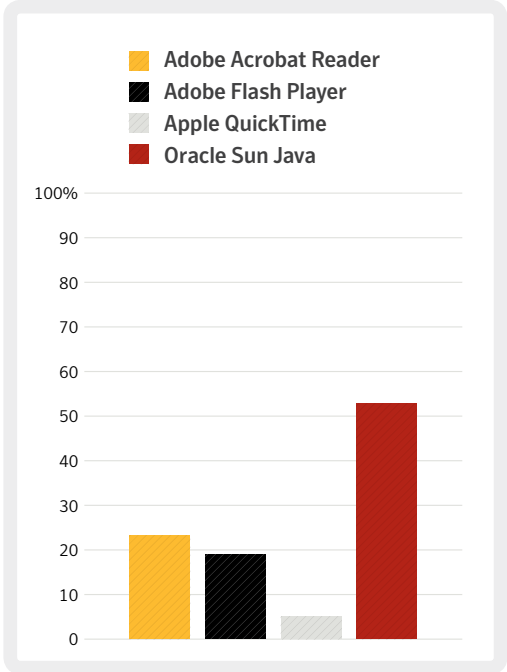
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

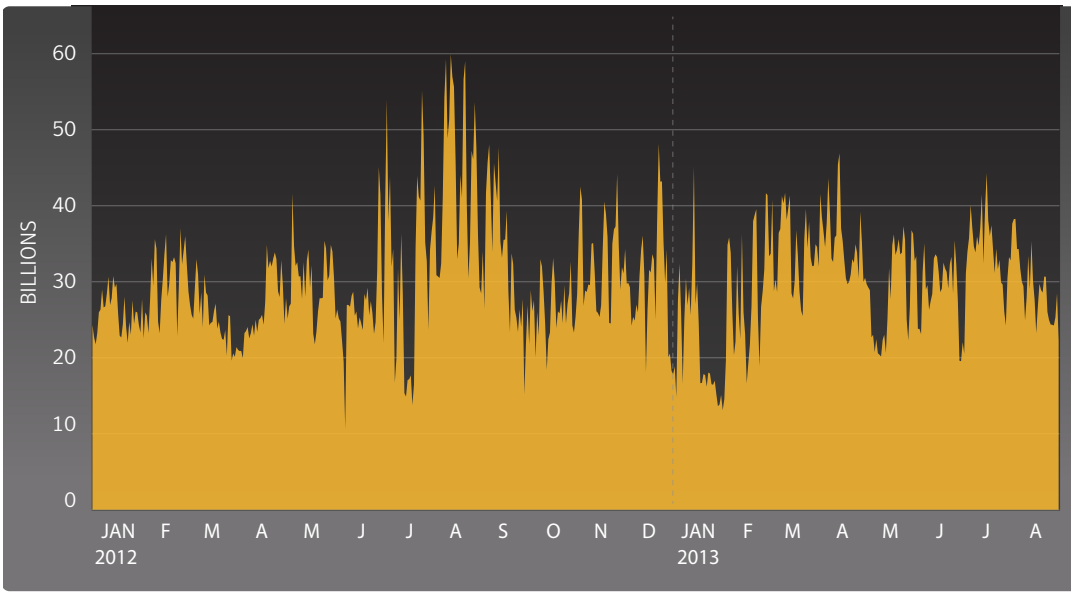
Spam

At a Glance

- The global spam rate dropped 2.4 percentage points in August to 65.2 percent, down from 67.6 percent in July.
- Education continues to be the most commonly targeted industry, as was the case in June and July.
- The top-level domain (TLD) for Poland, .pl, has topped the list of malicious TLDs for the second month in a row, comprising almost 48% of all spam-related domains in August.
- Sex/Dating spam continues to be the most common category, at 70.4 percent. Weight loss spam comes in second at 12.3 percent.

Global Spam Volume Per Day

Source: Symantec



Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Saudi Arabia	78.6%
Sri Lanka	76.1%
China	73.2%
Hungary	72.3%
Qatar	70.0%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	68.9%
Chem/Pharm	67.4%
Manufacturing	66.1%
Non-Profit	66.0%
Accom/Catering	65.6%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
India	6.98%
United States	6.66%
Spain	5.72%
Argentina	5.56%
Finland	5.44%
Italy	4.75%
Peru	4.46%
Brazil	4.25%
Iran	4.25%
Germany	3.48%

Average Spam Message Size*

Source: Symantec

*Month	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Jul	21.1%	28.2%	50.7%
Jun	22.2%	47.5%	30.3%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	64.6%
251-500	65.1%
501-1000	64.6%
1001-1500	65.7%
1501-2500	65.1%
2501+	65.5%

Spam by Category

Source: Symantec

Category	August
Sex/Dating	70.4%
Weight Loss	12.3%
Pharma	9.4%
Jobs	5.4%
Watches	1.7%

Spam URL Distribution Based on Top Level Domain Name*

Source: Symantec

*Month	.pl	.com	.ru	.net
Jul	47.8%	15.9%	14.3%	6.1%
Jun	58.9%	18.4%	n/a	8.7%

*Data lags one month

Phishing

At a Glance

- The global phishing rate is up in August, comprising one in every 625.6 email messages. In July this rate was one in 736.5.
- Financial themes continue to be the most frequent subject matter, with 66.8 percent of phishing scams containing this theme.
- Japan has seen an increase in phishing during the month of August, where one in 443 emails is a phishing scam.
- Not only that, but Japan tops the list of sources of phishing emails, responsible for distributing 55 percent of phishing scams.
- The Public Sector was the most targeted industry in August, with one in every 76.7 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	August
Japan	54.74%
Hong Kong	16.94%
United States	10.16%
United Kingdom	8.54%
South Africa	2.29%
Ireland	2.29%
Australia	1.84%
Sweden	0.63%
Denmark	0.51%
Singapore	0.40%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 609.1
251-500	1 in 799.8
501-1000	1 in 1,501.5
1001-1500	1 in 1,110.3
1501-2500	1 in 536.4
2501+	1 in 553.1

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 76.7
Education	1 in 384.0
Finance	1 in 467.5
Accom/Catering	1 in 508.8
Non-Profit	1 in 614.7

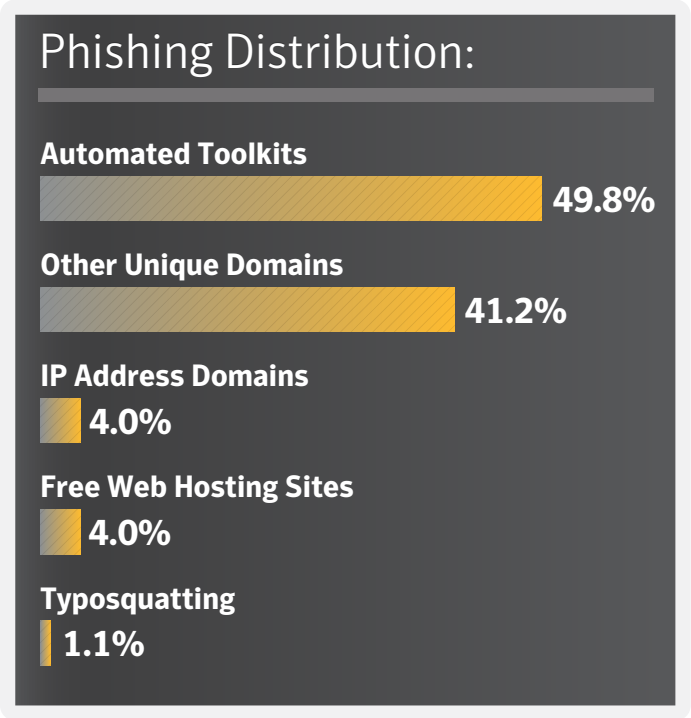
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
United Kingdom	1 in 246.1
South Africa	1 in 339.3
Japan	1 in 443.2
Australia	1 in 584.6
Italy	1 in 1,217.3

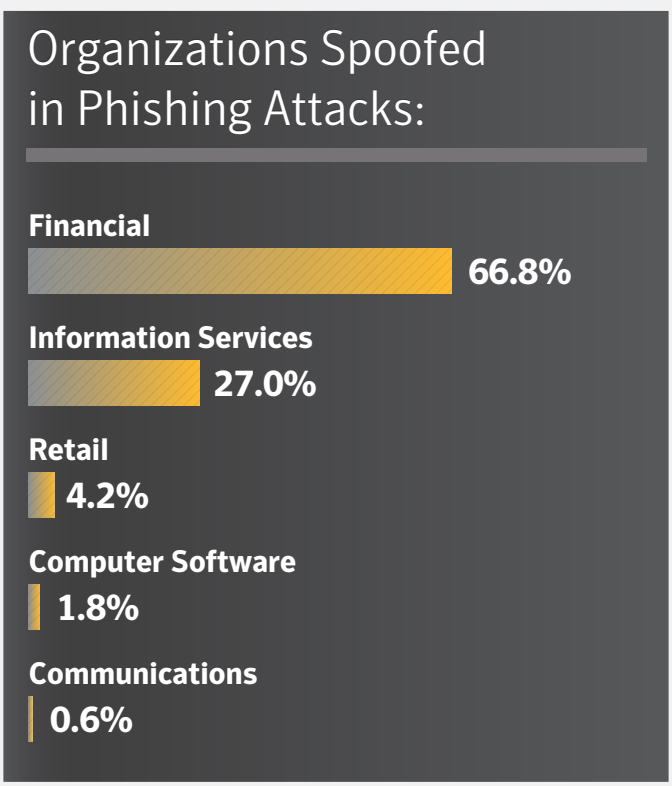
Phishing Distribution in August

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in August was one in 340.1 emails, compared to one in 465.1 in July.
- The United Kingdom topped the list of geographies, with one in 174.9 emails containing a virus, up from one in 258.4 during July.
- The United States was the largest source of virus-laden emails, making up 43.1 percent of all email-based viruses.
- Small-to-medium size businesses with 1-250 employees were the most targeted company size, where one and 311.6 emails contained a virus.

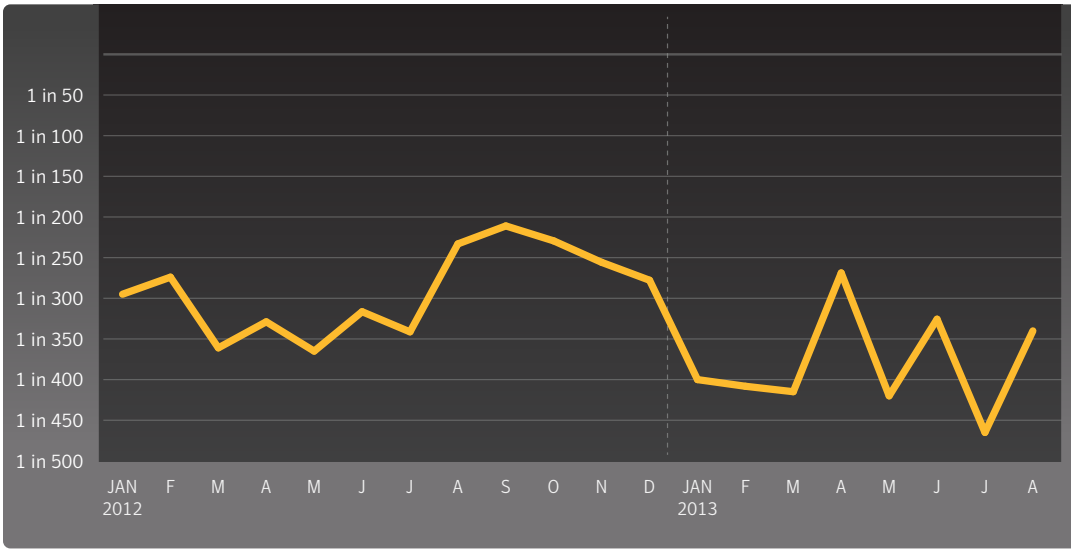
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United States	43.14%
United Kingdom	21.99%
Italy	5.44%
India	5.42%
Australia	5.27%
South Africa	3.38%
Ireland	2.72%
Hong Kong	1.67%
Netherlands	1.62%
Canada	1.11%

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 53.2
Education	1 in 258.9
Accom/Catering	1 in 265.7
Non-Profit	1 in 320.9
Marketing/Media	1 in 347.7

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
United Kingdom	1 in 174.9
United Arab Emirates	1 in 254.0
Australia	1 in 292.2
South Africa	1 in 314.5
Hungary	1 in 319.6

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 311.6
251-500	1 in 387.4
501-1000	1 in 511.3
1001-1500	1 in 408.2
1501-2500	1 in 327.9
2501+	1 in 323.8

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 16.4 percent of all malware blocked at the endpoint.
- In comparison, 7.9 percent of all malware were variants of W32.Sality.
- Approximately 39.4 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	August
W32.Sality.AE	7.13%
W32.Ramnit!html	6.40%
W32.Ramnit.B	5.72%
W32.Ramnit.B!inf	3.93%
W32.Almanahe.B!inf	3.63%
W32.Downadup.B	3.50%
W32.Virut.CF	2.54%
W32.SillyFDC.BDP!lnk	1.59%
Trojan.Maljava	1.56%
W32.SillyFDC	1.34%

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 47.4 percent of blocked Web activity in August.
- "Advertisement & Popups" was the second-most common trigger, comprising 22.4 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	47.43%
Advertisement & Popups	22.43%
Computing & Internet	2.72%
Streaming Media	2.59%
Peer-To-Peer	2.06%
Chat	1.98%
Hosting Sites	1.97%
News	0.79%
Games	0.75%
Entertainment	0.71%

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