Symantec

SYMANTEC INTELLIGENCE REPORT

JUNE ⌖ 2013

CONTENTS

Executive Summary

Welcome to the June edition of the Symantec Intelligence report. The 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 what has happened in a number of key sections of the threat landscape.

We delve deeper into the trends surrounding vulnerabilities, including zero-day, browser, and plug-in vulnerabilities. We also take a look at phishing trends over the last few months, as well as what has been happening in both the spam and malicious code areas of the threat landscape. Finally we include the latest high-level stats surrounding data breaches in June.

We've also provided a run-down on the biggest security stories for the month of June, 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

Apr	1 in 497
May	1 in 562
Jun	1 in 464

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

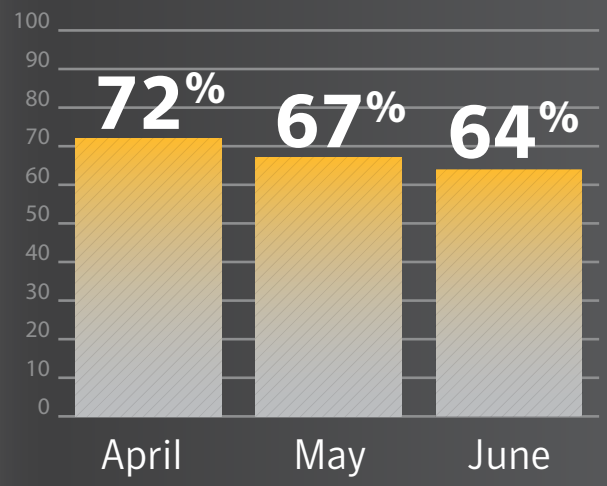
Apr	1 in 269
May	1 in 420
Jun	1 in 326

Mobile Vulnerabilities

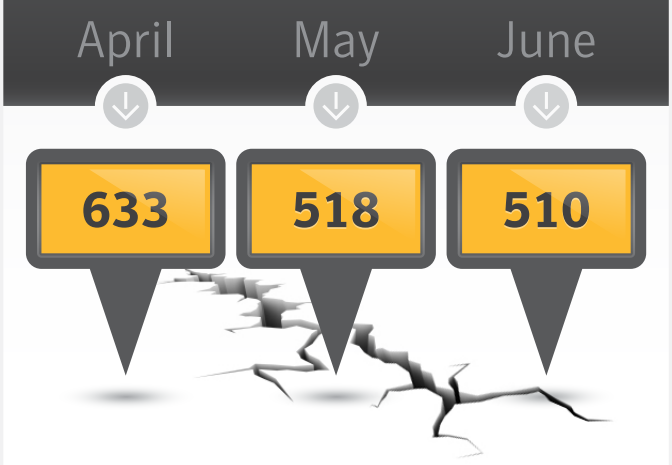
April	0
May	0
June	4

Estimated Global Email Spam Rate Per Day

SPAM AS PERCENT OF ALL EMAIL



New Vulnerabilities



Data Breaches

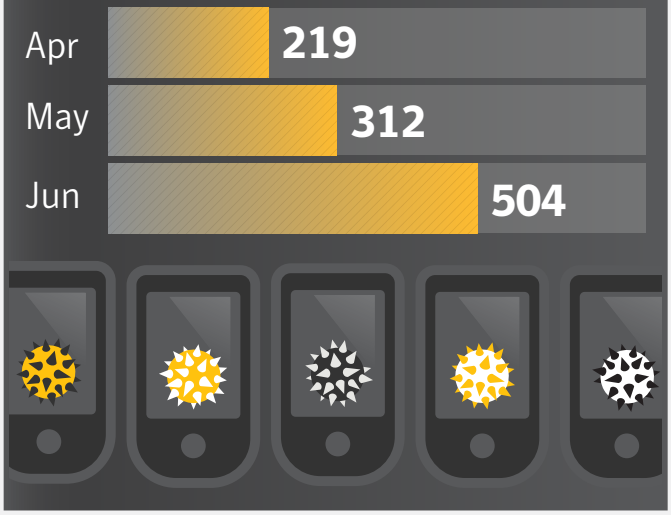
Number of Breaches (Year-to-Date)

85

Number of Identities Exposed (Year-to-Date)

84,068,805

Mobile Malware Variants



TIMELINE

June Security Timeline

June 04

The most advanced Android Trojan seen to-date emerged in early June. Android.Obad, or Obad for short, has capabilities that include opening a back door, downloading files, stealing information, sending SMS messages to premium numbers, and spreading malware using Bluetooth. Obad's sophistication lies in its use of code obfuscation and string encryption, making analysis difficult. Its discovery seems to not only suggest that the numbers of mobile threats are increasing, but also their level of complexity.

June 05

Symantec and the Ponemon Institute released the 2013 Cost of Data Breach Study: Global Analysis at the beginning of this month. The study revealed that the average global cost of a data breach in 2012 was US$136 per record. The study also found that sectors with strong regulation, such as pharmaceutical, financial, and healthcare industries encountered heavier costs than other sectors.

The report analyses the data breach experiences of 277 organizations across nine countries. It shows that while the global cost per compromised customer record had risen from the previous year, the total cost per data breach incident in the United States had declined. The authors credited this drop to the introduction of incident response policies, the strengthening of security programs, and the appointment of chief information security officers (CISOs) in many enterprises. The fact that two-thirds of data breaches examined in the report involved human errors and systems problems indicates that such measures can ultimately help companies control and reduce incidents of data breaches and their associated costs.

June 06

1,462 compromised computers used to spread the Citadel malware, a financial Trojan, were taken offline in early June.

Citadel is a variant of the Zeus botnet (Trojan.Zbot) and monitors a user's Internet activities to gain login credentials for online banking services. Its botnets have reportedly stolen US$500 million from bank accounts in the last 18 months. In existence since 2011, and typically sold for around $3000 in strict and secretive underground forums, Citadel is a full crimeware kit, providing the attackers with payload builders, a command-and-control (C&C) server infrastructure, and configuration scripts to target various banks.

The joint private/public take down operation was a concerted global effort involving the digital crimes unit of a well-known software corporation and law enforcement agencies across a host of countries.

While the take down has not completely destroyed Citadel, it does represent a significant disruption to the work of underground attackers designing and using the Citadel botnet.

June 06

A well-known professional networking website joined the procession of organizations adopting two-factor authentication (2FA). 2013 could already be described as the year of 2FA with several high-profile social media and information technology companies introducing the feature to help safeguard users' data. When accessing the site from an unrecognized device, the site's users will now have to log in using their password and a verification code sent to them via text message.

Companies are by and large hoping that 2FA will help to prevent embarrassing and costly data breaches. However, the introduction of two-factor authentication should not allow for any security complacency. For example, two threats that can overcome 2FA (detected by Symantec as SymbOS.Zeusmitmo and Android.Zeusmitmo) for mobile devices were discovered a few years ago. These threats are used by criminals in tandem with the desktop Zeus Trojan (Trojan.Zbot) to intercept incoming SMS messages from banking websites.

June 13

A new initiative that aims to curb incidents of smartphone theft has emerged in the US. The Secure Our Smartphones initiative endorses the introduction of a "kill switch" in each smartphone, which would render devices unusable if stolen. The multi-state initiative is led by state attorneys from New York and San Francisco and has already engaged with four smartphone manufacturers, the market leaders in production, in the hope of pushing technological innovation towards combating ever-rising smartphone crime. In San Francisco, 50 percent of robberies in

June Security Timeline

2012 involved a phone and in New York, 20 percent involved the theft of a smartphone. These stats alone seem to suggest that such an initiative and solution is widely needed.

June 20

June 20 marked the latest campaign from Anonymous, Operation Petrol or #OpPetrol. The hacktivist collective followed on from recent and somewhat similar operations such as #OpUSA and #OpIsrael.

Anonymous stated that they would mainly target oil and gas companies in the UK, US, Canada, Israel, China, Italy, France, Russia and Germany along with government departments involved in oil and gas in Saudi Arabia, Kuwait and Qatar.

There were at least two data leaks posted online, reportedly from large multinational oil companies, as well as a list of websites that have been hacked where attackers replaced the homepage with a message from Anonymous.

June 22

A bug within a tool of a popular social network system has exposed the personal data of 6 million users. The discrepancy occurred when a user downloads a copy of his or her data. This user may receive the phone number and email addresses of a person who they are connected to, but do not have the appropriate permissions to receive such information.

In related news, Symantec's new Norton Mobile Insight technology helped discover another privacy leak a few days later. It flagged the social network's Android app after discovering the problem. When a user launched the app, before they even logging in, their phone number was sent to the network's servers without their knowledge. A significant portion of the seven million Android app users may have been affected by this. Symantec duly informed of the social network of the leak, and a fix for the issue is to be included in their next Android release.

June 25

The Korean peninsula observed a series of cyberattacks coinciding with the 63rd anniversary of the start of the Korean War. While multiple attacks were conducted by multiple perpetrators, Symantec observed that one of the distributed denial-of-service (DDoS) attacks against South Korean government websites can be directly linked to the DarkSeoul gang and Trojan.Castov.

Symantec has found that the DarkSeoul gang is responsible for high-profile attacks against South Korean targets over the past four years. The group was behind the Jokra attacks seen in March of this year, which wiped hard drives in South Korean banks and media broadcasters and it also undertook the May attacks on South Korean financial firms.

DarkSeoul's campaigns follow similar methods of operation. They focus on high-profile South Korean targets on historically significant dates. The attacks usually involve hard disk wiping or DDoS attacks and they often use legitimate third party patching tools to spread across corporate networks.

As a result of Symantec's investigations into the group, a new threat was found which can delete files from infected computers. Detected as Trojan.Korhigh, this disk wiper can delete images, installers, videos, drivers, and libraries. It can gather system information about the compromised computer and can also overwrite the Master Boot Record (MBR) which can make the computer unusable.

VULNERABILITIES

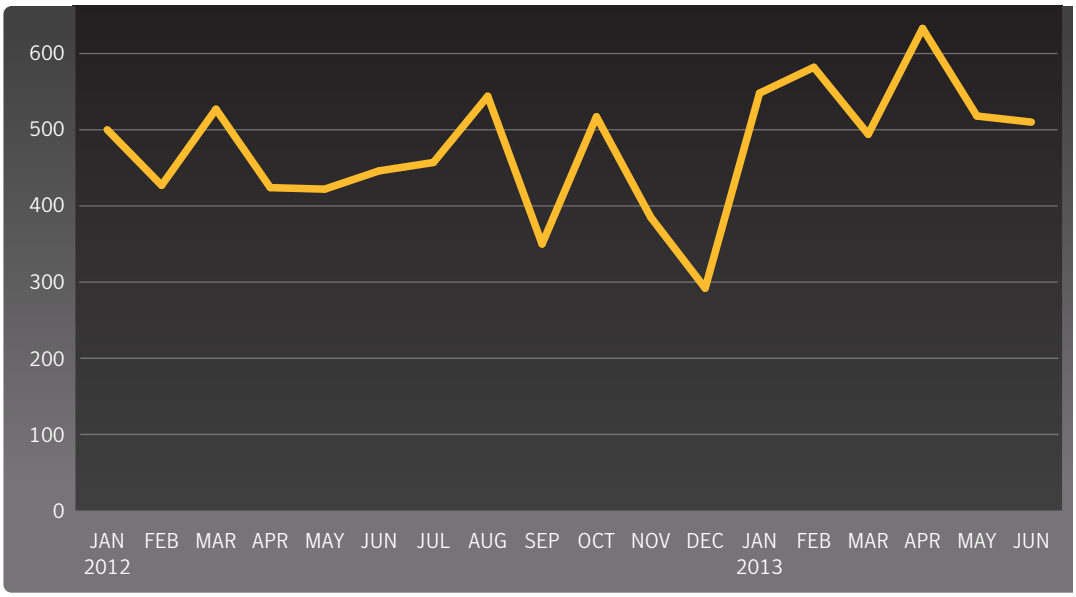
Vulnerabilities

At a Glance

- The total number of vulnerabilities in 2013 is up 16 percent so far when compared to what we saw in the same time period in 2012.
- The number of zero day vulnerabilities discovered for first half of 2013 has already reached a total of 12 so far. In comparison, there were only 14 found for the whole of 2012.
- In June 2013, there were 510 reported vulnerabilities and 3,285 in total for 2013 to-date, compared with 5,291 vulnerabilities in total reported in 2012.
- The average number of vulnerabilities reported each month in 2013 so far is up, at 300 and 600 per month, compared with 300 to 500 in 2012.
- Google's Chrome browser continues to lead in terms of reporting browser vulnerabilities, comprising 39 percent so far this year.
- Oracle's Java browser plug-in leads with the most number of reported plug-in vulnerabilities, making up almost half so far for the year-to-date.
- Four mobile vulnerabilities were reported in June, after two consecutive months with no disclosures, for a total of 37 in 2013 so far.

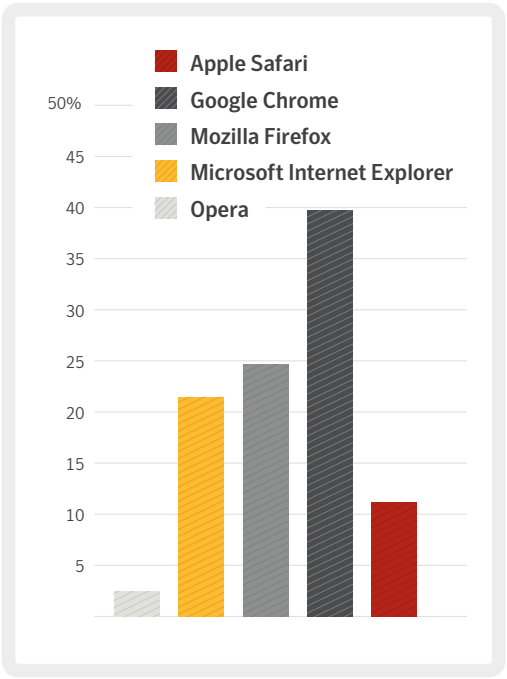
Total Vulnerabilities Disclosed by Month

Source: Symantec



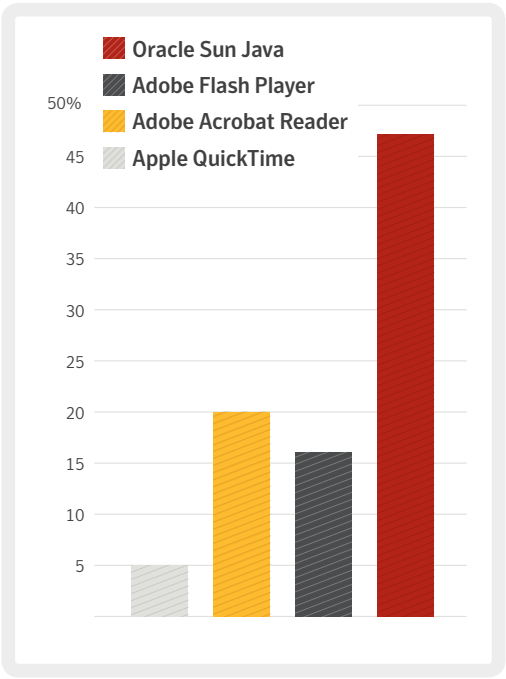
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

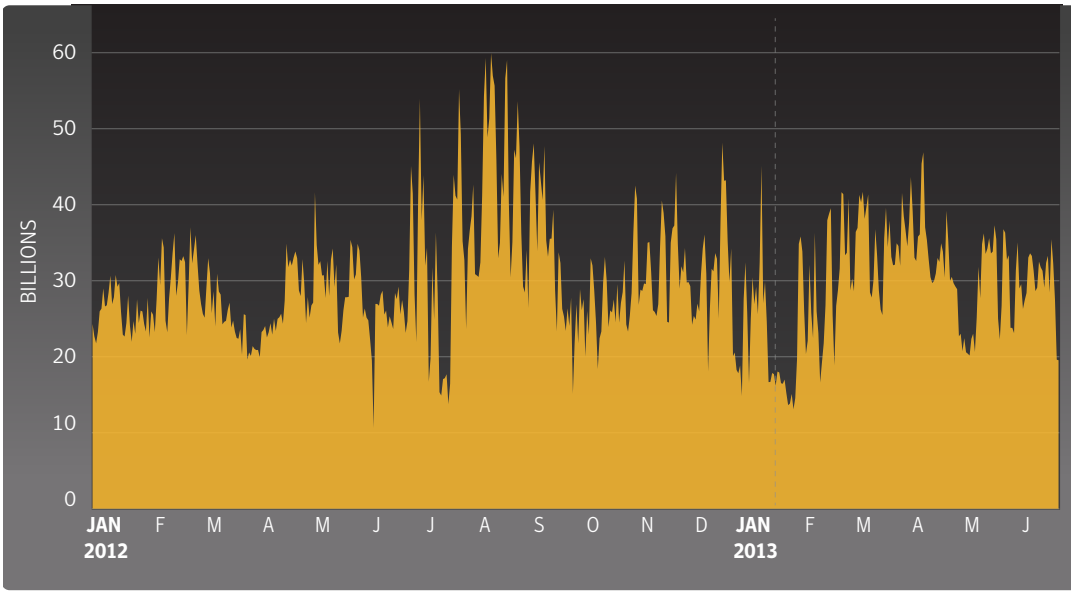
Spam

At a Glance

- The spam rate dropped to 64 percent in June, down from 67 percent in May, and 72 percent in April.
- There have been approximately 30 billion spam emails in circulation worldwide each day in 2013 to-date, which is in line with the average in 2012.
- Education was subject to the greatest frequency of spam in June at 68 percent,
- Saudi Arabia was the geography with the highest spam rate in June, at 81 percent.

Global Spam Volume Per Day

Source: Symantec



Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Saudi Arabia	81.2%
Sri Lanka	74.7%
China	71.4%
Hungary	69.3%
Peru	69.1%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Education	68.1%
Non-Profit	65.2%
Chem/Pharm	65.0%
Manufacturing	64.8%
Accom/Catering	64.6%

At a Glance

- The United States topped the list of sources of spam, followed by Finland and Spain. Interestingly, Belarus and Kazakhstan, both of which featured prominently in the last few months, have dropped off the top ten list since last month.
- The .pw top-level domain (TLD) continues to feature among to the most commonly used TLDs for spam. The TLD for Poland, .pl, has also entered the list, coming in third for June.
- Sex/dating spam continues to dominate the list of top spam categories, with 60 percent in June. However, this is down from May, where it reached 79 percent.
- The percent of spam based on company size in June was around 64 percent in all categories, with small-to-medium sized buisnesses having the lowest percentage, and organizations with 1501-2500 people the highest.

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
United States	8.26%
Finland	6.38%
Spain	6.36%
Brazil	5.89%
India	5.51%
Argentina	5.23%
Italy	4.69%
Canada	3.95%
Mexico	2.94%
Colombia	2.93%

Average Spam Message Size*

Source: Symantec

Month	0Kb – 5Kb	5Kb – 10Kb	>10Kb
May	33.8%	40.1%	26.1%
April	41.8%	31.1%	27.1%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	63.8%
251-500	64.2%
501-1000	64.0%
1001-1500	64.1%
1501-2500	64.5%
2501+	64.4%

Spam by Category

Source: Symantec

Category	June	May
Sex/dating	60.2%	78.7%
Pharma	20.6%	11.1%
Jobs	13.9%	2.5%
Watches	2.3%	4.7%
Software	1.4%	0.8%

Spam URL Distribution Based on Top Level Domain Name*

Source: Symantec

Month	.ru	.com	.pl	.pw
May	39.7%	22.0%	8.7%	5.3%
April	29.9%	30.8%	N/A	11.7%

*Data lags one month

Phishing

At a Glance

- The global average phishing rate in June was 1 in 464, compared with 1 in 562 in May, and 1 in 414 in 2012.
- The highest ratio of phishing attacks in June was identified in emails sent to small-to-medium-sized organizations (1-250), with 1 in 325 emails blocked as a phishing scam, compared with 1 in 293 for 2012.
- The Public Sector was subject to the greatest frequency of phishing attacks in June, with 1 in 142 emails blocked as phishing, compared with 1 in 95 for 2012.
- Australia was the geography with the highest phishing rate in June, with 1 in 174 emails blocked as phishing. In 2012 Australia was the thirteenth most frequently targeted geography.
- In June, the U.S. was the largest source of phishing attacks blocked, with approximately 48 percent of all scams blocked.

Top 10 Sources of Phishing

Source: Symantec

Source	June	May
United States	47.87%	49.63%
Germany	6.70%	6.99%
United Kingdom	5.15%	4.81%
Canada	3.26%	3.13%
Russia	3.00%	2.28%
Brazil	2.93%	3.06%
China	2.92%	1.99%
France	2.85%	2.69%
Netherlands	2.14%	2.02%
Poland	1.60%	1.61%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	1 in 325.6
251-500	1 in 499.4
501-1000	1 in 827.5
1001-1500	1 in 354.7
1501-2500	1 in 946.4
2501+	1 in 475.8

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Percent
Public Sector	1 in 142.8
Education	1 in 215.8
Finance	1 in 238.2
Marketing/Media	1 in 254.5
Non-Profit	1 in 274.9

Top 5 Activity for Phishing Destination by Geography

Source: Symantec

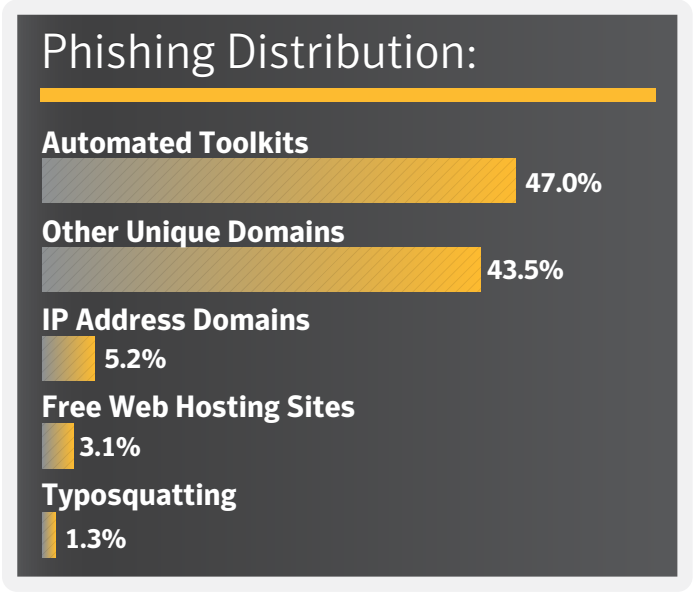
Geography	Percent
Australia	1 in 173.7
United Kingdom	1 in 245.6
South Africa	1 in 433.4
Italy	1 in 488.7
Belgium	1 in 529.4

At a Glance

- Automated phishing toolkits accounted for approximately 47 percent of phishing attacks, compared with 54 percent in 2012.
- In June, phishing attacks classified as utilizing 'other unique domains' accounted for 47 percent of phishing scams, compared with 39 percent in 2012.
- Phishing attacks spoofing financial organizations, including banks, accounted for 69 percent of phishing scams in June. This includes a variety of information and personal details that can be used for identity fraud, and theft of financial details can be quickly turned into large amounts of money, rather than goods which must be laundered first and require more time to process.

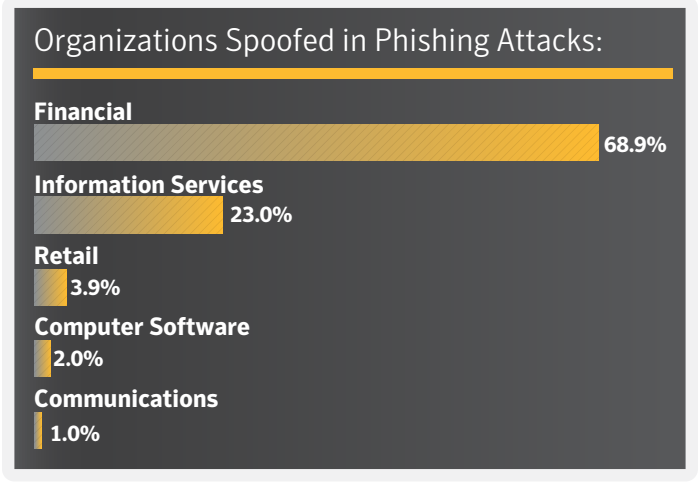
Phishing Distribution in June

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in June was 1 in 326, compared with 1 in 420 in May, and 1 in 269 for April.
- The highest ratio of email-based malware in June was identified in emails sent to organizations with 1001-1500 people, with 1 in 233 emails blocked, compared with 1 in 295 for 2012.
- The Public Sector was subject to the greatest frequency of email-based malware attacks in June, with 1 in 98 emails blocked, compared with 1 in 72 for 2012.
- Australia was the geography with the highest virus rate in June, with 1 in 173 emails blocked. In 2012 Australia the thirteenth most frequently targeted geographies.
- Australia was also the largest source of virus-based malware blocked, with approximately 34% of all malicious emails blocked.

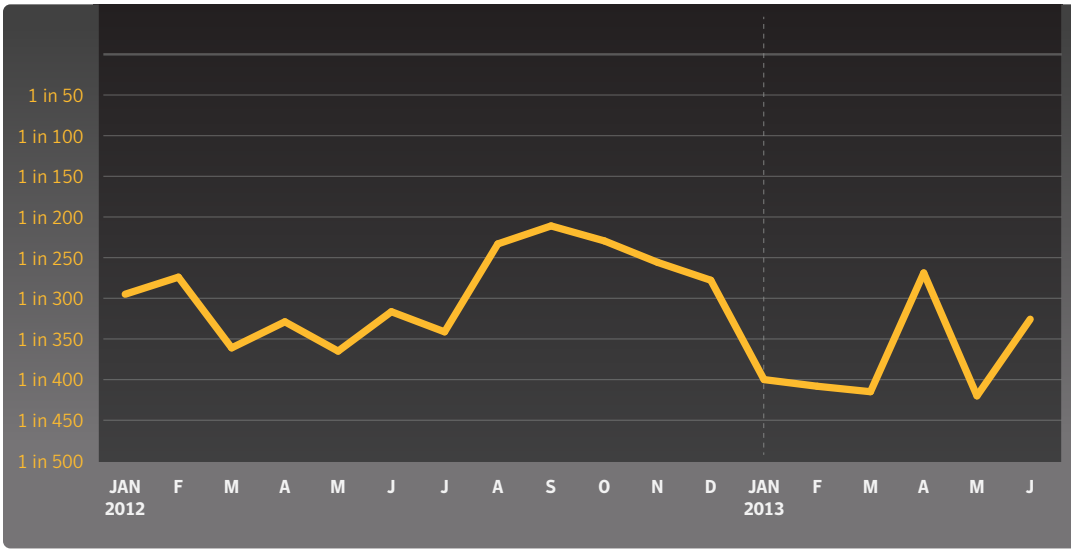
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
Australia	34.45%
United States	32.29%
United Kingdom	16.93%
South Africa	2.41%
India	2.38%
Norway	1.59%
Netherlands	1.55%
Germany	1.17%
Hong Kong	0.81%
Canada	0.81%

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 98.1
Education	1 in 172.7
Marketing/Media	1 in 199.2
Non-Profit	1 in 226.3
Telecoms	1 in 236.9

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
Australia	1 in 172.5
Germany	1 in 198.4
United Kingdom	1 in 214.9
Ireland	1 in 267.0
Switzerland	1 in 280.0

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 306.0
251-500	1 in 318.7
501-1000	1 in 337.3
1001-1500	1 in 233.4
1501-2500	1 in 500.1
2501+	1 in 327.8

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for approximately 18 percent of all malware blocked at the endpoint.
- In comparison, eight percent for all malware were variants of W32.Sality.
- Approximately 38 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	June	May
W32.Sality.AE	7.24%	6.91%
W32.Ramnit!html	6.76%	6.98%
W32.Ramnit.B	6.22%	5.86%
W32.Ramnit.B!inf	4.27%	4.32%
W32.Downadup.B	3.45%	3.79%
W32.Almanahe.B!inf	3.00%	2.87%
W32.Virut.CF	2.26%	2.25%
Trojan.Zbot	1.58%	1.22%
Trojan.StartPage	1.35%	no data
W32.SillyFDC	1.30%	no data

Web-based malware

At a Glance

- In June, Symantec Intelligence identified an average of 2,835 websites each day harboring malware and other potentially unwanted programs including spyware and adware.
- 31 percent of all malicious domains blocked were new in June, a decrease of 15 percentage points compared with May.
- Eleven percent of all Web-based malware blocked was new in June, an increase of 0.5 percentage points since May.
- The number of new spyware and adware websites blocked each day on average during June was 1,237, compared with 1,597 Web-based malware websites blocked each day.

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 "Advertisements & Popups" category, which accounted for 28.4 percent of blocked Web activity in July.
- "Social Networking" was the second-most common trigger, comprising 21.7 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Advertisement & Popups	28.4%
Social Networking	21.7%
Search	12.2%
Computing & Internet	4.9%
Peer-To-Peer	4.1%
Streaming Media	4.0%
Chat	3.9%
Hosting Sites	2.3%
Games	2.1%
Entertainment	1.7%

DATA BREACHES

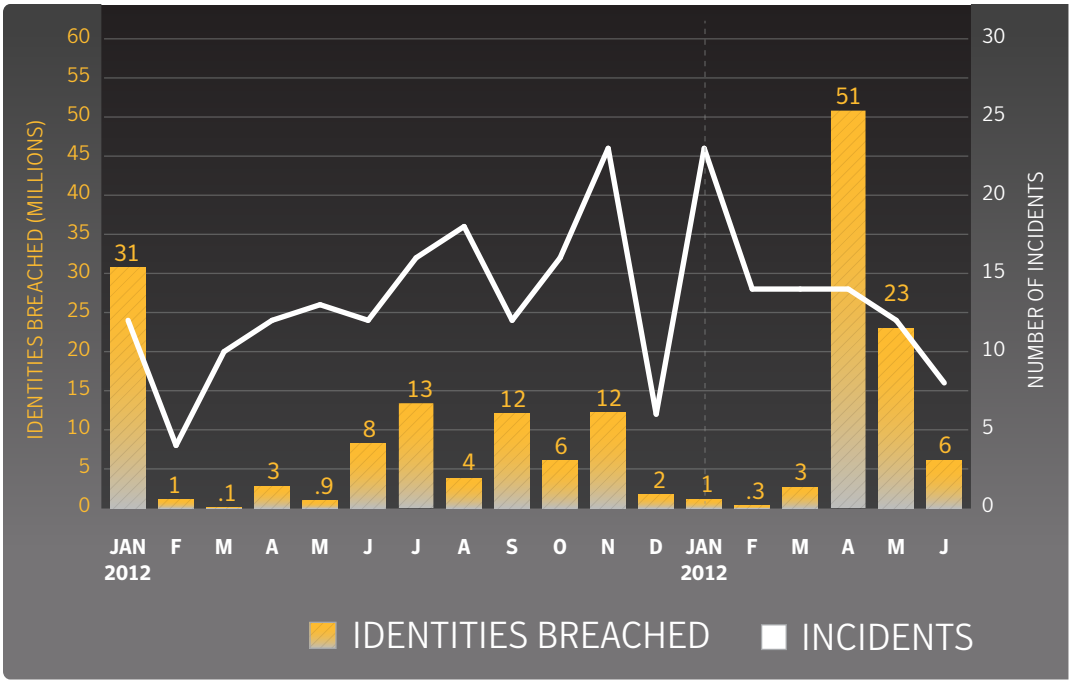
Data Breaches

At a Glance

- The number of identities breached is down this month, at six million for June, and 84 million so far for the year.
- The number of breaches reported so far this month is also down slightly, with 85 incidences reported so far this year.
- Healthcare continues to be the industry responsible for the most number of reported data breaches.
- The retail sector is responsible for the highest overall number of identities exposed.

Timeline of Data Breaches, Jan 2012 – May 2013

Source: Symantec



Top Industries for Data Breaches in June

Source: Symantec

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