Symantec

SYMANTEC INTELLIGENCE REPORT

MAY ⌖ 2013

CONTENTS

Executive Summary

Welcome to the May Symantec Intelligence report. This report includes many of the statistics that we have published on a monthly basis over the last few years, along with updates to material previously published in the annual Internet Security Threat Report. In it we will look at the threat landscape, digging deeper into the trends that appear over time.

In this month's report we take a look at what has happened in a number of key sections of the threat landscape since we published the Internet Security Threat Report XVIII. We delve deeper into the world of data breaches, mobile threats, spam, and malware, detailing what has happened so far in 2013 and bringing us up to speed through the month of May.

First we take a look at what is going on in the world of data breaches. Symantec and the Ponemon Institute have just completed their eighth annual Cost of a Data Breach study, based on actual data breach experiences of 277 companies around the globe. In it we discovered that the cost of a data breach for a compromised organization rose in 2012, to an average of $136 per identity lost. Looking ahead to 2013, and the data we compile monthly using the Norton Cybercrime Index, we see that the number of data breaches are up so far this year as well, and that we've borne witness to the largest data breach in two years—with over 50 million records stolen in one go.

The mobile threat landscape continues to show steady growth this year, with 21 new families of malware discovered so far in 2013. The overall number of mobile vulnerabilities that have been published is down significantly when compared to the same time period in 2012. By this point last year there had been 230 vulnerabilities published, but so far this year there have only been 33. This could point to mobile operating system developers shoring up their OSes, though it's still possible we'll see more vulnerabilities later in the year.

The spam rate in May of this year has dropped slightly to 67 percent, after increasing to 71.9 percent through March and April of this year. We are also seeing an increase in the amount of spam from countries such as Belarus and Kazakhstan this year, as well as an increase in the amount of spam coming from .pw top-level domains since they were made available for purchase by the general public earlier this year.

Other than that, we take a look at malware, where approximately one in 420.2 emails contained malware, and 39.3 percent of all malware on the end point was blocked using generic detections.

We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

Ben Nahorney

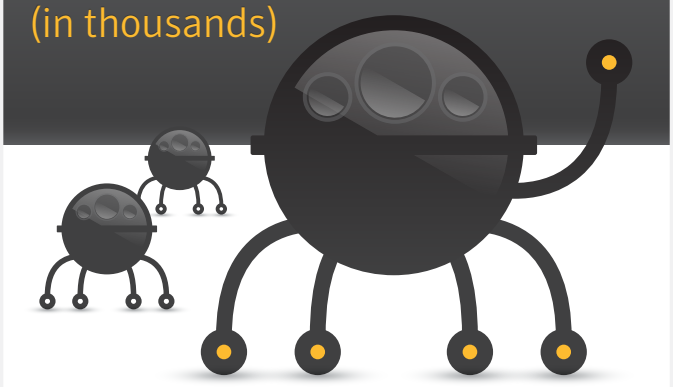
symantec_intelligence@symantec.com

BIG NUMBERS

Number of Identities Exposed in 2013 To-Date

77,996,740

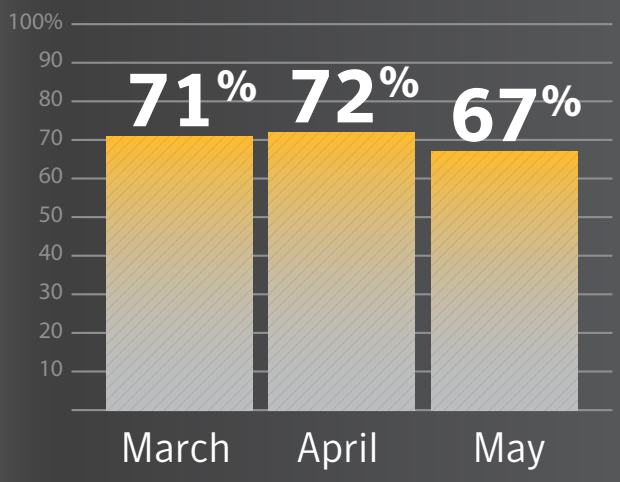
Bot Zombies
(in thousands)



March	347
April	221
May	162

Estimated Global Email Spam Rate Per Day

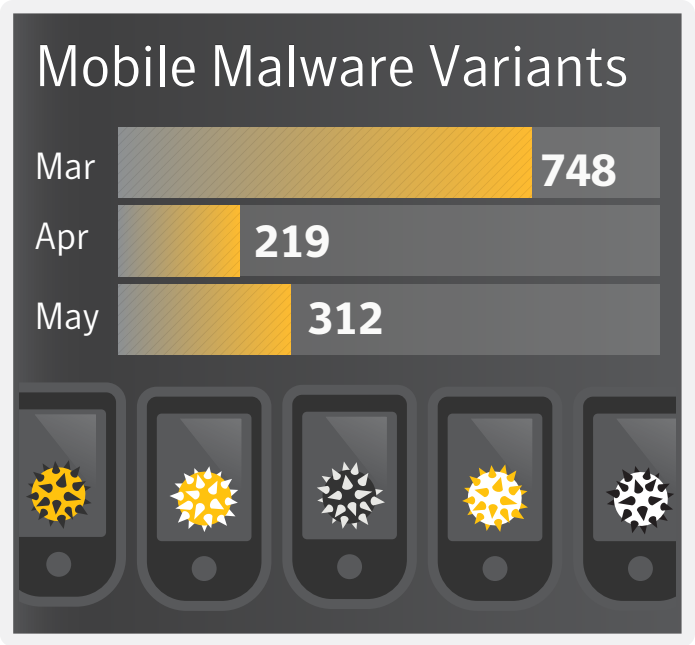
SPAM AS PERCENT OF ALL EMAIL

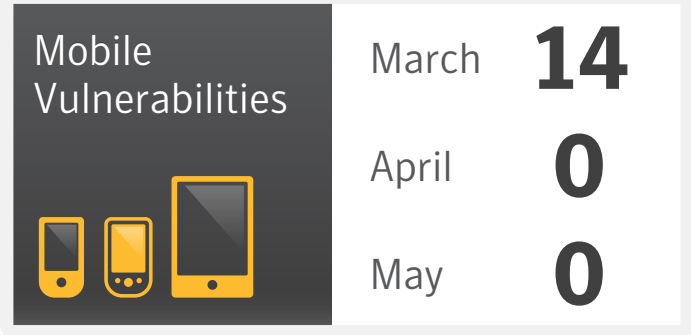


Overall Email Virus Rate, 1 In:

HIGHER NUMBER = LOWER RISK

Mar	415
Apr	469
May	420


Mobile Malware Variants
Mar
748
Apr
219
May
312


Mobile Vulnerabilities
March
14
April
0
May
0

TIMELINE

May Security Timeline

May 01

A US government website became the latest high-profile victim of a watering hole attack. A watering hole attack can be considered a form of targeted attack that involves compromising a legitimate website that a targeted victim might visit so as to install malware on their computer. The attack resulted in the site hosting malware that could infect visitors with the remote access Trojan, Poison Ivy. The malicious code redirected visitors to a site which hosted an exploit to take advantage of vulnerability within a browser. Ultimately, this meant that a victim's infected computer could be remotely monitored and data could be sent to command-and-control servers.

May 09

Seven men were arrested in New York in connection with their role in international cyber-attacks which resulted in the theft of $45 million across 26 different countries. The seven are accused of forming a New York based cell that used fake credit cards to steal $2.8 million from ATMs across the city. Withdrawal limits on accounts from two Middle East banks were removed when hackers gained unauthorized access, through high-end intrusion methods, to the computer networks of credit card processors. Taking control of debit cards, hackers were effectively able to pre-load enormous balances on to cards as well as eliminate any withdrawal limits. Global ground teams, including the New York cell, were then able to encrypt magnetic cards with the debit card data. This allowed the team to travel around the city and withdraw unlimited amounts of cash.

The seven accused face up to seven and a half years imprisonment on charges of conspiracy to commit access device fraud and ten years on money laundering charges.

May 12

A security warning was issued about the rise of a malicious browser extension which aims to take control of social networking accounts. The malware was first discovered in Brazil and targets popular browsers.

When the user installs this malicious browser extension, it updates itself with instructions from the malware's authors. It checks to see if the user is logged into a social network account and attempts to obtain a configuration file with a list of commands. It can undertake numerous commands from the user's profile, such as liking a page, sharing a link, posting, joining a group, inviting friends to join groups, chatting to friends and making comments.

Though the malware messages are written in Portuguese, it could be quite easily modified to target users with different languages. Ensure your devices have the latest security software to avoid inadvertently downloading the malware.

May 24

A highly respected media organization became the latest high profile hacking victim of the Syrian Electronic Army (SEA). The SEA has been targeting the websites and social media accounts of well-regarded news organizations to combat what they view as inaccuracies in the media coverage of the civil war in Syria. The activities of the pro-Assad group have contributed to the accelerated introduction of two-factor authentication for one social media platform. Last month, the SEA caused a drop in the Dow Jones following the release of an erroneous statement regarding the safety of the US President on a hacked social media account of a widely respected news organization.

May 28

A digital currency system based in Costa Rica was taken offline by US authorities after a multi-state investigation, while its founder was arrested in Spain on money laundering charges. Seen by US law enforcement agencies as a vehicle for criminals to process their ill-gotten gains, the digital currency is estimated to have processed $6 billion among its 1 million users worldwide. The attraction for criminals seems to have been in the relative ease and anonymity of opening and operating an account.

It is alleged that this ease and anonymity enabled criminals to launder profits by allowing them to add money in dollars or euro and transfer to other accounts, subject to small administrative fees. It is thought that this digital currency may have acted as the favored laundering method for those involved in the $45 million credit card hacking scam documented earlier. For now, underworld operators will look to use digital currencies for their laundering means.

DATA BREACHES

Data Breaches

At a Glance

- The number of breaches are up so far this year: 77 compared to 59 over the same time period last year.
- One 50 million identity breach in late April is the largest in two years.
- Hacking is no longer responsible for the most number of data breaches. Theft or loss made up for 36 percent of all data breaches.

Details

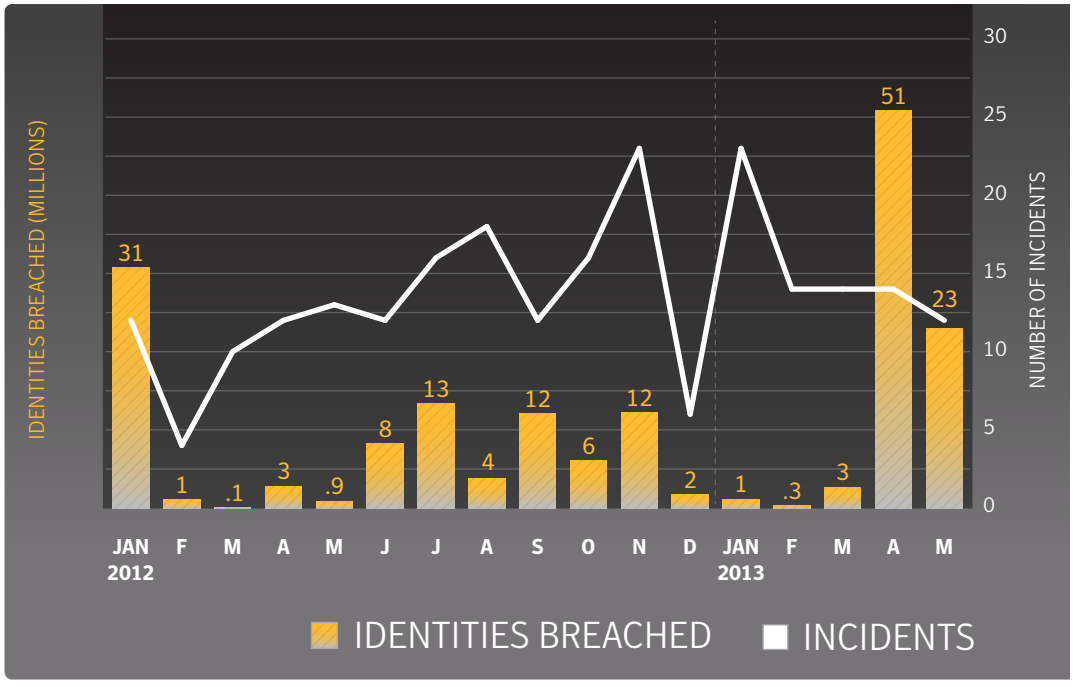
Hot off the presses, Symantec and the Ponemon Institute have released their joint 2013 Cost of Data Breach: Global Analysis study, providing a thorough and in-depth analysis of data breach trends for 2012. In it, we discovered that a data breach on average costs around $136 per record. The Healthcare industry also tops the list this year in terms of industries suffering the most costs due to data breaches.

We also keep track of data breaches on a monthly basis through the Norton Cybercrime Index[1]. So far in 2013 the number of data breaches are up, with 77 documented incidents, compared to 59 by the end of May last year. The number of identities stolen per breach is also up so far this year, with 1,164,130 identities for each breach on average. This can be partly attributed to two extremely large data breaches that took place in April and May, where hackers made off with 50 million identities in one hack—the largest data breach we've seen in two years—and 22 million in another. No doubt serious incidents, to put these hacks in perspective, there have been a total of around 78 million identities breached in total this year. This means these two hacks are responsible for 92 percent of the identities stolen in 2013.

While large hacks like this tend to skew averages, the median number of identities stolen tends to paint a clearer picture of what's happening in the threat landscape. In this case, the number is down significantly for the year, with a median of 3,500 identities per breach, compared to 8,350 in 2012 overall. This indicates that, while the occasional large data breach does occur, smaller and more frequent caches of data are getting exposed when breaches do occur.

Timeline of Data Breaches, Jan 2012 – May 2013

Source: Symantec

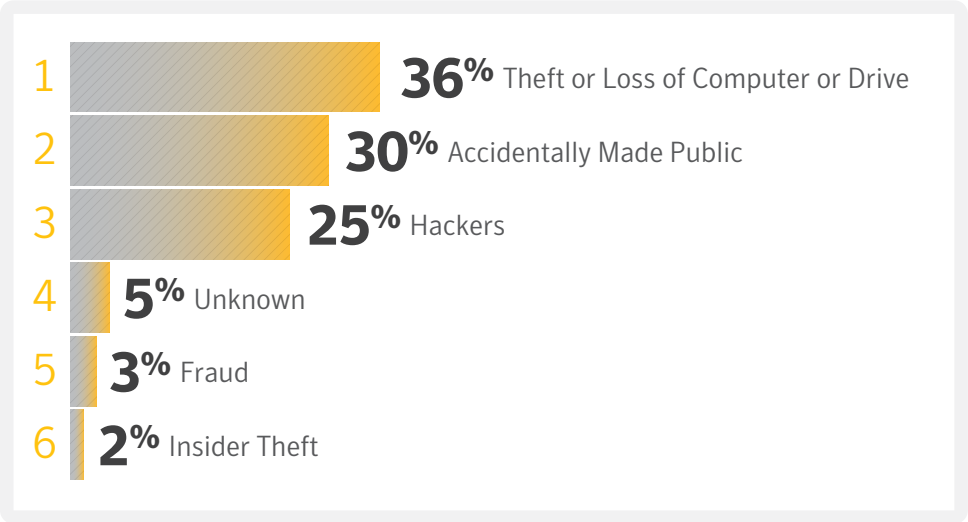


1 The Norton Cybercrime Index (CCI) is a statistical model that measures the levels of threats including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information. Using publicly available data the Norton CCI determines the sectors that were most often affected by data breaches, as well as the most common causes of data loss.

Naturally, since the very large data breaches were in the retail and information technology sectors, these industries make up the overwhelming majority of identities compromised. (It's worth noting that Retail lead in 2012 as well, but not by the margin it is so far in 2013 due to this 50-million-identity breach.) However, the healthcare industry continues to lead in terms of the number of breaches suffered. What's interesting to note so far this year is that hacking no longer leads the pack in terms of causes of data breaches, only making up 25 percent of all breaches. Instead, theft or loss of data tops the list at 36 percent and accidental disclosure of information comes in second at 30 percent.

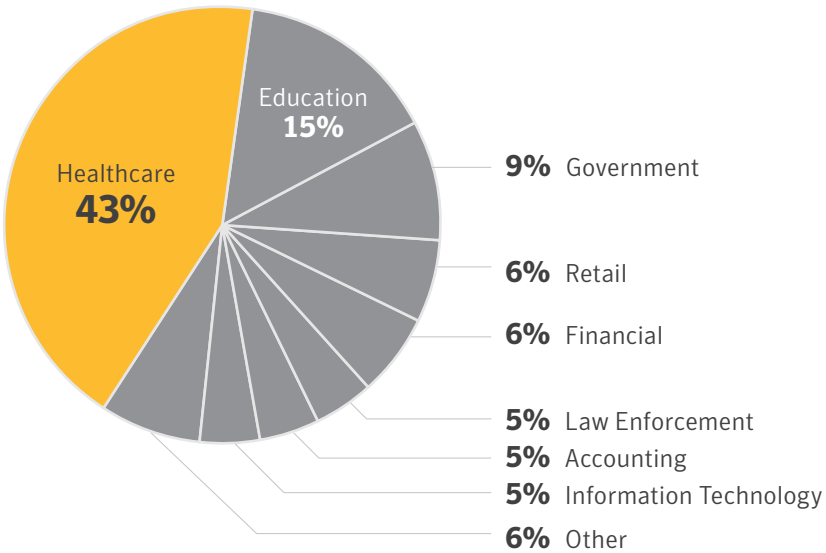
Top Causes of Data Breaches in 2013

Source: Symantec



Top Sectors by Number of Data Breaches

Source: Symantec



MOBILE

Mobile

At a Glance

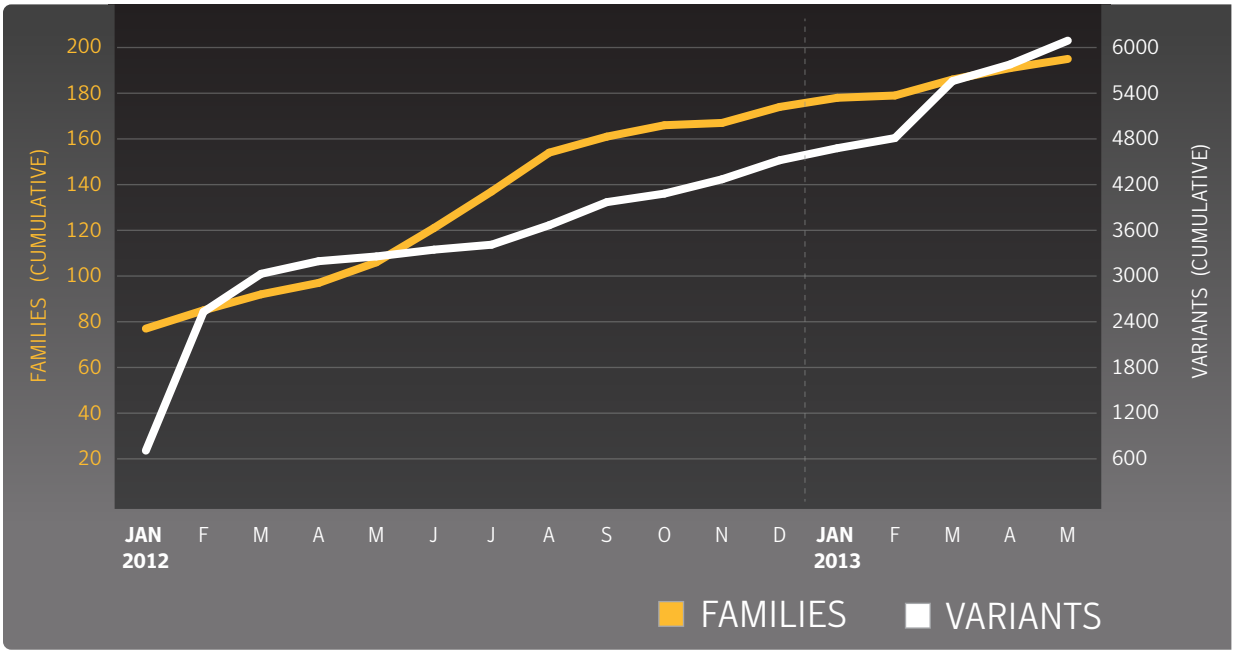
- Mobile malware continues to grow, with 21 new families and 1624 new variants so far this year.
- The slow growth of mobile vulnerabilities, which started near the end of 2012, continues into 2013, with only 33 vulnerabilities to-date this year.

Mobile malware continues to increase in 2013, with 21 new Android families introduced since the beginning of 2013. The variant rates within these families also continue to grow steadily, with 1624 new variants appearing so far this year. Clearly the Android operating system is the platform of choice for malicious developers, as threat activity on other mobile operating systems remains quiet so far, with no newly discovered threat families on other mobile operating systems.

In terms of published mobile vulnerabilities, activity has settled somewhat since the first half of 2012. So far this year, only 33 vulnerabilities have been published. In comparison, 230 vulnerabilities had been published by this point in 2012. In contrast to mobile malware, iOS continues to lead in this area, with 73 percent of the vulnerabilities published to Android's 27 percent. No other mobile operating systems have published vulnerabilities so far this year. As of late, the mobile vulnerability landscape appears to have gone quiet, with no new vulnerabilities published in April or May.

Cumulative Mobile Android Malware

Source: Symantec

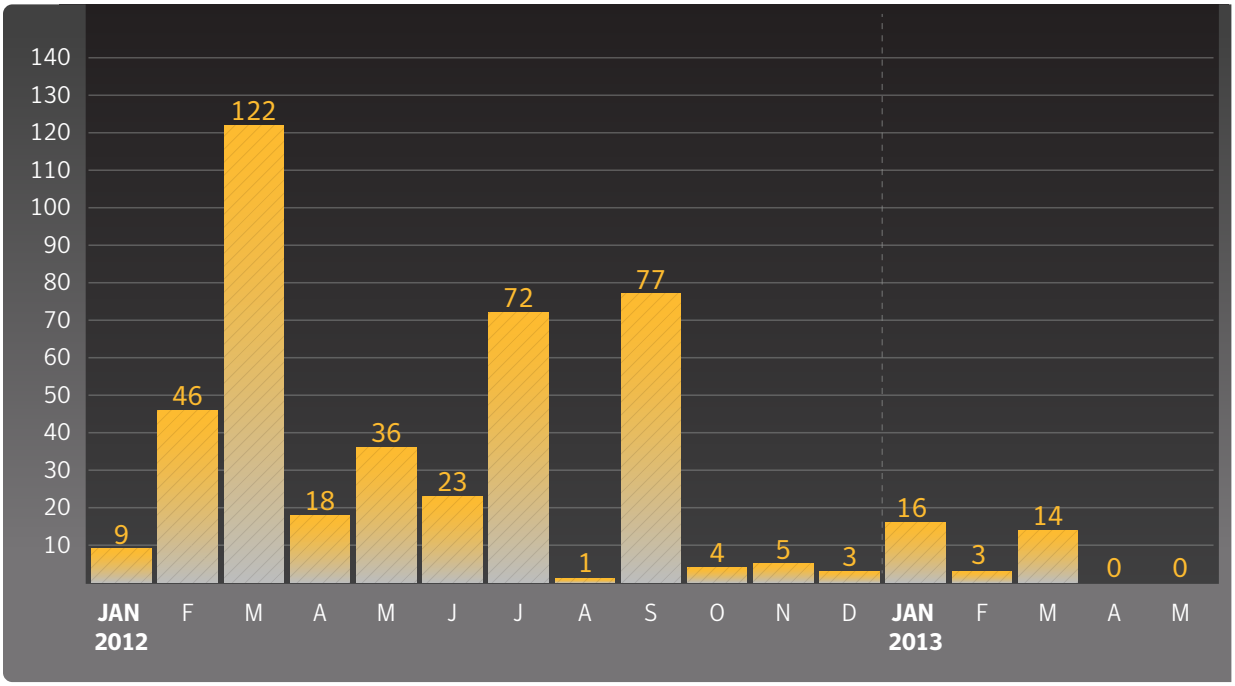


Why have vulnerabilities dropped off so far in 2013? It could be that mobile operating system developers are spending more time shoring up the security on their platforms instead of introducing new features. When looking at version releases over the last two years, fewer and fewer updates have been released. 2012 saw the release of iOS 5.1 and then iOS 6, along with three minor releases, while 2013 has only seen iOS 6.1 and four minor releases so far. In the case of Android, we saw eight operating system updates over three versions of the OS (Honeycomb, Ice Cream Sandwich, and Jelly Bean). In 2013, Android development has finally been consolidated under Jelly Bean, and only one update has been released this year.

Granted these numbers could change significantly in the latter half of 2013. With the scheduled release of iOS 7 later in the year, along with the possibility of Android's Key Lime Pie release, we could very well see further vulnerabilities disclosed and subsequently patched.

Mobile Vulnerabilities Publicly Disclosed

Source: Symantec



SPAM

Spam

At a Glance

- Spam rates have declined to 67 percent in the month of May, after reaching a peak of 71.9 percent in April.
- Belarus jumped to the top of spam-sending countries. Kazakhstan also rose to fourth.
- The .pw top-level domain has gained favor with spammers since being opened to the public.

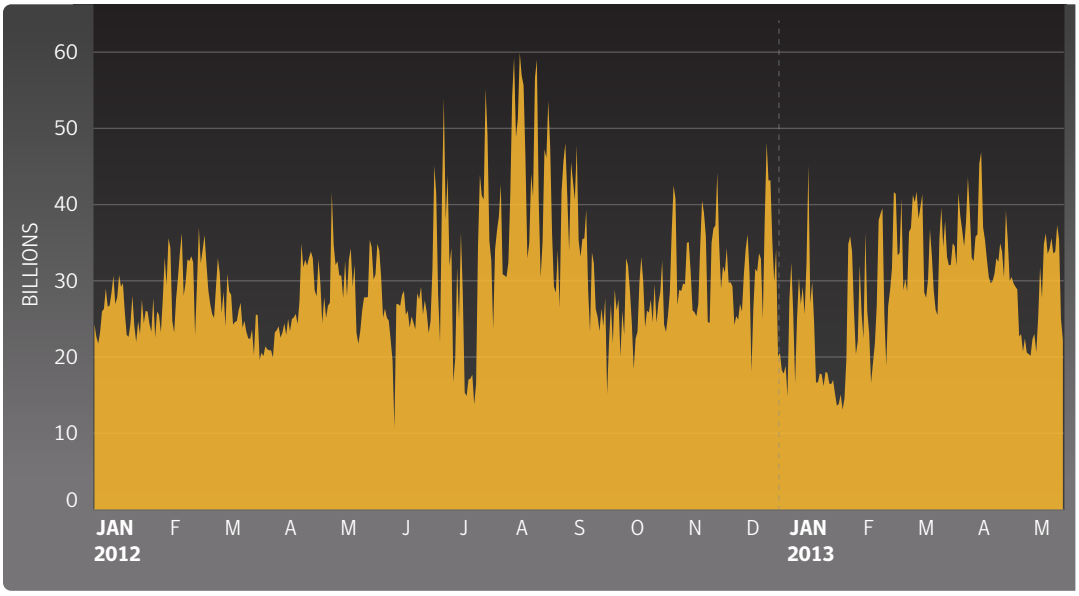
Details

In the last few months, we noticed an increase in the overall spam rate. While back in February the spam rate was 65.9 percent, it jumped 5.1 percentage points to 71.0 percent in March. This upward trend continued in April, where the spam rate continued to increase to 71.9 percent of all email messages. However it appears this spam run may have tapered off some, as the spam rate dropped back down to 67 percent for the month of May.

While a spam rate of almost 72 percent may seem high, this doesn't compare to last summer, when we saw the rate peak at 75 percent. Nor does it compare to the peaks reached in 2010 and 2011, where spam averaged out at 89 and 75 percent for the entire year, respectively.

Global Spam Volume Per Day

Source: Symantec



What's interesting in this latest spam push is the location where much of the spam was coming from. Back in March, we saw the country of Belarus jump to the top of our list of countries sending spam. Belarus suddenly made up 13.54 percent of all spam, having barely ranked among the top 20 spam countries previously. This continued to increase in the month of April, when 18.92 percent of all spam originated from the country, before dropping somewhat in May to 12.64 percent overall. Also notable is the increase in spam coming from Kazakhstan, which rose from a minor player to fourth place worldwide in March and April, before dropping to seventh place in May.

Another interesting recent change we've observed is the sudden appearance of the .pw top-level domain in the list of the top domains used in spam that exploits URLs. What's curious is that the .pw didn't appear in spam campaigns until April, and then suddenly made up 11.68 percent of all domains. The reason for this is likely tied to the fact that the top-level domain was only opened up to the public in March of this year, being a domain for the small Pacific Island country of Palau.

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
Belarus	12.64%
United States	7.85%
Ukraine	5.17%
Brazil	4.53%
Finland	4.04%
India	3.93%
Kazakhstan	3.92%
Spain	3.61%
Argentina	3.31%
Vietnam	3.06%

Average Spam Message Size*

Source: Symantec

Month	0Kb – 5Kb	5Kb – 10Kb	>10Kb
April	41.8%	31.1%	27.1%
March	49.6%	36.0%	14.5%

*Data lags one month

Spam by Category

Source: Symantec

Category	May	April
Sex/dating	78.7%	80.6%
Pharma	11.1%	11.9%
Watches	4.7%	4.4%
Jobs	2.5%	1.0%
Software	0.8%	0.6%

Spam URL Distribution Based on Top Level Domain Name*

Source: Symantec

Month	.com	.ru	.pw	.us
April	30.8%	29.9%	11.7%	5.7%
March	41.6%	26.0%	not listed	not listed

*Data lags one month

Top 5 Activity for Spam Destination by Geography

Source: Symantec

Country	Percent
Saudi Arabia	82.4%
Sri Lanka	74.9%
China	73.1%
Poland	71.1%
United States	70.9%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Finance	83.0%
Education	67.3%
Chem/Pharm	65.8%
Non-Profit	65.4%
Accom/Catering	65.2%

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	77.0%
251-500	64.6%
501-1000	64.4%
1001-1500	64.6%
1501-2500	65.8%
2501+	64.7%

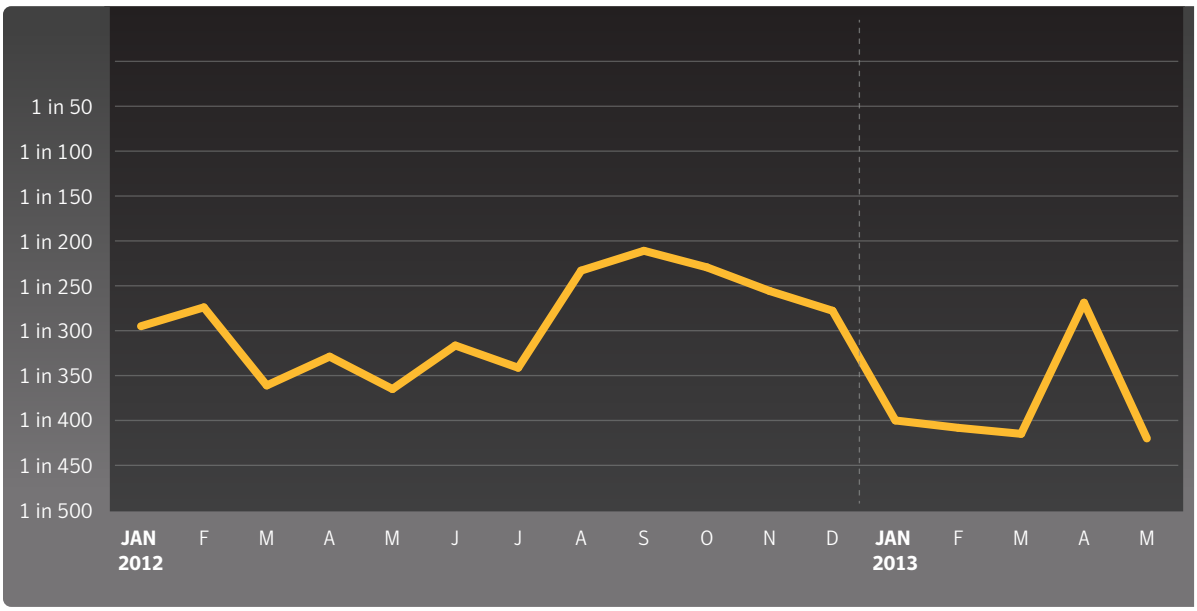
MALWARE

Malware

In May, one in 420.2 emails was malicious—or 0.238 percent of all email—a drop of 0.134 percentage points since April. Of the email considered malicious, 28.8 percent contained a link to a malicious website, a drop of 13.7 percent from the previous month.

Proportion of Email Traffic in Which Virus Was Detected

Source: Symantec



Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Country	Rate
South Africa	1 in 211.1
United Kingdom	1 in 232.9
Netherlands	1 in 246.8
Denmark	1 in 314.0
Ireland	1 in 318.4

In the UK, one in 232.9 emails was identified as malicious, compared with South Africa, where one in 211.1 emails was blocked as malicious. With one in 99.1 emails being blocked as malicious, the Public Sector remained the most targeted industry in May. Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 376.3 emails, compared with one in 397.4 for large enterprises (2500+). In terms of the sources of malicious files in email, 49.7 percent originated in the United States, while 19.6 percent came from computers located in the United Kingdom.

Top 5 Activity for Malware Destination by Industry

Source: Symantec

Industry	Rate
Public Sector	1 in 99.1
Estate Agents	1 in 148.0
Education	1 in 264.1
Accom/Catering	1 in 288.7
Marketing/Media	1 in 321.7

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 376.3
251-500	1 in 457.9
501-1000	1 in 560.2
1001-1500	1 in 456.4
1501-2500	1 in 563.1
2501+	1 in 397.4

Top 10 Email Virus Sources

Source: Symantec

Country	Percent
United States	49.70%
United Kingdom	19.60%
Australia	6.70%
South Africa	5.42%
Hong Kong	2.65%
Canada	2.61%
Netherlands	1.57%
Brazil	1.56%
Sweden	1.39%
France	1.20%

For much of 2013, variants of W32.Sality and W32.Ramnit had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 17.5 percent of all malware blocked at the endpoint, compared with 7.7 percent for all variants of W32.Sality.

Approximately 39.3 percent of the most frequently blocked malware last month was identified and blocked using generic detection. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

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 33.0 percent of blocked Web activity in July. Web-based advertisements pose a potential risk though the use of "malvertisements," or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless Web site.

Top 10 Most Frequently Blocked Malware

Source: Symantec

Malware	May	April
W32.Ramnit!html	6.98%	6.96%
W32.Sality.AE	6.91%	6.87%
W32.Ramnit.B	5.86%	5.61%
W32.Ramnit.B!inf	4.32%	4.34%
W32.Downadup.B	3.79%	3.54%
W32.Almanahe.B!inf	2.87%	2.50%
W32.Virut.CF	2.25%	2.17%
W32.SillyFDC.BDP!lnk	1.68%	1.42%
Trojan.Zbot	1.22%	no data
W32.Virut!html	1.13%	1.09%

Policy Based Filtering

Source: Symantec

Category	Percent
Advertisement & Popups	33.0%
Social Networking	26.9%
Computing & Internet	5.0%
Streaming Media	4.6%
Peer-To-Peer	3.7%
Search	3.3%
Chat	3.0%
Hosting Sites	2.3%
Unclassified	2.1%
Games	1.7%

Next Month

Vulnerabilities in 2013

Phishing trends

Web-based malware

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