Symantec Intelligence Report: August 2012

Data breaches; Fake antivirus warning appears to come from Symantec; New attacks from old groups

---

Welcome to the August edition of the Symantec Intelligence report, which provides the latest analysis of cyber security threats, trends, and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The data used to compile the analysis for this report includes data from May 2011 through August 2012.

Report highlights

- Spam – 72.3 percent (an increase of 4.7 percentage points since July): page 9
- Phishing – One in 312.9 emails identified as phishing (an increase of 0.109 percentage points since July): page 12
- Malware – One in 233.1 emails contained malware (a decrease of 0.14 percentage points since July): page 13
- Malicious Web sites – 1,099 websites blocked per day (a decrease of 49.8 percent since July): page 15
- The state of data breaches to date in 2012: page 2
- A look at a malicious email scam that pretends to come from Symantec: page 6
- A new Java zero-day vulnerability appears in the wild: page 7
- An overview of the Elderwood Project: page 8

Introduction

In this month's report we focus on data breaches—security incidents where user information becomes publically exposed or stolen. We compare what has happened in 2012 to a similar period in 2011, going back to the beginning of the Operation AntiSec campaign last year.

We also highlight an interesting attempt to install malicious software through an email spam campaign, appearing to come from Symantec. The spam emails attempt to tricking users into believing they have a worm on their computer and then downloading a tool that will remove it. If the file is downloaded and executed, an information-stealing Trojan is installed.

Finally, we discuss two new attacks coming from well-known attacker groups. First up is a new zero-day vulnerability in Java that is currently being used in the wild by the same folks that were behind last year's Nitro attacks. Then we provide an overview of the Eldderwood Project—a series of attacks carried out by the same folks that were behind the "Aurora" or Hydraq attacks.

I hope you enjoy reading this month's edition of the report, and please feel free to contact me directly with any comments or feedback.

Paul Wood, Cyber Security Intelligence Manager
paul_wood@symantec.com
@paulowoody

Report analysis

Data Breaches in 2012

In the spring of 2011, a hacking campaign began, dubbed Operation AntiSec[1]. Launched by the hacker collectives Anonymous and LULZSEC, the operation has carried out a long string of data breaches from a number of very prominent organizations, and continues to release data to this day.[2] While the existence of hacks exposing the private information of users stored by various organizations was not new, we had not previously seen the volume and fanfare around data breaches. It seemed that with each new day, a new breach made headlines—often times with the number of identities exposed in the hundreds of thousands, if not millions.

Data breaches are a serious issue for an organization. The exposure of customer data can lead to a loss of confidence in the organization by its users. Even worse, the organization could find themselves in violation of data privacy laws or on the receiving end of a lawsuit created by its users.

So while AntiSec data breaches are still making the news a year later, has the data breach climate improved overall? Are there more or less data breaches occurring? Are the numbers of data breaches rising or falling? We'll take a look at all of these points, and more.

In order to carry out our analysis of data breaches we took a look at the data collected by Symantec's Norton Cybercrime Index[3] (CCI). The Norton CCI is a statistical model which 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, including name, address, Social Security numbers, credit card numbers, or medical history. 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.

In order to make an accurate comparison, we examined data starting in late spring 2011 through the end of the year. We compared this data against a similar eight-month period from January through August of 2012. Comparing these 2011 and 2012 data sets helped identify data breach trends in 2012 to date.

Overall, the number of breaches during the same two periods is fairly consistent. The average number of breaches per month is down slightly, but not by statistically wide margin. The average number of breaches per month was 16.5 in our 2011 data set, while in 2012 this number dropped to 14.

The average number of identities stolen is down during the same period. In the last eight months of 2011 the average number of identities stolen was 1,311,629 per data breach. So far in 2012, this number is down to 640,169 identities per breach—that's a drop of more than half.

The reasons for this drastic drop in average number identities stolen point to the fact that, while the overall number of attacks where about the same, there number of records stolen in the biggest attacks in 2011 was much larger. The top five breaches in our 2011 data set all registered in the tens of millions of identities. In 2012, only one breach registered above 10 million.

It's tough to say exactly why there were fewer breaches of this size. It could indicate that after a few high-profile hacks in 2011, many large companies took steps to shelter their customer record databases from internet attacks. It could also be that hackers aren't going after the largest data breaches they can pull off, but rather smaller breaches that contain more sensitive information.

We may not see the sheer numbers of attacks per month like we did in our 2011 data set, but that doesn't mean that the threat has passed. Rather, it's possible data breaches today have simply become more targeted. While the numbers in 2012 are down compared to 2011—even hitting a low in February of this year—they do appear to be on an upward trajectory.

---

[1] *http://en.wikipedia.org/wiki/Operation_AntiSec*
[2] *http://news.cnet.com/8301-1009_3-57505925-83/fbi-finds-no-evidence-that-antisec-hacked-its-laptop*
[3] *http://us.norton.com/protect-yourself/promo*

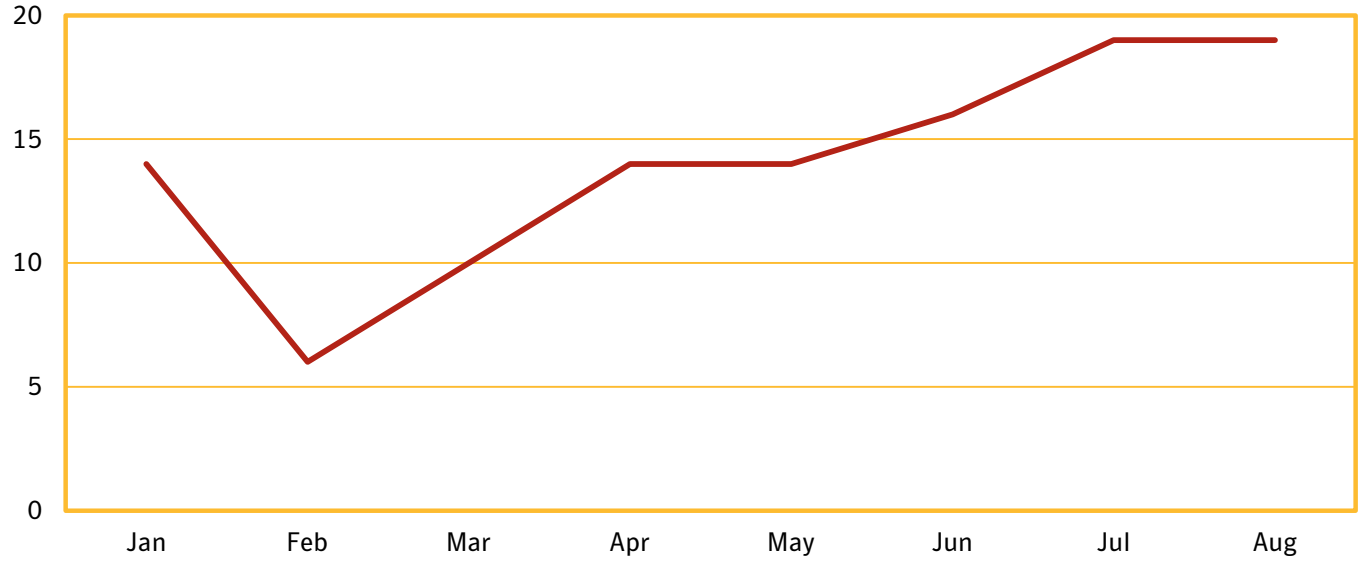


Figure 1 – Number of data breaches per month in 2012 to date

The biggest issue we encounter when looking at data breach numbers is the wild variance in the number of records from one breach to the next. In one instance there can be over a million identities stolen; in another there could be less than 10 identities stolen. This sort of variance makes the overall number of stolen identities harder to qualify and determine overall trends.

A few high-volume breaches in the 2011 data brought the average up overall. With this in mind, another way to look at this information would be by the median number of identities per breach. The median of identities stolen in 2012 is 6,800 per breach. That's 41% higher than the previous eight months, at 4,000 per breach. Looking at the numbers this way, it appears that the number of identities stolen in each breach is up.

This shows that while the overall average number of identities stolen is down, the core number of identities stolen, when accounting for variance, is increasing over time. This could indicate that the attackers are going after more select, targeted batches of data, as opposed to making off with big-number caches of data. The information that they are stealing could very well be smaller in size, but more useful for criminal activities.

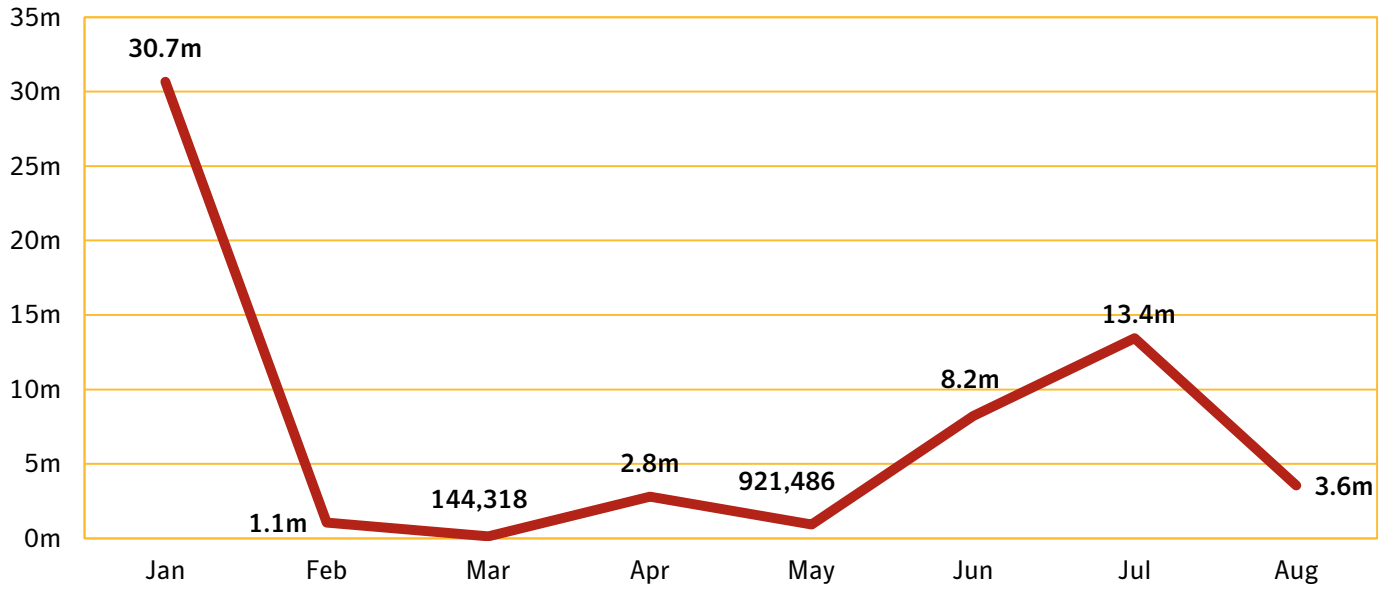


Figure 2 – Number of identities breached per month in 2012 to date

Symantec™

We know that not all data breaches are the result of cybercrime. Sometimes a laptop containing sensitive data is stolen simply to resell the hardware. Other times hardware is simply lost, never making its way back to the owner. In some cases website coding mistakes accidentally expose private data to the public.

Are private identities exposed during data breaches generally the result of hackers deliberately stealing data? As it turns out, the answer is overwhelmingly ”yes.” A whopping 88% of all identities stolen in data breaches during 2012 have been the result of hackers. The same was true for our 2011 data set, though the number for has grown—up 14% from 74% in May through December of 2011.

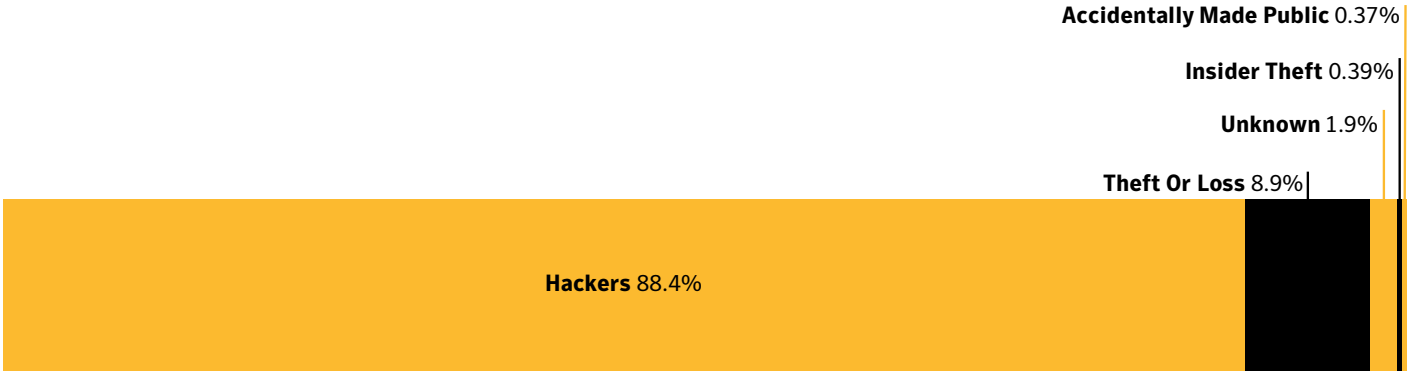


Figure 3 – Top causes for data breach by number of identities exposed in 2012 to date

However, while this shows who is responsible for the most identities exposed overall from data breaches, it can be skewed by individual breaches that are larger in size. Let’s look at the same data, but based on the number of breaches instead.

Hackers are still responsible for the highest number of data breaches at 40%, but other methods resulted in a majority of breaches overall. In fact, roughly 1 out of every 5 breaches was caused by the accidental exposure of data. The same can be said for theft or loss of hardware. So, while hackers are responsible for the largest number of data breaches and identities stolen, there are other factors that result in a large number of data breaches overall.

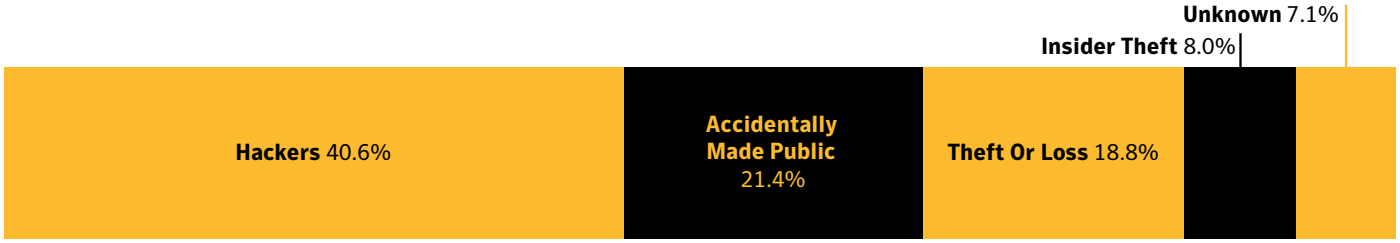


Figure 4 – Top causes for data breach by number of breaches in 2012 to date

We also examined which industries had the most data breaches. We divided the overall number of identities breached within an industry by the total number of breaches in that industry.

So which industries are responsible for the most data breaches? In our 2011 data set, information technology and computer software were top of the list, making up about 80% of total breaches. It seems these industries have done much to improve their standing, having been surpassed by the retail trade and telecoms in numbers of identities stolen.

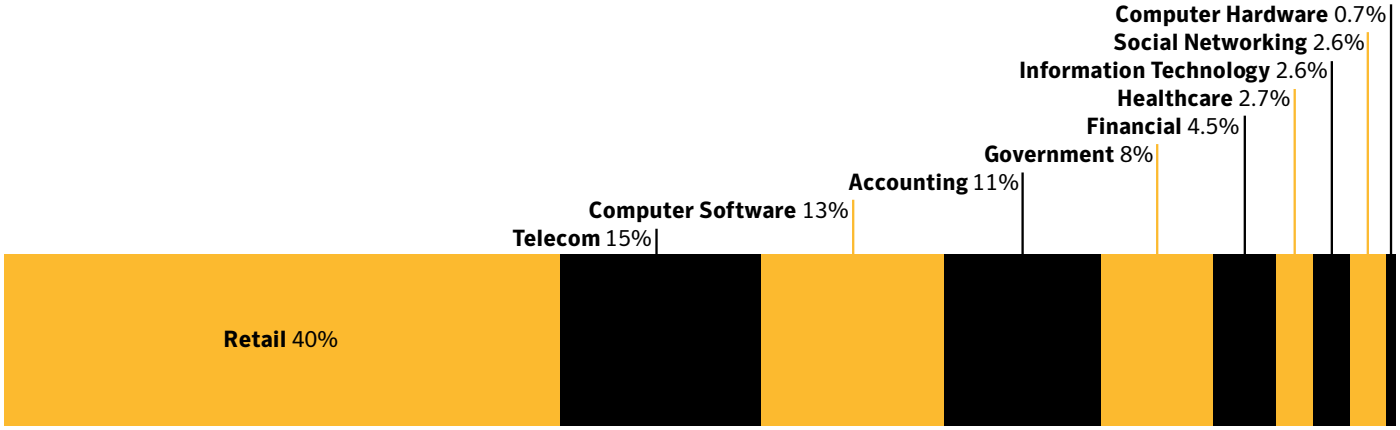


Figure 5 – Top sectors by number of identities exposed in 2012 to date

However, while this shows the number of identities exposed overall, it can also be influenced by particularly large breaches with high numbers of identities exposed. To compare, let's take a look at how the sectors break down by numbers of breaches.

In this case, the healthcare industry tops the list for number of overall breaches, with 34.1% of the overall number of breaches. Contrast this with the fact that this industry is only responsible for 2.7% of the overall number of identities exposed. Given the sensitive nature of medical records, this is a perfect example of a high number of attacks that result in small numbers of highly sensitive records being exposed.

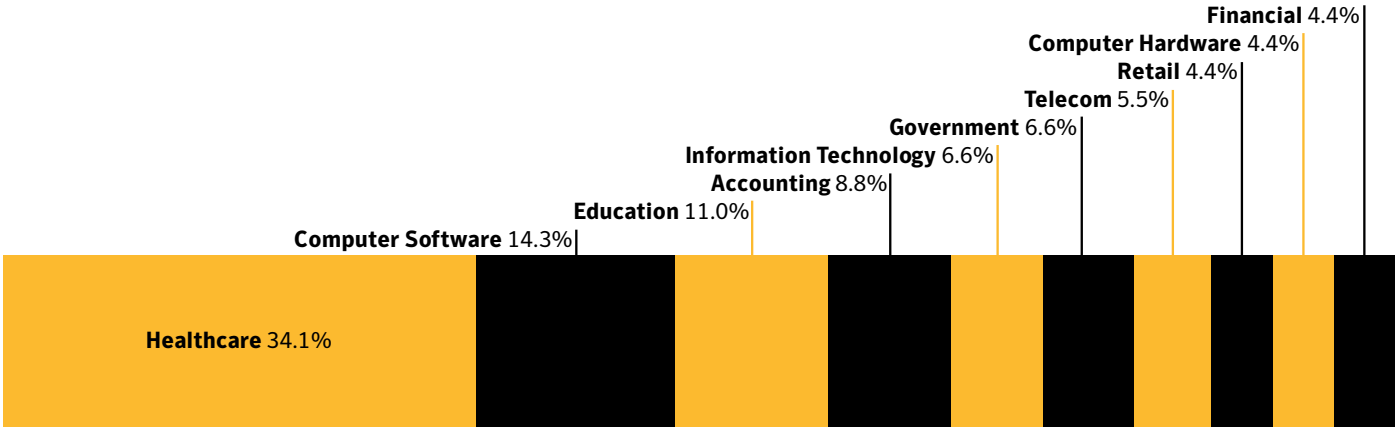


Figure 6 – Top sectors by number of data breaches in 2012 to date

So how does the state of the data breach landscape look now when compared to our 2011 data set? Overall it's a mixed bag. There's little doubt that hackers are responsible for the majority of data breaches occurring today, though the number of overall breaches remains about the same. Some industries have made strides to reduce their exposure, while new ones have found themselves the victim. And while the size of the average attack has dropped, it could be that attackers are simply targeting smaller caches of more valuable information. It appears that there is still much work to be done in order to bring down the overall numbers of data breaches.

Symantec™

Fake virus notification using Symantec logo

By Nicholas Johnston

We recently saw some malicious fake antivirus software. Such software often goes by generic names like “Windows Defender” or similar, but this particular software claims to be a Symantec product. An email claims that not only is the recipient infected—all users on the same network are as well. The email uses out-of-date Symantec branding, and links to a malicious application called RemovalTool.exe. Symantec does not produce a tool like this, nor does it email users in this way.

Figure 7 – Fake email pretending to come from Symantec

If a user downloads and executes the tool, a dialog box posing as a Java update, appears:

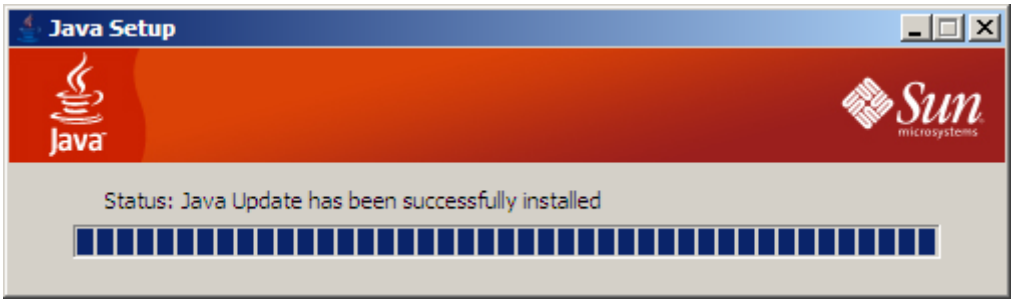


Figure 8 – Fake Java installation dialog box

One clue that this is a fake update is that it refers to Sun Microsystems, which developed Java, but was acquired by Oracle several years ago. In addition, the installer isn’t digitally signed. Compare this with a screenshot of the legitimate Java updater:

Figure 9 – Real Java installation dialog box

While the email may give the impression of being fake antivirus software, once installed the threat does not claim that the computer is infected. There are no visual indications that anything has been installed, though this might meet user expectations as the installer claims to be a simple removal tool, rather than a complete antivirus product. The malware downloads an information-stealing Trojan, which is detected as Infostealer.[4]

Special thanks to Sian John for reporting the scam.

Java Zero-Day Used in Targeted Attack Campaign

The following is an abridged version of two blog entries from the Security Response blog, published on 28 August & 30 August.

FireEye recently documented[5] a Java zero-day vulnerability (CVE-2012-4681[6]) in the wild that is thought to have been used initially in targeted attacks. Symantec is aware that attackers have been using this zero-day vulnerability since 22 August. We have located two compromised websites serving up the malware:

- ok.[REMOVED].net/meeting/applet.jar
- 62.152.104.[REMOVED]/public/meeting/applet.jar

One sample of malware downloaded by the exploit has been identified as Trojan.Dropper[7] (MD5 4a55bf1448262bf71707eef7fc168f7d). This particular sample connects to hello.icon.pk, which resolves to 223.25.233.244.

The Java exploit is being detected by Symantec as Java.Awetook.[8] The vulnerability consists of a privilege escalation due to a class that allows access to protected members of system classes, which should not be accessible. Because of this, malicious code can bypass the restrictions imposed by the sandbox and use the "*getRuntime().exec()*" function in order to execute a malicious payload. In our tests, we have confirmed that the zero-day vulnerability works on the

[4] *http://www.symantec.com/security_response/writeup.jsp?docid=2000-122016-0558-99*
[5] *http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html*
[6] *http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-4681*
[7] *http://www.symantec.com/security_response/writeup.jsp?docid=2002-082718-3007-99*
[8] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-082715-0841-99*

latest version of Java (JRE 1.7), but it does not work on the older version JRE 1.6. A proof of concept for the exploit has been published and the vulnerability has already been added in Metasploit.

Not only that, but this Java zero-day vulnerability has also been used in a targeted attack campaign. In October 2011, we documented a particular campaign – The Nitro Attacks.[9] In that instance, the attackers were primarily targeting chemical companies. Despite our work in uncovering and publishing the details behind these attacks, the attackers continued undeterred and even used our own report in their social engineering campaign!

The attackers have escalated their efforts, using this new Java zero-day vulnerability. We can confirm that some of the attackers behind this round of attacks are actually the Nitro gang.

The traditional modus operandi of the Nitro attackers is to send an email to victims. That email contains an attachment, which is a password-protected self-extracting zip file. The email claims to be an update for some piece of commonly installed software. The targeted user extracts it, runs it, and is infected with a copy of Backdoor.Darkmoon[10] (also known as Poison Ivy).

In these latest attacks, the attackers have developed a somewhat more sophisticated technique. They are using a Java zero-day, hosted as a .jar file on websites, to infect victims. As in the previous documented attacks, the attackers are using Backdoor.Darkmoon, re-using command-and-control infrastructure, and even re-using file names such as "Flash_update.exe". It is likely that the attackers are sending targeted users emails containing a link to the malicious jar file. The Nitro attackers appear to be continuing with their previous campaign.

As of 30 August, Oracle released an out-of-band patch[11] for CVE-2012-4681. Java users are advised to download the patch immediately.

The Elderwood Project

Symantec Security Response has recently published new research[12] about the activities of a group that has carried out targeted attacks over the last three years. The group first rose to prominence in 2009 with the "Aurora" or Hydraq attacks.[13] Security Response has dubbed this campaign the "Elderwood Project", based on a variable used in the source code by the attackers.

What sets the Elderwood Project aside from most targeted attacks is its heavy reliance on zero-day vulnerabilities. While most targeted attacks rely on malicious email attachments or known vulnerabilities (as we recently discussed in the June Intelligence Report[14]), Elderwood has used eight zero-day vulnerabilities over the last three years.

The attackers also make use of an exploitation technique called a "watering hole attack". In this scenario, the attackers compromise a website that caters to the interests of people working within the targeted organization. The attackers then wait for the target to come to them, rather than explicitly going after the target, in much the same way a predator in the savanna lies in wait for its prey near a source of water.

For more information on the Elderwood Project, such as who may be behind it, what their motivations are, and who are the main targets, download The Elderwood Project[15] whitepaper.

[9] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf*
[10] *http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99*
[11] *http://www.java.com/en/download/index.jsp*
[12] *http://www.symantec.com/connect/blogs/elderwood-project*
[13] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99*
[14] *http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_06_2012.en-us.pdf*
[15] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf*

Global Trends & Content Analysis

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

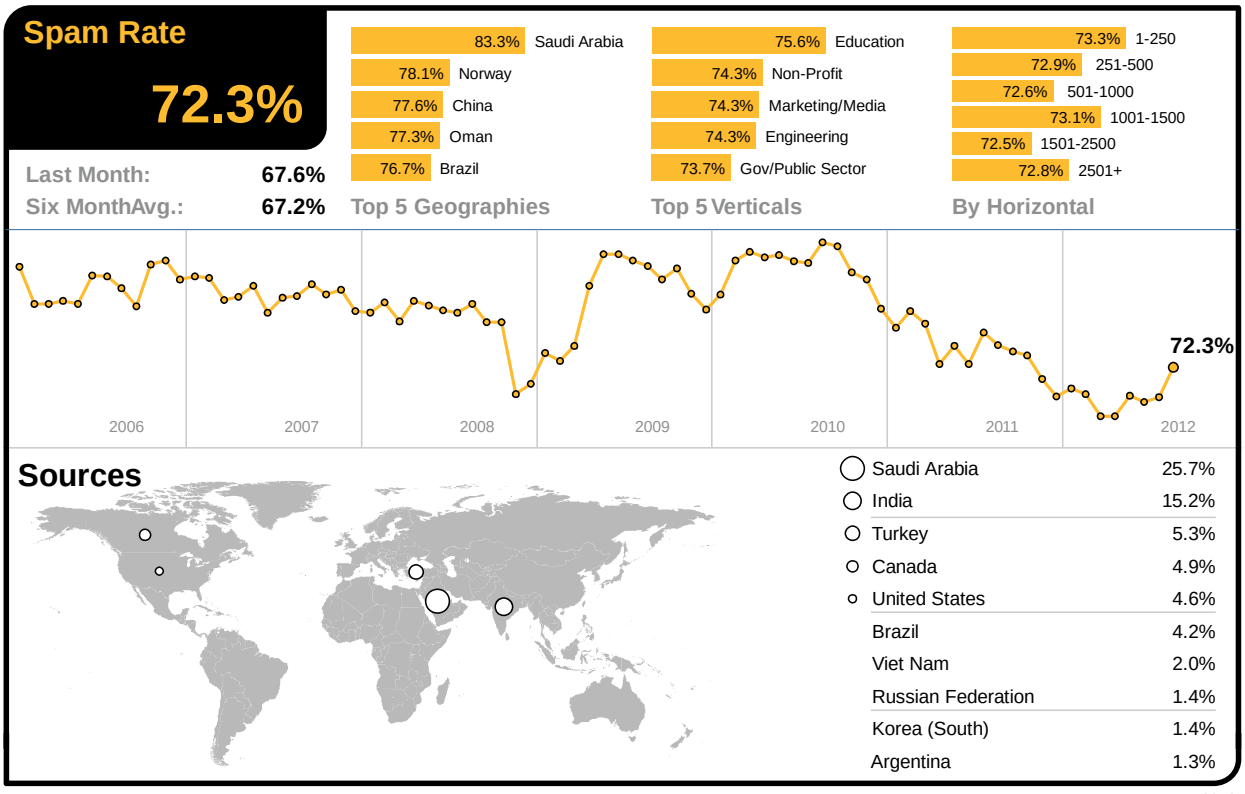
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

Spam, phishing and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is able to detect new and sophisticated targeted threats before reaching customers' networks. Over 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises and consumers the essential information to secure their systems effectively now and into the future.

Spam Analysis

In August, the global ratio of spam in email traffic rose by 4.7 percentage point since July, to 72.3 percent (1 in 1.38 emails).



August 2012

Global Spam Categories

The most common category of spam in August is related to the Sex/Dating category, with 42.51 percent.

Category Name	August 2012	July 2012
Sex/Dating	42.51%	23.46%
Pharma	32.61%	12.87%
Watches	8.55%	2.40%
Jobs	6.85%	1.52%
Software	5.86%	1.54%
Casino	1.60%	0.50%
419/scam/lotto	0.76%	0.08%
Degrees	0.60%	0.18%
Mobile	0.48%	0.07%
Weight Loss	0.11%	0.14%
Newsletters	0.07%	57.22%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com top-level domain increased in August, as highlighted in the table below. The .info top-level domain also made the list this month, pushing.br out of the top four.

TLD	August 2012	July 2012
.com	64.6%	63.9%
.net	8.3%	6.9%
.ru	7.0%	8.3%
.info	3.1%	N/A

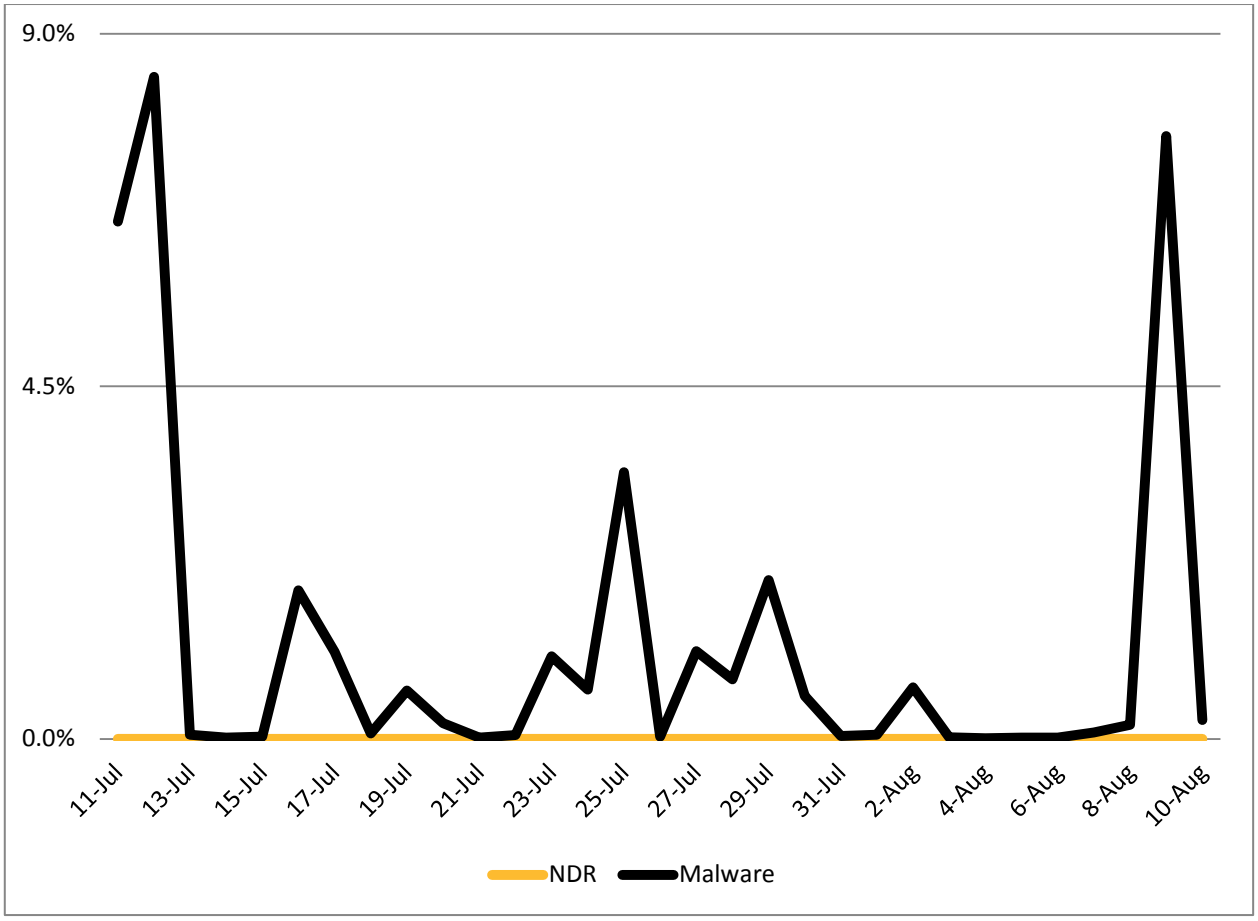
Average Spam Message Size

In August, the proportion of spam emails that were 5KB in size or less decreased by 3.4 percentage points. Furthermore, the proportion of spam messages that were greater than 10KB in size decreased by 1.1 percent, as can be seen in the following table.

Message Size	August 2012	July 2012
0Kb – 5Kb	44.3%	47.7%
5Kb – 10Kb	30.2%	25.8%
>10Kb	25.5%	26.6%

Spam Attack Vectors

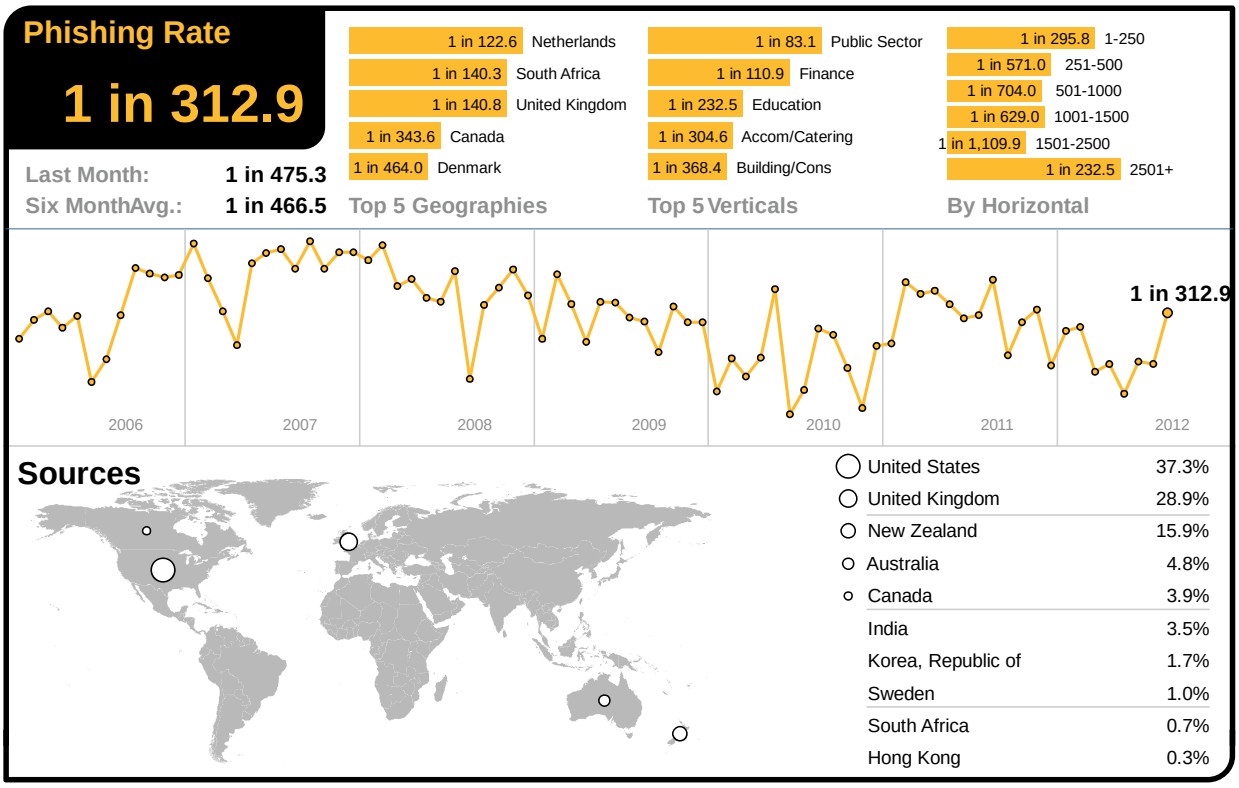
August highlights the decrease in spam emails resulting in NDRs (spam related non-delivery reports). In these cases, the recipient email addresses are invalid or bounced by their service provider.



NDR spam, as shown in the chart above, is often as a result of widespread dictionary attacks during spam campaigns, where spammers make use of databases containing first and last names and combine them to generate random email addresses. A higher-level of activity is indicative of spammers that are seeking to build their distribution lists by ignoring the invalid recipient emails in the bounce-backs. The list can then be used for more targeted spam attacks containing malicious attachments or links. This might indicate a pattern followed by spammers in harvesting the email addresses for some months and using those addresses for targeted attacks in other months.

Phishing Analysis

In August, the global phishing rate increased by 0.109 percentage points, taking the global average rate to one in 312.9 emails (0.32 percent) that comprised some form of phishing attack.



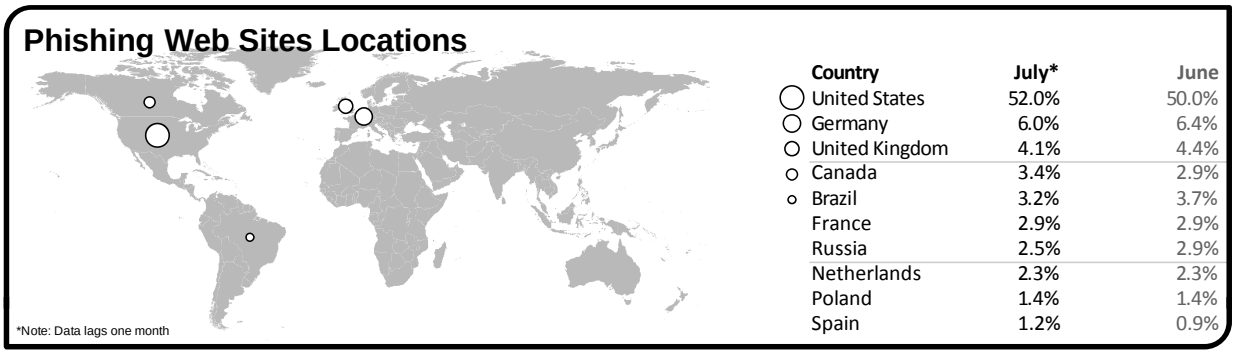
August 2012

Analysis of Phishing Web sites

Overall phishing increased by about 9.44 percent this month. Unique domains increased by about 38 percent as compared to the previous month. Phishing websites that used automated toolkits decreased by 7 percent.

Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) increased by about 24 percent. Webhosting services comprised of 3 percent of all phishing, a decrease of 13 percent from the previous month. The number of non-English phishing sites decreased by 51 percent. Among non-English phishing sites, Portuguese, French, Italian, and Chinese were highest in August.

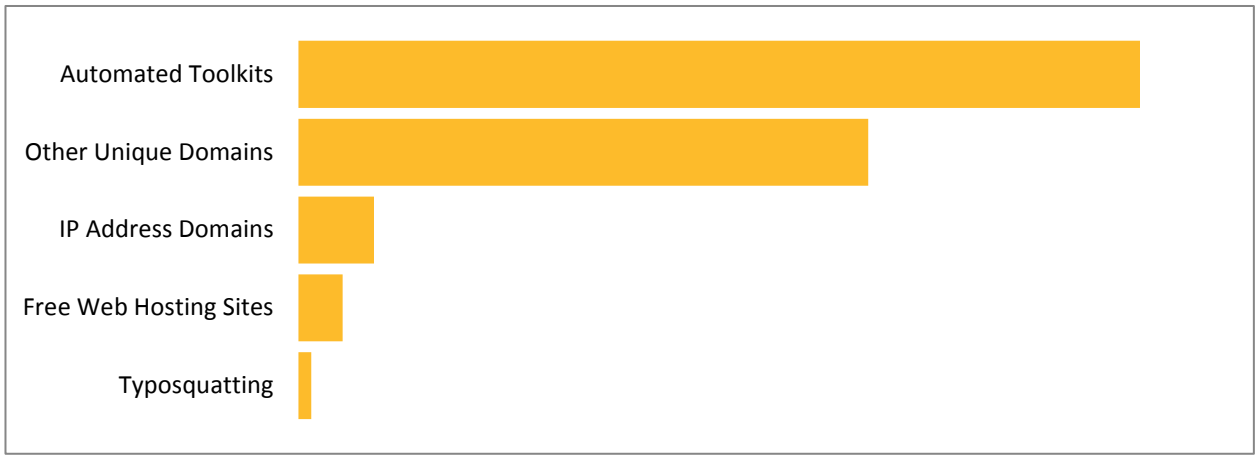
Geographic Location of Phishing Web Sites



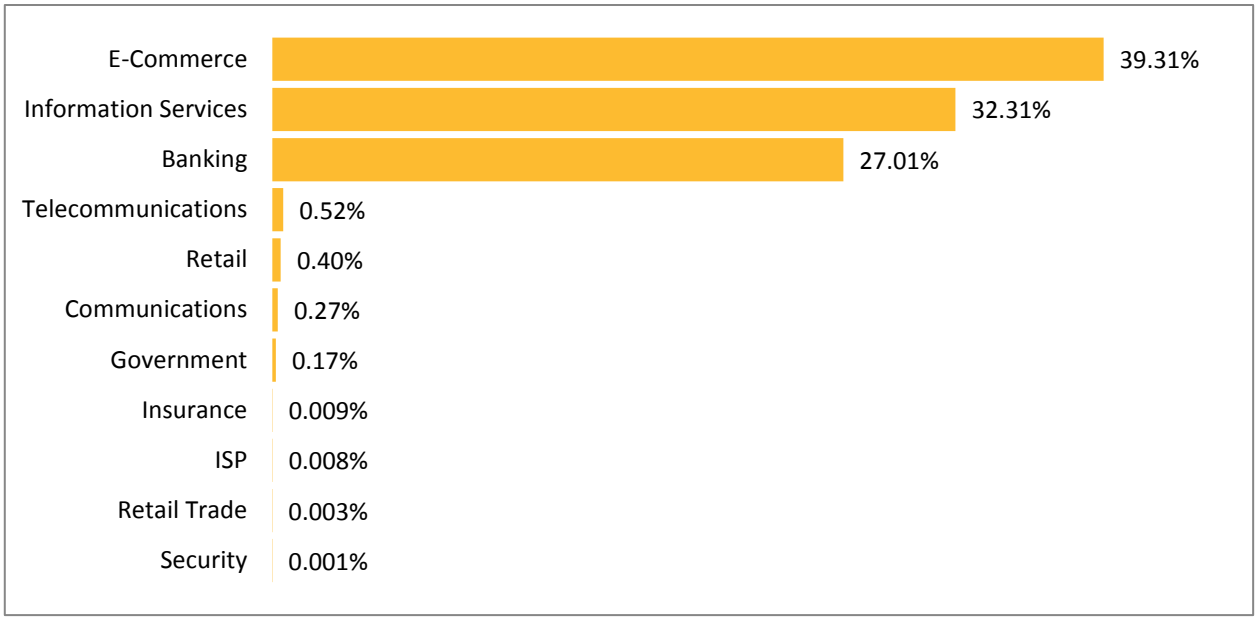
Country	July*	June
United States	52.0%	50.0%
Germany	6.0%	6.4%
United Kingdom	4.1%	4.4%
Canada	3.4%	2.9%
Brazil	3.2%	3.7%
France	2.9%	2.9%
Russia	2.5%	2.9%
Netherlands	2.3%	2.3%
Poland	1.4%	1.4%
Spain	1.2%	0.9%

August 2012

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry



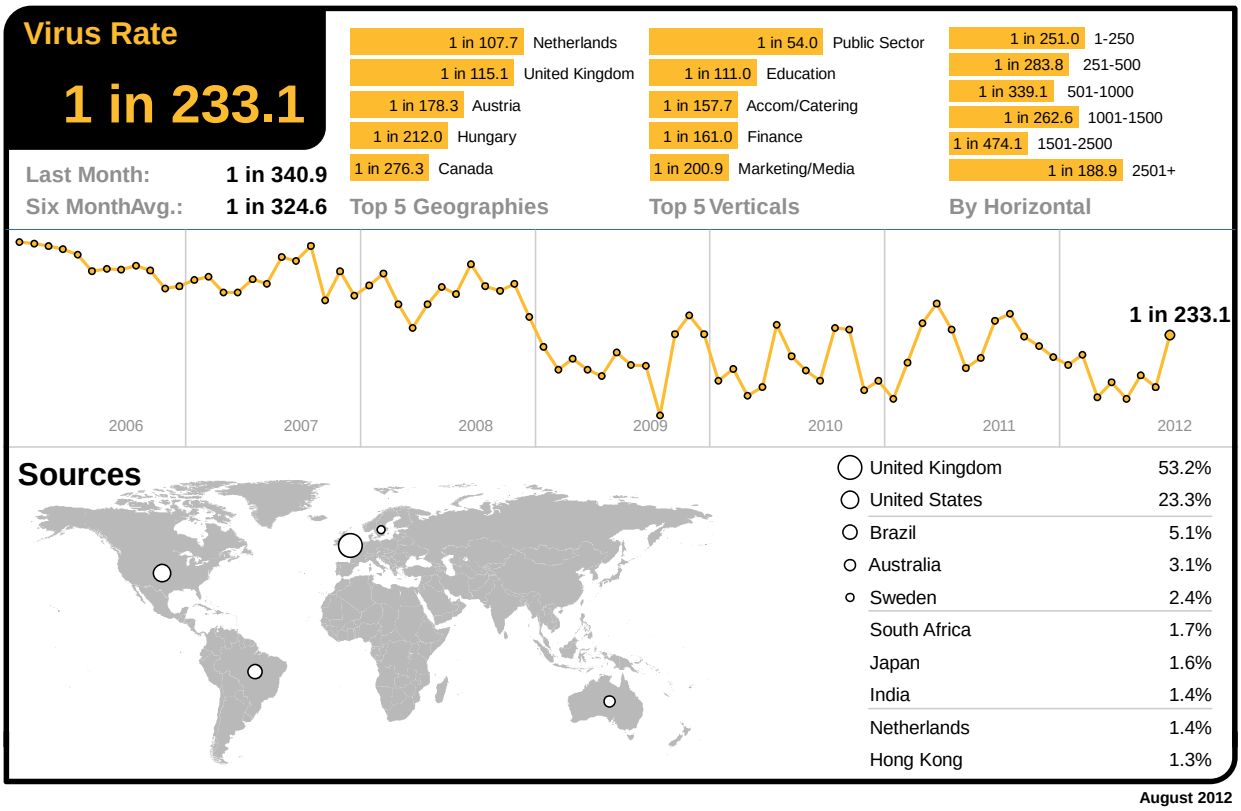
Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 233.1 emails (0.4 percent) in August, a decrease of 0.14 percentage points since July.

In August, 19.6 percent of email-borne malware contained links to malicious websites, 6.9 percentage points lower than July.



August 2012

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for August, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 37.6 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 18.2 percent of all email-borne malware blocked in August.

Malware Name	% Malware
W32/Bredolab.gen!eml.j	16.05%
Exploit/Link-generic-ee68	7.44%
W32/NewMalware-Generic	7.40%
W32/Bredolab.gen!eml.k	6.88%
W32/Bredolab.gen!eml.l	5.43%
HTML/JS-Encrypted.gen	4.50%
W32/BouncedNastyMail.gen.dam	2.56%
W32/NewMalware-ee73	2.09%
Exploit/BouncedGeneric	1.64%
Exploit.DarkPath.loc	1.53%

The top-ten list of most frequently blocked malware accounted for approximately 55.5 percent of all email-borne malware blocked in August.

Symantec™

Web-based Malware Threats

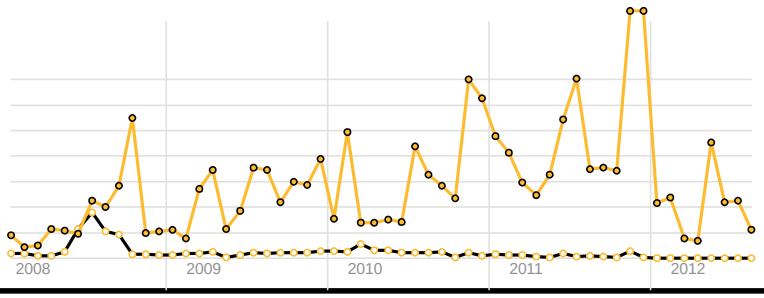
In August, Symantec Intelligence identified an average of 1,099 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 49.8 percent since July. This reflects the rate at which websites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

As detection for Web-based malware increases, the number of new websites blocked decreases and the proportion of new malware begins to rise, but initially on fewer websites. Further analysis reveals that 41.8 percent of all malicious domains blocked were new in August; a decrease of 11.7 percentage points compared with July. Additionally, 10.3 percent of all Web-based malware blocked was new in August; a decrease of 1.8 percentage points since July.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware	11/day
New sites with web viruses	1,088/day
Total	**1,099/day**



August 2012

The chart above shows the decrease in the number of new spyware and adware websites blocked each day on average during August compared with the equivalent number of Web-based malware websites blocked each day.

Web Policy Risks from Inappropriate Use

Some of the most common triggers for policy-based filtering applied by Symantec Web Security.cloud for its business clients are social networking, advertisements and popus, and streaming media category. Many organizations allow access to social networking websites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. 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 website. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Social Networking	30.2%	Trojan.JS.Iframe.BPN	11.8%	PUP:Generic.183433	9.3%
Advertisement and Popups	30.0%	Suspicious.Pythia	9.7%	PUP:Clkpotato!gen3	7.4%
Streaming Media	8.4%	Trojan.Generic.4315639	6.8%	Gen:Application.Heur	6.0%
Computing and Internet	4.1%	JS:Trojan.Crypt.FC	5.5%	PUP:Mediafinder	4.3%
Chat	4.0%	Trojan.JS.Iframe.BRV	5.1%	PUP:Agent.NLK	4.1%
Peer-To-Peer	2.9%	Gen:Trojan.Heur.PT.Ci4abmtlSyo	4.8%	PUP:9231	3.8%
Hosting Sites	2.7%	Trojan.Maljava!gen23	3.8%	PUP:Crossid	3.6%
Search	1.9%	Trojan.JS.Agent.GHF	2.6%	PUP:Android/DroidRooter.G	3.6%
News	1.6%	Trojan.JS.Agent.GLM	2.4%	PUP:Relevant.BH	3.6%
Games	1.5%	Trojan.Webkit!html	2.3%	PUP:Generic.183457	3.1%

August 2012

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing

mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

The table below shows the malware most frequently blocked targeting endpoint devices for the last month. This includes data from endpoint devices protected by Symantec technology around the world, including data from clients which may not be using other layers of protection, such as Symantec Web Security.cloud or Symantec Email AntiVirus.cloud.

Malware Name[16]	% Malware
W32.Sality.AE	6.78%
W32.Ramnit!html	5.99%
W32.Ramnit.B	4.78%
W32.Downadup.B	4.54%
W32.Ramnit.B!inf	3.44%
W32.Virut.CF	2.15%
W32.Almanahe.B!inf	2.05%
W32.SillyFDC.BDP!lnk	1.40%
W32.Mabezat.B	1.06%
W32.Virut!html	1.05%

For much of 2012, variants of W32.Sality.AE[17] and W32.Ramnit[18] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 14.4 percent of all malware blocked at the endpoint in August, compared with 7.4 percent for all variants of W32.Sality.

Approximately 43.9 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.

By deploying techniques, such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.

[16] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*
[17] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*
[18] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99*

About Symantec Intelligence

Symantec Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud Intelligence publishes a range of information on global security threats based on data captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary technology uses predictive analysis to detect new and sophisticated targeted threats, protecting more than 11 million end users at more than 55,000 organizations ranging from small businesses to the Fortune 500.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.