Symantec Intelligence Report: June 2012

A second look at Flamer, targeted attacks in the first half of 2012, and how attackers attempt targeted attacks

---

Welcome to the June 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 January through June 2012.

Report highlights

Introduction

This month we conclude our findings on the recent W32.Flamer threat. We show how there is a connection to Stuxnet and Duqu, discuss what we know about who may have created the threat, and highlight more information about what the threat can do.

We also take another look at targeted attacks in general to see what has changed since we last analyzed them in detail. We show how attacks have increased in the first half of 2012, what sectors are being targeted, and how there has been a shift in the size of companies that are being targeted.

Finally, we look in-depth at an attempted targeted attack recently carried out against a company in the aerospace industry. Breaking the attack down, we look at how the attackers attempt to entice employees in the company into launching malicious code that would give them access to the company's network, and what they could have done had the attack been successful.

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

Symantec™

Report analysis

W32.Flamer: What we know now

When releasing our May report, the media was alight with news about the discovery of Flamer. As we went to publication, analysis was still ongoing and it comes as no surprise that new information has come to light, which has both expanded and changed what we know about this threat.

In the May Report we answered a series of questions about Flamer based on what we knew at the time. Now that the threat has been thoroughly analyzed, let's go back and answer some of these questions in further detail.

Is Flamer related to Stuxnet and Duqu?

As it turns out, there is a connection. Early versions of Stuxnet contained a module called "Resource 207", which handled the spreading of the threat through USB and network drives. The code used for this propagation technique is identical in both Stuxnet and Flamer.

It appears as though this code was written for Flamer, and then co-opted for use in Stuxnet. Then in 2010, Resource 207 was pulled from Stuxnet and replaced by a different module that was used to spread the threat. Where or not Flamer and Stuxnet were developed by the same group of attackers, at the very least this shows that they shared code when developing the threats.

Who made Flamer?

A lot of circumstantial information on this topic has come to light recently. While there is a high probability that a nation state was involved in the development of this threat, no smoking gun exists that unquestionably implicates any particular source. What we can say with a high degree of certainty is that the developers behind Flamer were likely well-funded and well-organized. Anything beyond that is still in the realm of speculation.

What does Flamer do?

We mentioned previously that Flamer gathers information from the computers that it compromises. However, the sheer breadth of the information it gathers is largely unparalleled in the threat landscape. Trying to catalog all the information that Flamer scoops up has become a daunting task[1]—the extent is that large. The question becomes less about what it can gather, but if there is any information on a system that it could not, once resident on the computer.

In the last month we've learned much more about how Flamer spreads. Interestingly, it does not spread automatically, as the vast majority of traditional worms do. The threat must be instructed to spread by the attackers, giving the folks behind Flamer significant control over how, when, and to what computers the threat will compromise. This level of control helps to explain how Flamer managed to stay hidden in the threat landscape for so long.

Of particular note is the way Flamer can spread as a fake update to Windows. The threat does this by utilizing a digital certificate supplied by Microsoft.[2] This certificate, originating from a registered Terminal Services Licensing server, chained all the way up to the Microsoft Root Authority. This certificate improperly allowed code signing, which Flamer utilized to push its executable through Windows Update to targeted computers as though they were valid Microsoft executables. Exactly how the attackers behind Flamer managed to obtain the certificate remains somewhat of a mystery, but Microsoft has since revoked the trust of the certificates in question.

How come it hasn't been detected before?

One of the main objectives of a targeted attack is for the threat to remain off the radar while carrying out its malicious actions. Flamer was extremely good at this. It spread using incredibly covert methods, like Windows Update, and only when the attackers wished it to. The threat only garnered international attention when its behavior changed—the threat apparently went of the offensive[3] and drew attention to itself.

Targeted attacks often aim to gather information about the system and network topology for use in further attacks. Flamer seems to have done just that: it gathered reams of sensitive information that it then sent back to the attackers.

---

[1] *http://www.symantec.com/connect/blogs/w32flamer-enormous-data-collection*
[2] *http://www.symantec.com/connect/blogs/w32flamer-leveraging-microsoft-digital-certificates*
[3] *http://www.bbc.com/news/technology-17811565*

What really makes Flamer stand out as a targeted attack is how small the infection was—almost all instances of the threat reside in a fairly localized area in the Middle East. The attack gathered a large amount of data from a small number of computers.

In the grander scheme of things, very few computers were impacted by Flamer. But that is not to say that the threat, and targeted attacks like it, isn't a concern for security professionals and users alike. As we discuss in the next section, targeted attacks are a force to be reckoned with in today's threat landscape.

Targeted Attack Analysis: The first six months of 2012

We last discussed targeted attack data in the Internet Security Threat Report Volume 17,[4] which showed a significant growth in the number of targeted attacks in 2011, and also identified government and public sector organizations as the most commonly attacked. How does the first half of 2012 compare?

Growth of targeted attacks

After reaching a record high in December of 154 attacks per day, daily attacks dipped briefly in January before returning to similar levels in February. For the most part, the daily attack average remained around this level for the first half of 2012. This would have resulted in an average increase in targeted attacks per day of around 24% for the first half of 2012. The notable exception to this leveling off (discounted in the above, average increase) is the month of April, where the targeted attacks went through the roof, at an average of 468 per day.

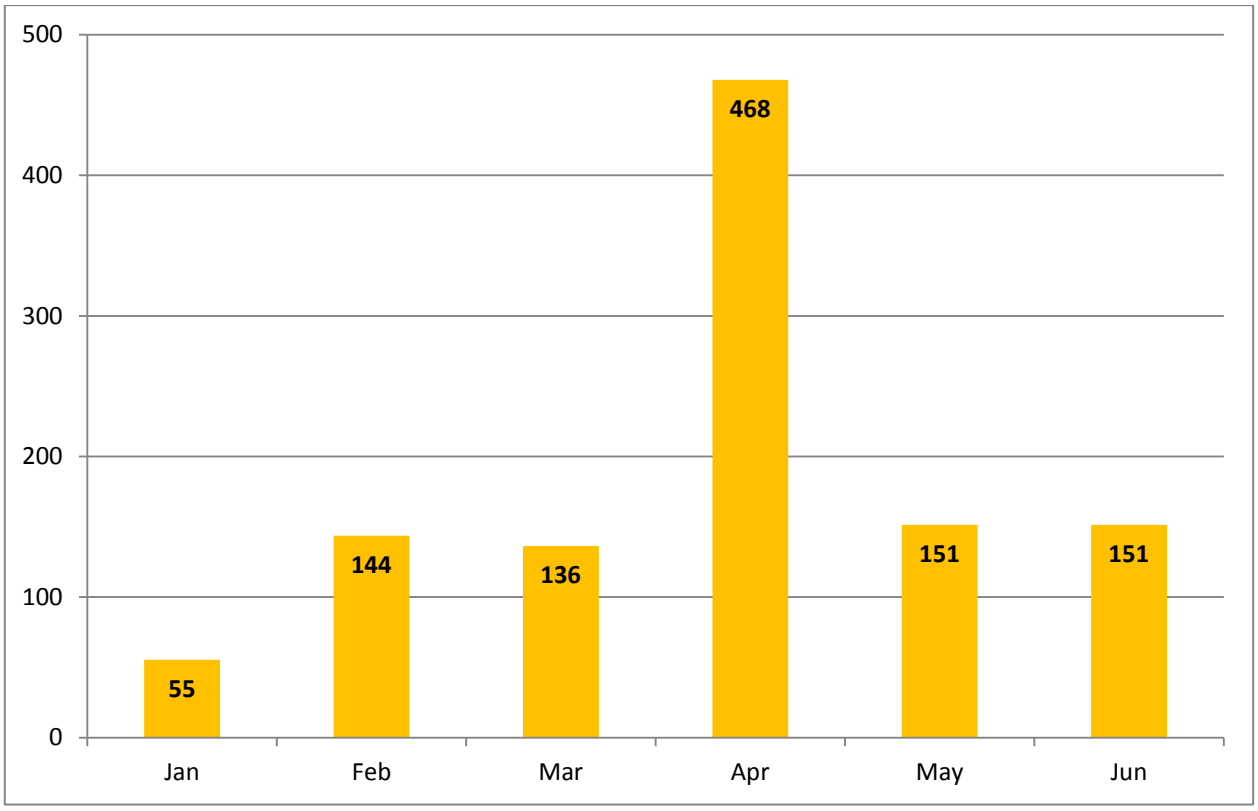


Figure 1 – Average targeted attacks per day during the first six months of 2012

A large amount of the increase can be attributed to one Symantec.cloud customer that came under a particularly intense attack. This is a very rare occurrence in terms of targeted attacks, where an attacker generally attempts the digital equivalent of putting on a disguise to sneak into a restricted area. In contrast, this particular attack would be more akin to lowering your shoulder and running full speed into the front door.

[4] *http://www.symantec.com/threatreport*

Once this attack subsided, the numbers returned to their previous levels in May and stayed almost exactly the same in June, further supporting the idea that this increase was an anomaly, as opposed to a trend. Given the nature and sheer scale of this attack, along with its ability to skew other data, we have removed it from the rest of our analysis.

Most frequently targeted industries

The breakdown for overall trends for industries targeted has remained largely the same in the first half of 2012 as it was in 2011. However, we've made some adjustments as to how industry data is displayed in order to give a clearer picture of where the attacker's efforts are being concentrated.

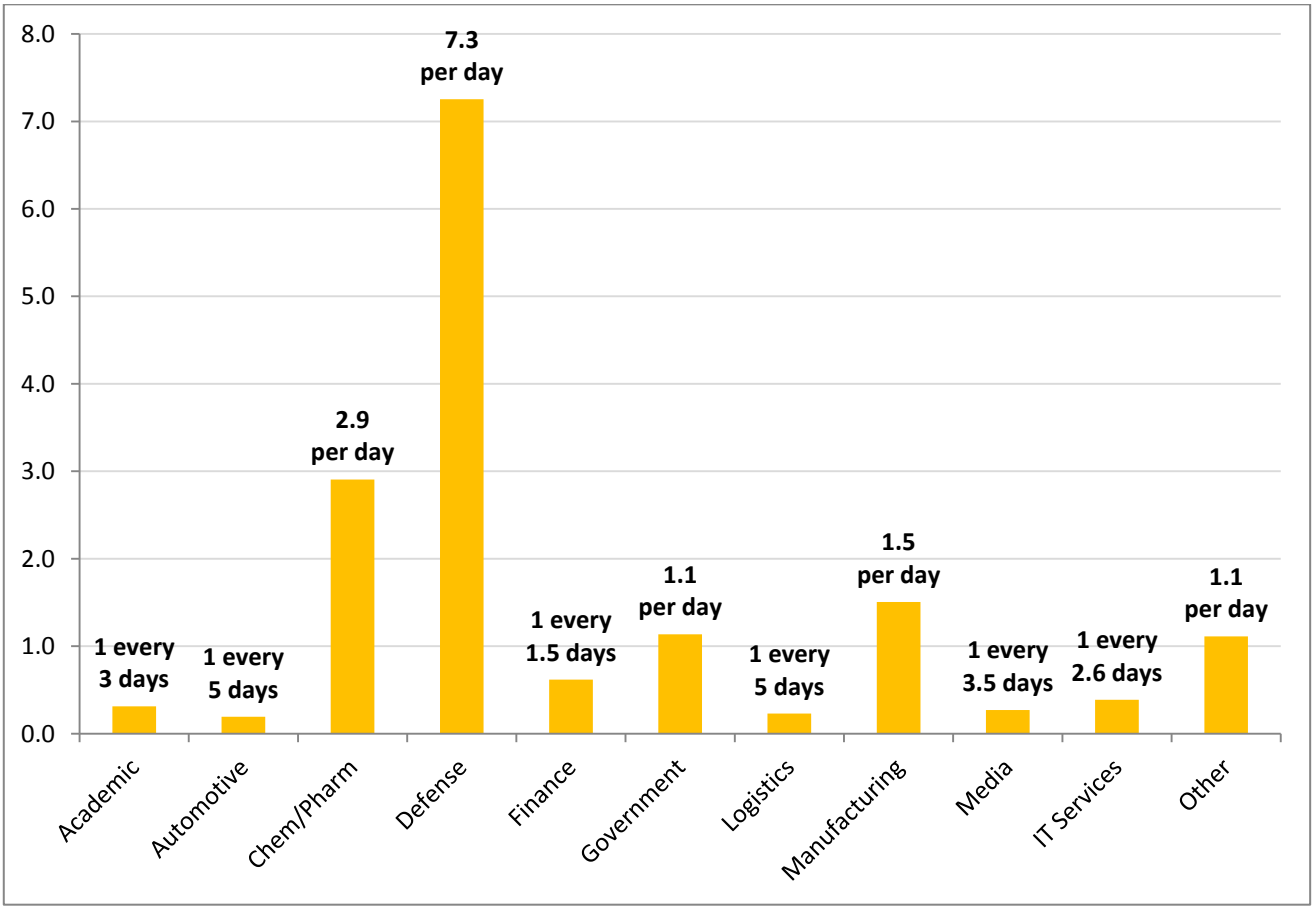


Figure 2 – Average number of targeted attacks blocked by Symantec.cloud per day by industry sector

Clearly the Defense industry has been the targeted industry of choice in the first half of the year, with an average of 7.3 attacks per day. In the past we've included this industry in the overall government sector, but with all other government sectors combined receiving around 1.1 targeted attacks per day on average, breaking Defense off into its own category helps indicate just how much attention this sector receives from attackers.

The Chemical/Pharmaceutical and Manufacturing sector maintain the number two and three spots. These targets have clearly received a smaller percentage of overall attention than in 2011, but the Chemical/Pharmaceutical sector are still hit by 1 in every 5 targeted attacks, while Manufacturing still accounts for almost 10% of all targeted attacks.

Targeted attacks by organization size

Larger organizations with more than 2500 employees continue to be the primary target of targeted attacks. However, there has been a shift from large companies towards small companies over the last six months. More than 36% of all targeted attacks are aimed at small companies, compared to 18% at the end of 2011. In fact, when looking at the trends month-by-month, there appears to be a direct correlation between a rise in attacks against small companies and a drop in attacks against larger ones. Attackers could very well be diverting resources directly from one group to the other.

This shift could be based on a perception that smaller business may be an easier point of entry. Without a full IT staff to look after attacks, smaller businesses could be seen as a weaker link in the supply chain. For instance, an email that appears to come from a particular individual of note (in reality a spoofed From address) could find itself automatically forwarded on to business contacts or partners within larger organizations within the same industry.

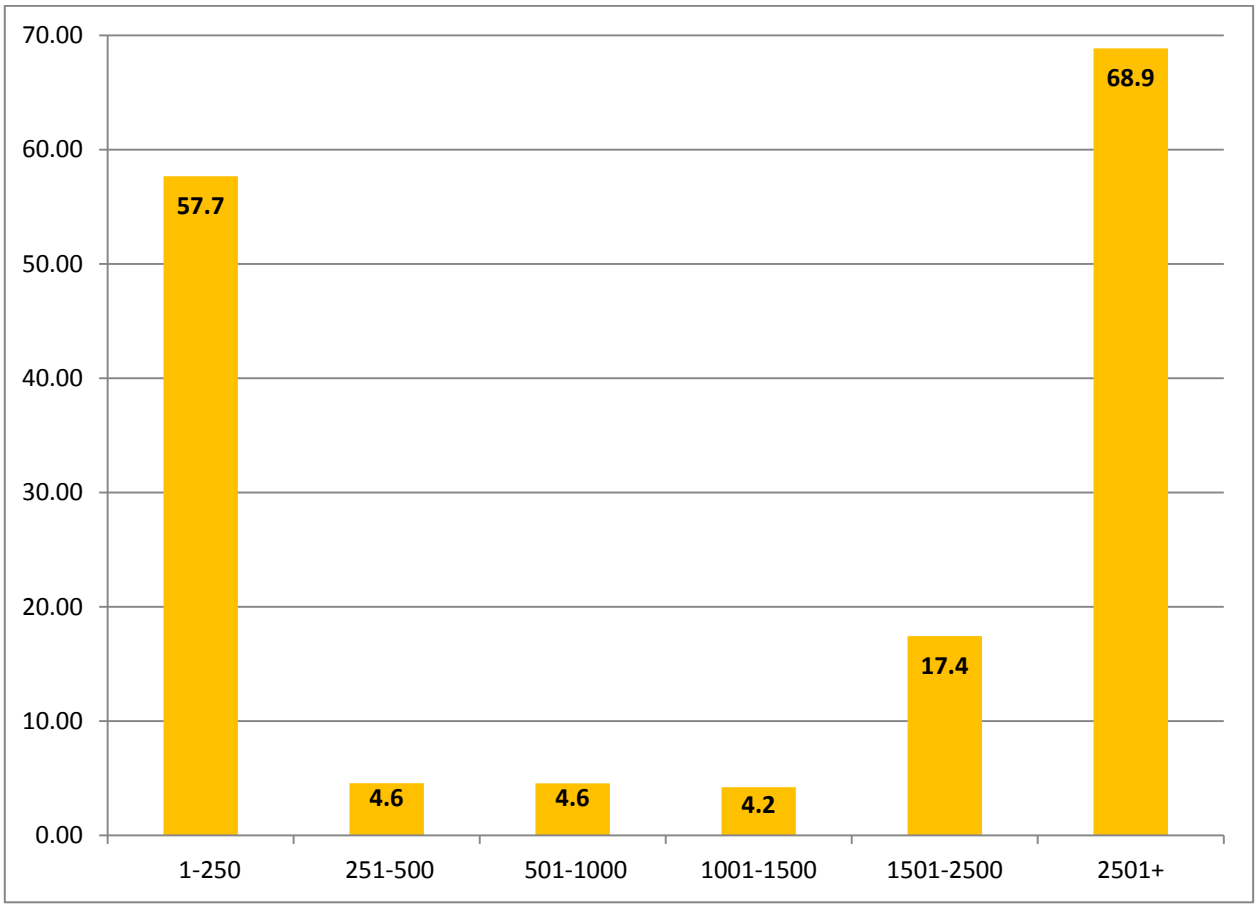


Figure 3 – Average number of targeted attacks blocked by Symantec.cloud per day by company size

Targeted attacks by geographical distribution

Finally, looking at countries that are attacked and the possible origins of these attacks, the United States tops both lists. In fact, many countries appear in both lists, such as Japan, China, and the United Kingdom.

It's worth noting that source countries do not automatically equate to "attacking countries". The actual attackers often use previously compromised computers as proxies. This affords the attacker some level of anonymity, since many such attacks can only be traced back to these systems.

An attacker may also find it easier to gain access to a system using a proxy within the same country as the computer they hope to compromise. In fact, in four of the top five source countries, their own country is either the first or second-most targeted country.

Source Countries

Geography	Percentage of attacks	Number of attacks
United States	31.27%	9859
Japan	17.78%	5606
Malaysia	10.99%	3464
China	10.89%	3434
Taiwan	9.97%	3143
Singapore	5.01%	1581
Poland	3.26%	1029
Greece	3.25%	1025
United Kingdom	1.05%	332
Pakistan	1.02%	321

Attacked Countries

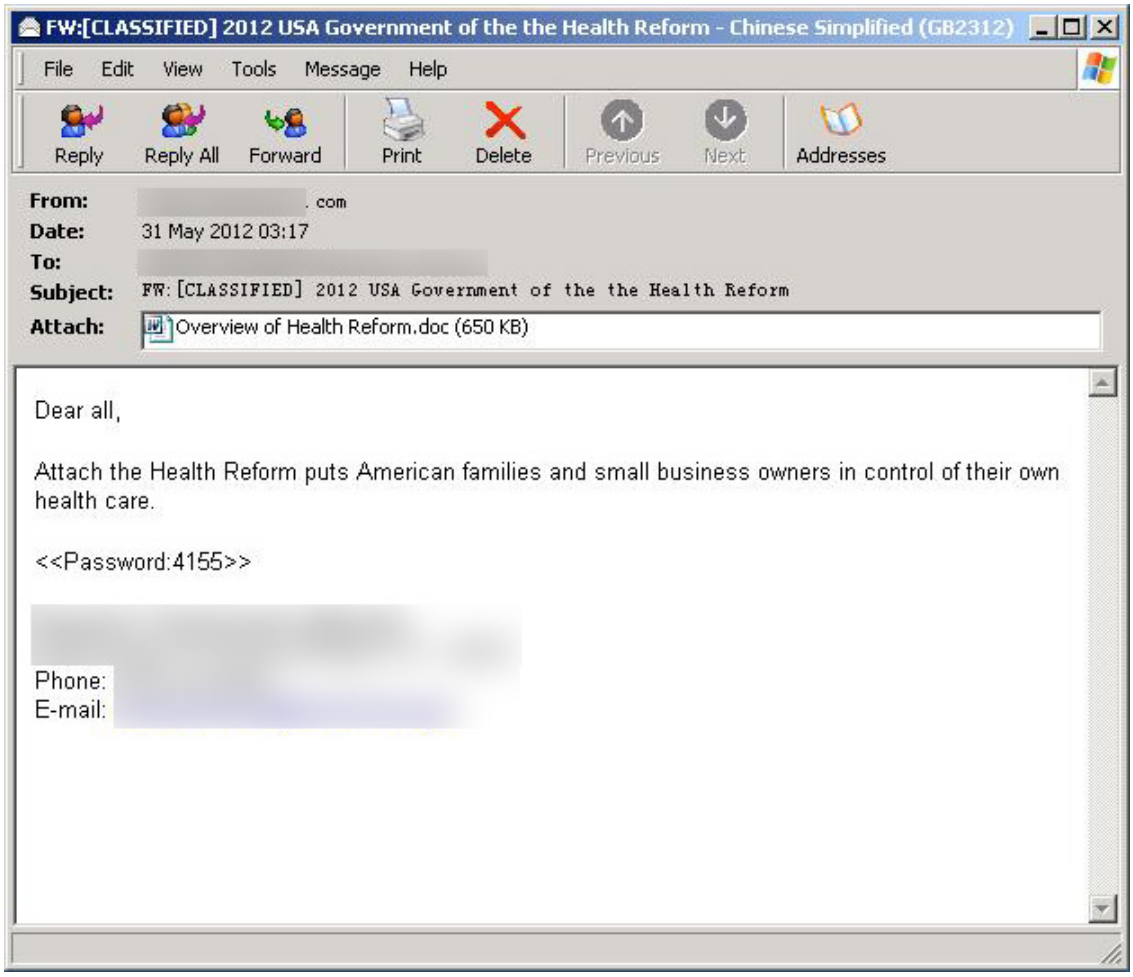
Banging on the Door: How targeted attackers breach a network

Let's take a look at a real-world example, where a particular company has been targeted, but our Symantec.cloud products have detected and blocked the attacks. This particular company is part of the international aerospace industry, manufacturing and maintaining aircraft, both civil and military, in three continents.

The line of attack used in this scenario, as is the case for many targeted attacks, is to send emails that contain malicious attachments. The attackers appear to have gathered a fairly long list of email addresses for the company. How exactly they obtained this list remains unclear, but it could be as easy as performing an internet search for a string with the company's domain name and the '@' symbol, then compiling a list from the results.

Next, the attackers decided to mimic the email address of a prominent executive from another organization involved in the aerospace filed and related sectors. The attackers could have chosen to pretend to be this individual based on past business dealings—something that could also be gleamed from an Internet search.

The contents of the mail center around the topic of healthcare reform in the US, and what this means for US employers.



Now at first glance, this topic may not seem all that relevant to a company that is located outside of the US. However, there are a few things that could make it worth a second look to someone in this company, enticing them to open the attachment. First, a large portion of this company's business comes from US companies. With the changes to US healthcare law, there has been a lot of discussion on how this can impact a US company's bottom line, ultimately determining how much capital it will spend on other things. This is a topic that could very well make an aerospace company sit up and take notice, especially if it can impact overall orders from its US customers.

Still, the level of interest of an aerospace company in this topic is tenuous at best, but the importance is driven home based on a few other items. For instance, the Subject of the email begins with "FW: [CLASSIFIED]" in big, capital letters. While the sender's company also works in the aerospace industry, they have ties to the intelligence community as well, and could appear to have insider information on upcoming changes to the healthcare system. The forwarded message body appears to come from a US Congressman, lending further credence to the idea that this information may be legitimate. Finally, the attachment name seems in line with the topic, being called "Overview of Health Reform.doc", which sounds like a tidy summary of the situation.

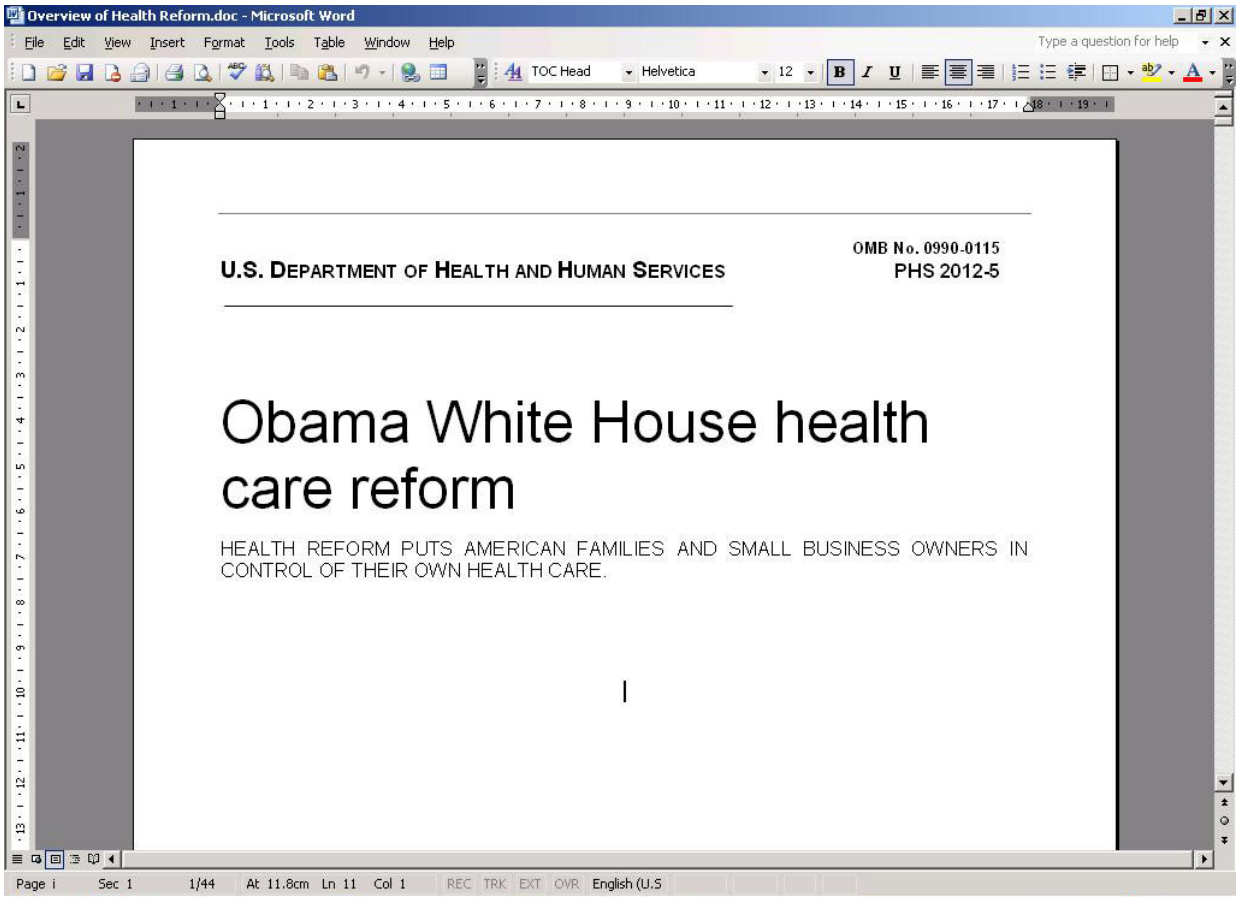
Things get particularly interesting when we look at the attachment. If the curiosity of an unsuspecting user is piqued and the attachment is opened, Word asks the user to enter a password, which can be found in the body of the email, and lends further credibility to the idea that this information is confidential. The attackers in this case have also craftily used Microsoft Office's built-in encryption here, with the hopes to sneak the malicious code contained with the file past antivirus software.

After the password is entered, the document appears for a split second before Word "crashes". In truth, the specially crafted document contains a copy of Trojan.Mdropper.[5] In this brief moment, the Trojan has exploited a vulnerability in Word, installing its malicious payload on the computer, leading Word to close, but leaving a copy of the actual, legitimate Word document behind in the Temp folder. The Trojan then launches this temp file, and the document

[5] *http://www.symantec.com/security_response/writeup.jsp?docid=2005-031911-0600-99*

appears to open as though nothing was wrong. This all takes a matter of seconds, and could easily go unnoticed by less observant users.

The document displayed is indeed about healthcare reform, but appears to be content that has simply been lifted from the Internet—nothing "confidential" here. A user may simply end up scanning this document, then closing it, none the wiser that a Trojan has been installed in the background.



The Trojan itself appears primed to slurp up all sorts of information from within the compromised computer. It collects IP addresses, user names, and system information and sends this information to a remote server. With back door capabilities included as well, this opens the door for the attackers to perform all sorts of actions, scouring the network for vulnerable systems, updating the malicious code, and generally gathering whatever information they are interested in.

Fortunately the attackers were not successful, and the attacks were blocked. This attack was distributed over a 60-hour period, with emails going out at seemingly random intervals—sometimes three mails in one hour, other times after a two hour break. Each of the 96 emails sent was identical; only the addressee was changed.

The attackers seemed to set the targeted company aside at this point, but only for a few weeks. The next wave of attempted intrusions came from a spoofed email address from the parent company of the target. The Subject and attachment were both titled "Strategy Meeting" and the attackers didn't even bother to hide the payload in a Word document, simply attaching a copy of Backdoor.Darkmoon[6] as an .exe file. The emails were sent out over a 9.5 hour period, covering an entirely new batch of email addresses within the company. 259 emails were sent in all, but this time a targeted user might see two or even three copies of the email appearing in their inbox.

Given how this attack was blocked, we do not know exactly what the attackers' goals were. However, given the highly sensitive nature of an aerospace company that works on both civil and military projects, it is possible that they could have been attempting to steal information on aerospace design documents or manufacturing processes. Alternatively,

[6] *http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99*

given how this company works as part of a larger international aerospace network, across multiple continents, and has close associations with other aerospace companies and organizations, the attackers may have viewed this company as an entry point, hoping to gain access and then work their way across the network of contacts and partnerships in the greater aerospace industry. Still, given how this attack was blocked by Symantec.cloud technology, we can only speculate as to the true motives of the attackers.

All in all, this whole targeted attack method might seem sloppy on the part of the attackers. There are plenty of weak points where the attack might not work, and it takes a lot of justification to rationalize why someone would fall for this ruse hook, line, and sinker. But keep in mind that there were hundreds emails send out across the company. All the attackers need in an attack like this is for one copy to be successfully installed. After that the doors are open.

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.

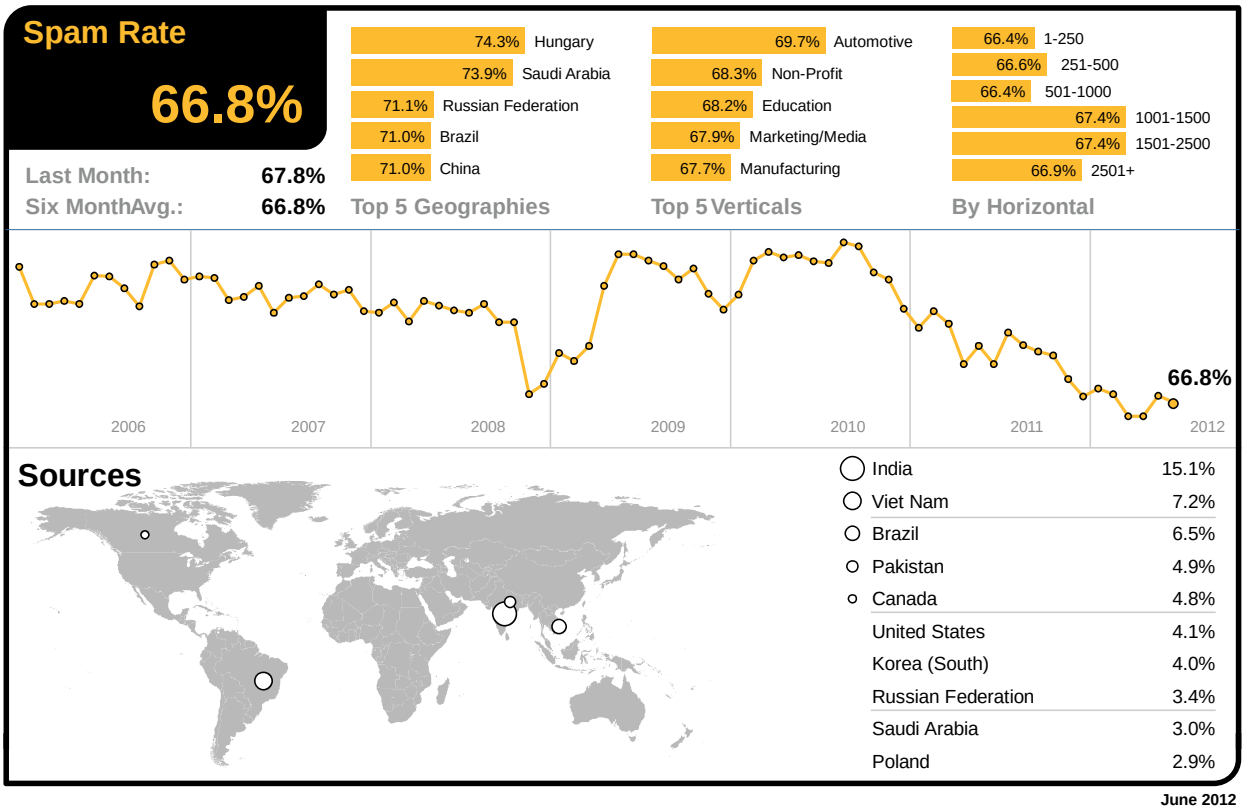
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

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 June, the global ratio of spam in email traffic fell by 1.0 percentage point since May, to 66.8 percent (1 in 1.5 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



June 2012

As the global spam rate decreased, Hungary was the most spammed geography in June, with a spam rate of 74.3 percent.

In the US, 66.4 percent of email was spam and 66.5 percent in Canada. The spam level in the UK was 67.2 percent. In the Netherlands, spam accounted for 68.9 percent of email traffic, 66.3 percent in Germany, 66.0 percent in Denmark and 66.1 percent in Australia. In Hong Kong, 65.9 percent of email was blocked as spam and 65.8 percent in Singapore, compared with 63.4 percent in Japan. Spam accounted for 66.8 percent of email traffic in South Africa and 71.0 percent in Brazil.

The Automotive sector was again the most spammed industry sector in June, with a spam rate of 69.7 percent; the spam rate for the Education sector was 68.2 percent. The spam rate for the Chemical & Pharmaceutical sector was 66.8 percent, compared with 66.4 percent for IT Services, 66.0 percent for Retail, 67.2 percent for Public Sector and 66.2 percent for Finance.

The spam rate for small to medium-sized businesses (1-250) was 66.4 percent, compared with 66.9 percent for large enterprises (2500+).

Global Spam Categories

The most common category of spam in June is related to the Adult/Sex/Dating category, though declining slightly since May, comprising a smaller overall percentage for the second month in a row.

Category Name	June 2012	May 2012
Adult/Sex/Dating	64.28%	70.16%
Pharma	18.76%	19.22%
Casino	5.24%	0.88%
Jobs	4.72%	3.47%
Watches	2.94%	3.45%
Software	1.67%	1.78%
Degrees	0.47%	0.57%
419/Scam/Lotto	0.27%	0.13%
Mobile	0.09%	0.14%
Newsletters	0.08%	0.03%
Weight Loss	<0.01%	0.08%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com top-level domain increased in June, as highlighted in the table below. This is in line with a slight decrease in all other top-level domains this month.

TLD	June 2012	May 2012
.com	74.7%	66.6%
.ru	4.1%	7.5%
.net	4.6%	5.8%
.br	2.9%	3.4%

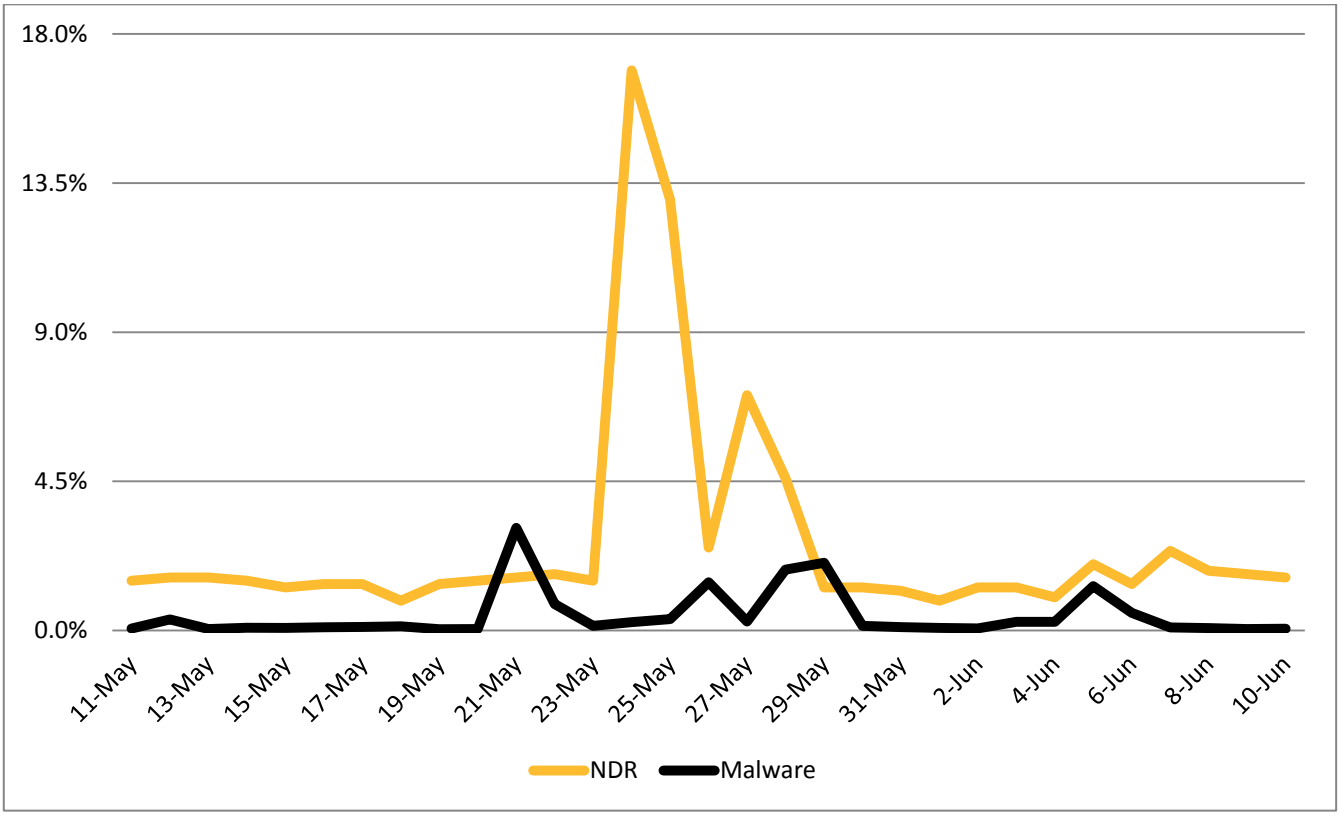
Average Spam Message Size

In June, the proportion of spam emails that were 5Kb in size or less decreased by almost 8 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size increased by 4 percent, as can be seen in the following table.

Message Size	June 2012	May 2012
0Kb – 5Kb	43.1%	51.1%
5Kb – 10Kb	33.3%	29.1%
>10Kb	23.6%	19.8%

Spam Attack Vectors

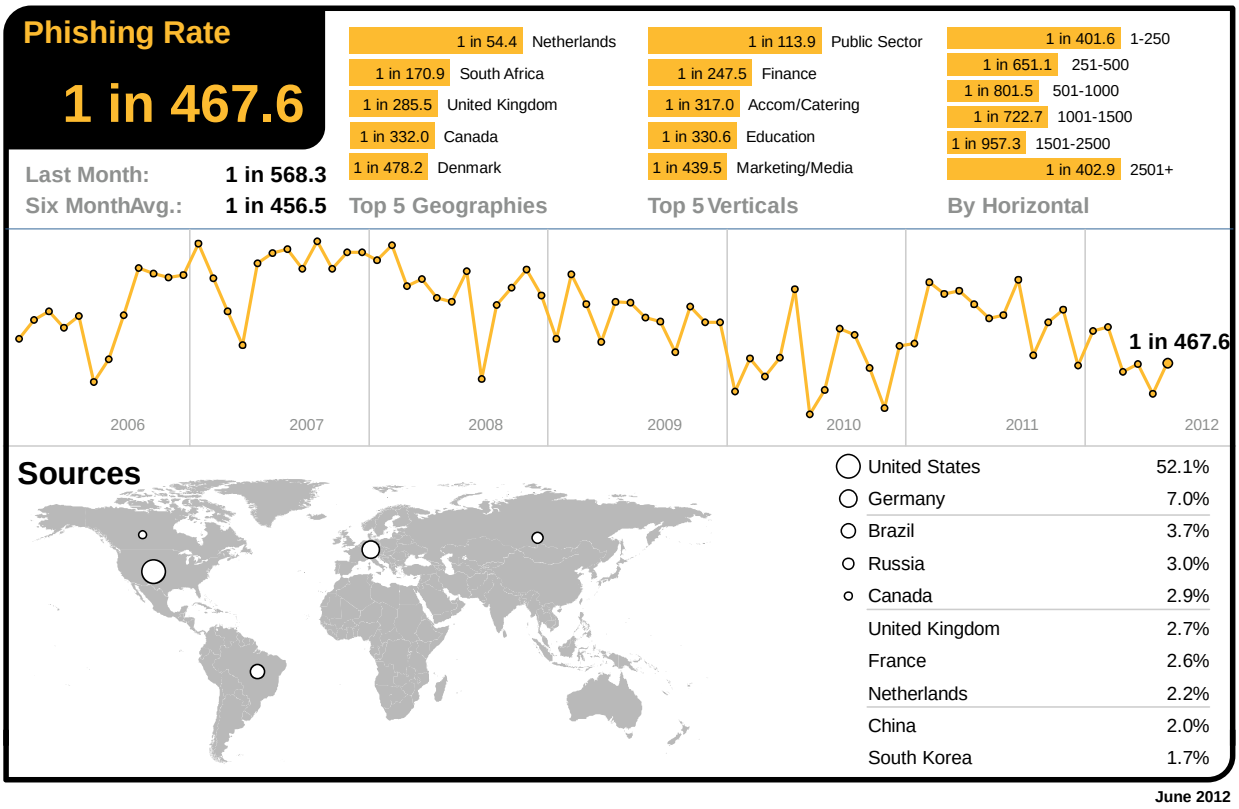
June highlights the increase in spam emails resulting in NDRs (spam related non-delivery reports). In these cases, the recipient email addresses are invalid or bounced by their service provider. The month appears to have been a quiet period for spam containing malicious attachments or links. The proportion of spam that contained a malicious attachment or link decreased, with just one spike of spam activity during the middle of the period, as shown in the chart below.



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 June, the global phishing rate increased by 0.04 percentage points, taking the global average rate to one in 467.6 emails (0.21 percent) that comprised some form of phishing attack.



The Netherlands was the country most targeted in June, with one in 54.4 emails identified as phishing attacks. South Africa was the second-most targeted country, with one in 170.9 emails identified as phishing attacks.

Phishing levels for the US reached one in 1,261.5 and one in 332 for Canada. In Germany phishing levels were one in 1,043.7, one in 478.2 in Denmark. In Australia, phishing activity accounted for one in 708.2 emails and one in 1,182.9 in Hong Kong; for Japan it was one in 8,005.7 and one in 2,679 for Singapore. In Brazil one in 713 emails was blocked as phishing.

The Public Sector remained the most targeted by phishing activity in June, with one in 113.9 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 1,201.2 and one in 986.8 for the IT Services sector, one in 835.3 for Retail, one in 330.6 for Education, one in 247.5 for Finance, and one in 2,114.3 for the Automotive industry.

Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 401.6 emails, compared with one in 402.9 for large enterprises (2500+).

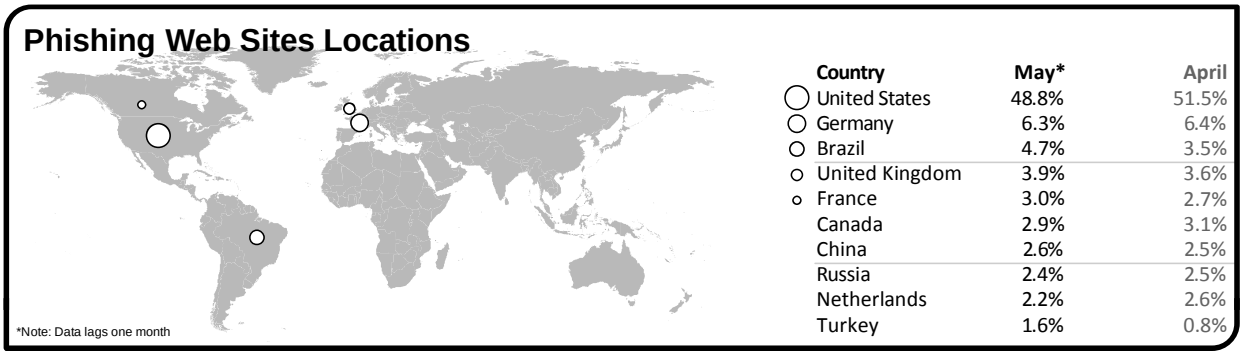
Analysis of Phishing Web sites

Overall, the number of phishing Web sites decreased by 12.8 percent in June compared with the previous month. The number of phishing Web sites created by automated toolkits decreased by approximately 10.4 percent, accounting for approximately 55.5 percent of phishing Web sites, including attacks against well-known social networking Web sites and social networking apps.

The number of unique phishing domains increased by 13.8 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), increased by 0.2 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 3.9 percent of all phishing Web sites, an increase of 0.7 percent compared with the previous month. The number of non-English phishing Web sites decreased by 2 percent.

Of the non-English phishing Web sites, Portuguese, French, Italian, and German were among the highest in June.

Geographic Location of Phishing Web Sites

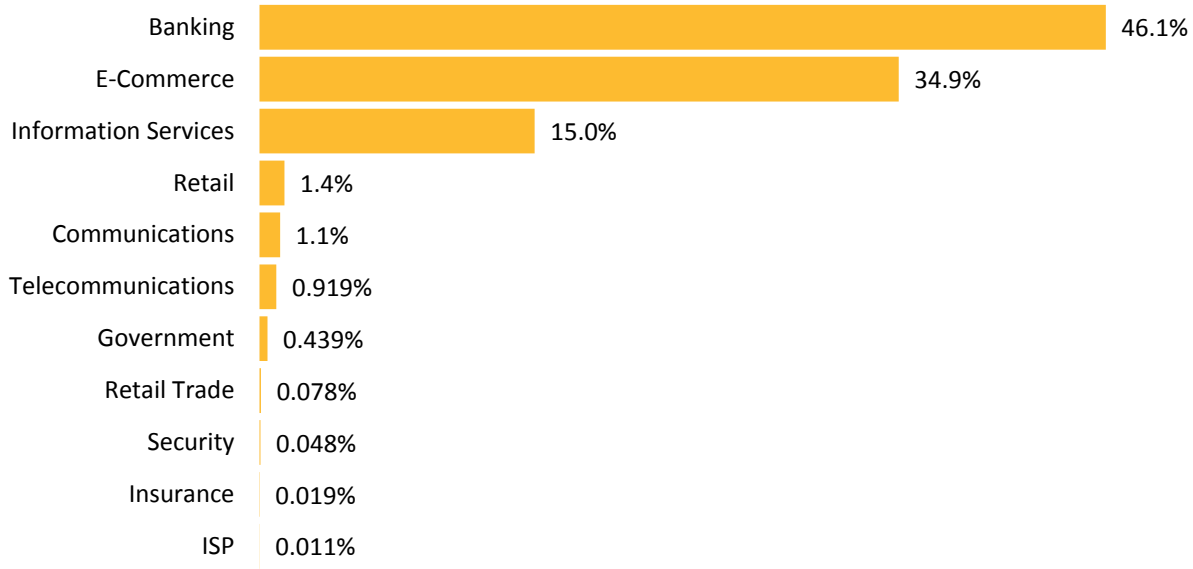


Country	May*	April
United States	48.8%	51.5%
Germany	6.3%	6.4%
Brazil	4.7%	3.5%
United Kingdom	3.9%	3.6%
France	3.0%	2.7%
Canada	2.9%	3.1%
China	2.6%	2.5%
Russia	2.4%	2.5%
Netherlands	2.2%	2.6%
Turkey	1.6%	0.8%

June 2011

Tactics of Phishing Distribution

Organizations Spoofed in Phishing Attacks, by Industry

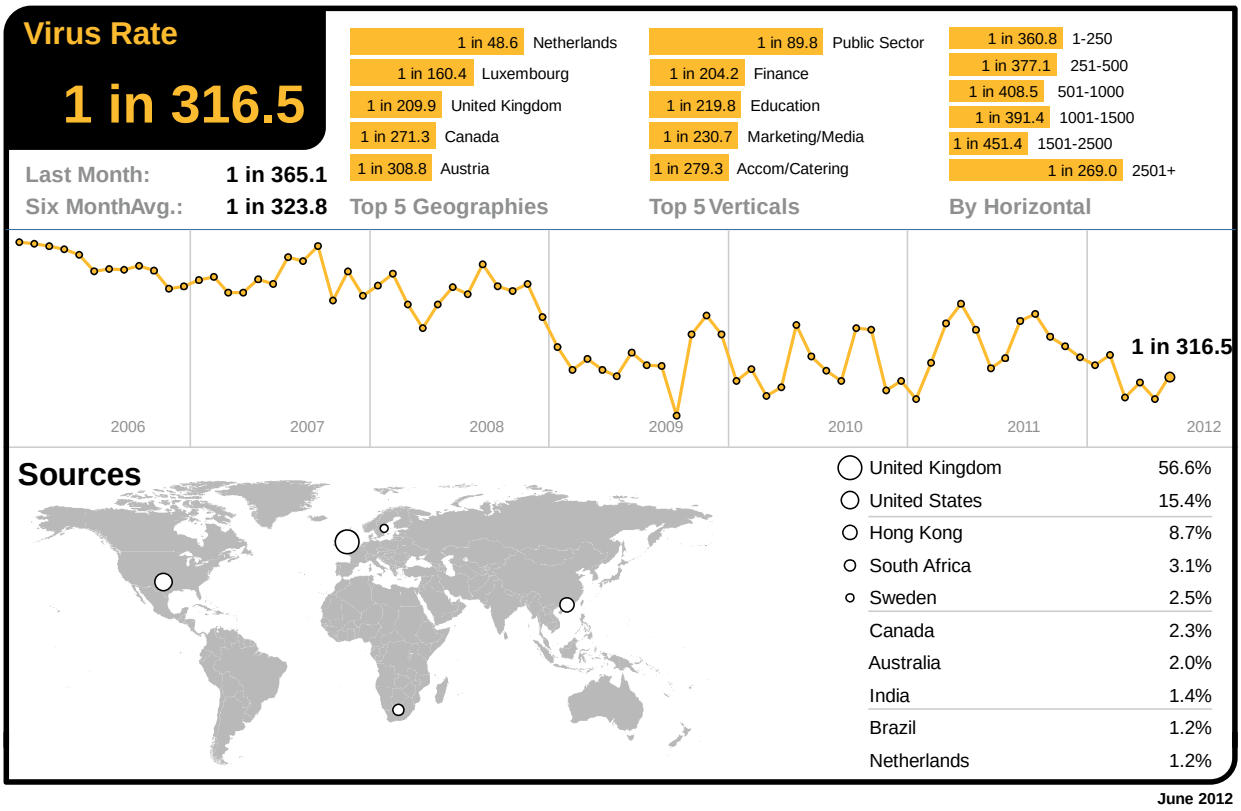


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 316.5 emails (0.31 percent) in June, an increase of 0.04 percentage points since May.

In June, 27.4 percent of email-borne malware contained links to malicious Web sites, 1.2 percentage points lower than May.



The Netherlands was the geography with the highest ratio of malicious email activity in June, with one in 48.6 emails identified as malicious.

In the UK, one in 209.9 emails was identified as malicious, compared with South Africa, where one in 414.1 emails was blocked as malicious. The virus rate for email-borne malware in the US was one in 570.2 and one in 271.3 in Canada. In Germany virus activity reached one in 385.4 and one in 438.4 in Denmark. In Australia, one in 598.3 emails was malicious. For Japan the rate was one in 2,372.8, compared with one in 862.7 in Singapore. In Brazil, one in 403.8 emails contained malicious content.

With one in 89.8 emails being blocked as malicious, the Public Sector remained the most targeted industry in June. The virus rate for the Chemical & Pharmaceutical sector reached one in 402.1 and one in 502.1 for the IT Services sector; one in 522.0 for Retail, one in 219.8 for Education and one in 204.2 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 306.8 emails, compared with one in 269.0 for large enterprises (2500+).

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for June, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 45.4 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 36.2 percent of all email-borne malware blocked in June.

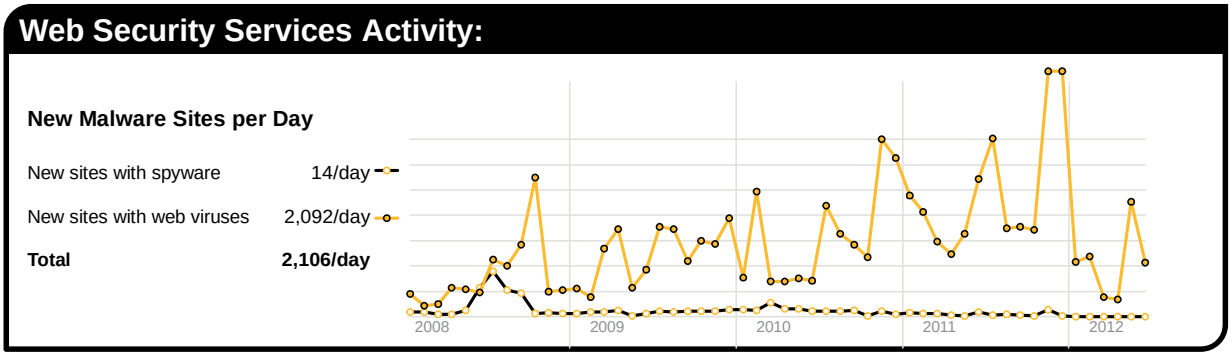
Malware Name	% Malware
W32/Bredolab.gen!eml.k	17.43%
W32/Bredolab.gen!eml.j	9.49%
Link-Exploit/Spam-3a71	3.82%
W32/NewMalware!16a0	3.48%
Exploit/Link-generic-ee68	3.22%
W32/NewMalware-Generic-a2a1-3477	2.34%
HTML/JS-Encrypted.gen	1.69%
Trojan.Bredolab	1.56%
W32/Bredolab.gen!eml-01cd	1.52%
Link-Gen:Variant.Barys.1516.dam	1.43%

The top-ten list of most frequently blocked malware accounted for approximately 33.7% of all email-borne malware blocked in June.

Web-based Malware Threats

In June, Symantec Intelligence identified an average of 2,106 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an decrease of 51.7 percent since May. This reflects the rate at which Web sites 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 Web sites blocked decreases and the proportion of new malware begins to rise, but initially on fewer Web sites. Further analysis reveals that 44.1 percent of all malicious domains blocked were new in June; an increase of 3.7 percentage points compared with May. Additionally, 13.0 percent of all Web-based malware blocked was new in June; a decrease of 0.3 percentage points since May.



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

Web Policy Risks from Inappropriate Use

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 29.9 percent of blocked Web activity in June. 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.

The second most frequently blocked traffic was categorized as Social Networking, accounting for 19.6 percent of URL-based filtering activity blocked, equivalent to approximately one in every 5 Web sites blocked. Many organizations allow access to social networking Web sites, 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. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Activity related to streaming media policies resulted in 8.4 percent of URL-based filtering blocks in June. 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. This rate is equivalent to one in every 11 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	29.9%	Trojan.JS.Agent.GHP	13.5%	PUP:ActualSpy	0.7%
Social Networking	19.6%	JS:Trojan.Crypt.DS	6.8%	PUP:Keylogger	5.2%
Chat	15.5%	JS.Runfore	5.2%	PUP:Lop	0.2%
Streaming Media	8.4%	Trojan.Script.12023	3.4%	PUP:AcePasswdSnif	0.2%
Computing and Internet	3.4%	Trojan.Iframe.ADD	3.3%	PUP:Aniquro.Toolbar.A	0.2%
Peer-To-Peer	3.0%	Trojan.JS.Agent.GHF	3.3%	PUP:9231	2.4%
Hosting Sites	2.5%	Gen:Trojan.Heur.LP.dq7@ayfQ64	2.7%	PUP:Nirsoft.SniffPass.A	0.2%
Search	1.7%	Trojan.JS.Iframe.BLX	2.5%	Riskware:W32/SuperScan.A	1.2%
News	1.5%	Trojan.Malscript!JS	2.4%	PUP:Heur.cmKfbiBPZXoO	2.6%
Blogs	1.5%	Trojan.HTML.Redirector.AI	2.3%	PUP:Heur.cmKfbiJBX0mO	0.2%

June 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[7]	% Malware
WS.Trojan.H	29.06%
W32.Sality.AE	6.81%
W32.Ramnit!html	6.01%
W32.Ramnit.B	5.61%
W32.Downadup.B	3.82%
W32.Ramnit.B!inf	3.53%
W32.Virut.CF	2.07%
Trojan.ADH.2	2.00%
W32.Almanahe.B!inf	1.83%
Trojan.ADH	1.43%

The most frequently blocked malware for the last month was WS.Trojan.H[8]. WS.Trojan.H is a generic, cloud-based, heuristic detection for files that possess characteristics of an as-yet unclassified threat. Files detected by this heuristic are deemed by Symantec to pose a risk to users and are therefore blocked from accessing the computer.

[7] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*

For much of 2012, variants of W32.Sality.AE[9] and W32.Ramnit[10] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 15.3% of all malware blocked at the endpoint in June, compared with 7.5% for all variants of W32.Sality.

Approximately 10.9 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.

[8] *http://www.symantec.com/security_response/writeup.jsp?docid=2011-102713-4647-99*
[9] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*
[10] *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.