Symantec Intelligence Report: August 2011

Turbulent financial markets trigger a return to stock pump-and-dump spam; Master Boot Record (MBR) malware may be making a comeback

Welcome to the August edition of the Symantec Intelligence report which, combining the best research and analysis from the Symantec.cloud MessageLabs Intelligence Report and the Symantec State of Spam & Phishing Report, 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 combined report includes data from July and August 2011.

Report highlights

Introduction

Overall spam levels were lower in August than last month. However, with the stock markets in turmoil once more, spammers are seeking to benefit from fluctuations in a turbulent market, most notably by sending large volumes of spam relating to certain "pink sheets" stocks that the scammers are trying to manipulate. Unlike companies on a stock exchange, companies quoted on the pink sheets system do not need to meet minimum requirements or file with the US Securities and Exchange Commission.

Phishing activity increased in August, with many increases coming from attacks related to major brand names such as those related to Apple's iDisk service, and a variety of Brazilian companies and services, including social networking and financial brand names.

An increase in malware activity also follows from an increase in boot-time malware or Master Boot Record (MBR) infections and finally, Symantec Intelligence takes a closer look at some of the techniques behind the Shady RAT operation recently in the news. Whilst the malware may not have been technically sophisticated or advanced in nature, it was nevertheless successful in penetrating some organizations that it was targeted towards – highlighting that targeted attacks do not always need to be advanced in order to be persistent.

Symantec™

Interestingly, in its MessageLabs Intelligence Annual Security Report for 2010[1], Symantec Intelligence predicted that in 2011, botnet controllers would begin to employ techniques such as steganography to conceal command and control instructions, and just such a system was employed in the Shady RAT analysis in this month's report.

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, Senior Intelligence Analyst
paul_wood@symantec.com
@paulowoody

Report analysis

Global Debt Crises News Drives Pump-and-Dump Stock Scams

Just as they sound, "pump-and-dump stocks" are promoted ("pumped") by their owners in order to inflate the price of the stocks as much as possible so that they may then be sold ("dumped") before their valuation crashes back to reality. The spam for these scams tries to convince the prospective mark that the penny stock is actually worth more than its valuation, or that it will soon skyrocket. Most of these claims are either misleading or false.

In a successful campaign, the deluge of spam will help artificially drive up the price of the stock to a point where the scammers decide to sell their shares. This usually coincides with them ending the spam campaign, which in turn reduces the interest in the stock, helping to drive its valuation back to its original low price (which can also be exploited in the market). A well-executed pump-and-dump spam campaign can produce substantial profits for the scammers in a matter of days.

In the current turbulent environment, many people may be convinced to invest in stocks that the scammers claim will benefit from the market turbulence.

For example, we have recently observed a spate of penny stock spam promoting Resource Exchange of America Corp. (RXAC.PK) stocks. The message is obfuscated with extraneous line breaks and spaces between the words. Similarly, the email headers contain broken words such as "`Stoc ks`" and "`m oney`". Poorly translated non sequiturs occur throughout the messages (e.g., "`United States still an AAA country, Obama says?!`").

Most of the spam originates from the United States and China, while a percentage is being generated from other countries in Asia. The majority of the attacks target North American users.

Examples of the subject lines of these messages include the following and can be seen in figure 1, below:

- `Stoc ks Ready to Bounce?`
- `There is a MASSIVE PROMOTION underway NOW!`
- `Been right on the m oney`

[1] *http://www.symanteccloud.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf*

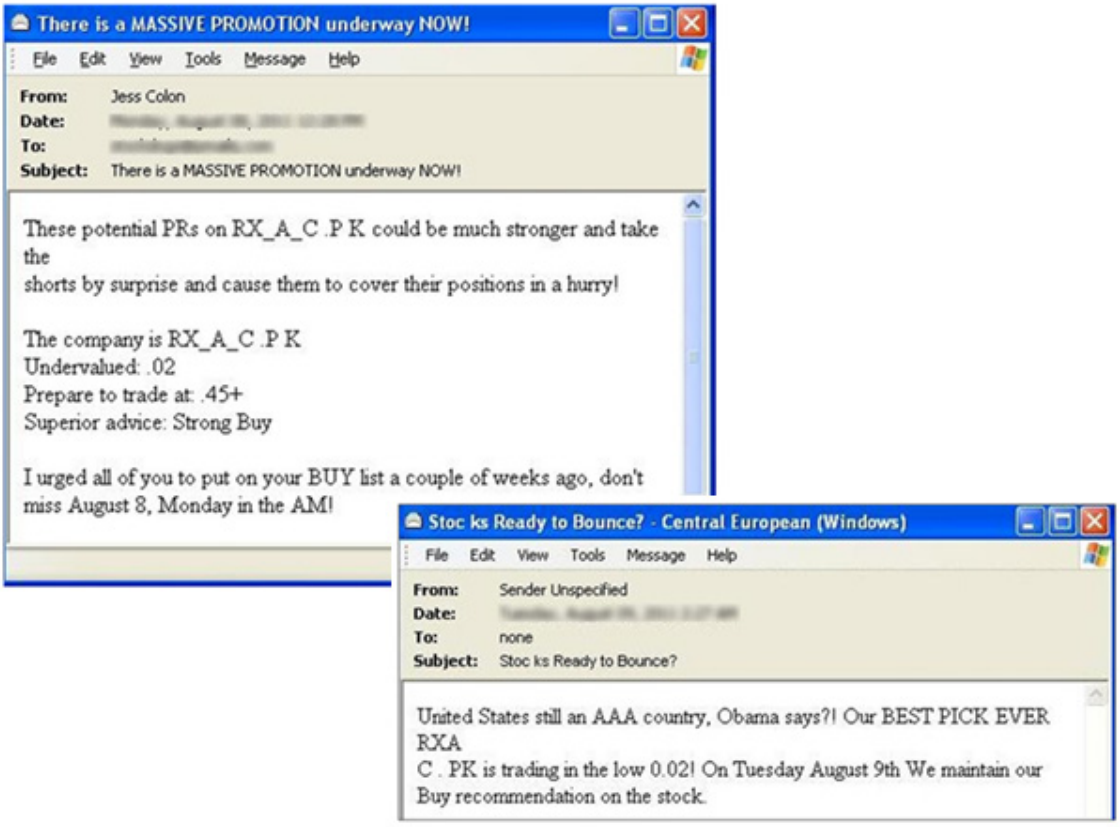


Figure 1: Examples of recent stock-spam email

This analysis was also published in a blog[2] post by Samir Patil on 10 August 2011.

Are MBR Infections Back in Fashion?

A Master Boot Record (MBR) is an area of the hard disk (usually the first sector) used by a computer to perform start up operations. It is one of the first things to be read and executed by the computer hardware when a computer is powered on, even before the operating system itself.

MBR infections offer great scope for deep infection and control of computers, which makes the idea attractive to malware creators. Contemporary MBR infection methods are a fairly complex affair usually executed by highly skilled individuals. This is probably one reason why after the creators of Trojan.Mebroot rediscovered the lost art of MBR infection, back in 2007 (based on work done by Soeder and Permeh of eEye Digital Security[3] in 2005 on BootRoot), not too many other malware creators have followed in their wake.

Mebroot was a significant piece of malware. It not only infected the MBR of the computer but also implemented direct disk access to write its own code into unused sectors of the hard disk and therefore place itself into an area that the host operating system wasn't even aware of. This type of low-level infection, coupled with a sophisticated rootkit, makes it difficult to detect and get rid of Mebroot from an infected computer.

While MBR infection has been a mainstay of Mebroot, another gang developed the highly sophisticated threat Backdoor.Tidserv (originally infected system driver files) back in the summer of 2010. Aside from Mebroot and Tidserv, there have been few other threats between 2008 and 2010 using the MBR infection technique, Trojan.Mebratix and Trojan.Bootlock being the only examples; it looked like MBR infections were going nowhere fast.

If we fast forward to August 2011, the picture for MBR malware has changed considerably. So far in 2011, we have seen Backdoor.Tidserv.M, Trojan.Smitnyl, Trojan.Fispboot, Trojan.Alworo, and Trojan.Cidox. This represents as

[2] *http://www.symantec.com/connect/blogs/global-debt-crises-news-drives-pump-and-dump-stock-scams*
[3] *http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-soeder.pdf*

many new MBR or boot time malware threats as there had been in the previous three years. This increase potentially indicates a comeback of boot time malware. What makes this exploit attractive in 2011 is that most of the "Research and Development" around this type of malware has been completed. With the release of the details for BootRoot and VBootkit, malware authors are able to take the research and proof of concept code and simply adapt them for their own needs.

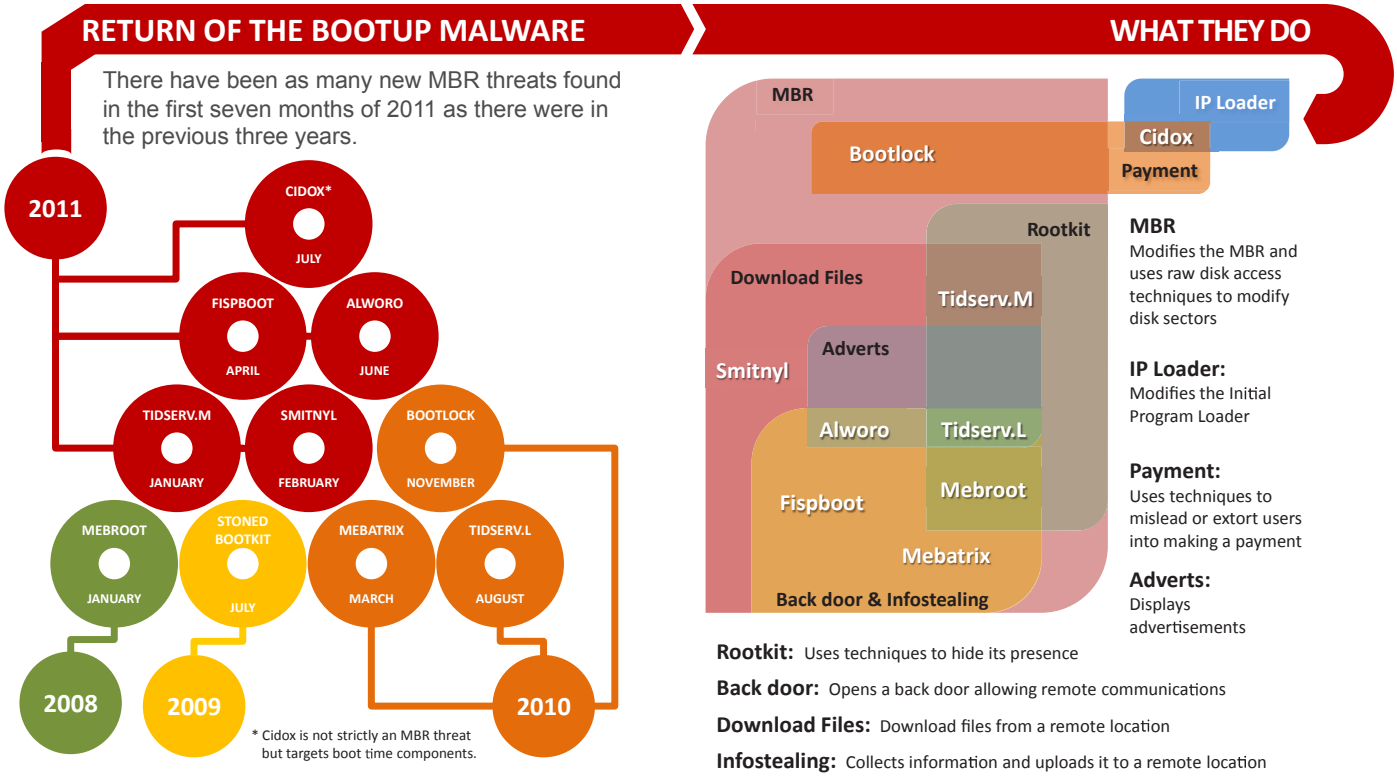


Figure 2: Infographic summary of MBR malware

According to analysis by the Symantec Intelligence team, it is evident that a number of MBR infecting malware families currently in circulation borrowed heavily from the BootRoot PoC. The arrival of short-lived ransomware type threats lends weight to the idea, because this type of malware can be considered as throw away code. Ransomware is made for a single purpose and are not expected to provide a long length of service so malware authors don't spend too much time and effort in creating and hiding them.

This is in sharp contrast to the more advanced examples of back door Trojans for whom the creators are trying to build a lasting and useful network of computers for profit. These are signs that the barrier to entry for this type of malware has been lowered. At this time, all the recent boot time malwares target the MBR with the exception of Trojan.Cidox which takes a slightly different approach. Instead of targeting the MBR, it infects the Initial Program Loader to achieve a similar overall effect; this is an innovation on the current MBR infection techniques.

Infecting the MBR is not a new technique per se; many of the old boot sector viruses from over a decade ago did something similar. The difference is modern MBR malware do so much more than just infecting the MBR. It certainly looks as if MBR malware is making a comeback in 2011.

This analysis was also published in a blog[4] post by Hon Lau on 8 August 2011. Additionally, Symantec has created a more detailed infographic[5] that summarizes these threats and what they do; an excerpt is shown in figure 2, above.

[4] *http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion-infographic*
[5] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mbr_malware_back.pdf*

Phishing Apple's iDisk

Apple's MobileMe is a collection of online services and software. Among its various services is a file-hosting service called iDisk. Recently, Symantec has recorded phishing sites that spoofed iDisk's Web page. The phishing sites were hosted on a free Web-hosting site.

So, what's in this service that interests phishers? The service is based on a paid subscription, with which files of up to 20 GB can be uploaded and shared. Phishers are looking to gain access to this service for free. This is an example of a phishing attack targeting user information for reasons other than financial gain.

Figure 3: Login prompt for MobileMe phishing Web site

The phishing site prompts the user to enter their password for logging in, as can be seen in figure 3. (In this case, the user ID was already populated on the phishing page.) After the password is entered, the page redirects to the legitimate Web page of Apple MobileMe with an error message for an invalid password, which creates the illusion that a common error had occurred.

The phishing URLs contained a query string in which a particular value represented a user's ID. Changing the value of this ID within the query string would accordingly be reflected on the phishing page. Below is a sample phishing URL:

`http://******.com/test?authenticate_username=******`

[Domain name and User name removed]

Typically, phishing sites are sent to customers through spam mails in which the message does not specify the customer's name. For example, spam email messages are addressed as "`Dear Valued Customer`" or "`Dear Member.`" By specifying the user ID, phishers are attempting to gain the user's confidence. This brings us to another question: from where do the phishers get these user IDs?

The user IDs are taken from email addresses. For example, in user001@example.com, phishers are considering "user001" as the user ID. The email addresses, on the other hand, are those that have been previously harvested by spammers. Although the user IDs retrieved in this manner may not necessarily represent an actual MobileMe user ID, phishers are simply trying their luck by targeting a large number of users.

This analysis was also published in a blog[6] post by Mathew Maniyara on 14 July 2011.

[6] *http://www.symantec.com/connect/blogs/phishing-apple-s-idisk*

Phishing Brazilian Brands

Symantec keeps track of the brands targeted by phishing and monitors trends in the countries in which the brand's parent company is based. Over the past couple of months, phishing sites have been increasingly targeting Brazilian brands. The number of phishing sites on Brazilian brands made up about 5 percent of all phishing sites. This is an increase of nearly three times that of the previous month. The phishing Web pages were in Brazilian Portuguese. The most targeted brand in these phishing sites was a social networking site.

Below are some noteworthy statistics on the trend observed to date, as highlighted in figure 4, below:

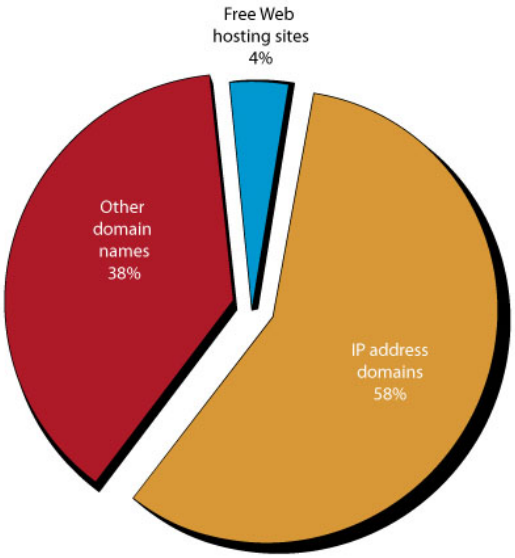


Figure 4: Types of domain names used in phishing Web sites for Brazilian brands

- The majority of the phishing on Brazilian brands, approximately 58 percent, used IP domains (e.g., domains such as http://255.255.255.255).
- Twelve Web-hosting sites were used to host 4 percent of the phishing sites on Brazilian brands.
- There were several banks attacked in phishing and the banking sector made up about 39 percent of the brands targeted. Phishing of the social networking sector primarily targeted one single brand and comprised 61 percent of the total. The remaining phishing sites (approximately 0.5 percent) spoofed an airlines brand.
- Approximately 64 percent of the phishing sites were created using automated phishing toolkits. The remaining 36 percent were unique URLs.

As the majority of the phishing attacks came from automated toolkits, we understand that phishers are trying to target more Internet users from Brazil. With the possession of these toolkits, phishers are able to create phishing sites in large numbers by randomizing URLs. Below are two randomizing URLs used in the toolkits:

```
http://***.***.***.***/~namo/login011/?accounts/ServiceLogin?
http://***.***.***.***/~namo/login008/?accounts/ServiceLogin?
```

[IP addresses removed]

The Truth Behind the Shady RAT

McAfee recently published a report about what they called Operation Shady RAT[7], focusing on a series of what some may call "advanced persistent threat" attacks. The attacks were dubbed in some quarters as "one of the largest series

[7] *http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109?*

of cyber attacks ever." While quite a bit of data was presented regarding the potential scale of these attacks, details on the threats and how the attacks were staged were somewhat limited.

The Symantec Intelligence team analyzed this threat and identified the initial attack vectors, the threats used and how the attack was staged. In addition, we have also uncovered what appears to be the same information source about the victims of the attacks that was used as the basis of the original report. This information is freely available on the attackers' command and control site, which is a strange oversight considering this type of attack is often described as "advanced" or "sophisticated."

The attack mainly comprises of three stages, which are detailed below.

STAGE 1:
Target organizations are selected and then emails are created and sent to individuals within those organizations. The emails follow the typical targeted attack modus operandi — that is they contain some subject or topic that may be of interest to the recipient, such as rosters, contact lists, budgets, and so forth. The attached file contains the details promised in the email text, as part of a social engineering ploy. In our investigations we've uncovered many such emails covering a whole gamut of topics.

Some recent examples of emails used in these attacks can be seen in figure 5, below. These emails contain various attachments, typically Microsoft Office files such as Word documents, Excel spreadsheets, PowerPoint presentations, and PDF documents. These files are loaded with exploit code, so that when the user opens the file the exploit code is executed, resulting in the computer becoming compromised.

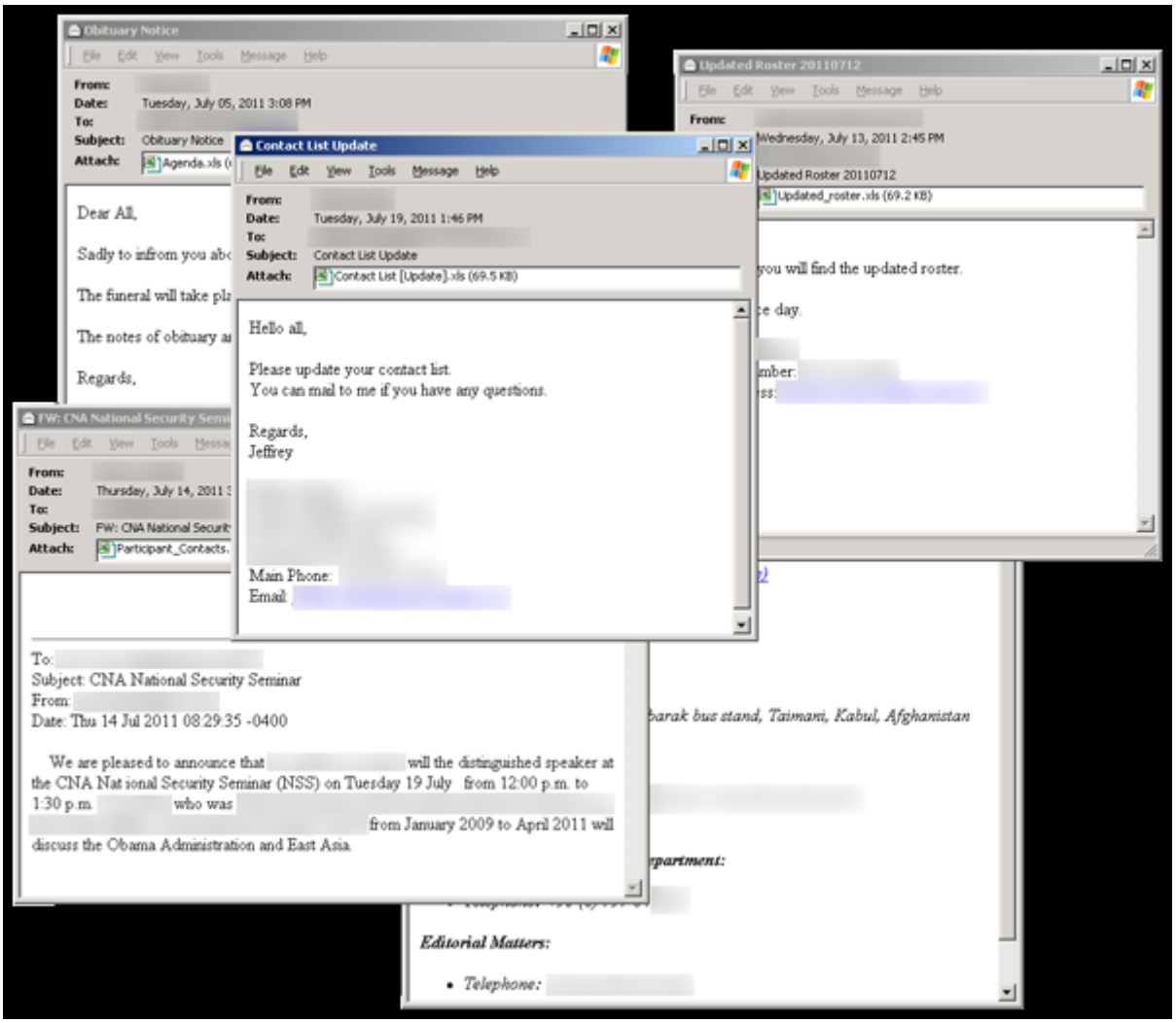


Figure 5: Examples of emails related to the attacks

Example attachment names included:

- `Participant_Contacts.xls`
- `2011 project budget.xls`
- `Contact List -Update.xls`
- `The budget justification.xls`

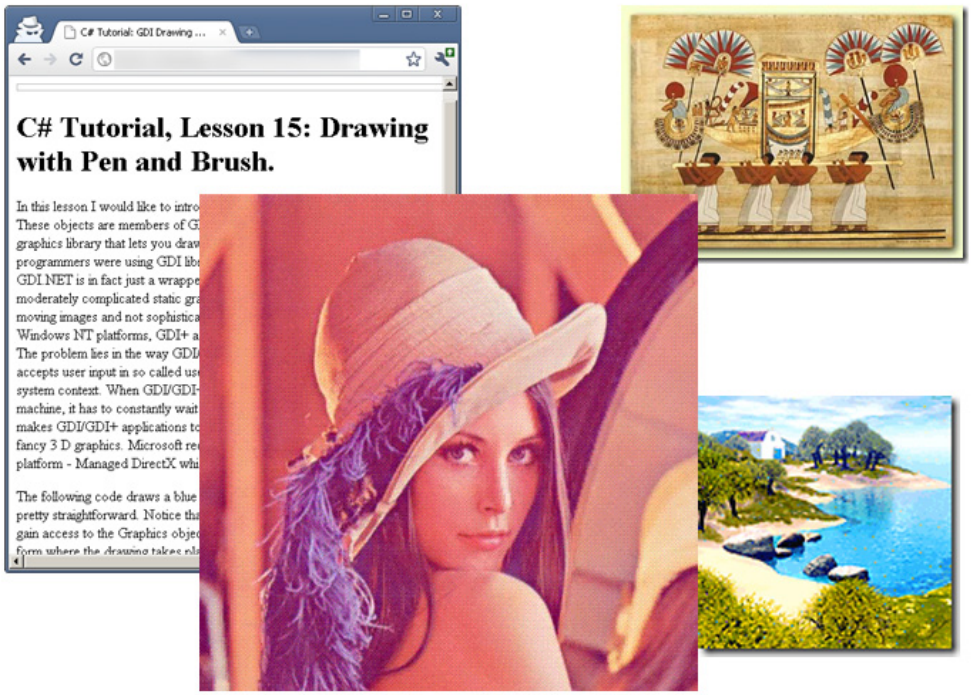
In the Excel files, we have seen the old, but clearly still effective Microsoft Excel 'FEATHEADER' Record Remote Code Execution Vulnerability[8] (detected by Bloodhound.Exploit.306[9]) being exploited. Once the file is opened on an unpatched computer, a clean copy of an Excel file is dropped and opened so that the user is not suspicious. A Trojan is also dropped and executed. One possible tell-tale sign of this exploit is that Excel appears to hang for a short time before it resumes, and the application may even crash and restart.

STAGE 2:
Once the Trojan is installed, it will attempt to contact a remote site that is hardcoded into the Trojan itself. Some recently used examples include:

- `www.comto[REMOVED].com/wak/mansher0.gif`
- `www.kay[REMOVED].net/images/btn_topsec.jpg`
- `www.swim[REMOVED[.net/images/sleepyboo.jpg`
- `www.comto[REMOVED].com/Tech/Lesson15.htm`

The first thing you will notice is that the URLs are pointing at image and HTML files. At first glance, they don't seem all that suspicious. This is an interesting ploy used by the attackers to hide the commands. Many firewalls are configured to allow image and HTML files to pass through HTTP traffic.

Without close inspection, based on the context provided by the Trojan sample, these images and HTML files look totally legitimate. Some examples are highlighted in figure 6, below.



[8] *http://www.securityfocus.com/bid/36945*
[9] *http://www.symantec.com/security_response/writeup.jsp?docid=2009-111306-5541-99*

Figure 6: Examples of images containing hidden commands found on the command and control server

Upon closer inspection of the file and the Trojan code, we can see that there are commands hidden in the image using steganography. These commands are totally invisible to the human eye, since the bits representing the commands are mathematically built into the data representing the image.

In the versions of the Trojans that are downloading HTML files, the commands are hidden in HTML comments that look like gibberish, but are actually encrypted commands that are further converted into base-64 encoding, as can be seen in the examples shown in figure 7, below.

```
<!-- {685DEC108DA731F1} -->
<!-- {685DEC108DA73CF1} -->
<!-- {eqNBb-Ou07WM} -->
<!-- {eqNBb-Ou07iM} -->
<!-- {eqNBb-Ou01OMOO++} -->
<!-- {eqNBb-Ou11O+} -->
<!-- {eqNBb-Ou2Ra+} -->
<!-- {uGu~iWA1,Q(iNyn'/} -->
<!-- {ujQ~iY,UnQ[!,hboZWg} -->
<!-- {ujQ~iY,UnQ[!,hmoZWg} -->
<!-- {ujQ~iY,UnQ[!,hvoZWg} -->
```

Figure 7: Examples of encoded commands hidden within HTML and image files

While these commands are clearly visible to a user if they view the HTML code in a text editor, they look completely harmless, and indeed are harmless unless the file is parsed by the Trojan on a compromised computer. The commands may be one of the following:

> **`run: {URL/FILENAME}`** — Downloads an executable to the `%Temp%` folder and then executes the new program.
>
> **`sleep:{NUMBER}`** — Sleeps for a specified amount of time, in minutes.
>
> **`{IP ADDRESS}:{PORT NUMBER}`** — Causes the Trojan to connect to a remote IP on the specified port. This command is really useful from the attacker's point of view, since it opens a direct connection to the specified IP address through the specified port number. Once the Trojan has opened the remote connection, after receiving the `{IP ADDRESS}:{PORT}` command, we are set for the next stage of the attack.

STAGE 3:

When the Trojan connects to a remote computer using the {IP ADDRESS}:{PORT} command, it establishes a remote shell with the computer. This enables the attacker at the remote site to directly issue shell commands to be run on the compromised computer. Of course all of this activity is invisible to the end user, since the shell is hidden and is a low-tech and lightweight way of accessing the computer.

When the Trojan connects to the remote IP on the specified port number, it waits to receive an "active" command. Once received, the back door sends the following string, which is a form of a handshake between the Trojan and the controller:

```
"/*\n
@***@*@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@>>>>\*\n\r"
```

The Trojan then copies the file %System%\cmd.exe (a DOS shell) to %Temp%\svchost.exe and then uses the copied file to open a remote shell on the compromised computer.

Next, the Trojan periodically checks with the remote server for one of the following commands:

`gf:{FILENAME}` — Retrieves a file from the remote server.

`pf:{FILENAME}` — Uploads a file to the remote server.

`http:{URL}.exe` — Retrieves a file from a remote URL, beginning with http and ending in .exe. The remote file is downloaded and executed.

`taxi: {COMMAND}` — Sends a command from the remote server.

`slp:{RESULT}` — Sends the results of the command executed above to the remote server to report the status.

This small collection of commands is enough for an attacker to stage a comprehensive breach into the affected organization. Any functions not available to the attacker in the Trojan itself can be easily downloaded onto the compromised computer and executed at will. Collected data is then simply uploaded back to the remote attacker using the `pf` command.

Victims of the attacks

A significant number of organizations worldwide were seemingly affected by this particular series of attacks. The attackers not only failed to secure their server properly, but also installed various Web traffic analysis tools to monitor their progress. This however makes it much easier to investigate such attacks. For example, on one of the sites we were able to see the statistics about computers contacting the command and control server to download command files; an example of this is shown in figure 8. Based on this information, we were also able to determine the organizations affected by this threat.

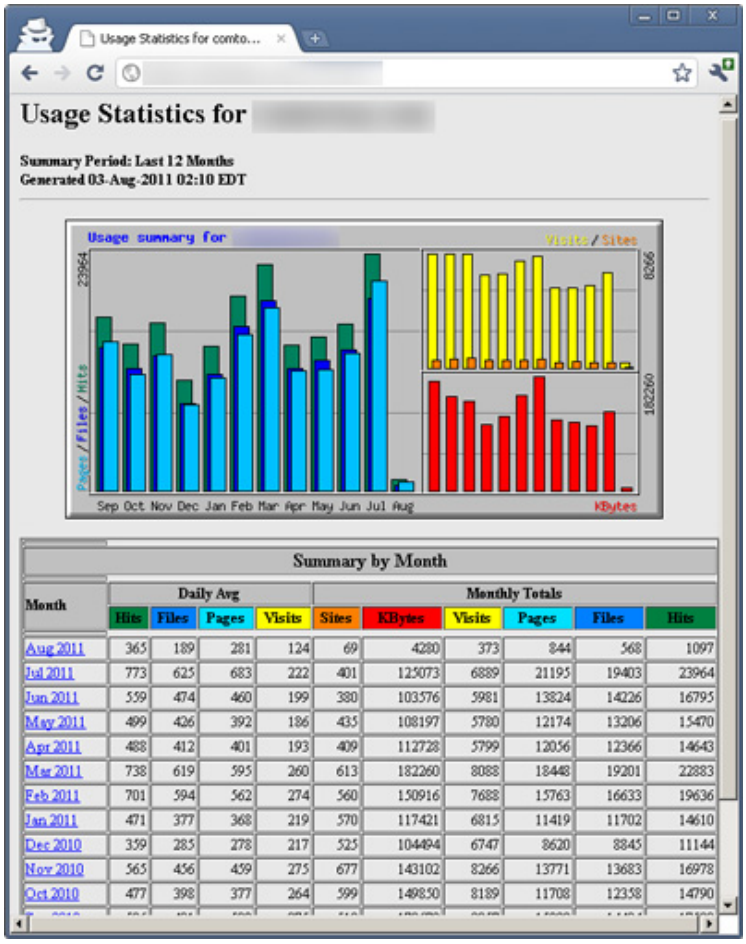


Figure 8: Example of Web traffic analysis tools installed on C&C Web server

As already discussed in the public domain, the victims ranged from government agencies to private companies. What's still unclear is the type of information the attackers were targeting. Due to the variety of organizations and individuals impacted, there is no clear motive. Not only are the victims located in various places around the globe, so too are the servers involved in these attacks.

Conclusions

While this attack is indeed significant, it is one of many similar attacks taking place daily. Continually, there are other malware groups targeting organizations in a similar manner in order to gain entry and pilfer secrets. While there is a need for information, there will always be those ready to supply it. We may not always know the true motivations and identities of those behind these attacks, but we can work to exploit mistakes they make in order to get a better view of what they are doing and bring us one step closer to tracking them down.

Going back to the earlier question, is the attack described in Operation Shady RAT a truly advanced persistent threat? We would contend that it isn't, but perhaps it didn't need to be advanced in order to succeed. However, considering the errors made in configuring the servers behind the command and control channels, and the relatively non-sophisticated malware and techniques used in this case, the people behind it are persistent, but no more so than the myriad of other malware groups out there such as those behind Zeus and Tidserv.

This analysis was also published in a blog[10] post by Hon Lau on 4 August 2011.

Spammers take advantage of Unicode normalisation to hide URLs

Spammers are never idle when it comes to finding new ways to bypass mail filters - after all, this is crucial to a spammer's success. Recently we've seen a low, but steady, number of spam messages where spammers are replacing characters in URLs (which point to spam sites) with Unicode characters which look similar or identical. This is yet another way of obfuscating URLs in an attempt to make it more difficult to analyse URLs. To understand how this technique works, a bit of knowledge of the Unicode standard is helpful. As well as specifying a large repertoire of characters, Unicode also provides normalisation rules for converting similar and/or equivalent characters to a single form.

For example, under various Unicode normalisation forms, an encircled number is considered equivalent to the corresponding ordinary number. This latest spammer obfuscation technique relies on the HTML rendering engine in mail clients (or Web browser for Web-based email) applying the appropriate Unicode normalisation to URLs.

For example, a spam message contains the following URL:

```
http://example.ⅼy/xyz
```

At first glance, the period or dot might look like a normal dot character, but it has actually been replaced with Unicode character **U+2024** ("ONE DOT LEADER"). The " **ⅼ** " in the top-level domain also appears like a normal Latin letter "l", but is actually Unicode character **U+217C** ("SMALL ROMAN NUMERAL FIFTY"). When a Web browser or mail client HTML rendering engine processes this URL, it typically applies Unicode normalization to it, replacing the "ONE DOT LEADER" character with a normal dot, and replacing the "SMALL ROMAN NUMERAL FIFTY" with a normal "l" character, allowing the user to visit the spam site.

A schematic for the process can be seen in figure 9, below.

[10] *http://www.symantec.com/connect/blogs/truth-behind-shady-rat*

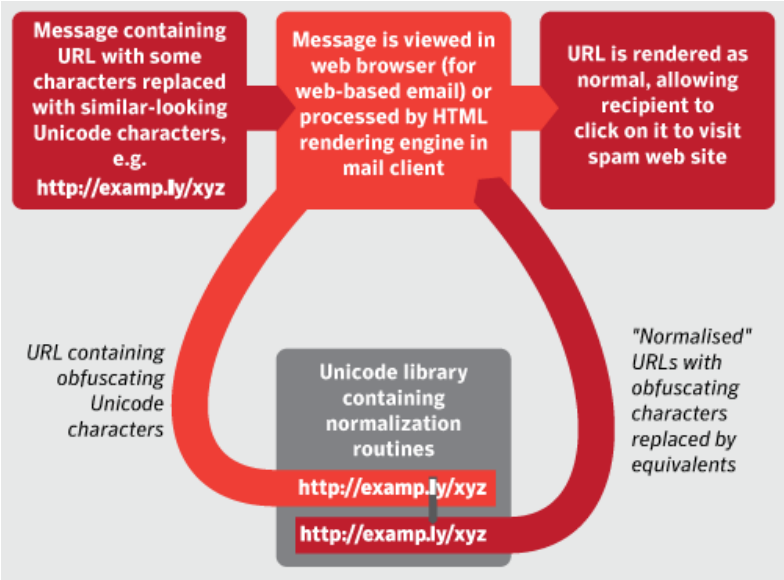


Figure 9: Infographic describing the Unicode normalization process

In a sense, this is similar to IDN (Internationalized Domain Name) homograph attacks[11] where similar-looking Unicode characters are used to lead users to fake sites, often for phishing. However, this technique differs as it involves using similar Unicode characters to obfuscate a site rather than fake or spoof a site.

Symantec.cloud and Symantec Brightmail customers are protected from these attacks by our URL filtering technologies which support handling these characters.

This analysis was also published in a blog[12] post by Nicholas Johnston and Francisco Pardo on 4 August 2011.

[11] *http://www.symantec.com/connect/blogs/spammers-taking-advantage-idn-url-shortening-services*
[12] *http://www.symantec.com/connect/blogs/spammers-take-advantage-unicode-normalisation-hide-urls*

Global Trends & Content Analysis

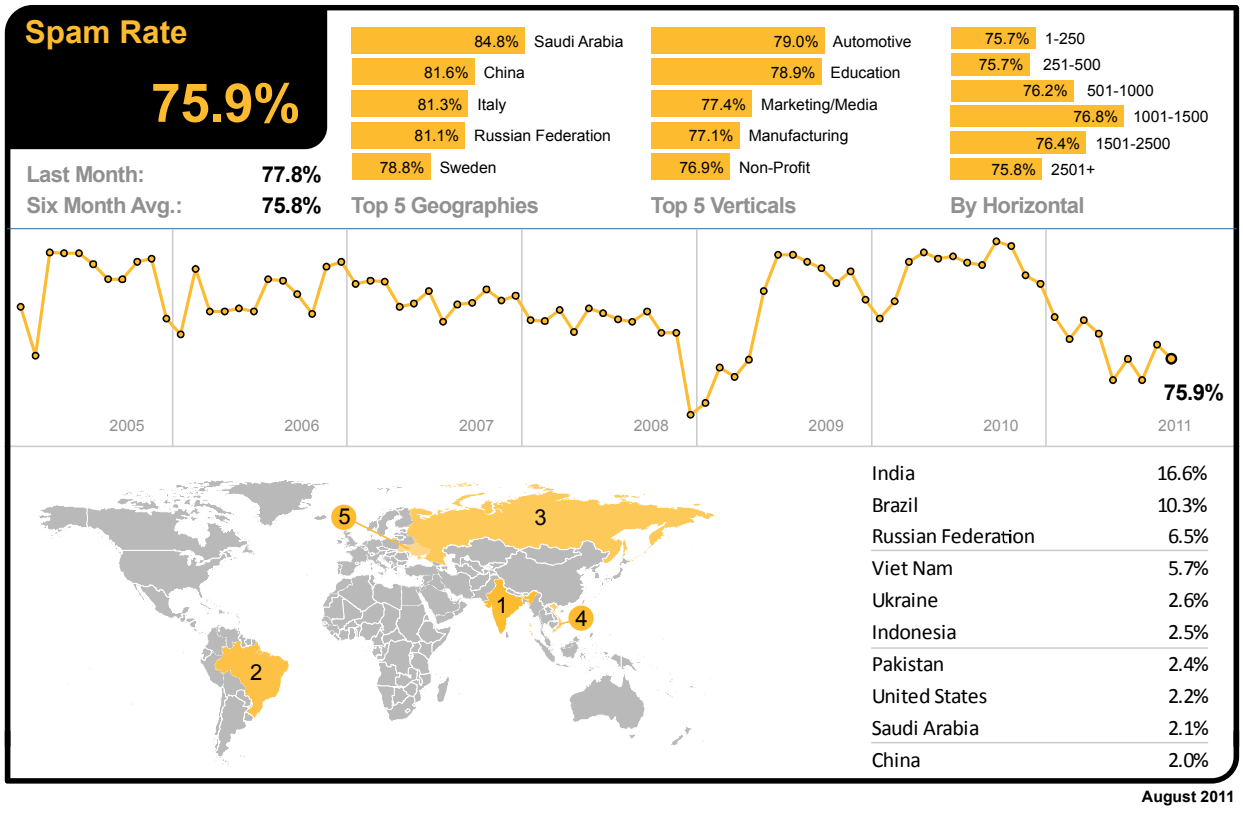
Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is also able to detect new and sophisticated targeted threats.

Data is collected from over 8 billion email messages and over 1 billion Web requests which are processed per day across 15 data centers, including malicious code data which is collected from over 130 million systems in 86 countries worldwide. Symantec intelligence also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give the Symantec Intelligence 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. If there is a malicious attack about to hit, we know about it first. We block it; we keep it from affecting our customers.

Spam Analysis

In August 2011, the global ratio of spam in email traffic declined to 75.9 percent (1 in 1.32 emails); a decrease of 1.9 percentage points when compared with July 2011.



As the global spam level diminished in August 2011, Saudi Arabia remained the most spammed geography, with a spam rate of 84.8 percent, and China overtook Russia to become the second most-spammed. The largest increase in spam in China was attributed to the IT Services sector (89.3 percent of email blocked as spam). Moreover, 90 percent of global spam is in English, but Russian is the most common non-English spam language and accounts for approximately 1.7 percent of spam; Chinese[13] spam now accounts for approximately 0.6 percent of global spam.

[13] *http://www.symantec.com/connect/blogs/rise-chinese-spam*

In the US, 75.8 percent of email was spam and 75.0 percent in Canada. The spam level in the UK was 76.5 percent. In The Netherlands, spam accounted for 77.4 percent of email traffic, 75.8 percent in Germany, 76.1 percent in Denmark and 73.7 percent in Australia. In Hong Kong, 75.2 percent of email was blocked as spam and 73.4 percent in Singapore, compared with 72.8 percent in Japan. Spam accounted for 74.0 percent of email traffic in South Africa and 77.0 percent in Brazil.

In August, the Automotive industry sector continued to be the most spammed industry sector, with a spam rate of 79.0 percent. Spam levels for the Education sector reached 78.9 percent and 75.5 percent for the Chemical & Pharmaceutical sector; 75.7 percent for IT Services, 75.7 percent for Retail, 75.4 percent for Public Sector and 75.3 percent for Finance.

Global Spam Categories

The most common category of spam in August was pharmaceutical related, but the second most common was related to adult/dating spam. Examples of many of these subjects can be found in the subject line analysis, below.

Category Name	August 2011	July 2011
Pharmaceutical	40.0%	47.0%
Adult/Sex/Dating	19.0%	14.5%
Watches/Jewelry	17.5%	7.5%
Unsolicited Newsletters	11.5%	7.5%
Casino/Gambling	7.0%	3.5%
Unknown/Other	2.5%	2.0%
Degrees/Diplomas	1.5%	2.5%
Jobs/Recruitments	1.0%	10.5%
Discount Products/Software	0.5%	<0.5%
Scams/Fraud/419	0.5%	<0.5%

Spam Subject Line Analysis

In the latest analysis, adult-related dating spam accounted for fewer of the most common spam subject lines in August, with blank subject lines being the most common, closely followed by pharmaceutical related subjects.

Rank	August 2011 Total Spam: Top Subject Lines	No. of Days	July 2011 Total Spam: Top Subject Lines	No. of Days
1	(blank subject line)	31	drop me a line	30
2	ED-Meds-Antidepressants-And-Pain Relief-Meds-8O%-OFF	31	r u online now?	30
3	Buy Advanced Penis Enlargement Pill now, it is selling fast.	31	hi darling..	30
4	Made of the most potent clinically proven natural herbs.	31	new email	30
5	Permanently increases length and width of your erection. Advanced Penis Enlargement Pill.	31	found you :)	30
6	Advanced Penis Enlargement Pill. Permanently increases length and width of your erection.	31	im online now	30
7	my hot pics :)	23	my new pics :)	30
8	found you :)	23	my new email	30
9	new pics for you..	24	my hot pics :)	30
10	im online now	23	I'm online now…	30

Spam URL TLD Distribution

The proportion of spam exploiting URLs in the .RU top-level domain fell by 3.5 percentage points in August, with the largest increase relating to spam URLs in the .com TLD.

TLD	August	July	Change (% points)
.com	57.6%	54.9%	+2.7
.ru	7.1%	10.6%	-3.5
.info	18.4%	18.3%	+0.1
.net	5.8%	6.2%	-0.4

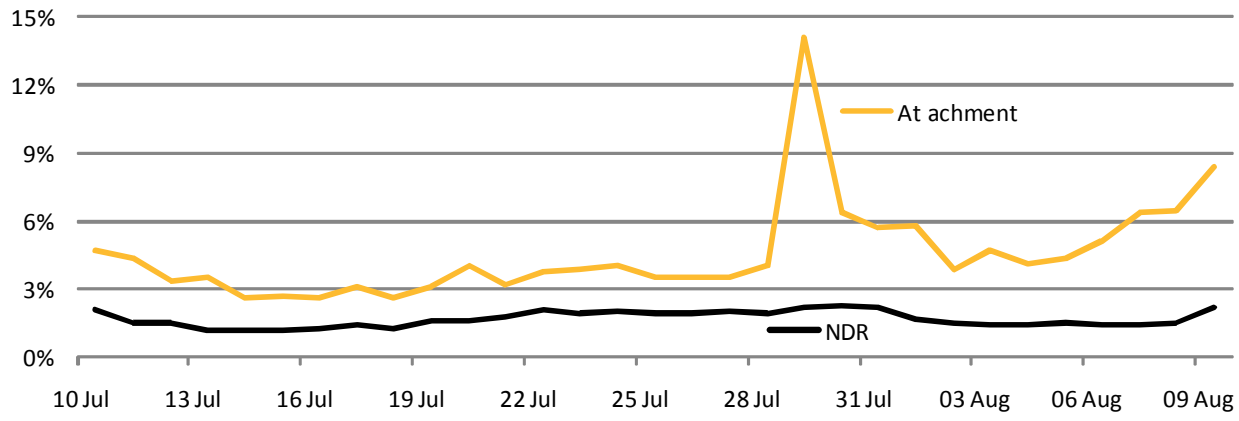
Average Spam Message Size

In August, almost half of all spam was 5Kb in size or less, compared with approximately two-thirds in July. Spam with attachments (including malware such as generic polymorphic malware hidden in ZIP file attachments), including image attachments often used in pharmaceutical spam, accounted for the increase in spam between 5Kb and 10Kb in size.

Message Size	August	July	Change (% points)
0Kb – 5Kb	49.7%	65.1%	-15.4
5Kb – 10Kb	35.2%	21.2%	+14.0
>10Kb	15.0%	13.7%	+1.3

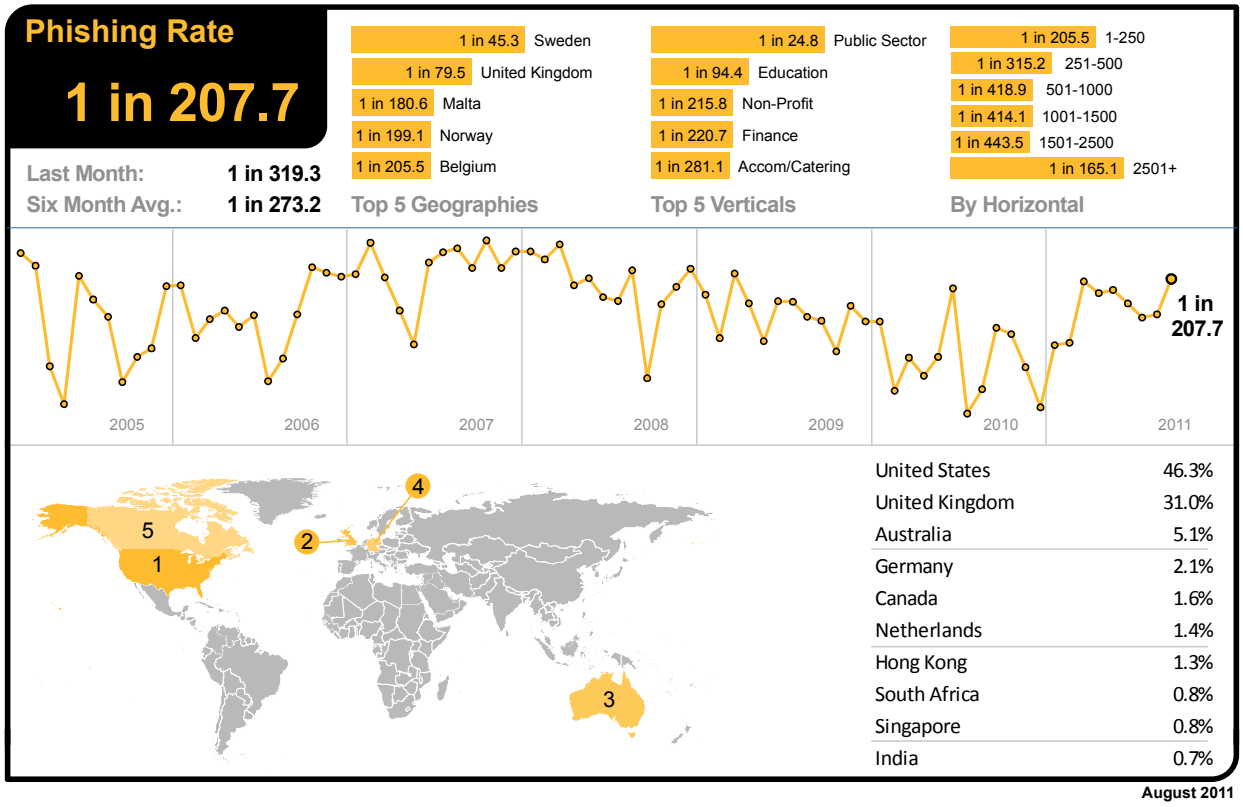
Spam Attack Vectors

It can be seen in the chart below that a major spike in attachment spam occurred on 29 July, but unlike a similar event on 29 June, this did not result in a surge in NDR spam (spam related non-delivery reports), which would be expected following a widespread dictionary attack. The growth in attachments also related to a large volume of pharmaceutical spam that contained image file attachments.



Phishing Analysis

In August, phishing email activity increased by 0.01 percentage points since July 2011; one in 319.3 emails (0.313 percent) comprised some form of phishing attack.



Phishing attacks in Sweden increased to overtake the UK and become the most targeted geography for phishing in August, with one in 45.3 emails identified as phishing. Phishing in the UK also increased, making it the second most targeted country, with one in 79.5 emails identified as phishing attacks. In Sweden, 51.6 percent of phishing attacks related to one well-known financial services brand, popular for servicing international money transfers and money orders.

Phishing levels for the US were one in 999.3 and one in 229.9 for Canada. In Germany phishing levels were one in 928.6, one in 508.2 in Denmark and one in 295.9 in The Netherlands. In Australia, phishing activity accounted for one in 914.5 emails and one in 2,178 in Hong Kong; for Japan it was one in 8,115 and one in 2,474 for Singapore. In Brazil, one in 445.7 emails was blocked as phishing and in South Africa the rate fell to 1 in 256.9.

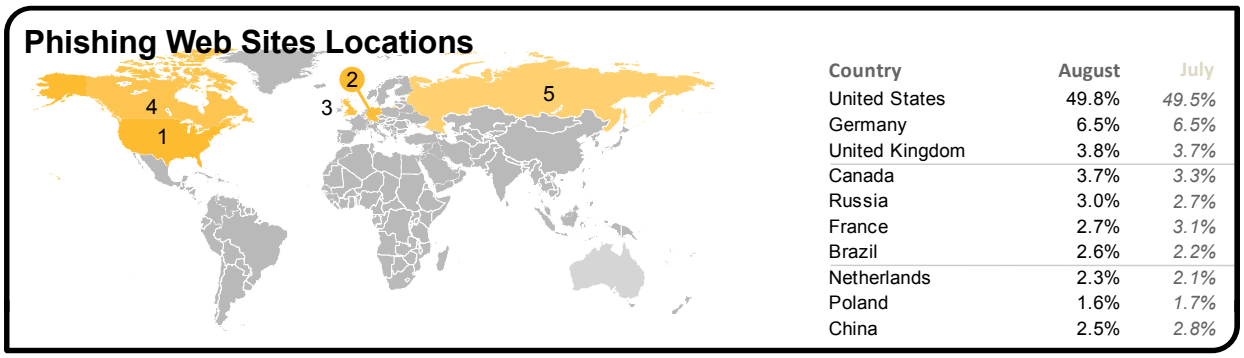
The Public Sector remained the most targeted by phishing activity in August, with one in 24.8 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 720.3 and one in 446.0 for the IT Services sector; one in 410.5 for Retail, one in 94.4 for Education and one in 220.7 for Finance.

Analysis of Phishing Web sites

The number of phishing Web sites decreased by 6.75 percent in August. The number of phishing Web sites created by automated toolkits decreased by about 18.3 percent. The number of unique phishing URLs also decreased by 1.67 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), increased by 18.34 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 9 percent of all phishing Web sites, a decrease of 16.81 percent from the previous month. The number of non-English phishing sites saw an increase of 9.07 percent.

The most common non-English languages identified in phishing Web sites during August included Portuguese, French, Italian and Spanish.

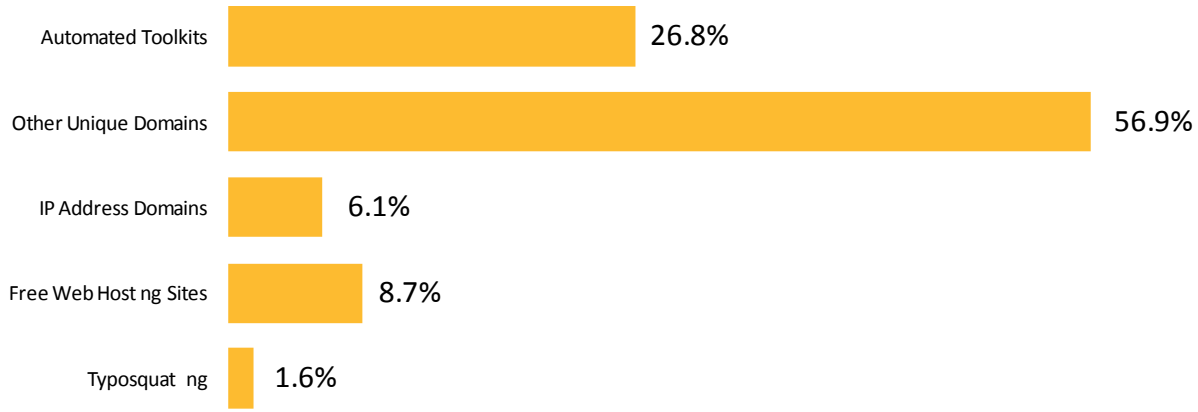
Geographic Location of Phishing Web Sites



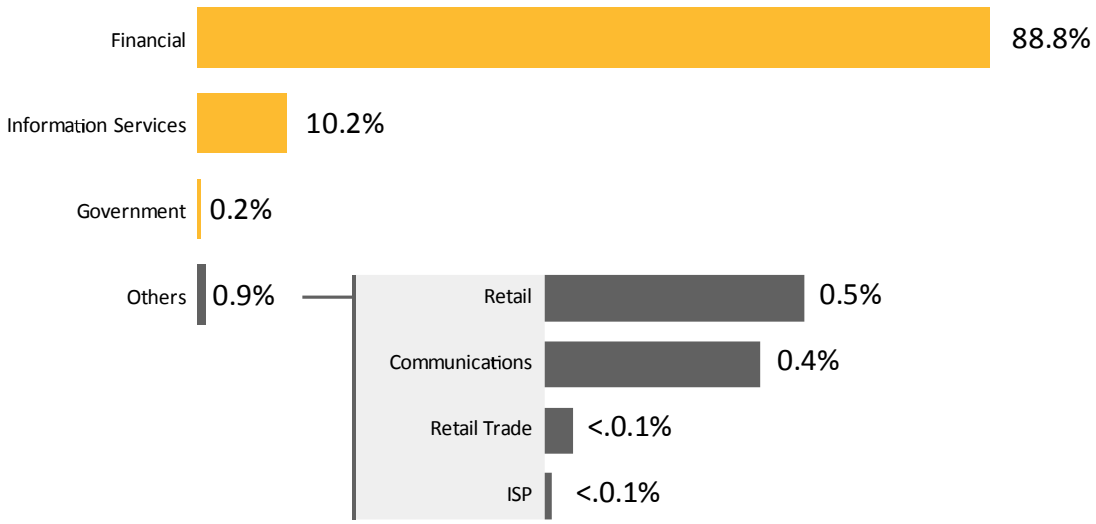
Country	August	July
United States	49.8%	49.5%
Germany	6.5%	6.5%
United Kingdom	3.8%	3.7%
Canada	3.7%	3.3%
Russia	3.0%	2.7%
France	2.7%	3.1%
Brazil	2.6%	2.2%
Netherlands	2.3%	2.1%
Poland	1.6%	1.7%
China	2.5%	2.8%

August 2011

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry Sector



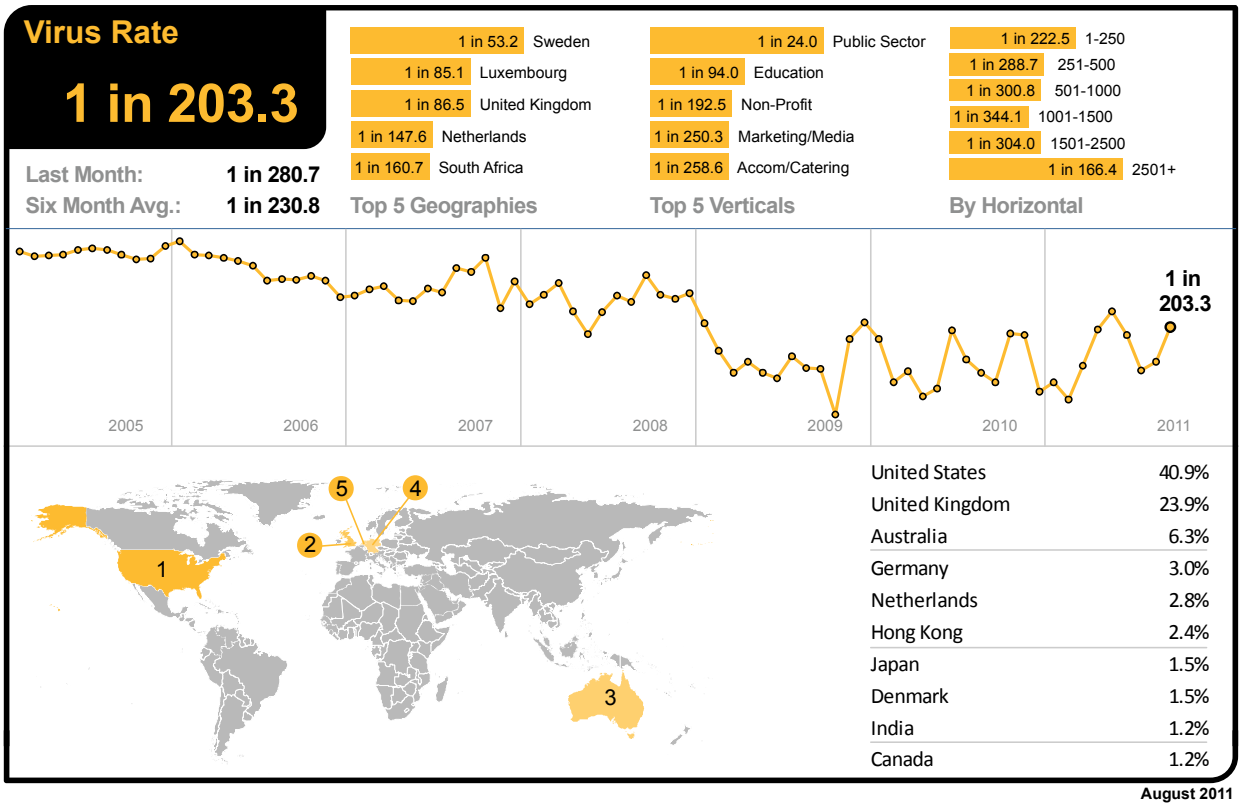
Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 203.3 emails (0.49 percent) in August, an increase of 0.14 percentage points since July 2011.

In August, 37.1 percent of email-borne malware contained links to malicious Web sites, a decrease of 7.6 percentage points since July 2011. Continuing the widespread attacks that were identified in July, a large proportion of emails contained generic polymorphic malware variants and accounted for 18.5 percent of all email-borne malware in August, compared with 23.7 percent in July; many included attached ZIP files that contained the generic malware.



Email-borne malware attacks increased to one in 53.2 emails in Sweden, propelling the country to the top of the list with the highest ratio of malicious emails in August. Luxembourg was the second most geography under fire in August, with one in 85.1 emails was identified as malicious in August. In Sweden, 44.6 percent of email-borne malware was identified as generic polymorphic malware, characteristic of that described in the Symantec Intelligence report[14] for July 2011.

In the UK one in 86.5 emails was blocked as malicious, and virus levels for email-borne malware reached one in 611.1 in the US and one in 219.6 in Canada. In Germany virus activity reached one in 369.2, one in 444.4 in Denmark and in The Netherlands one in 147.6. In Australia, one in 797.0 emails were malicious and one in 744.2 in Hong Kong; for Japan it was one in 1,912, compared with one in 918.0 in Singapore. In Brazil, one in 392.3 emails in contained malicious content and in South Africa the rate dropped to 1 in 160.7.

With one in 24.0 emails being blocked as malicious, the Public Sector remained the most targeted industry in August. Virus levels for the Chemical & Pharmaceutical sector were one in 334.6 and one in 345.3 for the IT Services sector; one in 374.6 for Retail, one in 94.0 for Education and one in 383.0 for Finance.

[14] *http://www.symanteccloud.com/mlireport/SYMCINT_2011_07_July_FINAL-EN.pdf*

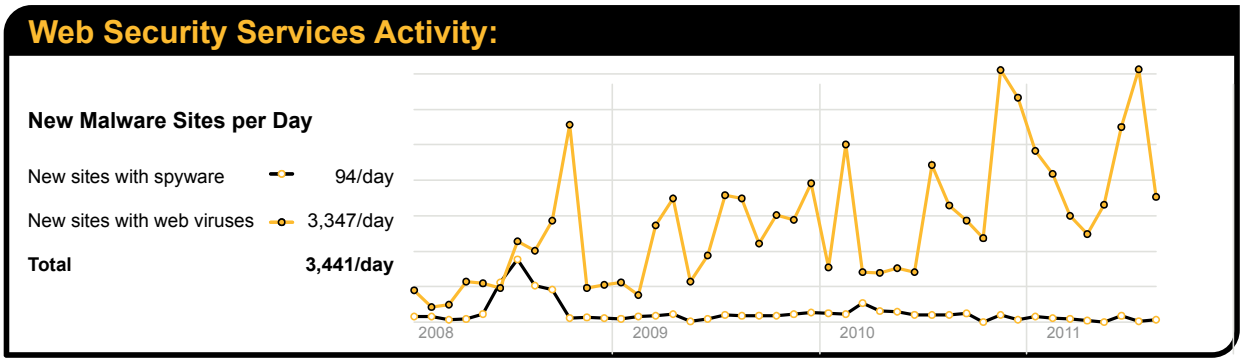
The table below shows the most frequently blocked email-borne malware for August, many of which take advantage of malicious hyperlinks. Overall, 18.5 percent of email-borne malware was associated with variants of generic polymorphic malware, including Bredolab, Sasfis, SpyEye and Zeus variants.

Malware Name	% Malware
Exploit/SuspLink-e958	7.20%
W32/Bredolab.gen!eml	4.90%
Exploit/SuspLink.dam	4.34%
W32/Generic.dam	2.09%
W32/Generic-6ac4	2.06%
Exploit/MimeBoundary003	1.69%
W32/Netsky.c-mm	1.56%
Exploit/Link-e88c	1.47%
VBS/Generic	1.36%
W32/Netsky.P-mm	1.34%

Web-based Malware Threats

In August, Symantec Intelligence identified an average of 3,441 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 49.4 percent since July 2011. 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 34.6 percent of all malicious domains blocked were new in August; a decrease of 1.3 percentage points compared with July 2011. Additionally, 17.3 percent of all Web-based malware blocked was new in August; a decrease of 3.8 percentage points since the previous month.



The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during August 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 42.4 percent of blocked Web activity in August. 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 17.6 percent of URL-based filtering activity blocked, equivalent to approximately one in every six 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 8.2 percent of URL-based filtering blocks in August. Streaming media is increasingly popular when there are major sporting events or high profile international news stories, such as the riots that affected the UK in August. 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 12 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	42.4%	Trojan.Gen	28.9%	PUP:Generic.168911	25.4%
Social Networking	17.6%	Dropped:Rootkit.49324	19.5%	PUP:Generic.182547	6.5%
Streaming Media	8.2%	Gen:Variant.Dropper.26	7.3%	PUP:Clkpotato!gen4	5.8%
Computing and Internet	4.4%	VBS/Generic	6.6%	PUP:Generic.178280	5.5%
Chat	4.3%	Infostealer.Gampass	4.7%	PUP:Agent.NGZ	4.4%
Peer-To-Peer	2.1%	Trojan:GIF/GIFrame.gen!A	4.2%	PUP:Generic.183433	3.7%
Search	1.9%	Dropped:Trojan.PWS.OnlineGames.KDVN	2.0%	Application.Generic.190952	3.7%
Hosting Sites	1.9%	VBS.LoveLetter.CI	1.7%	PUP:SW.9231	3.1%
Games	1.7%	W32.Almanahe.B	1.1%	PUP:Agent.NFU	2.7%
News	1.6%	Trojan.Script.474851	0.9%	PUP:Generic.173909	2.7%

August 2011

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[15]	% Malware
W32.Ramnit!html	8.68%
W32.Sality.AE	8.44%
Trojan.Bamital	8.10%
W32.Ramnit.B!inf	6.84%
W32.Downadup.B	3.63%
W32.SillyFDC.BDP!lnk	2.59%
W32.Virut.CF	2.58%
W32.Almanahe.B!inf	2.38%
W32.SillyFDC	1.75%
Trojan.ADH.2	1.74%

The most frequently blocked malware for the last month was W32.Ramnit!html. This is a generic detection for .HTML files infected by W32.Ramnit[16], a worm that spreads through removable drives and by infecting executable files. The worm spreads by encrypting and then appending itself to files with .DLL, .EXE and .HTM extensions. Variants of the Ramnit worm accounted for 15.8 percent of all malicious software blocked by endpoint protection technology in August.

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

[16] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99&tabid=2*

For much of 2010, W32.Sality.AE[17] had been the most prevalent malicious threat blocked at the endpoint.

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. Approximately 17.4 percent of the most frequently blocked malware last month was identified and blocked using generic detection.

[17] *http://www.symantec.com/connect/blogs/sality-whitepaper*

Best Practice Guidelines for Enterprises

1. **Employ defense-in-depth strategies**: Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.
2. **Monitor for network threat, vulnerabilities and brand abuse.** Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious site reporting.
3. **Antivirus on endpoints is not enough:** On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:
    - Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
    - Browser protection for protection against obfuscated Web-based attacks;
    - Consider cloud-based malware prevention to provide proactive protection against unknown threats;
    - File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
    - Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
    - Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
    - Device control settings that prevent and limit the types of USB devices to be used.
4. **Use encryption to protect sensitive data:** Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.
5. **Use Data Loss Prevention to help prevent data breaches:** Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.
6. **Implement a removable media policy**. Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.
7. **Update your security countermeasures frequently and rapidly:** With more than 286M variants of malware detected by Symantec in 2010, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.
8. **Be aggressive on your updating and patching:** Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.
9. **Enforce an effective password policy**. Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple

Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

10. **Restrict email attachments:** Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.
11. **Ensure that you have infection and incident response procedures in place:**
    - Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
    - Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
    - Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
    - Isolate infected computers to prevent the risk of further infection within the organization;
    - If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
    - Perform a forensic analysis on any infected computers and restore those using trusted media.
12. **Educate users on the changed threat landscape:**
    - Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
    - Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
    - Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
    - Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;
    - Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
    - Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
    - Only download software (if allowed) from corporate shares or directly from the vendors Web site;
    - If users see a warning indicating that they are “infected” after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.

Best Practice Guidelines for Users and Consumers

1. **Protect yourself**: Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:
    - Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;
    - Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
    - Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;
    - Browser protection to protect against obfuscated Web-based attacks;
    - Reputation-based tools that check the reputation and trust of a file and Web site before downloading; URL reputation and safety ratings for Web sites found through search engines.
2. **Keep up to date**: Keep virus definitions and security content updated at least daily if not hourly. By deploying the latest virus definitions, you can protect your computer against the latest viruses and malware known to be spreading in the wild. Update your operating system, Web browser, browser plug-ins, and applications to the latest updated versions using the automatic updating capability of your programs, if available. Running out-of-date versions can put you at risk from being exploited by Web-based attacks.
3. **Know what you are doing**: Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
    - Downloading “free” “cracked” or “pirated” versions of software can also contain malware or include social engineering attacks that include programs that try to trick you into thinking your computer is infected and getting you to pay money to have it removed.
    - Be careful which Web sites you visit on the Web. While malware can still come from mainstream Web sites, it can easily come from less reputable sites sharing pornography, gambling and stolen software.
    - Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.
4. **Use an effective password policy:** Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or Web sites. Use complex passwords (upper/lowercase and punctuation) or passphrases.
5. **Think before you click**: Never view, open, or execute any email attachment unless you expect it and trust the sender. Even from trusted users, be suspicious.
    - Be cautious when clicking on URLs in emails, social media programs even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using previews or plug-ins.
    - Do not click on links in social media applications with catchy titles or phrases even from friends. If you do click on the URL, you may end up “liking it” and sending it to all of your friends even by clicking anywhere on the page. Close or quit your browser instead.
    - Use a Web browser URL reputation solution that shows the reputation and safety rating of Web sites from searches. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
    - Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor’s Web site.
6. **Guard your personal data**: Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested and used in malicious activities such as targeted attacks, phishing scams.
    - Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.

About Symantec.cloud Intelligence

Symantec.cloud 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 live data feeds from more than 15 data centers around the world scanning billions of messages and Web pages each week. Team Skeptic™ comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of Web pages, email and IM messages they monitor each day on behalf of 31,000 clients in more than 100 countries. More information is available at www.messagelabs.com/intelligence.

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.