EXHIBIT 3

Symantec Intelligence Report: November 2011

November sees a four-fold increase in the number of daily targeted attacks since January; lowest global spam rate for three years, but Russian spammers continue to innovate in disguising their messages.

Welcome to the November 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 October and November 2011.

Report highlights

- Spam – 70.5 percent (a decrease of 3.7 percentage points since October 2011): page 13
- Phishing – One in 302.0 emails identified as phishing (an increase of 0.04 percentage points since October 2011): page 16
- Malware – One in 255.8 emails contained malware (a decrease of 0.03 percentage points since October 2011): page 17
- Malicious Web sites – 4,915 Web sites blocked per day (an increase of 47.8 percent since October 2011): page 19
- A Review of Targeted Attacks in 2011: page 2
- Revolution of Russian Phone Number Spam: page 10
- Best Practices for Enterprises and Users: page 22

Introduction

With targeted attacks and advanced persistent threats being very much in the news this year, we thought it would be a good time as the end of the year draws closer to begin our review of targeted attacks and look more closely at what has been described as "advanced persistent threats" or APTs for short. Terms such as APT have been overused and sometimes misused by the media, but APTs are a real threat to some companies and industries.

In November, one in 255 emails was malicious, but approximately one in 8,300 of those were highly targeted. This means that highly targeted attacks, which may be the precursor to an APT, account for approximately one in every two million emails, still a rare incident rate. Targeted malware in general has grown in volume and complexity in recent years, but as it is designed to steal company secrets, it can be very difficult for recipients to recognize, especially when the attacker employs compelling social engineering techniques, as we highlight in this report.

A persistent threat residing inside your company's network may be the by-product of a successful targeted attack, rather than the targeted email itself containing an APT, it is likely to contain a downloader component for the actual APT. Hence, targeted attacks of this nature can lead to an APT being deployed on your network if you don't have the right defenses in place.

Global spam is now at the lowest it has been since November 2008, when the rogue ISP McColo was closed-down. The effect on spam volumes back then were very dramatic and spam accounted for 68.0% of global emails. More recently the decline has been much slower, but spammers have also adapted to using more targeted approaches and exploiting social media as alternatives to email. Moreover, pharmaceutical spam is now at the lowest it has been since we started tracking it, accounting for 35.5% of spam, compared with 64.2% at the end of 2010.

This will be the final Symantec Intelligence report in 2011; work is already underway on our annual review of the security landscape in 2011. 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

A Review of Targeted Attacks in 2011

Targeted malware and advanced persistent threats (APTs) have been very prominent in the news during 2011, particularly in the wake of the Stuxnet attacks that took place in 2010, and more recently with the discovery of Duqu[1], which is was created from the same source code as Stuxnet. Although the source code for Stuxnet is not available on the Internet, this does not mean that the original authors were also the authors of Duqu; the source code may have been shared or even stolen.

Defining what is meant by targeted attacks and APT is important in order to better understand the nature of this mounting threat and to make sure that you have invested in the right kinds of defenses for your organization.

Targeted attacks have been around for a number of years now, and when they first surfaced back in 2005, Symantec.cloud would identify and block approximately one such attack in a week. Over the course of the following year, this number rose to one or two per day and over the following years it rose still further to approximately 60 per day in 2010 and 80 per day by the end of the first quarter of 2011. The types of organizations being targeted tended to be large, well-known multi-national organizations, and were often within particular industries, including the public sector, defense, energy and pharmaceutical. In more recent years the scope has widened to include almost any organization, including smaller and medium-sized businesses. But what do we really mean by targeted attacks and advanced persistent threats?

Defining targeted attacks

An attack can be considered as targeted if it is intended for a specific person or organization, typically created to evade traditional security defenses and frequently makes use of advanced social engineering techniques. However, not all targeted attacks lead to an APT; for example, the Zeus banking Trojan can be targeted and will use social engineering in order to trick the recipient into activating the malware, but Zeus is not an APT. The attacker doesn't necessarily care about who the individual recipient is; they may have been selected simply because the attacker is able to exploit information gathered about that individual, typically harvested through social networking Web sites.

Social engineering has always been at the forefront of many of these more sophisticated types of attack, specially designed to penetrate a company's defenses and gain access to intellectual property or in the case of Stuxnet, to interfere with the physical control systems of an operation. Without strong social engineering, or "head-hacking," even the most technically sophisticated attacks are unlikely to succeed. Many socially engineered attacks are based on information we make available ourselves through social networking and social media sites. Once the attackers are able to understand our interests, hobbies, with whom we socialize, and who else may be in our networks; they are often able to construct more believable and convincing attacks against us.

Profile of a highly targeted attack

A highly targeted attack is typically the precursor to an APT, and the typical profile of a highly targeted attack will commonly exploit a maliciously crafted document or executable, which is emailed to a specific individual, or small group of individuals. These emails will be dressed-up with a social engineering element to make it more interesting and relevant, as highlighted in figure 1, below.

For example, a PDF attached to an email advertising half-price "green-fees" may be more appealing if the recipient is a golf fan; they may be receptive to such a bargain. Ideally, the attacker wants to create a document that the recipient feels more compelled to open. Sometimes the attack may be through a compromised Web site, where the recipient is required to click on a link contained in the email, that may result in a drive-by attack, or from which they will download the infected document.

---

[1] *http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit*
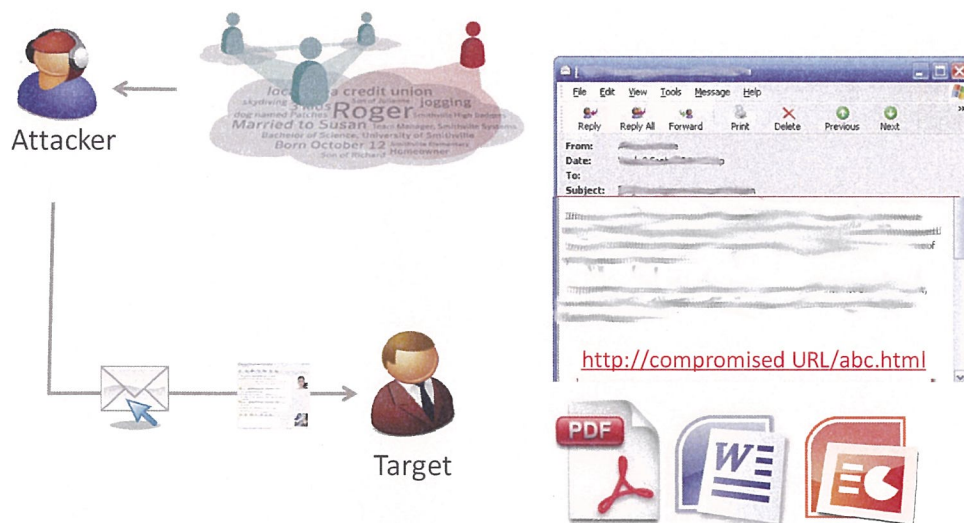
✓Symantec.™

Figure 1: Typical lifecycle of a targeted attack

In April 2011, MessageLabs Intelligence (now Symantec Intelligence), reported[2] attacks using the CVE-2011-0609 exploit. These attacks were blocked by Symantec.cloud, it was widely reported at the time that similar attacks using the same exploit were also sent to individuals at RSA. In that case, the attack comprised of a spreadsheet document apparently detailing the recruitment plan for the coming financial year. It was also dressed-up to appear to have been sent from a recruitment agency the HR team had been working with, a technique known as "spear phishing." It is human nature to be interested in gossip, so if an attacker were to send a document called "staff_salaries.doc" then it may have a greater chance of being opened.

Once such a malicious document is opened, the victim's machine becomes compromised and additional malicious code (often referred to as the "second stage") is subsequently downloaded and installed. It is this second stage that allows remote access to the compromised machine, and facilitates the egress of data. This becomes a stepping stone into the rest of the company's network, forming a kind of beachhead. Moreover, it is really only at this stage that the attack might be considered an APT; it hasn't been blocked by the corporate security defenses and the computer is now under the control of the attackers.

Evolution of APTs

Hence, the term "APT" has evolved to describe a unique category of targeted attacks that are specifically designed to target a particular individual or organization. APTs are designed to stay below the radar, and remain undetected for as long as possible, a characteristic that makes them especially effective, moving quietly and slowly in order to evade detection. Unlike the fast-money schemes typical of more common targeted attacks, APTs may have international espionage and/or sabotage objectives. The objective of an APT may include military, political or economic intelligence gathering, confidential or trade secret threat, disruption of operations, or even the destruction of equipment. Stuxnet was a good, albeit extreme example of the latter: the malware enabled an attacker to disrupt the industrial control systems within the Uranium enrichment process of a particular target.

Another characteristic of an APT is that it will also be part of a longer-term campaign, and not follow the opportunistic "smash-and-grab" approach typical of most malware in circulation today. Its purpose will be to remain undetected for as long as possible, perhaps using a variety of attacks over that period; if one attack fails then a process of continual monitoring will ensure that a follow-up attack may be more likely to succeed a few weeks later with a different approach. If successful, an attacker can use the compromised systems as a beachhead for subsequent attacks.

---

[2] *http://www.symanteccloud.com/mlireport/MLI_2011_04_April_FINAL_en-us.pdf*

Symantec™

All of which illustrate how these attacks can be both advanced and persistent threats: A threat because its purpose is to steal data or interfere with the operations of the targeted company, and potentially exploit the compromised network now under the attacker's control to target users in other organizations. They are advanced because of the methods employed to avoid detection, such as the use of zero-day exploits, and the means used to communicate with the command and control network; command and control instructions often involve encrypted traffic, typically sent in small bursts and disguised as normal network traffic. The key to ensuring that any stolen information can be exfiltrated without detection requires the attacker to avoid using easily detectable encryption, and to use common protocol channels that would not look out of place, but whilst making sure the data remains hidden.

Furthermore, they can be described as persistent because the aim is to maintain a foothold within the compromised company's infrastructure, and in order to achieve this, the attacker will use numerous methods to achieve this. The attackers have a very clear and specific objective, they are well-funded and well-organized and without the right protection in place, these threats have both the capability and the intent to achieve their desired goals.

Growth of targeted attacks

Figure 2, below shows the growth in volume of highly targeted attacks that could lead to an APT. These attacks would be sent to specific individuals within each of the organizations under fire, and spread throughout the year. The attacks would use multiple "kill-chains" (a variety of attack vectors, such as different types of malware using several exploits over a long period of time). Sometimes these attacks would make use of zero-day exploits; when an attacker has identified a means to take advantage of an unpatched vulnerability in an application for which no patch is available to mitigate the exploit. Zero-day vulnerabilities on the whole are rare and in 2010 there were only 14 recorded[3] by Symantec and 11 to date in 2011; Stuxnet made use of four zero-day vulnerabilities.
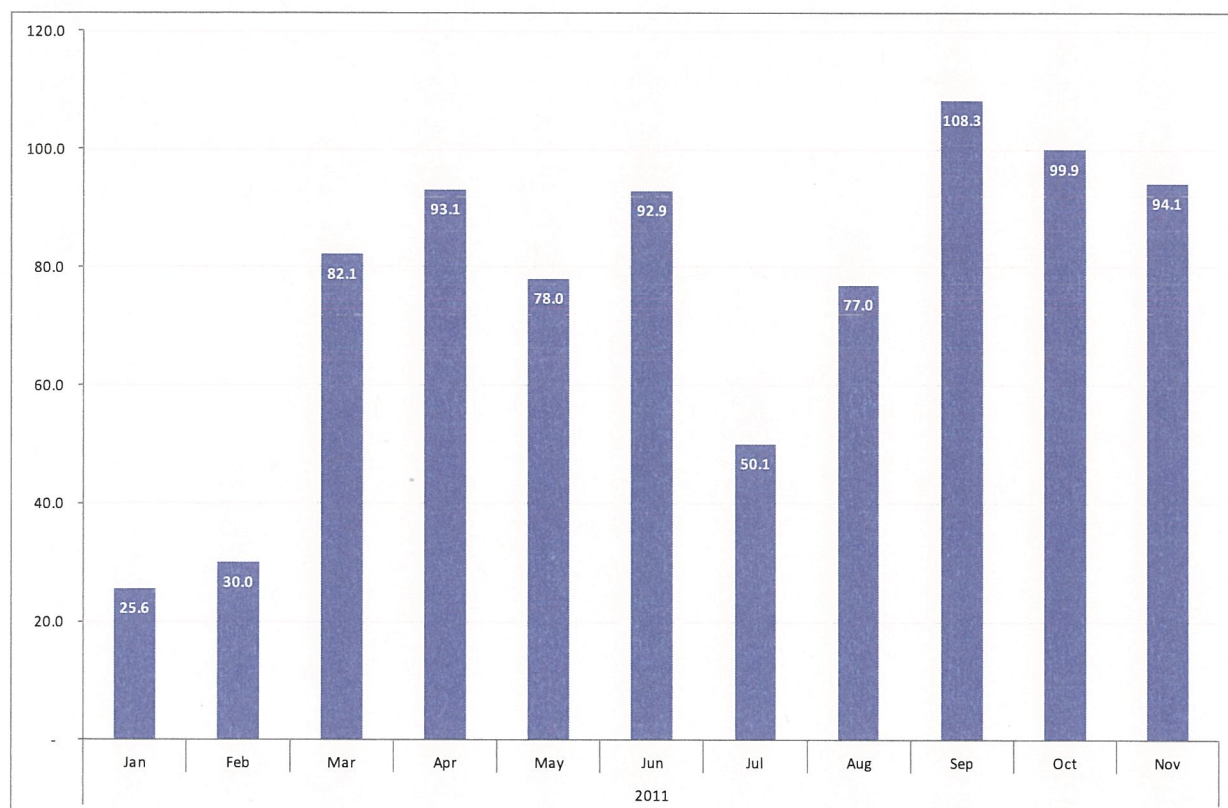

Figure 2 – Average number of targeted attacks blocked overall by Symantec.cloud per day worldwide in 2011

---

[3] *http://www.symantec.com/business/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities*

✓Symantec™

In November, approximately 94 such attacks were blocked by Symantec.cloud each day, four times the number blocked in January of the same year. When this is put in perspective, one in 255 emails in November contained some form of malware, but only one in 8,300 of these were actual highly targeted attacks that could lead to an APT. Overall, that means that one in every two million emails contains a targeted attack that could lead to an APT.

With an estimated 48 billion emails in circulation each day, a highly targeted attack of this nature accounts for a very small percentage of email traffic, but they are certainly not as rare as at the end of 2010. These attacks all have the potential to seriously impact an organization, and in the longer-term they represent a significant threat against the economic prosperity of many companies.

Most frequently targeted industries

The chart in figure 3 below shows that the public sector has been the most frequently targeted industry during 2011, with approximately 20.5 targeted attacks blocked each day. The chemical & pharmaceutical industry was second highest ranked, with 18.6 blocked each day. In this latter case, many of these attacks surfaced later in the year, and fit into the profile described in the Nitro[4] attacks. Similarly, this is also the case for the manufacturing sector, which was placed third mosttargeted with approximately 13.6 attacks blocked each day.

The aim of these targeted attacks each day was to establish persistent access to the targeted organization's network, in many cases with the aim of providing remote access to confidential data.
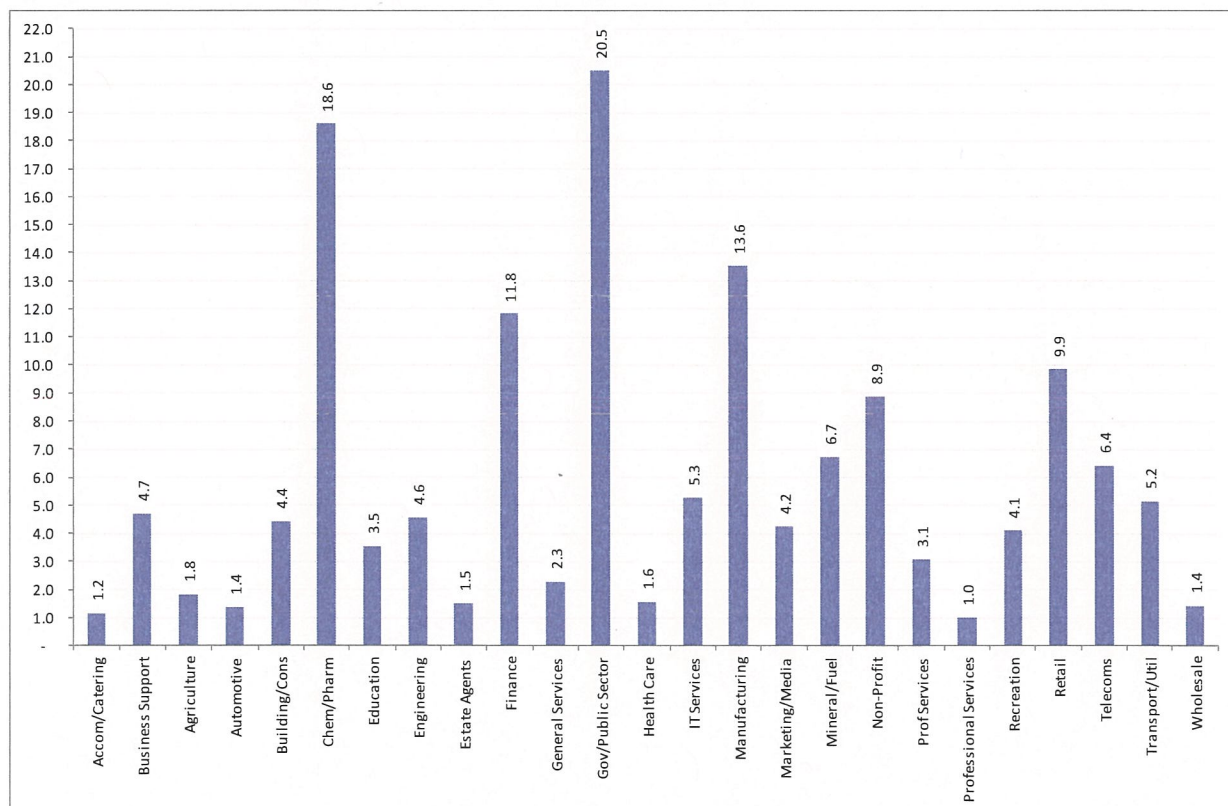
Figure 3 – Average number of targeted attacks blocked by Symantec.cloud per day by industry sector in 2011

As noted above, the objective of an APT can be to disrupt operations or even destroy equipment. While the ability for malware to disrupt physical machinery is rare and extremely difficult to achieve, the first reported case since Stuxnet

---

[4] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf*

✓Symantec.

of a similar incident came to light on November 8, when it was reported that a U.S. water plant had been compromised and the SCADA (Supervisory Control and Data Acquisition) system was accessed in an unauthorized fashion in order to turn on and off a pump, causing it to eventually fail and resulting in a partial shutdown to the plant in Illinois. It was suspected that the initial breach occurred with the developer of the controller software for the industrial devices. Perhaps the information and credentials collected in that attack were then used to commit the subsequent attacks against the water plant. However, the FBI and the Department of Homeland Security maintain they have not found evidence of a cyber intrusion.

Targeted attacks by organisation size

The chart shown in figure 4, below, identifies the targeted organizations by their size, showing that large enterprises consisting of more than 2,500 employees received the greatest number of attacks, with 36.7 being blocked each day.

By contrast, the small-to-medium sized business sector with less than 250 employees had 11.6 attacks blocked daily.
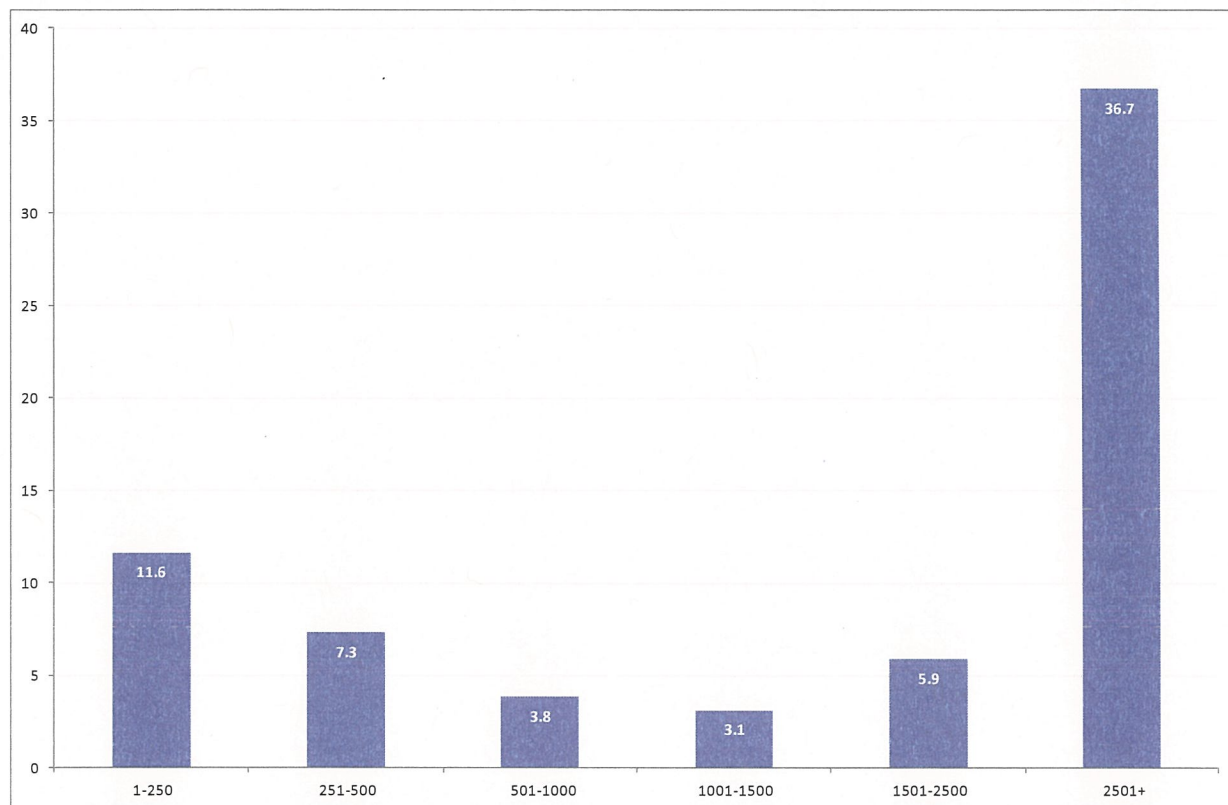

Figure 4 – Average number of targeted attacks blocked by Symantec.cloud per day by company size in 2011

Targeted attacks by geographical distribution

In the final analysis, we looked at the targeted attacks broken down by geographical distribution, based on the location of the intended recipients. This is shown in figure 5, below, and reveals that in the U.S. at least one attack is being blocked each day, and that one in 389 users may be the recipient of such an attack. Contrast this with Japan where at least one attack is blocked nearly every nine days, and may only be sent to one in 520 individuals.

Geography	One attack per N days	One attack per N users
United States	1.0	389
United Kingdom	1.2	407
Hong Kong	2.9	127
Australia	3.1	1,139
France	3.2	396
Singapore	3.3	114
Switzerland	3.4	455
Middle East	4.0	539
India	4.4	82
Belgium	4.5	176
Denmark	5.1	666
Netherlands	7.0	3,307
Canada	8.8	513
Japan	8.8	520
Germany	9.4	2,790
Philippines	14.0	99
Norway	14.7	2,591
China	16.3	4
Malaysia	17.2	7,433
Hungary	18.2	196
Italy	28.1	1,310
Spain	28.1	6,522
Sweden	30.9	24,134
Taiwan	44.1	68
Israel	44.1	880
Finland	44.1	3,686
New Zealand	61.8	3,479
Ireland	61.8	5,104
Sri Lanka	77.3	2,241
Luxembourg	154.5	665
Vietnam	154.5	843
South Africa	154.5	4,878

Figure 5 – Table showing the frequency and ratio of attacks per user in the most frequently targeted regions

Symantec™

Case-study of a targeted organization

A recent example, which we'll use as a case-study can be seen in figure 6, and focuses on a company that produces video games, and a series of attacks have been conducted over a period of at least two years. The purposes of these attacks seem to be to gain access to the intellectual property used within their products.
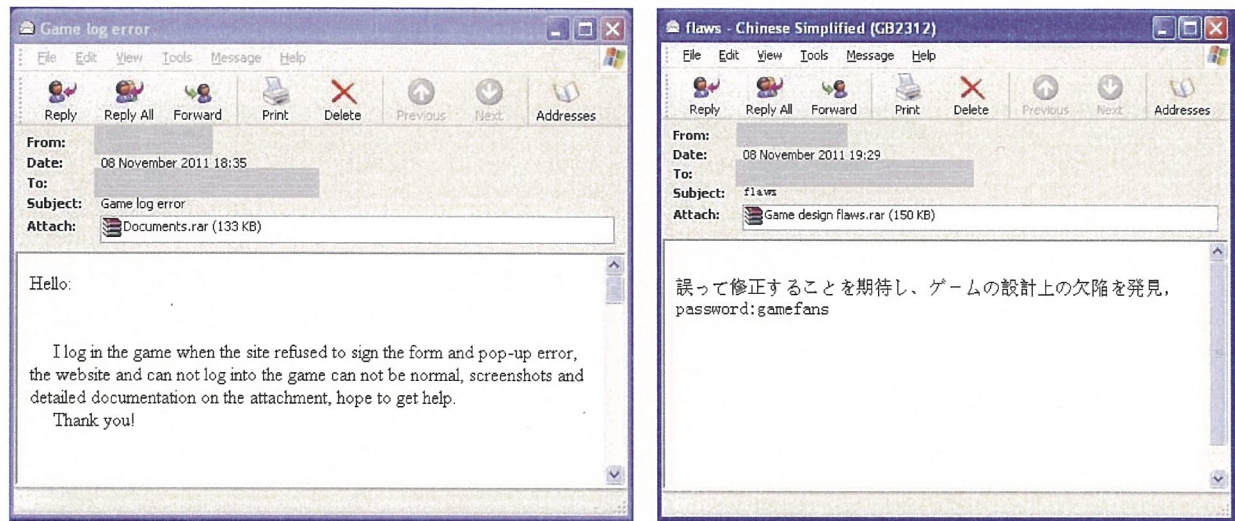
Figure 6 – Examples of targeted attack emails destined for a video games company

The Japanese text shown in the second example from figure 6, translates to, "Hope to correct accidentally discovered a design flaw in the game."

The majority of these attacks originated from the U.S. but this is not surprising given that many of the emails were sent from a variety of free, online Webmail services. Similar emails were also sent from Japan, South Korea and Taiwan, again using free Webmail providers as the source.

Figure 7, below, show that these attacks tend to be spaced two or three months apart and often occur in small waves, the most recent attacks taking place in November 2011.

Symantec.

Figure 7 – Pattern of targeted attacks blocked by Symantec.cloud against one company over time

The file types used in each attack have changed over time, seeking to exploit vulnerabilities in a variety of common office applications. As each previous attempt was blocked, the attackers were forced to find an alternative method of intrusion.
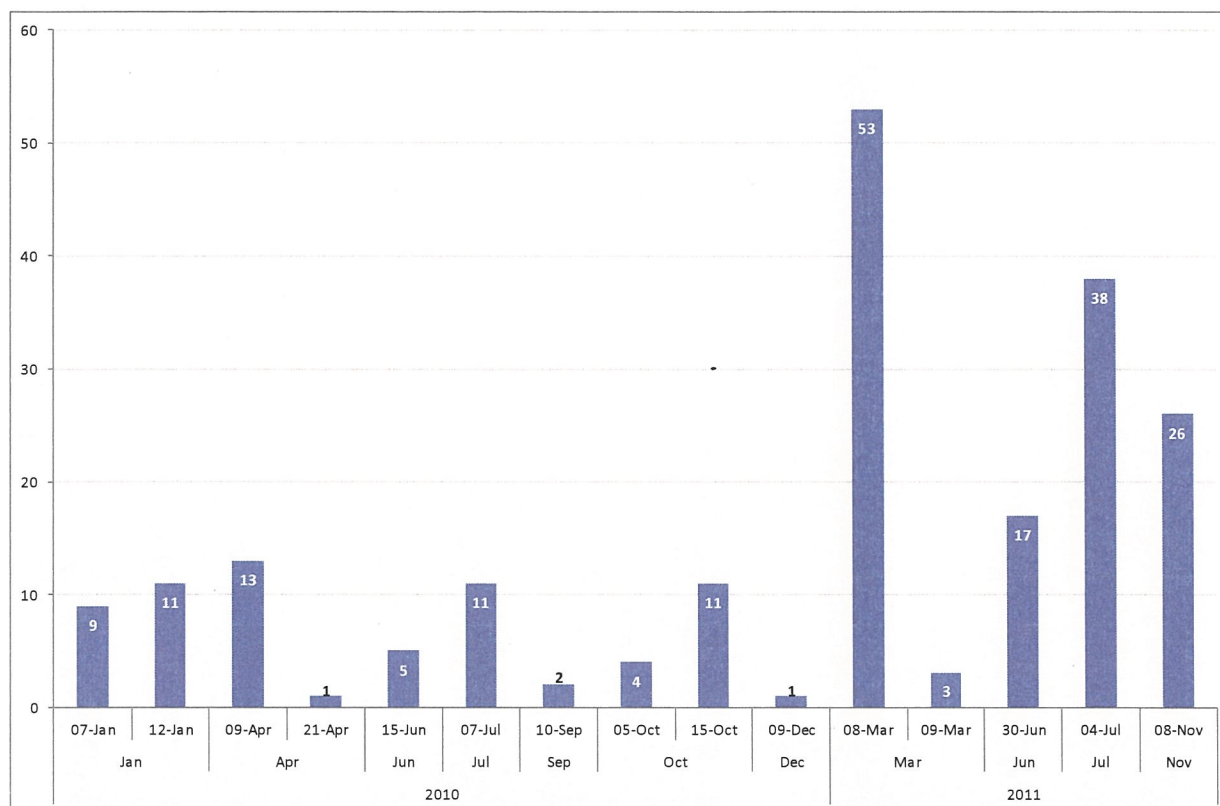
Potential impact of targeted attacks

It can be difficult to quantify the true scale of this problem, but hopefully the data from Symantec.cloud in this report will help to illustrate the seriousness of this issue. The challenge now lies in understanding whether your organization is likely to be targeted in this way, and that can be very difficult. It may be that your company is not the primary target, but an attacker may use your organization as a stepping-stone to attack another company. You do not want your business to be the weakest link in the supply chain. Information is power, and the attackers know this, and successful attacks can result in significant financial advantage for the cyber criminals behind them. Access to intellectual property and strategic intelligence can give them huge advantages in a competitive market. Hopefully, we have shown how the means by which these attacks take place have grown more sophisticated and have advanced considerably over time.

Symantec has worked with and helped some companies who have been the victims of APTs and at a minimum you should try to understand these new techniques and learn what you can do to protect yourself and your business. Begin by reinforcing your defenses now.

For further information about targeted attacks and APTs, please download[5] the latest white paper on this topic.

---

[5] *http://go.symantec.com/apt*

Revolution of Russian Phone Number Spam

Most of the Russian spam emails we encounter nowadays are about online advertising, product promotion, and training workshops. These spam emails typically are sent out from free or hijacked personal email accounts unsolicited, without opt-out, and has randomized subjects to avoid being caught by the spam filters. Regardless of the randomness, we observed that spammers like to list phone numbers in the email content as the only contact information instead of URL links.

Figure 8, below, shows an example of a recent Russian product promo spam.

Translation:

Figure 8: Russian-language spam promotion

Are you able to spot any abnormalities in the body content? Look closely at the phone numbers: Some digits are not written as numbers but instead letters. Spammers have replaced the number digits with English/Russian characters in the phone number; a technique that we will take a closer look at in this article.

The following are a few examples of how spammers employed this trick in the past few years. First, a simple set of contact information phone numbers as listed below:

(495)1234000
(495) 4321000
7(495)1234000
7-495-4321000

Then, spammers start to embellish the phone number by inserting some random symbols between the numbers:

(4~9~5)1~2~3~40~0~0
(4^95)1^2^3^40^00
495 43:21;000
(4_9_5) 4_3_21000

Later on, the spammers become more sophisticated and begin to replace numbers with look-alike Russian or English alphabets. Figure 9 shows a list of characters that resemble numbers in both Russian and English.

	English	Russian
1	l i I	N/A
2	Zz	N/A
3	N/A	Зз Ээ
4	N/A	Чч
6	N/A	ЬьБб
0	Oo	Oo

Figure 9 – table of Russian and English letters that resemble numbers

Using the chart in figure 9, with some creativity the original list of phone numbers now looks like this:

(Ч^95)1^2^3^40^Oo
(495) I 2 3 – 4O – 0 0
/495/ Ч 3=2I;0 00
(Ч~9~5) 43~2~I~0~0~O

Anti-spam technology has been more effective in identifying and filtering out these spam patterns over time, which leaves the spammers with no choice but to get even more creative and come out with new tricks. In 2010, we observed that spammers were beginning to spell out phone numbers in actual Russian words, highlighted in figure 10, below.

	Russian	English
1	один	one
2	два	two
3	три	three
4	Четыре	four
5	пять	five
6	шесть	six
7	семь	seven
8	восемь	eight
9	девять	nine
0	ноль	ten

Figure 10 – table of Russian and English words for numbers

✔Symantec™

Using this approach, and original example above, the list of phone numbers now looks more complicated and longer, as follows:

(Ч^95)1 ^2^ три ^40^ ОО
(495) один 2 3 – 4 0 – 00 ⎬ (495)123400

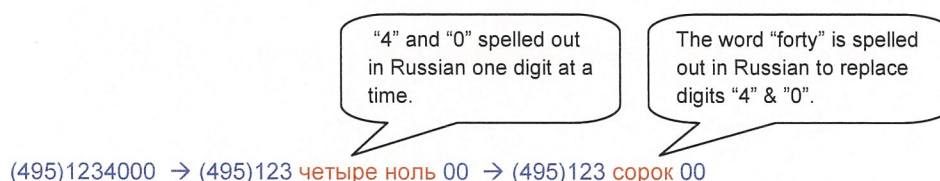/495/ Ч;3 =2 I 00 0
(Ч~9~5) 43~2~ один~о~о~0 ⎬ (495)432100

Moreover, the spammers' creativity did not end there; they then came up with the idea of replacing the area code with the actual name of the city which it represents. Take the city Moscow, for example - the area code for Moscow is 495. Therefore, area code 495 will be replaced by the word "Москва", "Moscow" or their abbreviated city name code:

(Москва) 1 ^2^ три ^40^ ОО
(Moscow) один 2 3 – 4 0 – 00 ⎬ (495)123400

(MOW) 4~3~2~1~0~ 00
(Мос) четерь 3 2;I=0О ноль ⎬ (495)432100

However, more recently, we observed yet another way to spoof the digits. In previous spam email shown above, the digits were spelled out in Russian, one digit at a time. Now, the spelling has progressed into double-digits or factor-digits, as shown in the example in figure 11, below.

	English spelling	Russian spelling
10	ten	десять
40	forty	сорок

Figure 11 – Examples of double-digit spelling used in spam

"4" and "0" spelled out in Russian one digit at a time.

The word "forty" is spelled out in Russian to replace digits "4" & "0".

(495)1234000 → (495)123 четыре ноль 00 → (495)123 сорок 00

It's always interesting to observe the kinds of tricks spammers often come up with in order to evade detection by spam filters. Fortunately, all of these tricks discussed above are easily caught using the latest technology. Unfortunately for spammers, they will have to think much harder to come up with some new tricks. Symantec intelligence always keeps a vigilant watch over the latest spam trends so that we can develop the best strategy in dealing with tricks like the Russian phone number puzzle presented here.

Article contributed by Emily Liu, Security Response Technician, Symantec

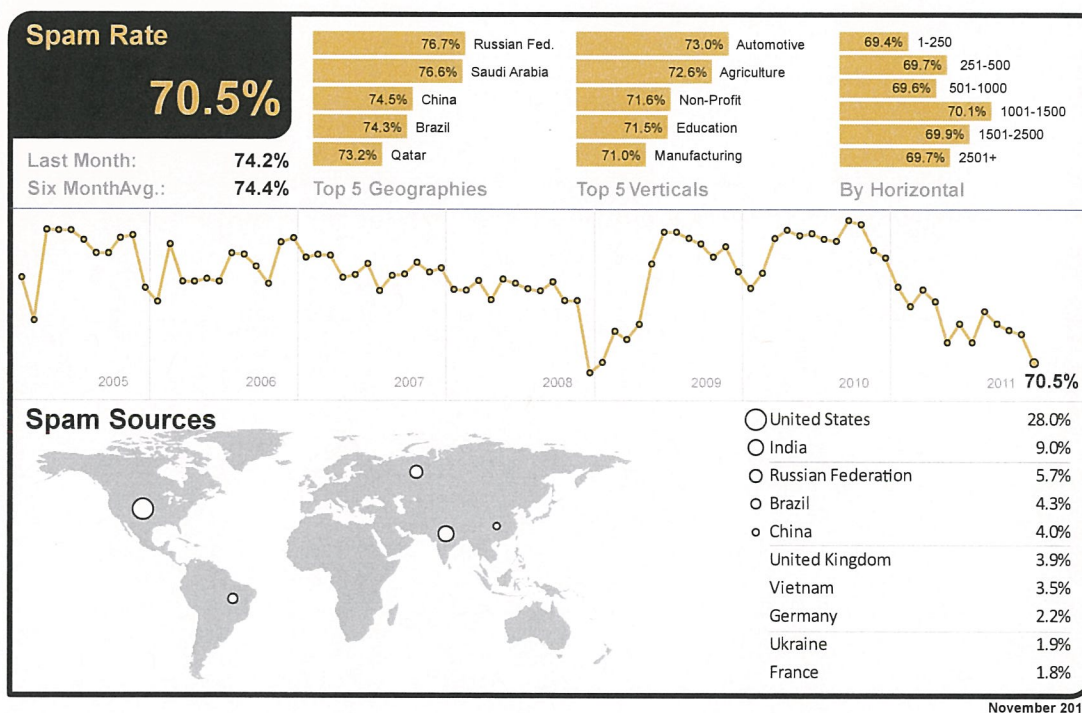Symantec™

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 November 2011, the global ratio of spam in email traffic fell by 3.7 percentage points since October to 70.5 percent (1 in 1.42 emails).

Spam Rate			
70.5%			
Last Month: **74.2%**			
Six MonthAvg.: **74.4%**			

Top 5 Geographies: 76.7% Russian Fed., 76.6% Saudi Arabia, 74.5% China, 74.3% Brazil, 73.2% Qatar

Top 5 Verticals: 73.0% Automotive, 72.6% Agriculture, 71.6% Non-Profit, 71.5% Education, 71.0% Manufacturing

By Horizontal: 69.4% 1-250, 69.7% 251-500, 69.6% 501-1000, 70.1% 1001-1500, 69.9% 1501-2500, 69.7% 2501+

Spam Sources:

United States	28.0%
India	9.0%
Russian Federation	5.7%
Brazil	4.3%
China	4.0%
United Kingdom	3.9%
Vietnam	3.5%
Germany	2.2%
Ukraine	1.9%
France	1.8%

November 2011

As the global spam rate fell, Russia became the most spammed geography in November; with a spam rate of 76.7 percent and Saudi Arabia was the second most-spammed with 76.6 percent of email traffic blocked as spam.

In the US, 69.9 percent of email was spam and 69.5 percent in Canada. The spam level in the UK was 69.5 percent. In The Netherlands, spam accounted for 70.5 percent of email traffic, 70.1 percent in Germany, 70.4 percent in Denmark and 68.6 percent in Australia. In Hong Kong, 69.2 percent of email was blocked as spam and 68.0 percent in Singapore, compared with 66.6 percent in Japan. Spam accounted for 70.1 percent of email traffic in South Africa and 74.3 percent in Brazil.

✓ Symantec™

With a drop in spam this month, the Automotive industry became the most spammed industry sector in November, with a spam rate of 73.0 percent. The spam rate for the Education sector was 71.5 percent and 69.1 percent for the Chemical & Pharmaceutical sector, compared with 69.3 percent for IT Services, 69.0 percent for Retail, 68.8 percent for Public Sector and 69.2 percent for Finance.

The spam rate for small to medium-sized businesses (1-250) was 69.4%, compared with 69.7.1% for large enterprises (2500+).

Global Spam Categories

The most common category of spam in November 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	November 2011	October 2011
Pharmaceutical	32.5%	37.5%
Watches/Jewelry	19.5%	15.0%
Unsolicited Newsletters	17.5%	6.5%
Adult/Sex/Dating	12.5%	2.5%
Weight Loss	8.0%	4.5%
Unknown/Other	4.0%	1.5%
Casino/Gambling	2.0%	23.5%
Software	2.0%	1.5%
Scams/Fraud/419	1.5%	6.0%
Degrees/Diplomas	<0.5%	0.5%
Jobs/Recruitments	<0.5%	0.5%
Malware	<0.5%	0.5%
Phishing	<0.5%	0.5%

Spam Subject Line Analysis

In the latest analysis, spam touting discounted software and emails relating to watches & jewelry accounted for some of the most common spam subject lines in November, perhaps a timely shift on the part of the spammers in the runup to the holiday season and around Christmas in December. Pharmaceutical related messages still feature among the most common spam subject lines.

Rank	November 2011 Total Spam: Top Subject Lines	No. of Days	October 2011 Total Spam: Top Subject Lines	No. of Days
1	Re: Windows 7, Office 2010, Adobe CS5 …	9	NACHA security nitification	2
2	New notification from Facebook	9	ACH Payroll Cancelled	2
3	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 ...	9	ACH Transfer Review	6
4	Penis Enlargement Pills - Enlarge you Penis Naturally Gain Up To 4 Inches In Length	9	Re: Back to School Software Sale	6
5	Enlarge you Penis Naturally Gain Up To 4 Inches In Length And Up To 25% Girth Increase.	9	0	6
6	Re: software outlet online purchase	9	Facebook Administration has sent you a notification	9
7	(blank subject)	9	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 …	18
8	High quality Replica Watches at Watch Replica World at $145	9	Re: Windows 7, Office 2010, Adobe CS5 …	18
9	Replica watches - THE MOST POPULAR MODELS All our replica watches have the same look and feel of the original product	9	Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 …	18
10	Save-8O%-0ff-Viagra©-Cia1is©-Levitra©	9	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 …	18

✓Symantec™

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com and .net top-level domains fell by 2.2 and 0.5 percentage points respectively, with the only increase by one percentage point, relating to spam URLs in the .ru TLD.

| TLD	November	October	Change (% points)
.com	55.1%	57.3%	-2.2
.ru	9.4%	8.4%	+1.0
.net	6.0%	5.3%	-0.5
.org	7.4%	N/A	N/A

Average Spam Message Size

In November, with a small decline, approximately 3 in every 5 spam emails was 5Kb in size or less; moreover, spam between 5Kb and 10Kb in size rose by 4.9 percentage point.

Message Size	November	October	Change (% points)
0Kb – 5Kb	57.8%	59.0%	-1.2
5Kb – 10Kb	31.2%	26.3%	+4.9
>10Kb	11.0%	14.7%	-3.7

Spam Attack Vectors

It can be seen in the chart below that the number of malicious attacks that contained a malicious attachment was much less than during the first half of October; however, the frequency of attacks has increased since the end of October. Many of these attachments continue to be related to generic polymorphic malware variants, as discussed in previous[6] Symantec Intelligence reports.
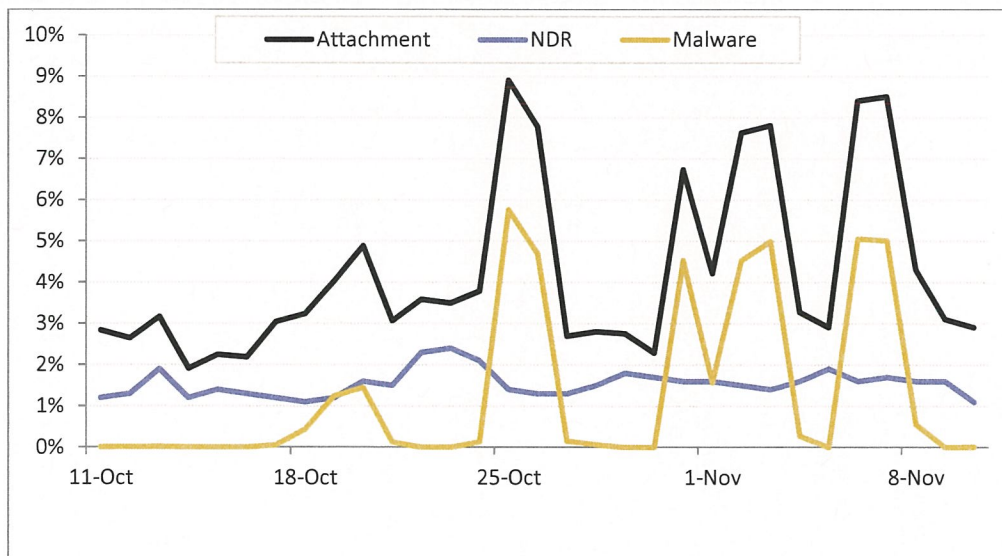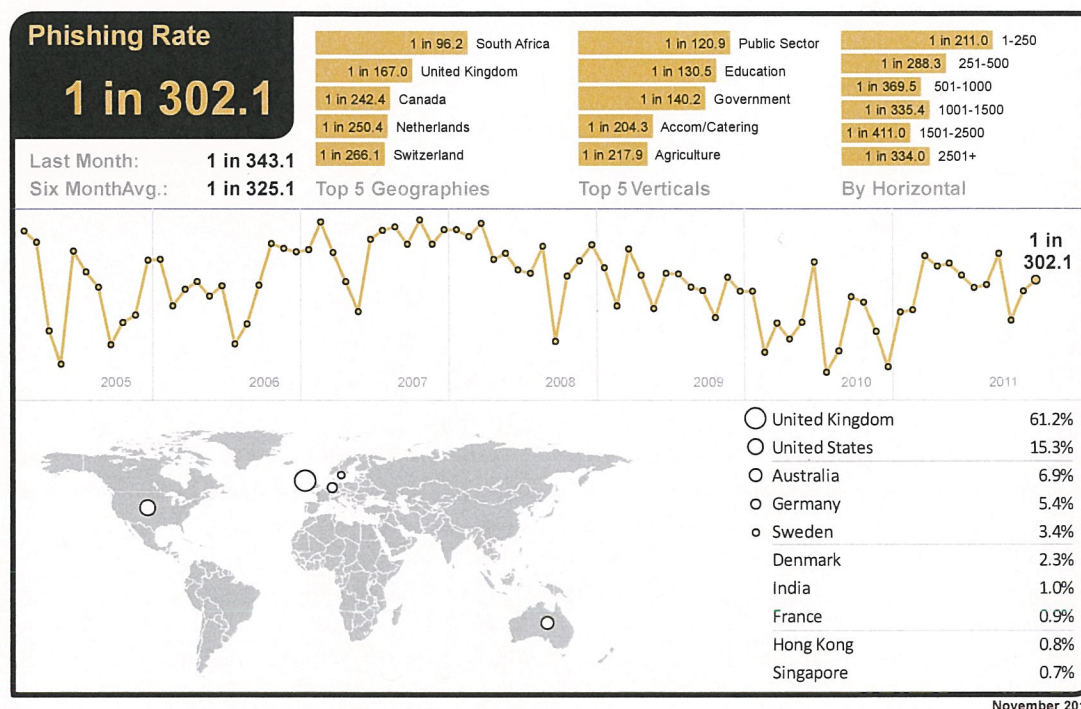

In November, the number of spam emails resulting in NDRs (spam related non-delivery reports), has been consistently stable, suggesting the attackers may be using valid email distribution lists to conduct these attacks. NDRs

---

[6] http://www.symanteccloud.com/intelligence

✓Symantec™

often result following widespread dictionary attacks, using databases of first and last names. This is indicative that spammers are maintaining their distribution lists in order to minimize bounce-backs, since IP addresses are more likely to appear on anti-spam block-lists if they become associated with a high volume of invalid recipient emails.

Phishing Analysis

In November, the global phishing rate increased by 0.04 percentage points, taking the average to one in 302.0 emails (0.33 percent) that comprised some form of phishing attack.

Phishing Rate			
1 in 302.1			
Last Month: **1 in 343.1**			
Six Month Avg.: **1 in 325.1**			

Top 5 Geographies	Top 5 Verticals	By Horizontal	
1 in 96.2 South Africa	1 in 120.9 Public Sector	1 in 211.0 1-250	
1 in 167.0 United Kingdom	1 in 130.5 Education	1 in 288.3 251-500	
1 in 242.4 Canada	1 in 140.2 Government	1 in 369.5 501-1000	
1 in 250.4 Netherlands	1 in 204.3 Accom/Catering	1 in 335.4 1001-1500	
1 in 266.1 Switzerland	1 in 217.9 Agriculture	1 in 411.0 1501-2500	
		1 in 334.0 2501+	

1 in 302.1

United Kingdom	61.2%
United States	15.3%
Australia	6.9%
Germany	5.4%
Sweden	3.4%
Denmark	2.3%
India	1.0%
France	0.9%
Hong Kong	0.8%
Singapore	0.7%

November 2011

South Africa once again became the country most targeted for phishing attacks in November, with one in 96.2 emails identified as phishing. The UK was the second most targeted country, with one in 167.0 emails identified as phishing attacks.

Phishing levels for the US were one in 461.8 and one in 242.4 for Canada. In Germany phishing levels were one in 426.2, one in 781.5 in Denmark and one in 250.4 in The Netherlands. In Australia, phishing activity accounted for one in 361.0 emails and one in 517.0 in Hong Kong; for Japan it was one in 2,058 and one in 609.7 for Singapore. In Brazil one in 775.3 emails was blocked as phishing.

The Public Sector remained the most targeted by phishing activity in November, with one in 120.9 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 407.5 and one in 377.0 for the IT Services sector, one in 397.0 for Retail, one in 130.5 for Education and one in 331.7 for Finance.

Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 211.0 emails, compared with one in 334.0 for large enterprises (2500+).
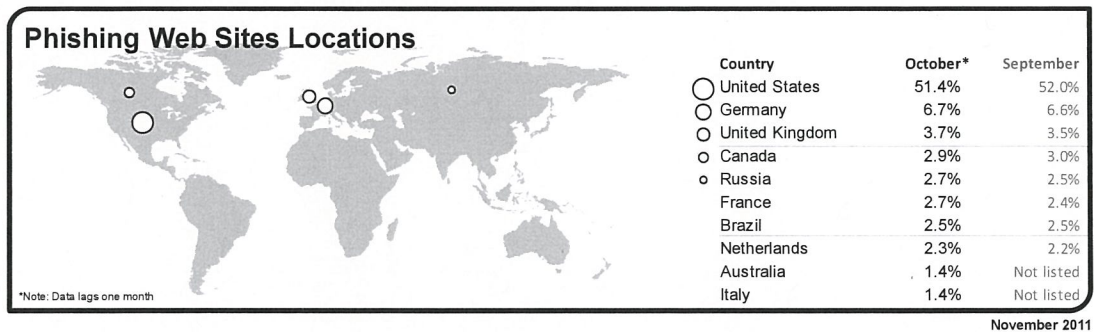
Analysis of Phishing Web sites
The number of phishing Web sites increased by 66.1 percent in November. The number of phishing Web sites created by automated toolkits increased four-fold, by approximately 316.1 percent, accounting for approximately 54.6 percent

✓Symantec™

of phishing Web sites. The majority of these related to attacks against a well-known social networking Web site, and accounted for approximately 78 percent of all toolkit-based attacks.
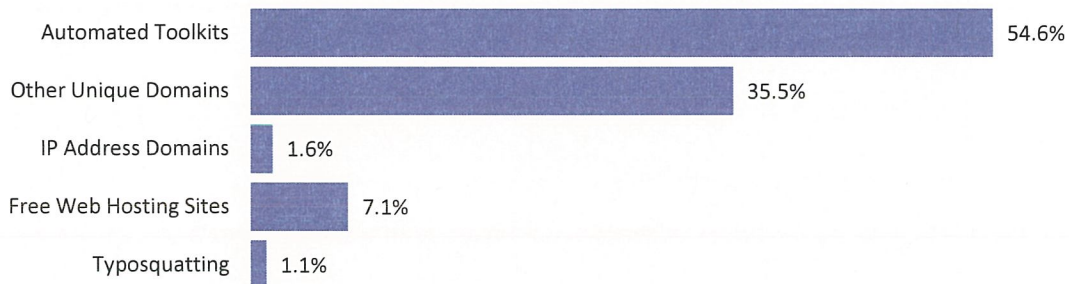
The number of unique phishing URLs decreased by 3.7 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), decreased by 36.1 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 7.1 percent of all phishing Web sites, a decrease of 10.7 percent from the previous month. The number of non-English phishing sites saw a fall of 4.0 percent.

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

Geographic Location of Phishing Web Sites

Phishing Web Sites Locations

Country	October*	September
United States	51.4%	52.0%
Germany	6.7%	6.6%
United Kingdom	3.7%	3.5%
Canada	2.9%	3.0%
Russia	2.7%	2.5%
France	2.7%	2.4%
Brazil	2.5%	2.5%
Netherlands	2.3%	2.2%
Australia	1.4%	Not listed
Italy	1.4%	Not listed

*Note: Data lags one month

November 2011

Tactics of Phishing Distribution

Automated Toolkits	54.6%
Other Unique Domains	35.5%
IP Address Domains	1.6%
Free Web Hosting Sites	7.1%
Typosquatting	1.1%

Organizations Spoofed in Phishing Attacks, by Industry Sector

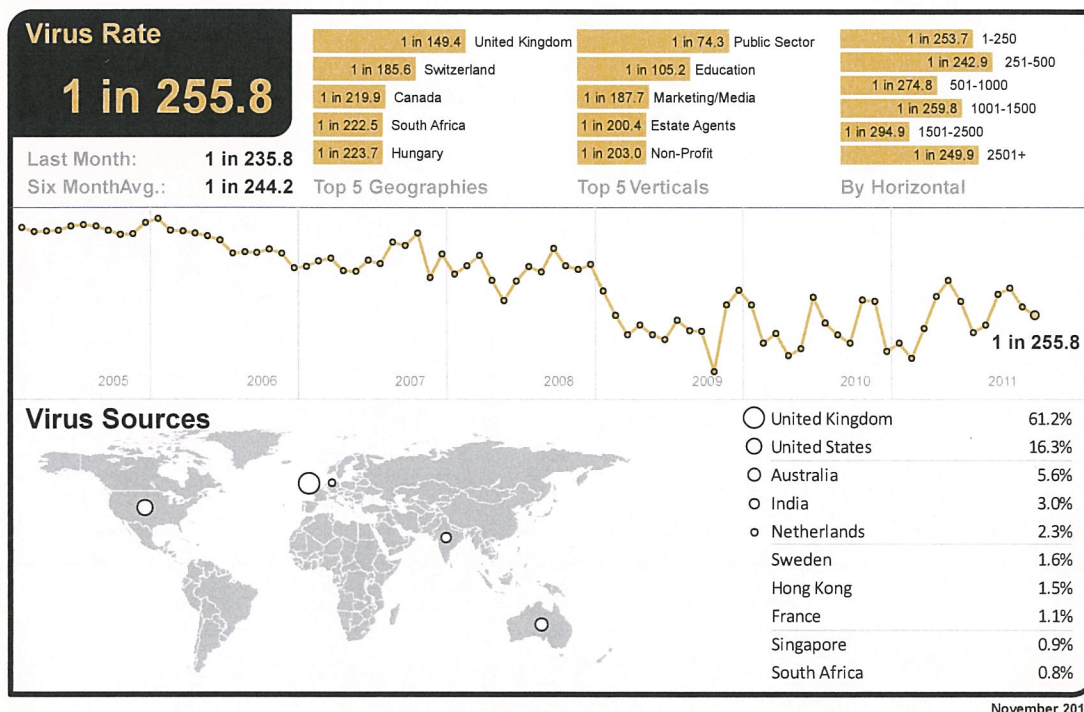|	
Financial	88.3%
Information Services	9.0%
Others	2.6%
Government	0.1%

✓ Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 255.8 emails (0.39 percent) in November, a decrease of 0.03 percentage points since October 2011.

In November, 40.2 percent of email-borne malware contained links to malicious Web sites, an increase of 20.1 percentage points since October 2011.

Virus Rate

1 in 255.8

Last Month: **1 in 235.8**
Six Month Avg.: **1 in 244.2**

Top 5 Geographies	
1 in 149.4	United Kingdom
1 in 185.6	Switzerland
1 in 219.9	Canada
1 in 222.5	South Africa
1 in 223.7	Hungary

Top 5 Verticals	
1 in 74.3	Public Sector
1 in 105.2	Education
1 in 187.7	Marketing/Media
1 in 200.4	Estate Agents
1 in 203.0	Non-Profit

By Horizontal	
1 in 253.7	1-250
1 in 242.9	251-500
1 in 274.8	501-1000
1 in 259.8	1001-1500
1 in 294.9	1501-2500
1 in 249.9	2501+

1 in 255.8

2005 2006 2007 2008 2009 2010 2011

Virus Sources

◯	United Kingdom	61.2%
◯	United States	16.3%
◯	Australia	5.6%
◦	India	3.0%
◦	Netherlands	2.3%
	Sweden	1.6%
	Hong Kong	1.5%
	France	1.1%
	Singapore	0.9%
	South Africa	0.8%

November 2011

The UK remained at the top of the table with the highest ratio of malicious emails in November, with one in 149.4 emails identified as malicious. Switzerland had the second highest rate, with one in 185.6 emails identified as malicious.

In South Africa returned to the top-5 list this month with one in 222.5 emails blocked as malicious. Virus levels for email-borne malware in the US reached one in 360.1 and one in 219.9 in Canada. In Germany virus activity reached one in 275.0, one in 710.5 in Denmark and in The Netherlands one in 238.2. In Australia, one in 326.2 emails was malicious. For Japan the rate was one in 1,147, compared with one in 450.0 in Singapore. In Brazil, one in 570.6 emails in contained malicious content.

With one in 74.3 emails being blocked as malicious, the Public Sector remained the most targeted industry in November. Virus levels for the Chemical & Pharmaceutical sector reached one in 275.5 and one in 276.6 for the IT Services sector; one in 337.1 for Retail, one in 105.2 for Education and one in 386.6 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 253.7 emails, compared with one in 249.9 for large enterprises (2500+).

✓Symantec.™

The table below shows the most frequently blocked email-borne malware for November, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 40.8 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware, such as Bredolab, Zeus and SpyEye, accounted for 29.6 percent of all email-borne malware in November; equivalent to 50.4 percent of all generic malware.

Malware Name	% Malware
Exploit/Link-generic-ee68	6.53%
Exploit/Link-generic.dam	3.83%
Trojan.Bredolab!eml-6c19	3.58%
W32/Generic-fdc7-c476-c476	2.48%
Trojan.Bredolab!eml-f101	1.98%
W32/Generic-6900	1.90%
W32/Generic.dam	1.72%
W32/NewMalware!0575	1.61%
W32/Generic-8426-e566	1.54%
Trojan.Bredolab!eml-47bf	1.51%

The top ten list of most frequently blocked malware accounted for approximately 26.7% of all email-borne malware in November.

Web-based Malware Threats

In November, Symantec Intelligence identified an average of 4,915 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 47.8 percent since October 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.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware   277/day
New sites with web viruses   9,268/day
Total   9,545/day

November 2011
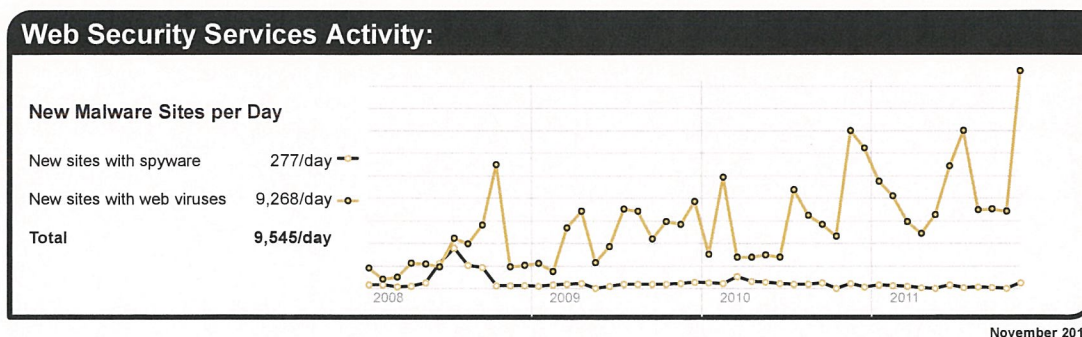
The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during November compared with the equivalent number of Web-based malware Web sites blocked each day.

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 32.4 percent of blocked Web activity in November. 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 19.3 percent of URL-based filtering activity blocked, equivalent to approximately one in every 5 Web sites blocked. Many organizations

Symantec.

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 11.1 percent of URL-based filtering blocks in November. 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 9 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	32.4%	Trojan.Gen.2	22.1%	PUP:ZBL	25.2%
Social Networking	19.3%	Suspicious.Emit	14.5%	PUP:MyWebSearch.EC	18.6%
Streaming Media	11.1%	Gen:Trojan.Heur.amKfbDF29Mpi	12.3%	PUP:JS.Script.C	8.8%
Computing and Internet	4.6%	Gen:Trojan.Heur.Cu9@Y!CHhQgi	8.5%	PUP:W32/Eshoper.B	8.0%
Search	4.1%	Gen:Trojan.Heur.amKfbr2TVGoi	4.1%	PUP:FakeAntiVirus.L	6.4%
Chat	3.4%	Trojan.Script.12023	2.9%	PUP:Generic.192950	4.5%
Hosting Sites	2.6%	Gen:Trojan.Heur.Mx9@XcmYEfei	2.7%	PUP:Clkpotato!gen3	3.3%
Peer-To-Peer	2.5%	VBS/Generic	2.2%	PUP:Generic.183433	2.8%
News	2.0%	Trojan.Maljava	1.7%	PUP:9231	2.6%
Entertainment	1.7%	Trojan.JS.Redirector.MY	1.5%	PUP:Agent.NGR	2.3%

November 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[7]	% Malware
WS.Trojan.H	21.93%
W32.Sality.AE	6.37%
W32.Ramnit!html	6.29%
Trojan.Bamital	5.74%
W32.Ramnit.B!inf	5.40%
W32.Downadup.B	3.00%
Trojan.ADH.2	2.25%
W32.SillyFDC.BDP!lnk	1.89%
Trojan.ADH	1.78%
W32.Virut.CF	1.73%

The most frequently blocked malware for the last month was WS.Trojan.H[8]. WS.Trojan.H is generic cloud-based heuristic detection for files that posses characteristics of an as yet unclassified threat. Files detected by this heuristic

---

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

[8] http://www.symantec.com/security_response/writeup.jsp?docid=2011-102713-4647-99

✓Symantec™

are deemed by Symantec to pose a risk to users and are therefore blocked from accessing the computer. For much of 2010, W32.Sality.AE[9] had been the most prevalent malicious threat blocked at the endpoint.

Variants of W32.Ramnit accounted for approximately 11.9% of all malware blocked at the endpoint, compared with 7.2% for all variants of W32.Sality.

Approximately 15.0 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.

---

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

✔Symantec™

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:

   o Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;

   o Browser protection for protection against obfuscated Web-based attacks;

   o Consider cloud-based malware prevention to provide proactive protection against unknown threats;

   o 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;

   o Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;

   o Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;

   o 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:**

    o 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;

    o 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;

    o Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;

    o Isolate infected computers to prevent the risk of further infection within the organization;

    o If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;

    o Perform a forensic analysis on any infected computers and restore those using trusted media.

12. **Educate users on the changed threat landscape:**

    o 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;

    o Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;

    o Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;

    o 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;

    o 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;

    o Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;

    o Only download software (if allowed) from corporate shares or directly from the vendors Web site;

    o 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 Consumers

1. **Protect yourself**: Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

   o Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;

   o Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;

   o Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;

   o Browser protection to protect against obfuscated Web-based attacks;

   o 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.

   o 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.

   o 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.

   o 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.

   o 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.

   o 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.

   o 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.

   o 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 via social networks) as it may be harvested and used in malicious activities such as targeted attacks and phishing scams.

   o 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.

Symantec.