

# Symantec Intelligence Report: October 2011

Spammers now operating spam-friendly URL-shortening services using free, open-source software; Eastern Europeans targeted by premium-rate SMS dialer app; and Duqu, a precursor to the next Stuxnet

---

Welcome to the October 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 September and October 2011.

## Report highlights

- Spam – 74.2 percent in October (a decrease of 0.6 percentage points since September 2011): page 7
- Phishing – One in 343.1 emails identified as phishing (an increase of 0.07 percentage points since September 2011): page 10
- Malware – One in 235.8 emails in October contained malware (a decrease of 0.11 percentage points since September 2011): page 11
- Malicious Web sites – 3,325 Web sites blocked per day (a decrease of 4.3 percent since September 2011): page 13
- 43.9 percent of all malicious domains blocked were new in October (a decrease of 0.7 percentage points since September 2011): page 13
- 15.2 percent of all Web-based malware blocked was new in October (an increase of 0.7 percentage points since September 2011): page 13
- Spammers setting up more URL shortening services: page 2
- Social engineering example from the East : page 4
- New Symantec Research: W32.Duqu - Precursor to the Next Stuxnet: page 5
- New Symantec Research: The Motivations of Recent Android Malware: page 6
- Best Practices for Enterprises and Users: page 16

## Introduction

With the advent of social networking we have all become accustomed to using URL shortening services in our online lives, and as their use by cyber criminals has increased, Symantec Intelligence has also tracked how these legitimate services have been used in different ways for malicious purposes in the dissemination of malware and spam over the past few years. Following on from the preceding advance in May 2011, when spammers appeared to have established their own shortening services, albeit a Web site that would redirect visitors to the same spam Web site. On that occasion there was no actual shortening service in use, it was a simple redirection that gave the appearance of a shortened URL. However, for the first time, Symantec Intelligence has identified that spammers have now established a genuine URL shortening service that is publically available and will generate real shortened links. These have so far only been found in spam emails.

Furthermore, this month a premium rate SMS dialer was also discovered targeting users in Eastern Europe. Premium SMS dialers have always been a problem on the mobile threat landscape, especially in Eastern Europe and this example is no exception. It attempts to pass itself off as a legitimate application by playing off the name of a popular VoIP/messaging app. It is written in J2ME and targets Apple iPhone™ devices running a JVM.

At the time of writing, Symantec researchers were in the midst of analyzing a newly discovered targeted threat that shares a great deal of code in common with the infamous Stuxnet malware. Of note, it is apparent that the authors of this new threat, dubbed “Duqu,” had access to the Stuxnet source code, not just Stuxnet binaries. Thus, it is possible Duqu was created by the same attackers that created Stuxnet.

Duqu's purpose is to gather intelligence data and assets from entities, such as suppliers to industrial facilities, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on an industrial facility. Thus, Duqu is essentially the precursor to a future Stuxnet-like attack.

Finally, a new whitepaper from Symantec looks at the future of mobile malware and we have observed a marked increase in threats targeting mobile devices in 2011; particularly the Android platform. This new analysis highlights how most current efforts to monetize mobile malware have only a low revenue-per-infection ratio and this has severely limited the return on investment achievable by attackers. It also offers detailed insight into the top current mobile malware monetization schemes, including how each works and examples of the malware presently being used to carry them out. It is only if the current monetization schemes and those likely to be seen in the near future, succeed that will attackers continue to invest in the creation of mobile malware.

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](mailto:paul_wood@symantec.com)

[@paulwoody](#)

## Report analysis

### Spammers setting up more URL shortening services

*By Nick Johnston, Senior Software Engineer, Symantec*

In the May 2011 Symantec Intelligence Report (then known as MessageLabs Intelligence), we explained how spammers had set up their own URL shortening services to better conceal their spam sites and make them harder to block.

In October, we recently discovered a spam gang with at least 80 URL shortening sites. These all used a similar naming pattern, and used the .info top-level domain. However, unlike the URL shortening sites we discovered in May, these sites are effectively public URL shortening sites. Anyone can create a shortened URL on these sites; the form to do so is also publically available, as shown in figure 1.

Spammers are using a free, open source URL shortening scripts to operate these sites. At the time of writing, 87 different domains were identified as being used in this fashion.

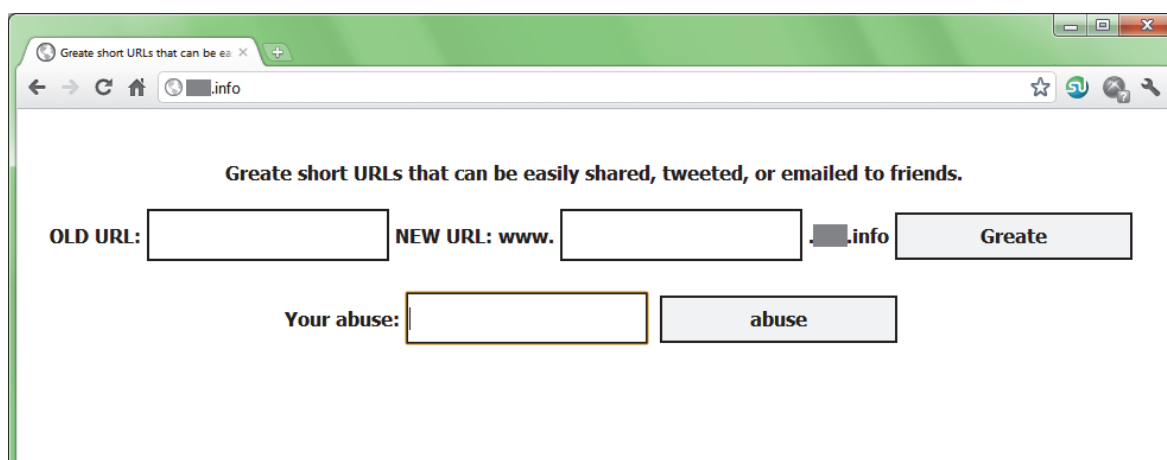


Figure 1 – landing page of spammers' URL shortening Web site

After creating many shortened URLs with their own service, the spammers then send spam including these URLs. These particular spammers use a mixture of blank subjects and subjects designed to get recipients to open the message, like "It's a long time since I saw you last!", "It's a good thing you came" and so on. This is a common social engineering tactic, as seen in figure 2.

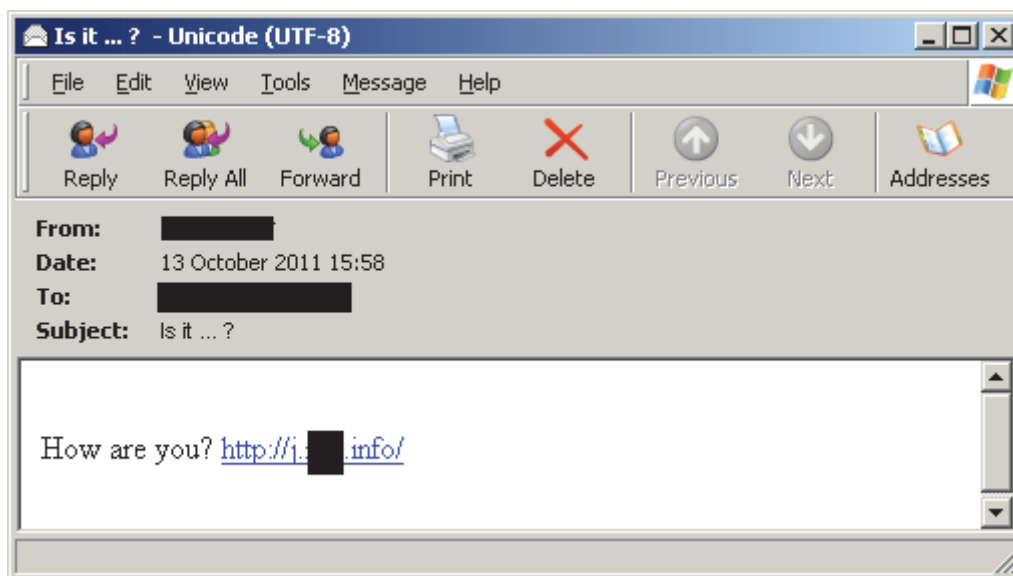


Figure 2 – Example of spam email containing spammers' own URL shortened link

The URL in the message points to one of the spammer's URL shortening sites, and then redirects to a "Pharmacy Express" pharmaceutical spam site. An example can be seen in figure 3, below.



Figure 3 – Spam website redirected via the bespoke spam URL shortening service

The domains used for the URL shortening sites all have the same contact information, with all contacts based in Moscow. The domains are all hosted by a UK subsidiary of a large hosting company. We have informed the company.

It is possible that spammers are setting up their own URL shortening sites since legitimate URL shortening sites, who have long suffered with abuse, have slightly improved their detection of spam and other malicious URLs. It's not fully clear why the sites are public. Perhaps this is simply due to laziness on the spammers' part, or perhaps an attempt to make the site seem more legitimate.

It can be seen from the chart in figure 4 that the use of legitimate URL shortening services continues, but not at the same rate as had been seen previously in the year. Although the number of legitimate URL shortening services is

significant and growing all the time, many of the major, well-known ones have made it more difficult for spammers to abuse their services and when they do, the links are often taken down very quickly.

In October approximately 0.5% of all spam contained a shortened URL from a legitimate service, with peaks of between 2% and 3% on occasion.

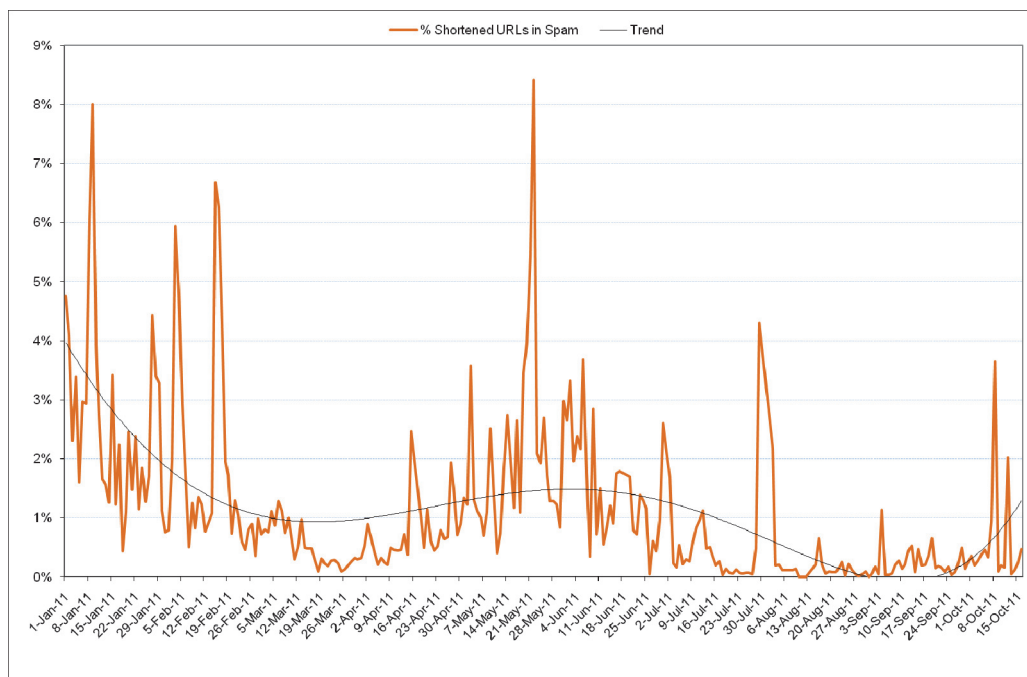


Figure 4 – Trend showing % of spam that contains a link from a legitimate URL shortening service

However, we expect spammers to continue to abuse URL shortening services and continue to try to conceal their spam sites as much as possible.

### Social engineering example from the East

By Shunichi Imano, Senior Security Response Manager, Symantec

Recently, a new threat, [Android.Fakeneflic](#)<sup>1</sup>, has [taken advantage of gaps in the availability](#)<sup>2</sup> of a legitimate video streaming service in order to target mobile users in North America. This is another example of social engineering at work; however, this time the users that are being targeted are in Eastern Europe.

Premium SMS dialers have always been a problem on the mobile threat landscape, especially in Eastern Europe, where dialers showed up on mobile phones not too long after the introduction of the micro edition of the Java Virtual Machine (JVM) for mobile devices. It should therefore come as no surprise that the authors responsible for leveraging this lucrative revenue source appear to be making a switch to newer platforms.

The latest example of a dialer that has come to our attention attempts to pass itself off as a legitimate application by imitating a popular VoIP/messaging app. It is written in J2ME and targets Apple iPhone™ devices running a JVM. In this case, the author has even gone to the extent of setting up a dummy website to promote the app, as shown in figure 5, below.

<sup>1</sup> [http://www.symantec.com/business/security\\_response/writeup.jsp?docid=2011-101105-0518-99](http://www.symantec.com/business/security_response/writeup.jsp?docid=2011-101105-0518-99)

<sup>2</sup> <https://www-secure.symantec.com/connect/blogs/will-your-next-tv-manual-ask-you-run-scan-instead-adjusting-antenna>



Figure 5 – Example of dummy Web site used to promote the rogue dialer app

Smartphones are widely used as communication tools in the enterprise environment as they have similar functionality to a computer, but fit in the palm of your hand. Smartphones provide convenience to users, yet simultaneously pose a significant danger as they are often overlooked when it comes to protecting them. Therefore, it is important that proper privileges and policies akin to corporate computers should be implemented on such devices. Since originally discovering the rogue Web site and the threat in early October, it has now been taken offline.

### New Symantec Research: W32.Duqu - Precursor to the Next Stuxnet

On October 14, Symantec was alerted by the Laboratory of Cryptography and System Security (CrySyS) in the Department of Telecommunications, Budapest University of Technology and Economics – a research lab with strong international connections – to a newly discovered targeted threat that shares a great deal of code in common with the infamous Stuxnet malware. Symantec researchers have been analyzing the threat, and of greatest note is that it is apparent that the authors of this new threat, dubbed W32.Duqu, had access to the Stuxnet source code, not just Stuxnet binaries. Thus, it is possible Duqu was created by the same attackers that created Stuxnet.

Duqu's purpose differs from Stuxnet; however, as it is designed to gather intelligence data and assets from entities, such as suppliers to industrial facilities, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on an industrial facility. Thus, Duqu is essentially the precursor to a future Stuxnet-like attack.

A technical paper on this threat has also been written by Symantec and can be found [here](#)<sup>3</sup>.

Symantec has also determined that some of the malware files associated with the W32.Duqu threat were signed with private keys associated with a code signing certificate which has subsequently been revoked. Our investigation into the key's usage leads us to the conclusion that the private key used for signing Duqu was stolen, and not fraudulently generated for the purpose of this malware. At no time were Symantec's roots and intermediate CAs at risk, nor were there any issues with any CA, intermediate or other VeriSign or Thawte brands of certificates.

#### Highlights:

- Executables using the Stuxnet source code have been discovered. They appear to have been developed since the last Stuxnet file was recovered.
- The executables are designed to capture information such as keystrokes and system information.

<sup>3</sup>[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_duqu\\_the\\_precursor\\_to\\_the\\_next\\_stuxnet.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf)

- Current analysis shows no code directly related to industrial control systems, exploits or self-replication.
- The executables have been found in a limited number of organizations, including those involved in the manufacturing of supplies to industrial facilities.
- The exfiltrated data may be used to enable a future Stuxnet-like attack.

## New Symantec Research: The Motivations of Recent Android Malware

By Eric Chien, Technical Director, Symantec

For years now, we in the cyber security industry have been saying an explosion of mobile malware is just around the corner. Beginning in earnest this year, we have indeed observed a marked increase in threats targeting mobile devices – particularly the Android platform. However, it's probably not accurate to say the expected explosion has in fact occurred. The reality is that cybercriminals are still very much in the exploratory phase of figuring out how to monetize the exploitation of mobile devices.

Above all else, our analysis highlights how most current efforts to monetize mobile malware have only a low revenue-per-infection ratio. This has severely limited the return on investment achievable by attackers. It also offers detailed insight into the top current mobile malware monetization schemes observed by Symantec, including how each works and examples of the malware presently being used to carry them out. These schemes are:

- Premium-rate number billing scams
- Spyware
- Search engine poisoning
- Pay-per-click scams
- Pay-per-install schemes
- Adware
- Stealing mobile transaction authentication numbers (mTAN)

However, the research also points out that the currently struggling revenue-per-infection ratio is primed to improve. The trigger will likely be advances in mobile payment-type technology and the widespread adoption of using mobile devices for both payment and accepting payment. The key is that these applications rely on devices to transmit financial information —such as mobile banking credentials—backed by real monetary funds. We've learned in the PC world just how lucrative the exploitation and sale of this kind of information can be for enterprising cyber criminals.

Many vendors are now using mobile devices such as smartphones and tablets as point-of-sale devices. For example, a farmer's market vendor or a taxi driver may now swipe your credit card through their personal smartphone rather than a dedicated point-of-sale device. Alternatively, a big box retailer may replace their existing point-of-sale devices with well known smartphones or tablets. A malicious attacker who has infected these devices, which is likely easier than infecting existing point-of-sale devices, could potentially skim every credit card transaction.

Additional potential revenue-generating schemes likely to be seen in the near future are discussed as well. These include:

- Selling stolen International Mobile Equipment Identity (IMEI) numbers for use on previously blocked or counterfeit phones.
- Peddling fake mobile security products—another tactic that has been highly successful in the PC realm.

The paper surmises that only if the current monetization schemes and those likely to be seen in the near future, succeed will attackers continue to invest in the creation of Android malware.

Full whitepaper (PDF): [Motivations of Recent Android Malware](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf)<sup>4</sup>

---

<sup>4</sup>[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/motivations\\_of\\_recent\\_android\\_malware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf)

## Global Trends & Content Analysis

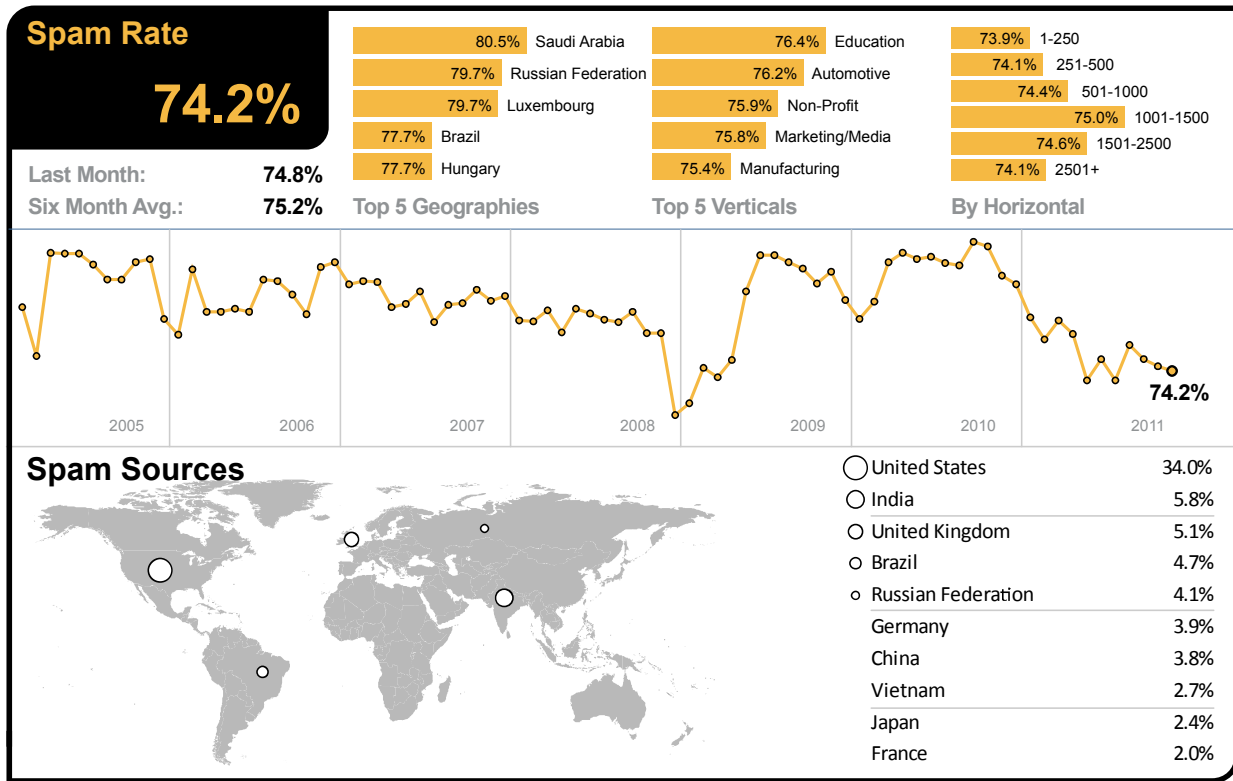
Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Sceptic™, the Symantec.cloud 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 October 2011, the global ratio of spam in email traffic declined slightly to 74.2 percent (1 in 1.35 emails), a decrease of 0.6 percentage points when compared with September 2011.



October 2011

As the global spam level remained relatively unchanged in October 2011, Saudi Arabia remained the most spammed geography; with a spam rate of 80.5 percent and Russia also remained the second most-spammed with 79.7% spam in email traffic.

In the US, 73.8 percent of email was spam and 73.2 percent in Canada. The spam level in the UK was 74.8 percent. In The Netherlands, spam accounted for 75.6 percent of email traffic, 74.8 percent in Germany, 75.7 percent in Denmark and 72.8 percent in Australia. In Hong Kong, 73.4 percent of email was blocked as spam and 72.2 percent in Singapore, compared with 70.8 percent in Japan. Spam accounted for 74.8 percent of email traffic in South Africa and 77.7 percent in Brazil.

Despite a small drop in spam, the Education sector overtook the Automotive industry to become the most spammed industry sector in October, with a spam rate of 76.4 percent. The spam level for the Chemical & Pharmaceutical sector was 74.0 percent, compared with 73.8 percent for IT Services, 74.0 percent for Retail, 73.8 percent for Public Sector and 73.5 percent for Finance.

The spam rate for small to medium-sized businesses was 73.9%, compared with 74.1% for large enterprises.

### Global Spam Categories

The most common category of spam in October 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	October 2011	September 2011
Pharmaceutical	37.5%	52.5%
Casino/Gambling	23.5%	16.0%
Watches/Jewelry	15.0%	7.5%
Unsolicited Newsletters	6.5%	14.5%
Scams/Fraud/419	6.0%	<0.5%
Weight Loss	4.5%	1.5%
Adult/Sex/Dating	2.5%	3.5%
Unknown/Other	1.5%	4.0%
Software	1.5%	0.5%
Jobs/Recruitments	0.5%	1.0%
Degrees/Diplomas	0.5%	<0.5%
Malware	0.5%	0.5%
Phishing	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 October, with the most frequent being associated with a surge in generic polymorphic malware, spoofing the identity of an international delivery service. Pharmaceutical related subjects are also becoming increasingly more common.

Rank	October 2011 Total Spam: Top Subject Lines	No. of Days	September 2011 Total Spam: Top Subject Lines	No. of Days
1	NACHA security nification	2	UPS notification	6
2	ACH Payroll Cancelled	2	Uniform traffic ticket	4
3	ACH Transfer Review	6	You have notifications pending	22
4	Re: Back to School Software Sale	6	SALE OFF: Pharmacy store!	2
5	0	6	(blank subject line)	31
6	Facebook Administration has sent you a notification	9	Re: Windows 7, Office 2010, Adobe CS5 ...	12
7	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18	Sarah Sent You A Message	11
8	Re: Windows 7, Office 2010, Adobe CS5 ...	18	Ed-Meds-Antidepressants-And-Pain Relief-Meds-80%-OFF	25
9	Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	9
10	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 ...	18	Fw: Windows 7, Office 2010, Adobe CS5 ...	9

### Spam URL TLD Distribution

The proportion of spam exploiting URLs in the .com and .info top-level domains fell by 2.2 and 2.3 percentage points respectively, with the only increase relating to spam URLs in the .ru TLD.

TLD	October	September	Change (% points)
.com	57.3%	59.5%	-2.2
.info	8.2%	10.5%	-2.3
.ru	8.4%	8.1%	+0.3
.net	5.3%	5.8%	-0.5

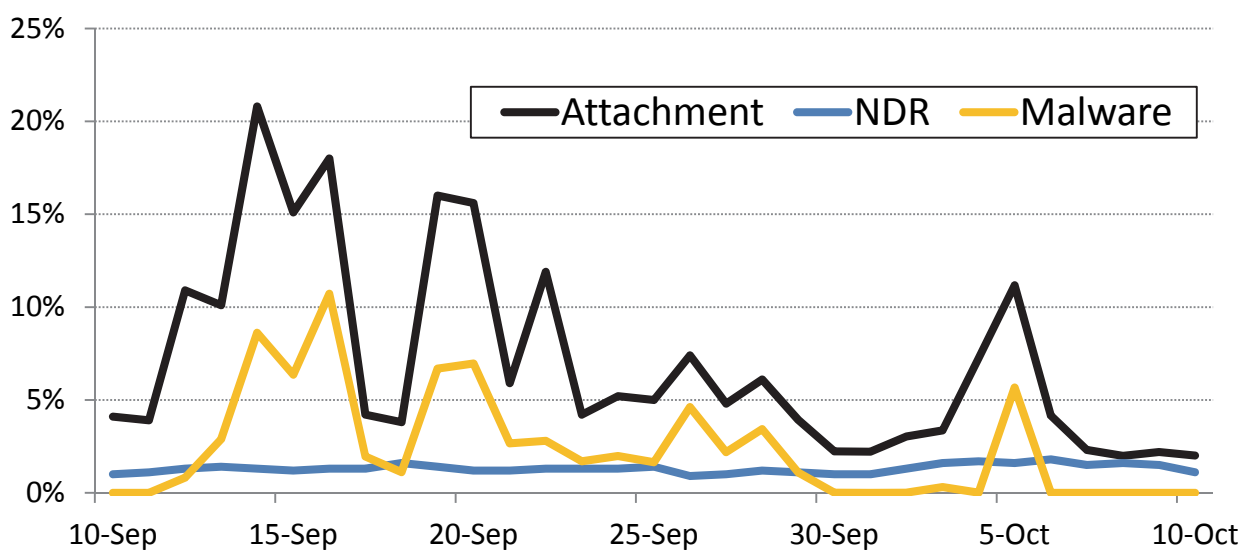
### Average Spam Message Size

In October, approximately 3 in every 5 spam emails was 5Kb in size or less, however, spam with a larger file size, including attachments diminished by 11.5 percentage points compared with September, as the number of malware attacks utilizing generic polymorphic malware variants decreased in October.

Message Size	October	September	Change (% points)
0Kb – 5Kb	59.0%	48.1%	+10.9
5Kb – 10Kb	26.3%	25.6%	+0.7
>10Kb	14.7%	26.2%	-11.5

### Spam Attack Vectors

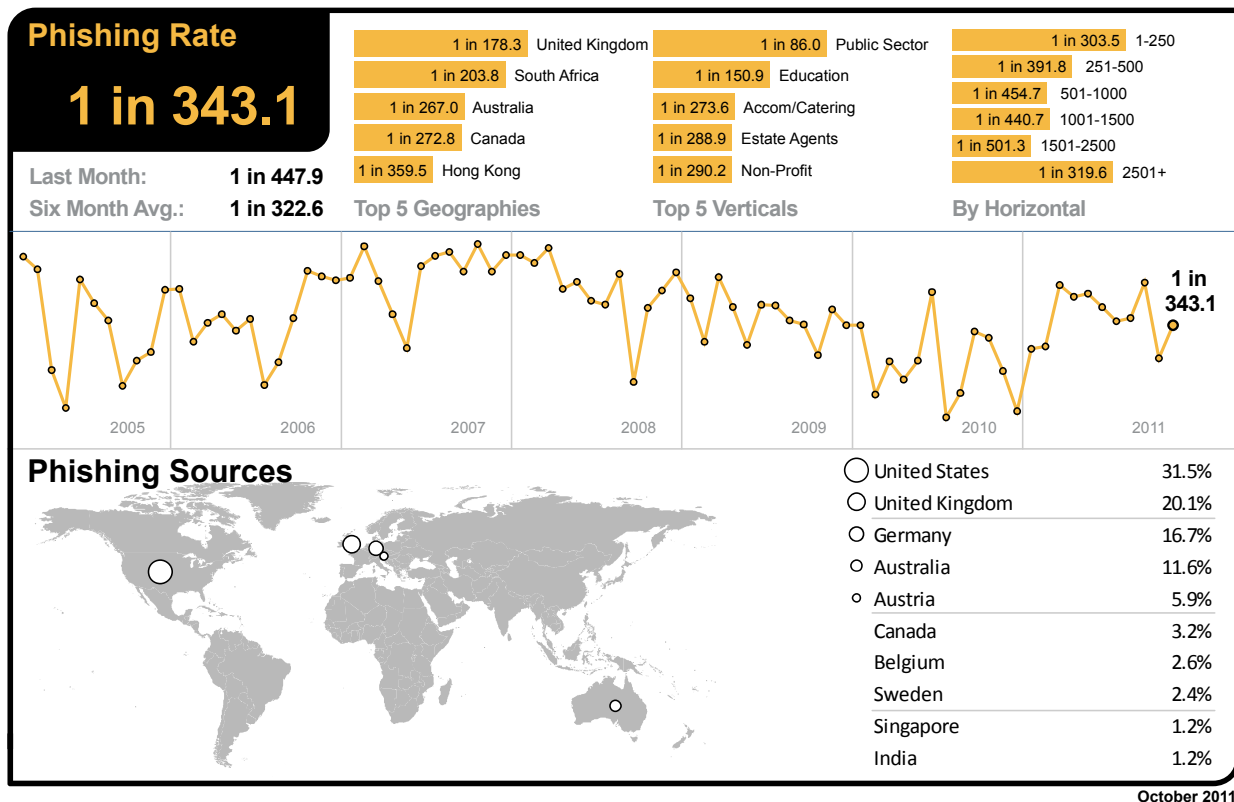
It can be seen in the chart below that the number of malicious attacks that contained a malicious attachment fell from the end of September. The number of attacks was much lower in October. Many of these attachments were connected to a rise in volume of generic polymorphic malware variants, as discussed in the September report.



In October, the number of spam emails resulting in NDRs (spam related non-delivery reports), has been stable during October, suggesting the attackers may be using valid email distribution lists to conduct these attacks. NDRs 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 October, phishing email activity diminished by 0.07 percentage points since September 2011; one in 343.1 emails (0.29 percent) comprised some form of phishing attack.

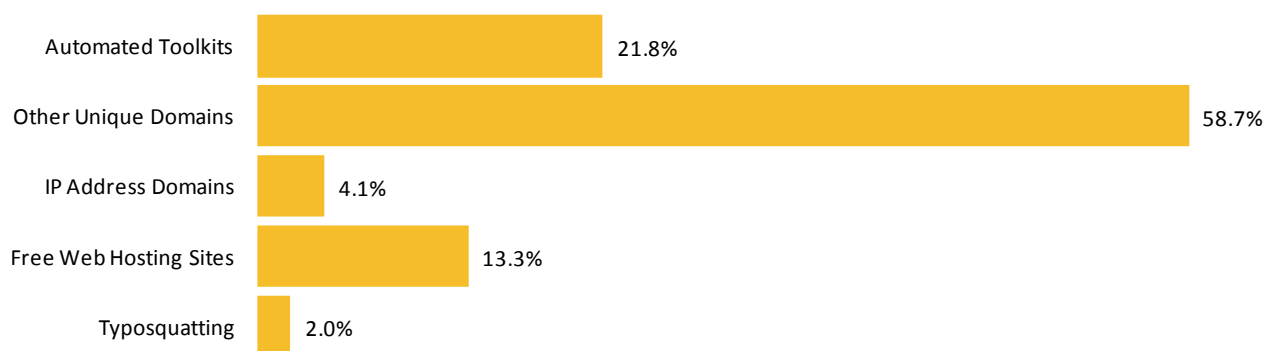


## Geographic Location of Phishing Web Sites



October 2011

## Tactics of Phishing Distribution



## Organizations Spoofed in Phishing Attacks, by Industry Sector

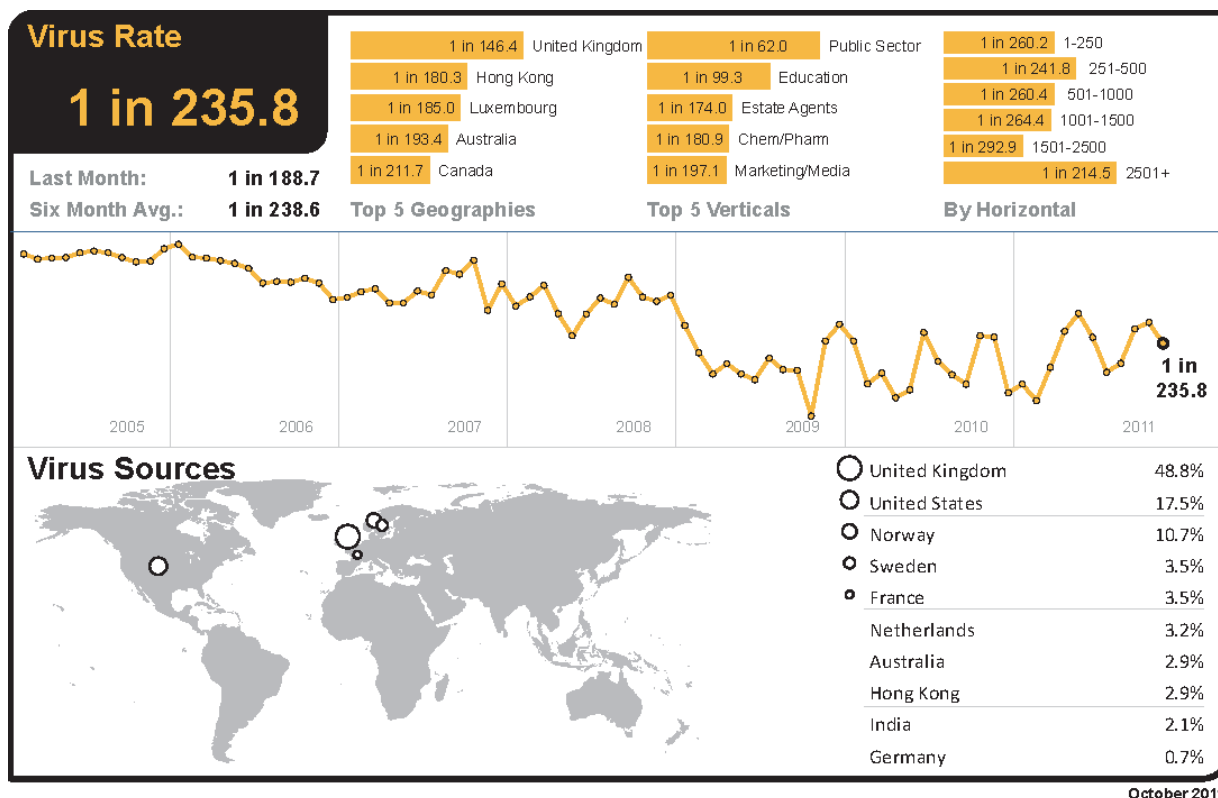


# Malware Analysis

## Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 235.8 emails (0.42 percent) in October, a decrease of 0.11 percentage points since September 2011.

In October, 20.1 percent of email-borne malware contained links to malicious Web sites, an increase of 3.6 percentage points since September 2011. Emails that contained generic polymorphic malware variants accounted for 45.1 percent of all email-borne malware in October, compared with 72.0 percent in September; many included attached ZIP files that contained the generic malware.



The UK climbed to the top of the table with the highest ratio of malicious emails in October, with one in 146.4 emails identified as malicious. Hong Kong was the geography with the second highest rate, with one in 180.3 emails identified as malicious in October.

The previous month's top spot belonged to South Africa, which dropped to eleventh position in October, with one in 326.0 emails blocked as malicious. Virus levels for email-borne malware in the US reached one in 330.2 and one in 211.7 in Canada. In Germany virus activity reached one in 330.9, one in 457.1 in Denmark and in The Netherlands one in 319.4. In Australia, one in 193.4 emails was malicious. For Japan the rate was one in 1048, compared with one in 272.4 in Singapore. In Brazil, one in 421.7 emails contained malicious content.

With one in 62.0 emails being blocked as malicious, the Public Sector remained the most targeted industry in October. Virus levels for the Chemical & Pharmaceutical sector reached one in 180.9 and one in 257.3 for the IT Services sector; one in 355.4 for Retail, one in 99.3 for Education and one in 332.9 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses accounted for one in 260.2 emails, compared with one in 214.5 for large enterprises.

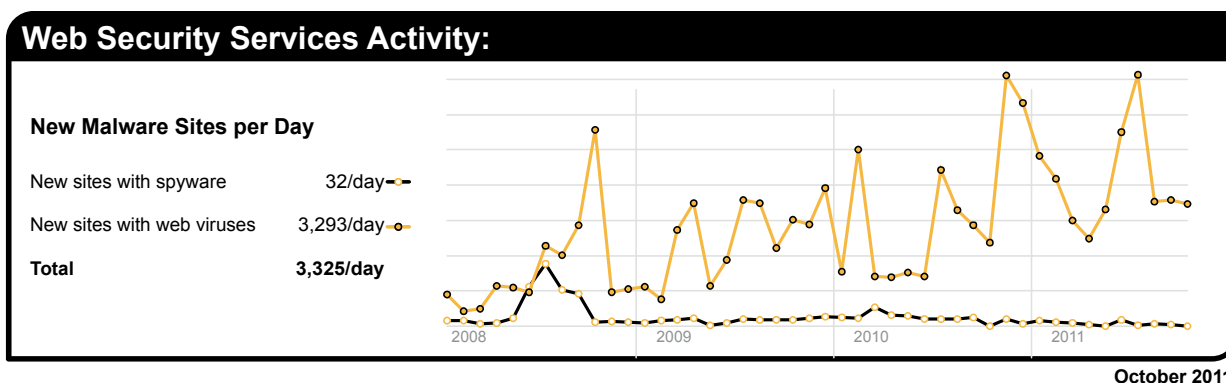
The table below shows the most frequently blocked email-borne malware for October, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Overall, 45.1 percent of email-borne malware was associated with variants of generic polymorphic malware, including Bredolab, Sasfis, SpyEye and Zeus variants.

Malware Name	% Malware
Gen:Trojan.Heur.FU.bqW@a8hiAJoi	6.51%
W32/Generic-0922-13ca-13ca	5.95%
Exploit/Link-generic-ee68	5.86%
Gen:Variant.Ursnif.16	3.91%
Trojan.Bredolab!eml-866c	3.28%
Gen:Trojan.Heur.FU.bqW@aS39a0fi	2.02%
Trojan.Bredolab!eml-4e1b	1.96%
Gen:Trojan.Heur.FU.bqW@a0CDPdfi	1.74%
W32/Generic-703e-4489	1.55%
Exploit/FakeAttach	1.43%

### Web-based Malware Threats

In October, Symantec Intelligence identified an average of 3,325 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 4.3 percent since September 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 43.9 percent of all malicious domains blocked were new in October; a decrease of 0.7 percentage points compared with September 2011. Additionally, 15.2 percent of all Web-based malware blocked was new in October; an increase of 0.7 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 October 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 37.5 percent of blocked Web activity in October. 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 18.1 percent of URL-based filtering activity blocked, equivalent to approximately one in every 5.5 Web sites blocked. Many organizations

allow access to social networking Web sites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Activity related to Streaming Media policies resulted in 8.9 percent of URL-based filtering blocks in October. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This rate is equivalent to one in every 11.2 Web sites blocked.

Web Security Services Activity:					
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	37.5%	VBS/Generic	45.3%	PUP:Generic.188886	34.7%
Social Networking	18.1%	Trojan.ADH.2	16.2%	PUP:9231	20.4%
Streaming Media	8.9%	Trojan:GIF/GIFrame.gen!A	7.2%	PUP:W32/CnsMin.S	7.4%
Computing and Internet	4.1%	Gen:Trojan.Heur.gq0@vj7DnZiix	6.2%	PUP:Generic.192303	6.0%
Unclassified	3.8%	W32.Downadup.B	1.8%	PUP:Generic.62006	4.5%
Chat	3.4%	Trojan.Gen	1.6%	PUP:Generic.183433	3.4%
Search	3.0%	Trojan.Gen.2	1.3%	PUP:Generic.183172	3.0%
Peer-To-Peer	2.3%	Infostealer.Gampass	1.2%	PUP:Keylogger	2.9%
Hosting Sites	2.0%	Gen:Variant.Kazy.32829	1.2%	PUP:Agent.NGG	2.2%
Gambling	1.6%	Trojan.Maljava	1.0%	PUP:JS.Script.C	2.0%

October 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 <sup>5</sup>	% Malware
W32.Sality.AE	7.19%
W32.Ramnit!html	7.18%
Trojan.Bamital	6.03%
W32.Ramnit.Blinf	5.72%
WS.Trojan.H	5.70%
W32.Downadup.B	3.19%
W32.SillyFDC.BDP!Ink	3.05%
W32.Virut.CF	2.74%
Trojan.ADH.2	2.58%
Trojan.ADH	2.55%

The most frequently blocked malware for the last month was W32.Sality.AE<sup>6</sup>, a virus that spreads by infecting executable files and attempts to download potentially malicious files from the Internet. For much of 2010, W32.Sality.AE had been the most prevalent malicious threat blocked at the endpoint.

<sup>5</sup>For further information on these threats, please visit: [http://www.symantec.com/business/security\\_response/landing/threats.jsp](http://www.symantec.com/business/security_response/landing/threats.jsp)

<sup>6</sup> <http://www.symantec.com/connect/blogs/sality-whitepaper>

Variants of W32.Ramnit accounted for approximately 13.1% of all malware blocked at the endpoint, compared with 8.1% for variants of W32.Sality.

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

## 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 prevent 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.message-labs.com/intelligence](http://www.message-labs.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](http://www.symantec.com).

Copyright © 2011 Symantec Corporation. All Rights Reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the US and other countries. Other names may be trademarks of their respective owners.

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043.