Symantec Intelligence Report: October 2012

Scammers take to Instagram; Spam rates drop by 10 percentage points; Ransomware evolves

---

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

Report highlights

- Spam – 64.8 percent (a decrease of 10.2 percentage points since September): page 9
- Phishing – One in 286.9 emails identified as phishing (a decrease of 0.059 percentage points since September): page 12
- Malware – One in 229.4 emails contained malware (a decrease of 0.04 percentage points since September): page 13
- Malicious websites – 933 websites blocked per day (an increase of 19.7 percent since September): page 15
- Scammers attempt to leverage Instagram: page 2
- Why global spam rates are down this month: page 5
- The evolution of Ransomware: page 7
- Other stories in the threat landscape this month: page 8

Introduction

In this month's report we investigate a new social networking avenue that scammers are attempting to leverage: Instagram. They're doing so in order to gather personal details and persuade users to sign up for premium-rate mobile services, among other things. The scams take on a number of forms, from spam comments, to fake followers, to liking photos in the hopes people will check out their profiles, which in turn often contain more spam links.

We've also noticed a significant drop in email spam volumes this month. The global spam rate has dropped by more than 10%, from 75% of email traffic in September, down to 64.8% in October. We take a look at some of the likely causes for this significant drop.

Finally, we take a look at the evolution of 'ransomware' and discuss some of the most recent discoveries in the threat landscape during October.

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

Paul Wood, Cyber Security Intelligence, Symantec
symantec_intelligence@symantec.com

@symantec, @symanteccloud, @norton, @threatintel, @paulowoody

Report analysis

Instaspam: Scammers take to Instagram

by Ben Nahorney, Cyber Security Threat Analyst, Symantec

As an amateur photographer and fan of image effects, I've taken a liking to Instagram. I'm far from alone in this, given how the photo app has recently crossed the 100 million user mark.[1] Unfortunately, spammers have noticed this too and are attempting to take advantage of those using the popular service. They're approaching it from a variety of angles, in much the same way as they have on other social networks.

I discovered this recently with my own account. Since the photos I post lean towards an artistic bent, containing little or no personally identifiable information, I've opted to leave them publically viewable. Generally this isn't an issue, save for a sudden uptick in activity that seemingly came out of nowhere.

It all began when I received a notification on my phone about an Instagram comment. It came from an unfamiliar account, had nothing to do with the photo, and was obviously spam:

```
Hi there, Get a FREE Game in my Profile, OPEN it up, Get 85.90$ :-) xx
```

I went to check out the user, who appeared to be a rather attractive woman with followers in the thousands, but surprisingly for a photo-sharing service, not a single photo.

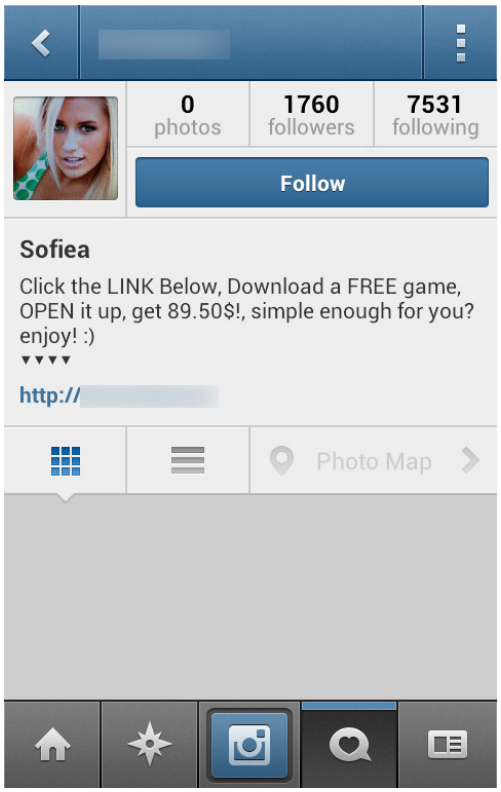


Figure 1 – Comment spam profile

Who was this mysterious lady? Her profile bio said largely the same thing as the comment she left me, but also included a shortened URL. What was interesting about this spam, setting it apart from similar comment spam you might see in a blog, was that the link resided on the profile rather than in the spam message. It even included explicit instructions about visiting the profile and opening the link. This could be due to URL monitoring carried out by Instagram, which could automatically remove a suspicious link if it was included in a comment. Regardless, I decided to see where this led. (Note: this was done under controlled conditions, avoiding potentially malicious activity. Do not try this at home, as you could compromise your device.)

[1] *http://mashable.com/2012/09/11/instagram-100-million/*

The link ended up pointing to a premium mobile service that offered to send me videos of cute animals for only €4.50 per month. To avail of this service, all I had to do was give them my phone number, and I'd no longer have to watch such videos for free on YouTube.

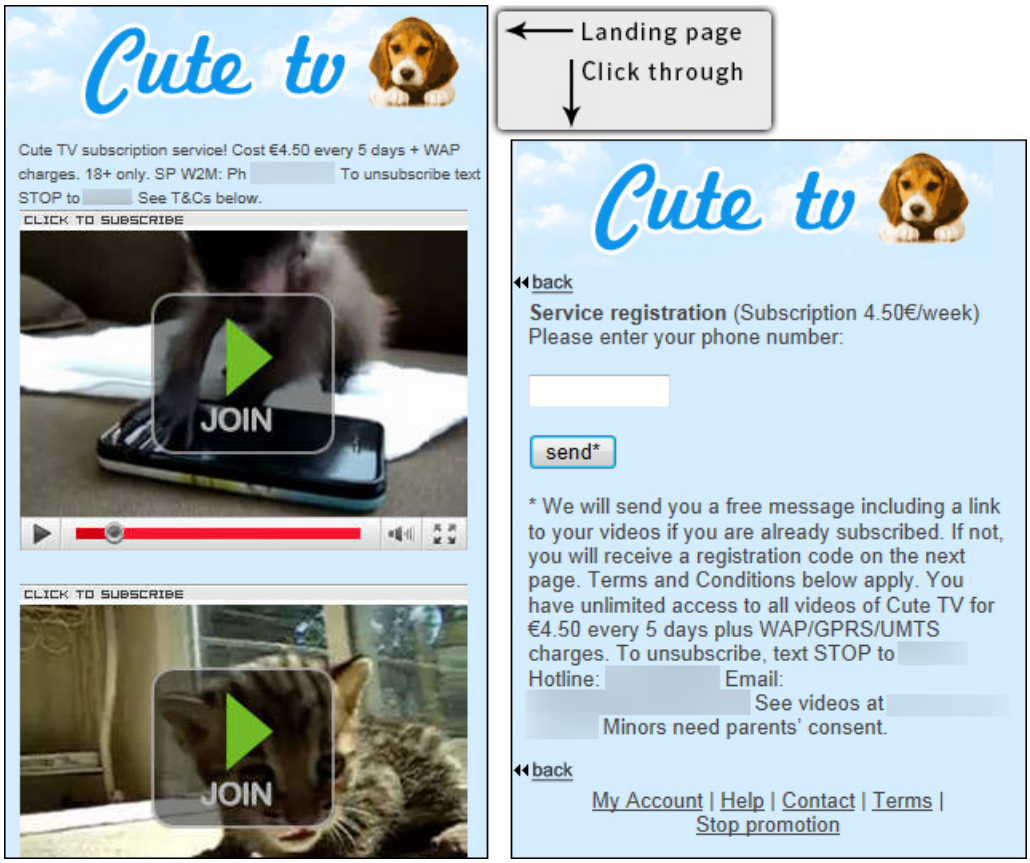


Figure 2 –Premium-rate service

I was happy to delete the comment and leave well enough alone, except I noticed something else: my follower numbers had not only gone up, but doubled. This was unusual in its own right, but it happened within a two-hour period.

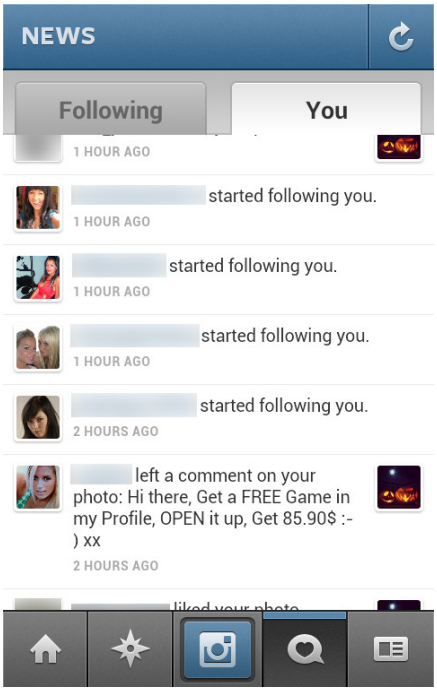


Figure 3 – Sudden increase in followers

Symantec™

So what led to this sudden popularity? Did I end up taking a particularly spectacular photo, garnering newfound fame, and eventually hitting Instagram's Popular page? Or was something else in the mix here? All of these new followers had a few things in common:

- They were all "women" with attractive profile pictures.
- None of them had posted any photos.
- Their profile Bios included a quote, followed by a shortened URL.

While the shortened URL was different in each profile, they all lead to the same location—an advertisement for fake jobs working in social media. All you had to do to "Get Paid $250/Day To Mess Around on Facebook And Instagram" was give them your name and email address.

Figure 4 – Fake follower profile leading to phishing scam

This type of spam could lead to phishing scams. What's disconcerting is that each profile had followers in the thousands. This is likely due to the "call and response" nature of many social networks: you follow me and I'll follow you. Each account was following far more profiles than were following it, further supporting this idea.

I figured that this would be it, but was surprised to be hit by a third scam wave. I noticed a significant increase in "likes" for my last photo. These likes came from what appear to be real profiles, with uploaded pictures. However, all the photos, the user names used, and bio information center on advertising income referral programs. The sole purpose of these accounts appears to be to get you to sign up for the program, resulting in the profile owner earning money for every member referred. This is in contrast to situations where a legitimate account has been compromised and used to send out messages. Most of the photos were meme-type pictures, advertising the referral program, pictures of expensive items seemingly purchased with the money made, or shots of guys holding large bundles of $100 bills. These programs could be likened to classic pyramid schemes—only those involved are now using social networking to advertise them.

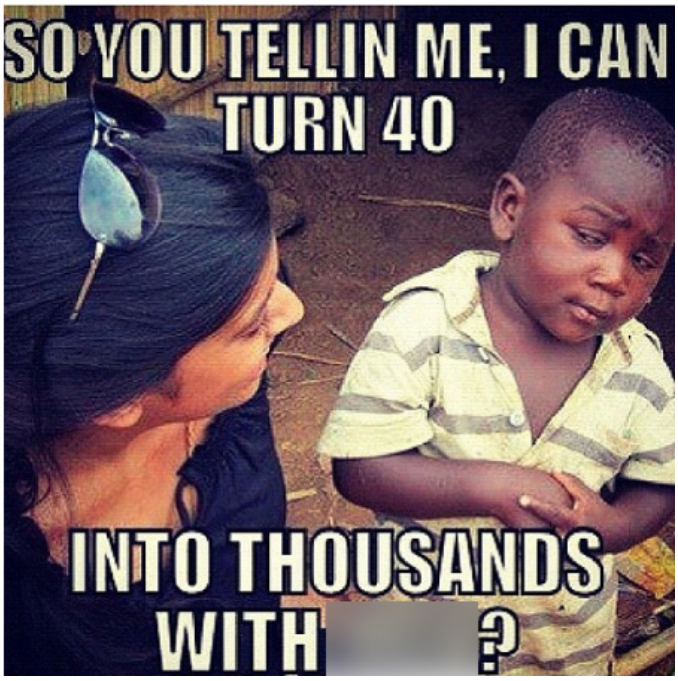


Figure 5 – User showing money supposedly made through scheme; meme-type picture advertising referral program.

How successful are these various scam campaigns? It turns out they could be fairly lucrative. For instance, we were able to determine that the URL on my commenter's profile has been clicked close to 10,000 times in little more than a month. If only a fraction of users sign up for the premium rate service, give away personal information, or join the semi-legitimate referral service, the scammers could consider their efforts successful.

It's important to note that Instagram isn't alone when it comes to scams like these, and most social networks have methods to deal with them. Posting spam clearly violates Instagram's community guidelines and accounts found guilty of doing so are quickly disabled. In fact Instagram actively monitors for certain content and has put together a detailed privacy and safety how-to covering how to report inappropriate comments and users.[2]

In addition to this, the following best practices will help you stay safe:

- Set your account to Private. This way you have control over who follows you and who doesn't.
- Don't follow arbitrary followers. If you suspect an account isn't real, ignore it.
- Don't click shortened URLs unless you know where they lead.
- Optional: Don't follow or accept followers without photos. The exception to this rule is if you know the person. Some people do like to view photos, but don't like to take them.
- Finally, report any suspicious accounts or comments to Instagram and follow their Privacy & Safety guidelines.[3]

Why October spam fell by 10 percentage points

We noticed something interesting this month when analyzing our spam rates: there's been a 10 percentage point drop in the global spam rate for the month. We decided to take a closer look at what may be responsible for the drop.

We took a look at the spam rates over seven day averages. These averages peaked in mid-September, at around 43 million messages per day, and then began their decline, bottoming out around the beginning of October.

[2] *http://help.instagram.com/customer/portal/articles/95788*
[3] *http://help.instagram.com/customer/portal/topics/43528-privacy-safety/articles*

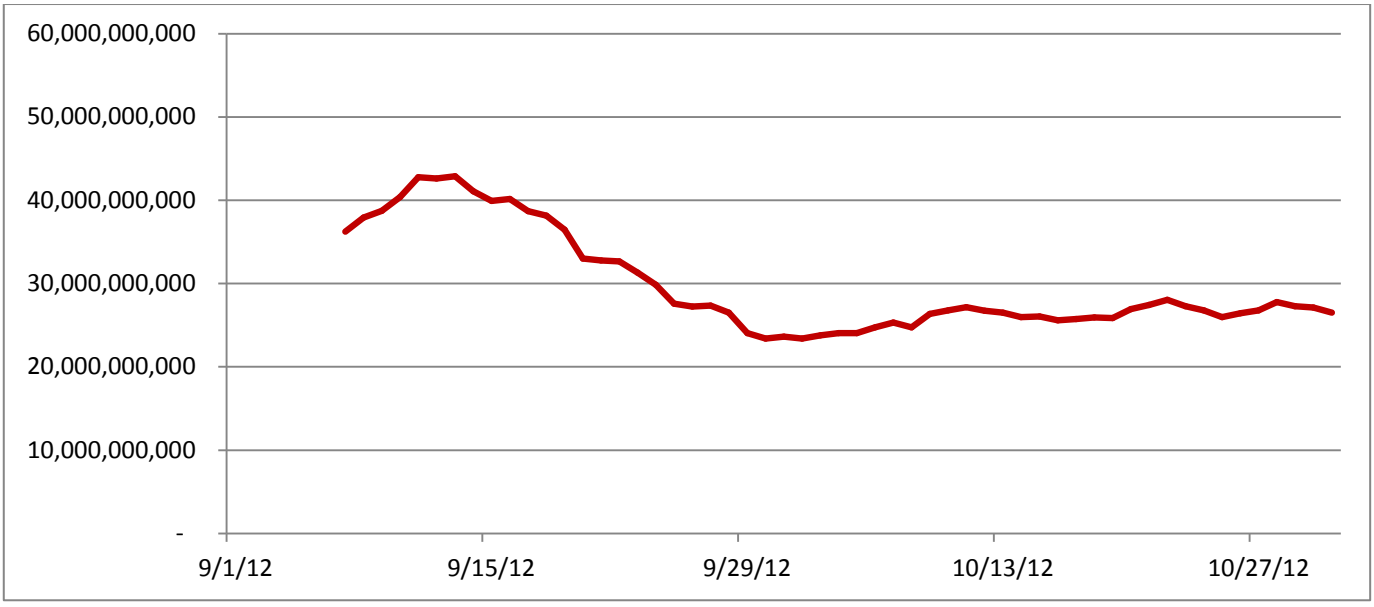


Figure 6 – Seven-day averages of spam rates for September and October. (NB. Dates in MM/DD/YYYY format)

It appears that the Festi botnet has recently gone quiet and could be partly responsible for this sudden decline. This botnet was very active in early September before all but disappearing in October.

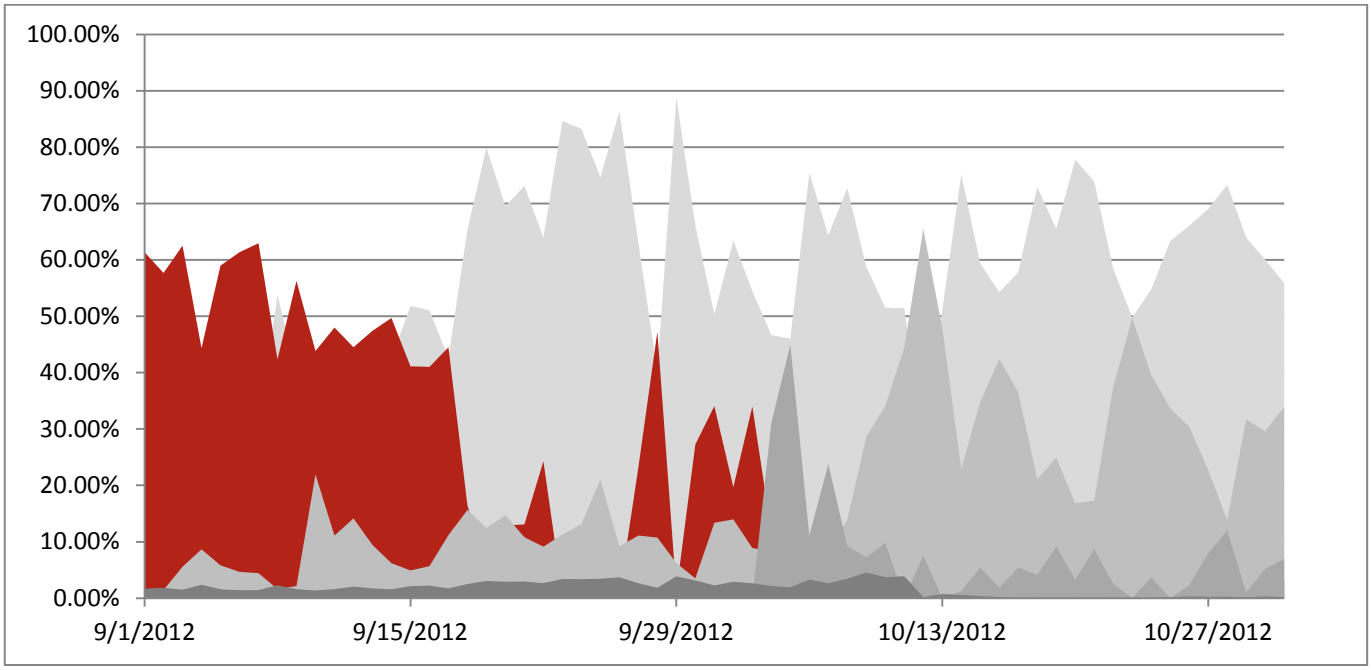


Figure 7 – Festi botnet disappears in October. (NB. Dates in MM/DD/YYYY format)

This drop is most evident when looking at Saudi Arabia. Previously a hotbed for Festi-related spam in recent months, the botnet seems to have become largely dormant in the country—so much so that the country has gone from having the highest spam rate worldwide to completely dropping out of the top ten in October.

Does this mean we're winning the war against botnets and spam? We're pleased to see that a 10 percentage point drop in the global spam rate can result in a 50 percent drop in spam volume over a two-month period. Unfortunately, we've seen drops like this before, where other botnets soon jump in to pick up the slack, or a "dead" botnet is reincarnated in a slightly different manifestation. For example, the Kelihos botnet is now believed to be in at least its third incarnation since Microsoft targeted the botnet in the company's efforts to disrupt the botnet over 12 months ago. Still it's certainly good news, and persistent efforts to uncover and shut down such botnets should continue to pay dividends.

Ransomware Evolution: The Journey Continues…

by Hon Lau, Security Response, Symantec

This year has seen a ramping up in the presence of ransomware, not just in terms of the sheer numbers seen in the wild, but also in terms of the incorporation of new techniques.

In the early days, ransomware creators were content with simply locking the screen and displaying simple and straight-forward messages asking for payment of a ransom to restore access to your computer. They may even encrypt files and request payment for a decryption key. These techniques tell of a lack of imagination, but at least the technique was tried and tested. They represented the initial efforts of cybercriminals to extort money from innocent users. The use of embarrassing materials, such as displaying pornographic images on the screen of a locked computer, was fairly effective and used often.

More recently, ransomware purporting to be from law enforcement, with content localized to the country of the user, has become the norm. Typically, the lock-up screen in these examples uses social engineering to inform the user that they have been caught engaging in illegal online activity. The threats subsequently threaten to involve law enforcement or take legal action in order to coerce the user to comply.

As shown in a report from November 2011,[4] about 46 percent of adults in the US have acquired copyright materials through less than legitimate means. For the 18-29 age group, an even larger percentage of 70% have engaged in such activity. If these statistics do indeed reflect the reality on the ground, then you can be sure that this law enforcement-inspired social engineering trickery has a good chance of working, particularly when combined with other techniques, such as screen and input device locking.

It is against this backdrop that we have recently observed a new variant (Trojan.Ransomlock.Y)[5] demonstrating further innovation on the part of the ransomware creators.

Figure 9 – Example Ransomware lock screen

[4] *http://piracy.americanassembly.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf*
[5] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-100921-0457-99&tabid=2*

This variant, utilizes many of the existing techniques already previously described, but it also repeatedly plays an audio file. The audio file states:

FBI warning: Your computer is blocked for violation of federal law!

This ties in nicely with the FBI-inspired lockup screen in order to give a compelling reason to the user to act quickly. What this recent development goes to show is that the culprits behind the ransomware are getting more creative, with powerful financial motives at play. We can expect to see further innovations in the near future, as they attempt to milk a possible cash cow further. Don't be surprised to see crossover techniques, once used in fake antivirus, adapted for use the context of ransomware, and whatever else these attacker's minds can think up.

Further reading:
The Ransomlock family has been at the forefront of the recent growth in ransomware. For an overview of the Ransomlock family of Trojans, you can read our recently published Trojan.Ransomlock family writeup.[6]

Security Response is also publishing a new whitepaper about Ransomware. You can download a copy of this paper entitled: Ransomware: A Growing Menace.[7]

Other news in the Threat Landscape

contributions by Eamonn Young and Jarrad Shearer

At the beginning of the summer, Symantec analyzed a new threat by the name of W32.Flamer.[8] The level of sophistication of this threat was only matched by that of W32.Stuxnet[9] and W32.Duqu.[10] It came to our attention that this threat had been operating for the past two years and had been primarily targeting computers in the Middle East.[11]

Recently, we discovered a new module of this threat.[12] This is one of those previously unknown components using one of the supported protocols. We named this new component W32.Flamer.B,[13] which opens a back door on a compromised computer and allows an attacker to steal information.

A new version of the Blackhole toolkit[14] also appeared in October. Deemed Blackhole 2.0, the newer version of the toolkit has removed previous patched vulnerabilities and is now providing a number of new features to make it harder for antivirus software to detect and defend against exploit attacks. For instance, the new version includes single-use URL generation, and can manage multiple domains from one administrative panel.

Finally, some good new broke this month as authorities in Australia, Canada, and the US joined forces to shut down global tech support scams responsible for cold-calling users and erroneously telling them their computers are infected with viruses.[15] Canadian authorities announced that they had shut down two companies[16] and fined them over $500,000 in total. Meanwhile, US authorities announced that they froze the assets of six operators[17] and initiated legal action against 16 companies and 17 individuals.

While a victory for the good guys, it won't likely stop this type of scam entirely, as others will very well take their place. Remember to remain vigilant and know that tech companies won't call unsolicited. If you receive a call from someone claiming to be a technical support agent, it's likely a scam.

---

[6] *http://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99*
[7] *http://bit.ly/RCJbYy*
[8] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99*
[9] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99*
[10] *http://www.symantec.com/security_response/writeup.jsp?docid=2011-101814-1119-99*
[11] *http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east*
[12] *http://www.symantec.com/connect/blogs/w32flamerb-additional-module-discovered*
[13] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-101611-2743-99*
[14] *http://www.symantec.com/connect/blog-tags/blackhole*
[15] *http://www.youtube.com/watch?v=WhV6rIgyQ-s*
[16] *http://www.crtc.gc.ca/eng/com100/2012/r121003.htm*
[17] *http://www.ftc.gov/opa/2012/10/pecon.shtm*

Global Trends & Content Analysis

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

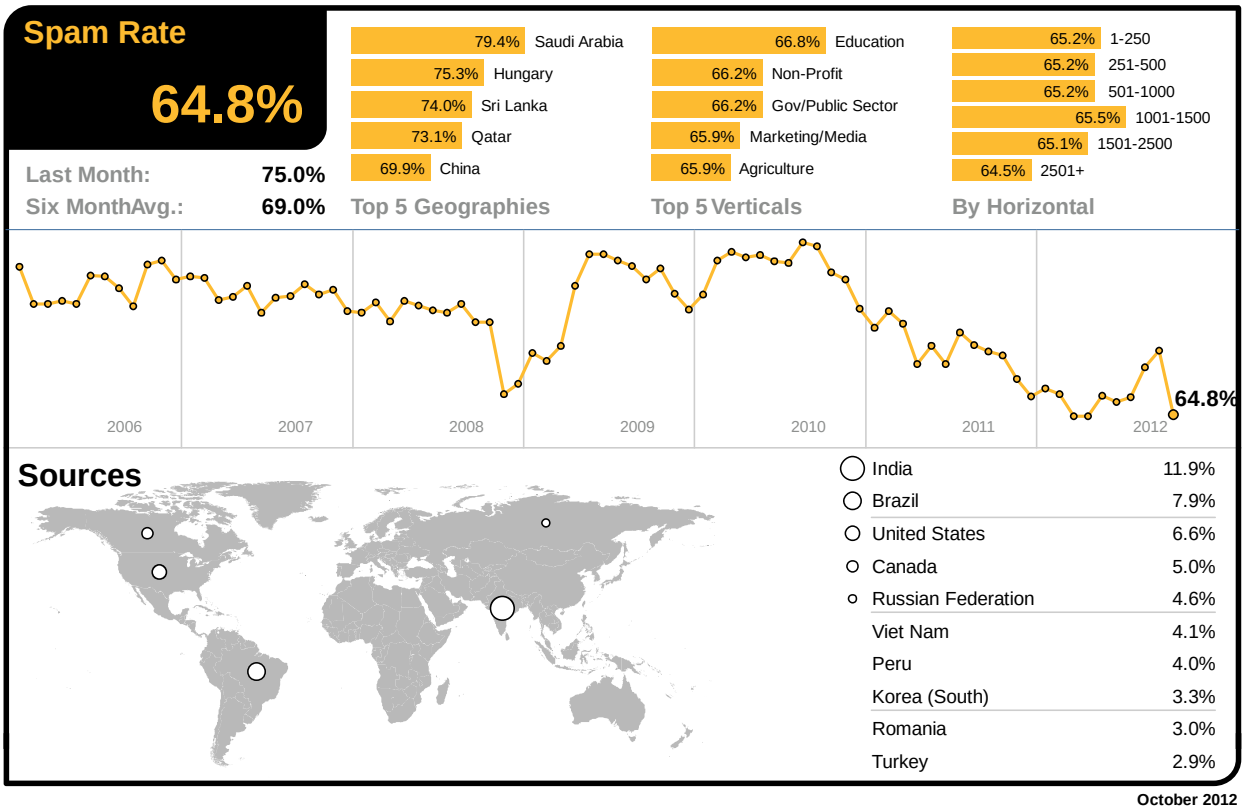
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

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

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

Spam Analysis

In October, the global ratio of spam in email traffic fell by 10.2 percentage point since September, to 64.8 percent (1 in 1.54 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



Global Spam Categories

The most common category of spam in October is related to the Sex/Dating category, with 62.73 percent.

Category Name	October 2012	September 2012
Sex/Dating	62.73%	47.93%
Jobs	10.45%	7.83%
Pharma	9.79%	27.64%
Watches	3.74%	12.49%
Software	2.49%	1.20%
Casino	0.75%	2.26%
Degrees	0.35%	0.15%
Mobile	0.19%	0.17%
419/scam/lotto	0.11%	0.14%
Newsletters	0.04%	0.05%
Weight Loss	0.01%	<0.01%

Spam URL Distribution based on Top Level Domain Name

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

TLD	October 2012	September 2012
.com	63.1 %	60.4 %
.net	6.8 %	6.3 %
.ru	4.3 %	12.1 %
.info	3.3 %	3.7 %

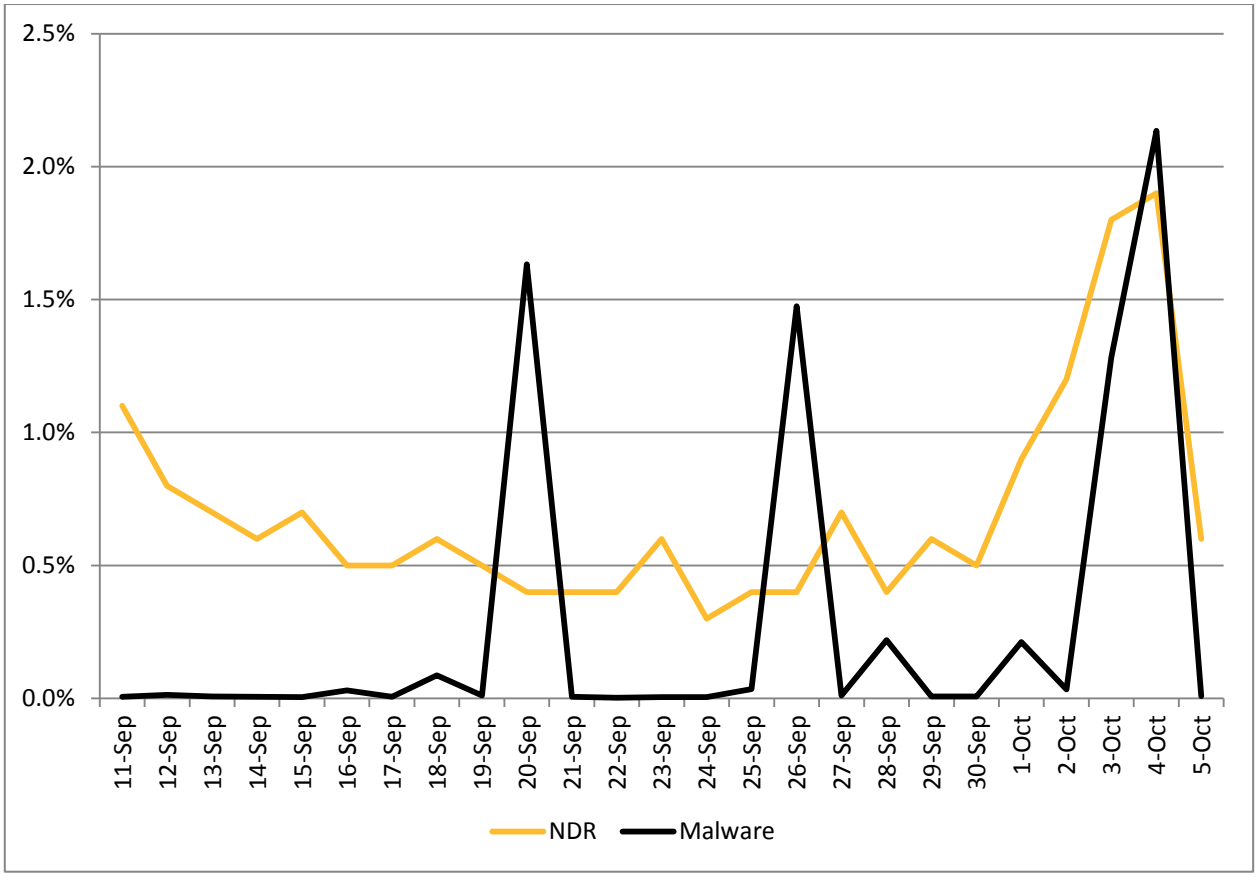
Average Spam Message Size

In October, the proportion of spam emails that were 5Kb in size or less decreased by 20.3 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size increased by one percent, as can be seen in the following table.

Message Size	October 2012	September 2012
0Kb – 5Kb	41.8 %	62.1 %
5Kb – 10Kb	40.9 %	21.7 %
>10Kb	17.3 %	16.3 %

Spam Attack Vectors

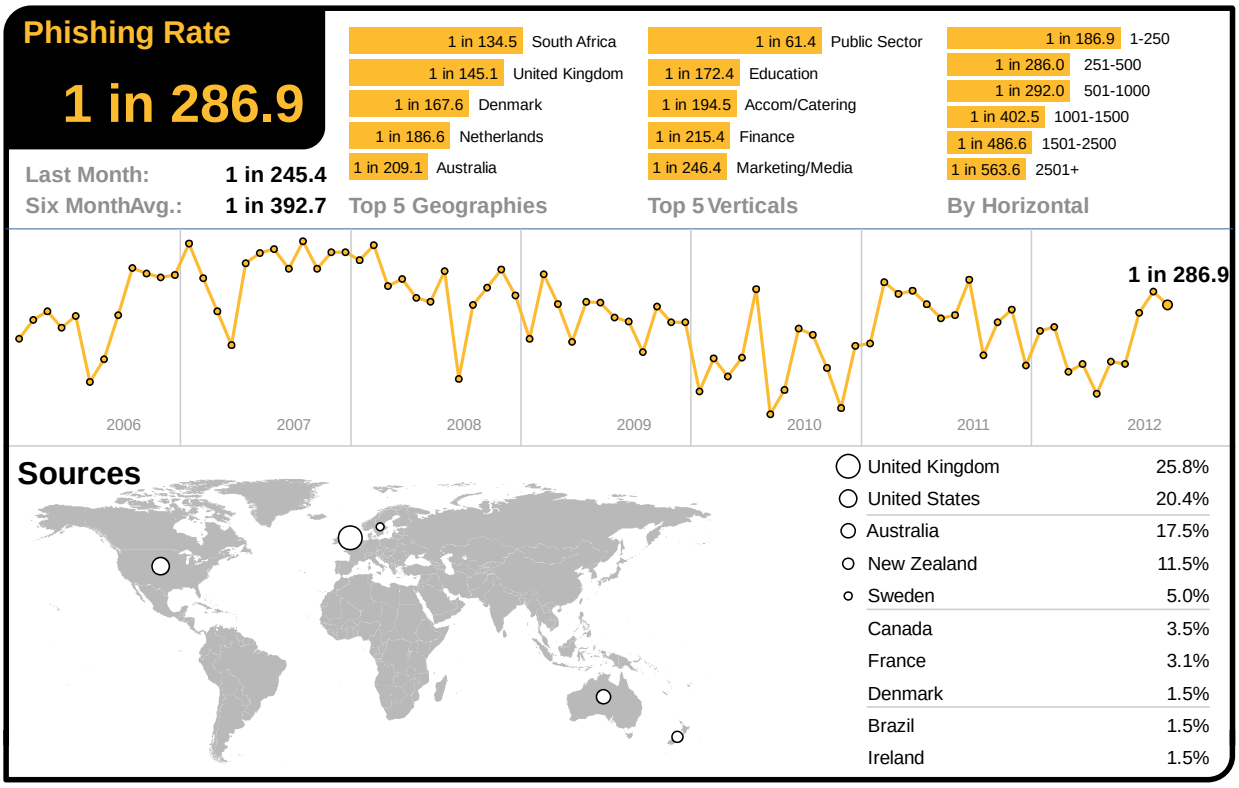
October highlights the increase in spam emails resulting in NDRs (spam related non-delivery reports). In these cases, the recipient email addresses are invalid or bounced by their service provider. The proportion of spam that contained a malicious attachment or link increase, with periodic spikes of spam activity during the period, as shown in the chart below.



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

Phishing Analysis

In October, the global phishing rate decreased by 0.059 percentage points, taking the global average rate to one in 286.9 emails (0.35 percent) that comprised some form of phishing attack.

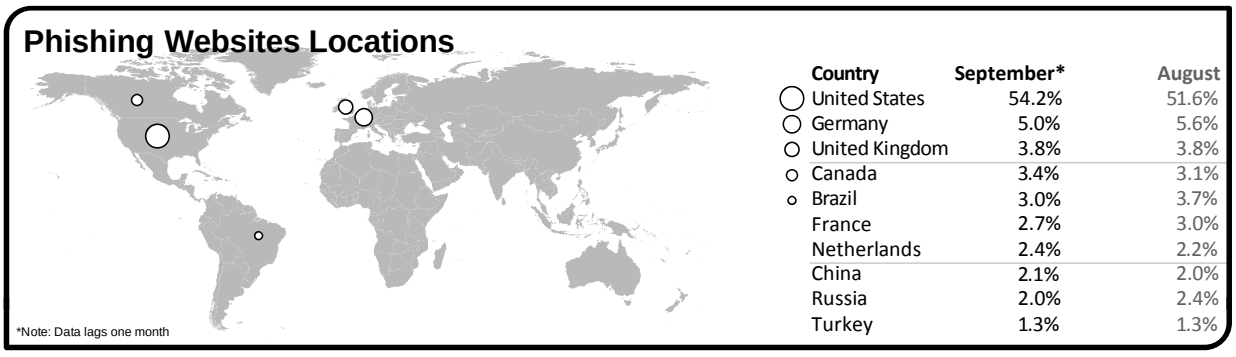


October 2012

Analysis of Phishing Websites

The overall phishing decreased by about 22 percent this month. Unique domains decreased by about 13 percent as compared to the previous month. Phishing websites that used automated toolkits increased by 5 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 30 percent. Webhosting services comprised of 4 percent of all phishing, a decrease of 4 percent from the previous month. The number of non-English phishing sites increased by 17 percent. Among non-English phishing sites, French, Italian, Portuguese, and Chinese were highest in September.

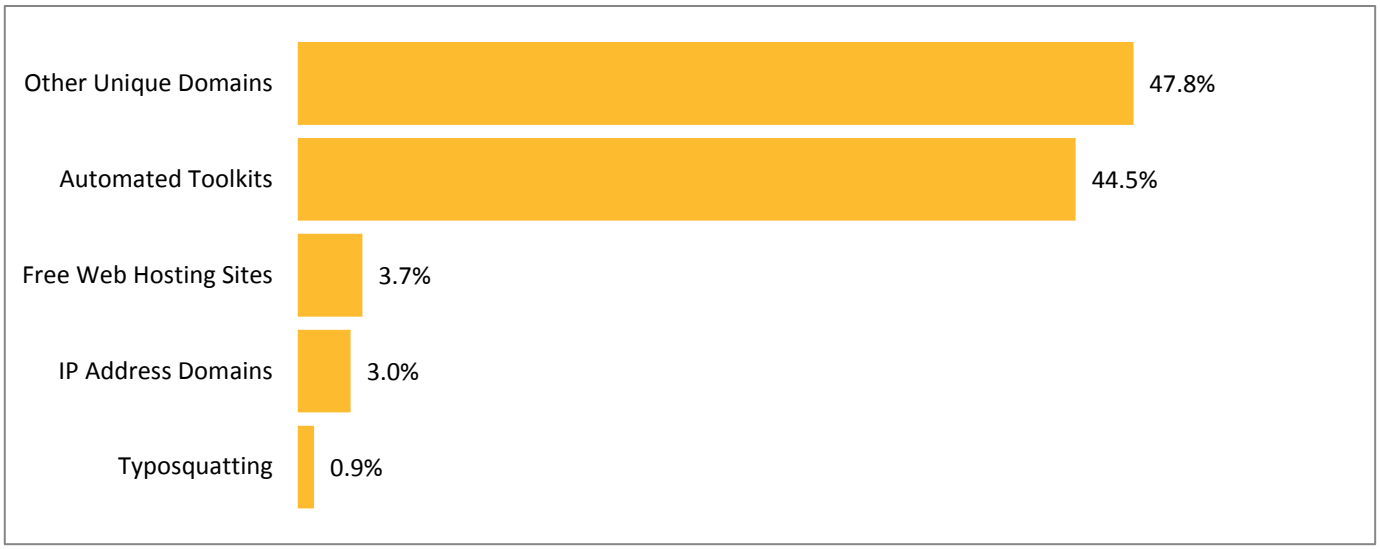
Geographic Location of Phishing Websites



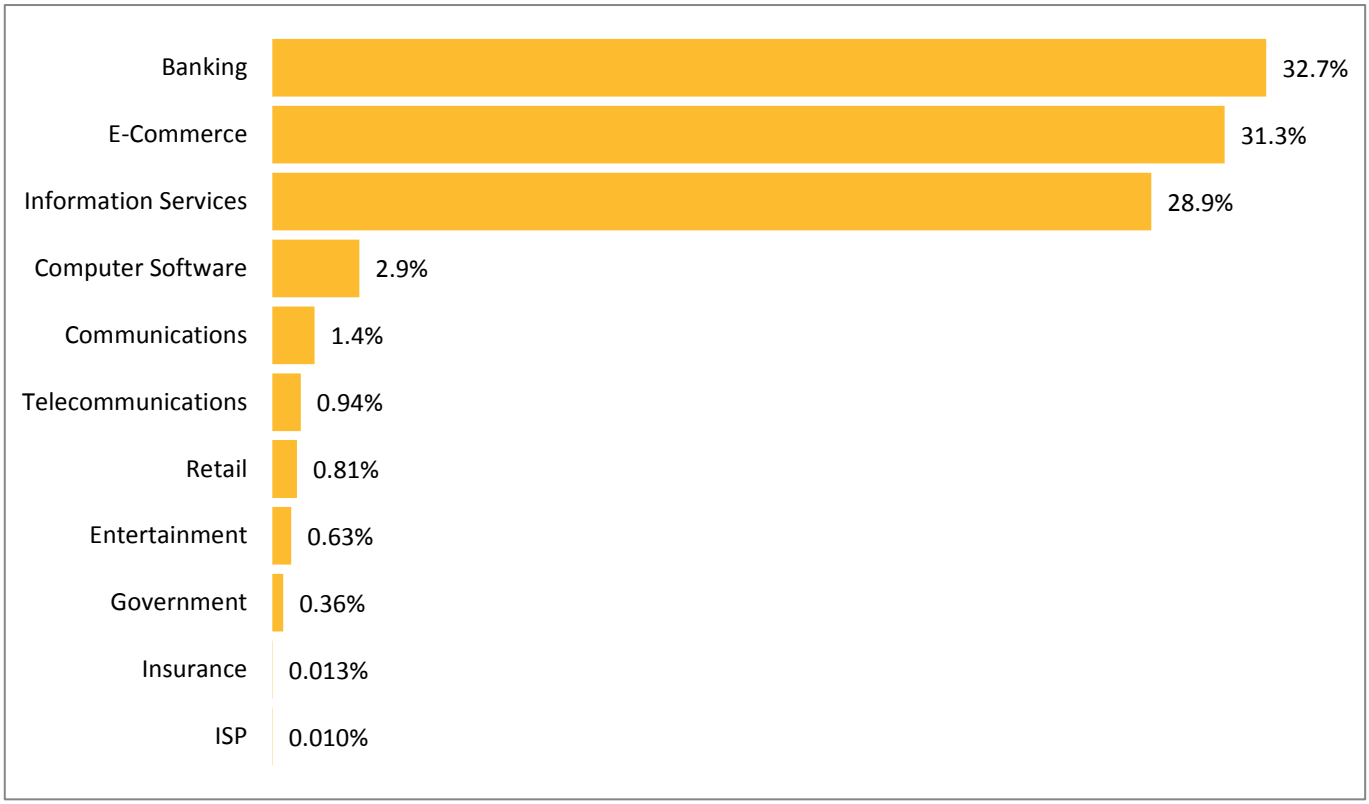
Country	September*	August
United States	54.2%	51.6%
Germany	5.0%	5.6%
United Kingdom	3.8%	3.8%
Canada	3.4%	3.1%
Brazil	3.0%	3.7%
France	2.7%	3.0%
Netherlands	2.4%	2.2%
China	2.1%	2.0%
Russia	2.0%	2.4%
Turkey	1.3%	1.3%

October 2012

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry



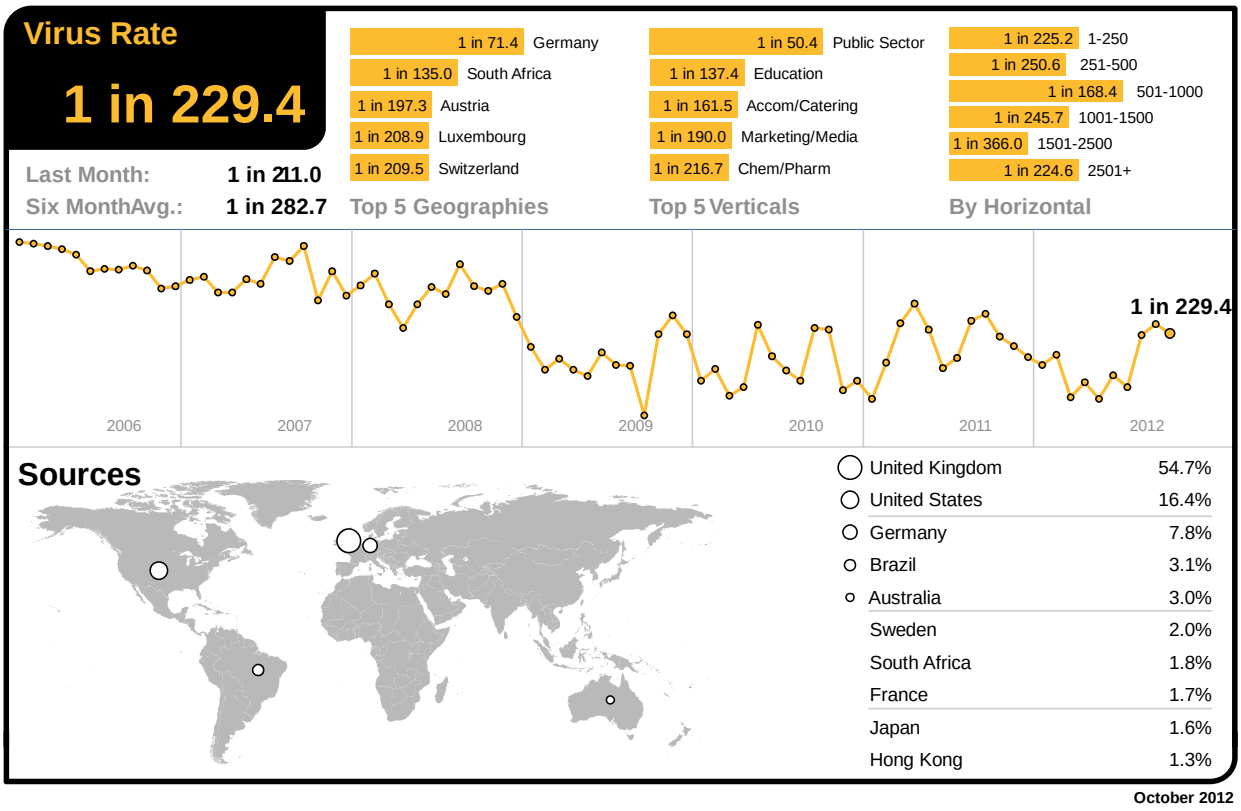
Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 229.4 emails (0.44 percent) in October, a decrease of 0.04 percentage points since September.

In October, 23.5 percent of email-borne malware contained links to malicious websites, 1.3 percentage points higher than September.



October 2012

Frequently Blocked Email-borne Malware

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. Approximately 35.4 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 15.2 percent of all email-borne malware blocked in October.

Malware Name	% Malware
Suspicious.JIT.a-SH	15.42%
Suspicious.JIT.a.dam	6.74%
W32/Generic.dam	6.24%
W32/Bredolab.gen!eml.k-SH	5.85%
Exploit/Link-generic-ee68	5.44%
W32/Bredolab.gen!eml.j-SH	5.16%
Trojan.Sasfis.dam	3.68%
EML/Worm.XX.dam	2.99%
Link-Trojan.Blackhole.I	2.62%
W32/Bredolab.gen!eml.j	1.77%

The top-ten list of most frequently blocked malware accounted for approximately 55.9 percent of all email-borne malware blocked in October.

Web-based Malware Threats

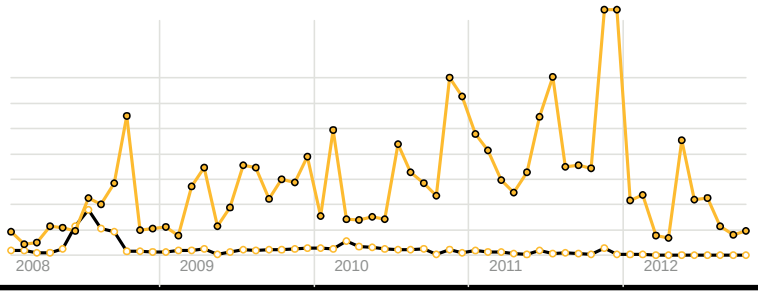
In October, Symantec Intelligence identified an average of 933 websites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 19.2 percent since September. This reflects the rate at which websites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

As detection for Web-based malware increases, the number of new websites blocked decreases and the proportion of new malware begins to rise, but initially on fewer websites. Further analysis reveals that 38.5 percent of all malicious domains blocked were new in October; an increase of 1.63 percentage points compared with September. Additionally, 11.0 percent of all Web-based malware blocked was new in October; a decrease of 0.4 percentage points since September.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware	7/day
New sites with web viruses	926/day
Total	**933/day**



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

Web Policy Risks from Inappropriate Use

Some of the most common triggers for policy-based filtering applied by Symantec Web Security.cloud for its business clients are social networking, advertisements and pop-ups, and streaming media category. Many organizations allow access to social networking websites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. Web-based advertisements pose a potential risk though the use of “malvertisements,” or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless website. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Social Networking	30.8%	JS:Trojan.Script.EY	8.1%	Adware.Generic.262597	83.2%
Advertisement and Popups	28.1%	Gen:Trojan.Heur.hu9@X2ifIMki	7.6%	Application.DirectDownloade r.A	7.6%
Streaming Media	6.9%	Trojan.JS.Redirector.AWF	7.2%	Spyware.PCAcme	5.2%
Computing and Internet	4.5%	Trojan.JS.Iframe.CCW	4.8%	Application.Heur.fq1@b0InQscO	0.4%
Peer-To-Peer	3.9%	Gen:Trojan.Heur.hu9@Y!7zjnpi	4.7%	Adware.Solimba.K	0.3%
Chat	2.9%	Exploit:Java/CVE-2012-4681.H	4.3%	Adware.Generic.251050	0.3%
Gambling	2.8%	Trojan.Script.12023	4.2%	Adware.Generic.249333	0.2%
Hosting Sites	2.6%	Trojan.JS.Agent.GHF	3.0%	Application.Generic.407192	0.2%
Games	1.7%	Gen:Trojan.Heur.hu9@XQiT3mki	2.8%	Application.NSIS.Shortcut.A	0.2%
Search	1.5%	Trojan.Maljava!gen23	2.4%	Spyware.Ardakey	0.2%

October 2012

Endpoint Security Threats

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

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

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

Malware Name[18]	% Malware
W32.Sality.AE	6.2%
W32.Ramnit!html	5.3%
W32.Ramnit.B	4.5%
W32.Downadup.B	4.3%
W32.Ramnit.B!inf	3.5%
W32.Virut.CF	1.9%
W32.Almanahe.B!inf	1.8%
W32.SillyFDC.BDP!lnk	1.7%
W32.SillyFDC	1.2%
Trojan.Maljava	1.1%

For much of 2012, variants of W32.Sality.AE[19] and W32.Ramnit[20] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 13.6% of all malware blocked at the endpoint in October, compared with 6.9 percent for all variants of W32.Sality.

Approximately 12.7 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.

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

About Symantec Intelligence

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

About Symantec

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