EXHIBIT 4

Symantec Intelligence Report: December 2012

Welcome to the December 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 November through December 2012.

Report highlights

- Spam – 70.6 percent (an increase of 1.8 percentage points since November): page 2
- Phishing – One in 377.4 emails identified as phishing (an increase of 0.225 percentage points since November): page 5
- Malware – One in 277.8 emails contained malware (a decrease of 0.03 percentage points since November): page 6
- Malicious websites – 762 websites blocked per day (a decrease of 58.7 percent since November): page 8

Introduction

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.

Ben Nahorney, Cyber Security Threat Analyst
symantec_intelligence@symantec.com

@symantec, @symanteccloud, @norton, @threatintel

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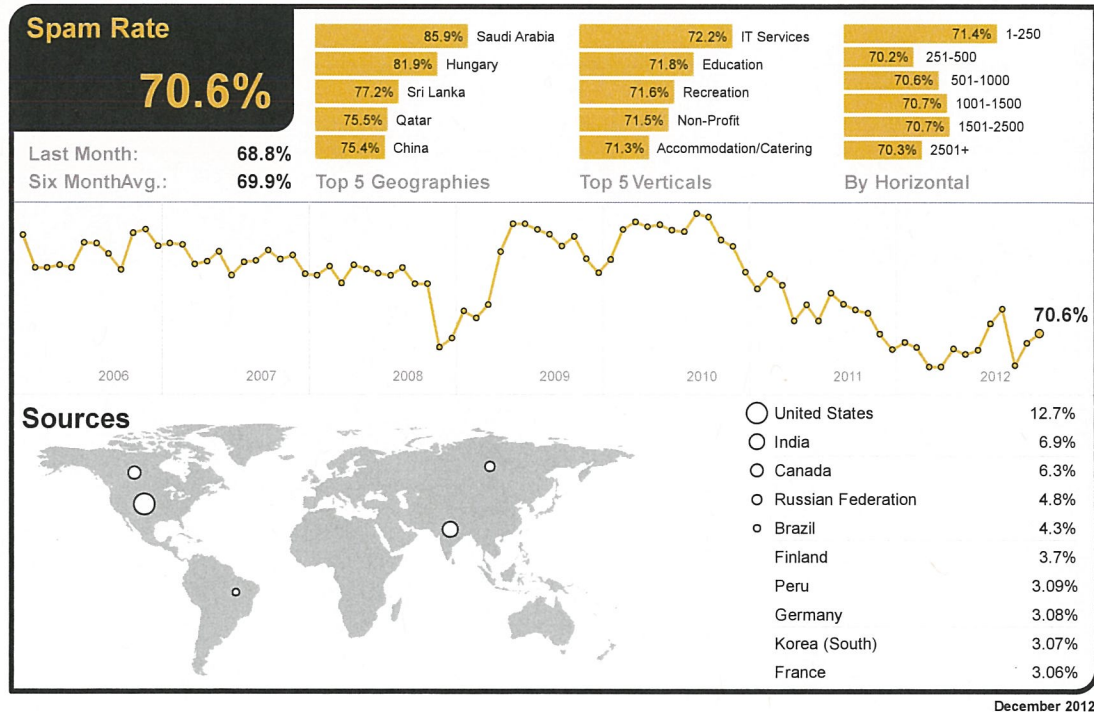
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

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 December, the global ratio of spam in email traffic rose by 1.8 percentage point since November, to 70.6 percent (1 in 1.42 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.

Spam Rate		
70.6%		
Last Month:	**68.8%**	
Six MonthAvg.:	**69.9%**	

Top 5 Geographies	
85.9%	Saudi Arabia
81.9%	Hungary
77.2%	Sri Lanka
75.5%	Qatar
75.4%	China

Top 5 Verticals	
72.2%	IT Services
71.8%	Education
71.6%	Recreation
71.5%	Non-Profit
71.3%	Accommodation/Catering

By Horizontal	
71.4%	1-250
70.2%	251-500
70.6%	501-1000
70.7%	1001-1500
70.7%	1501-2500
70.3%	2501+

Sources

○	United States	12.7%
○	India	6.9%
○	Canada	6.3%
○	Russian Federation	4.8%
○	Brazil	4.3%
	Finland	3.7%
	Peru	3.09%
	Germany	3.08%
	Korea (South)	3.07%
	France	3.06%

December 2012

✓Symantec™

Global Spam Categories

The most common category of spam in December is related to the Sex/Dating category, with 82.62 percent.

Category Name	December 2012	November 2012
Sex/Dating	82.62%	57.72%
Pharma	9.04%	14.71%
Watches	4.49%	12.69%
Jobs	1.45%	5.46%
Software	1.22%	3.38%
Newsletters	0.75%	0.08%
Mobile	0.14%	3.77%
419/Scam/Lotto	0.06%	0.20%
Casino	0.04%	1.23%
Degrees	0.02%	0.01%

Spam URL Distribution based on Top Level Domain Name

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

| TLD	December 2012	November 2012
.com	60.0%	64.1%
.ru	11.0%	6.2%
.net	6.6%	6.5%
.info	6.1%	n/a

Average Spam Message Size

In December, the proportion of spam emails that were 5Kb in size or less increased by 14.8 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size decreased by 14.2 percent, as can be seen in the following table.

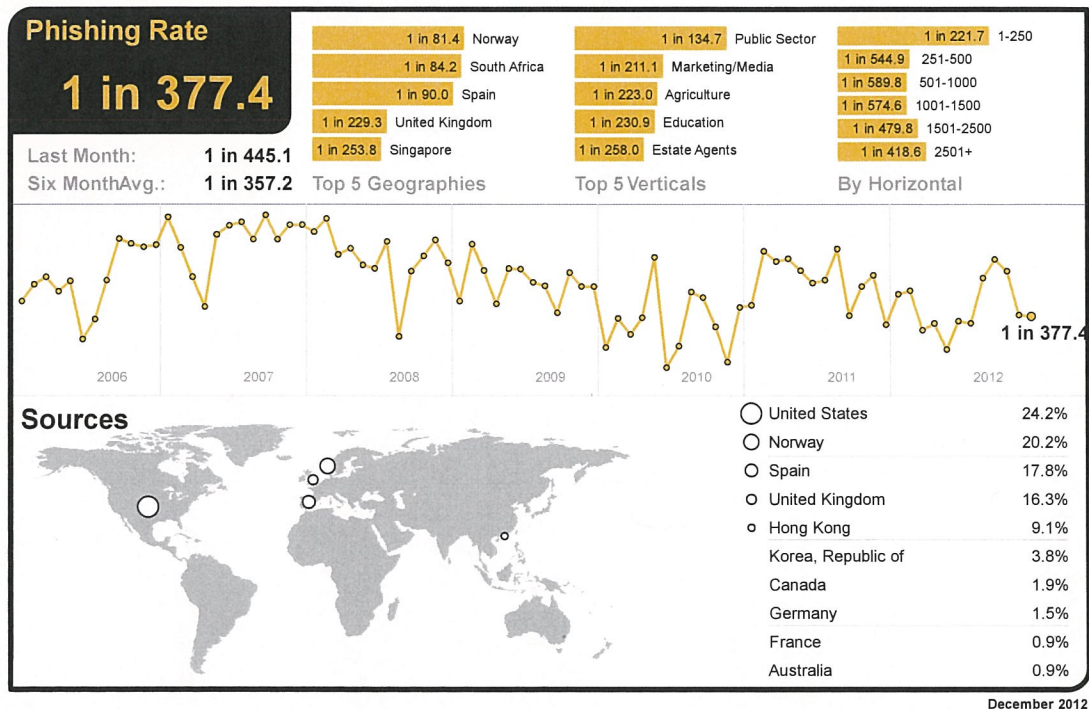| Message Size	December 2012	November 2012
0Kb – 5Kb	51.6%	36.8%
5Kb – 10Kb	24.3%	24.9%
>10Kb	24.1%	38.3%

Spam Attack Vectors

December highlights the decrease 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.

✓Symantec.
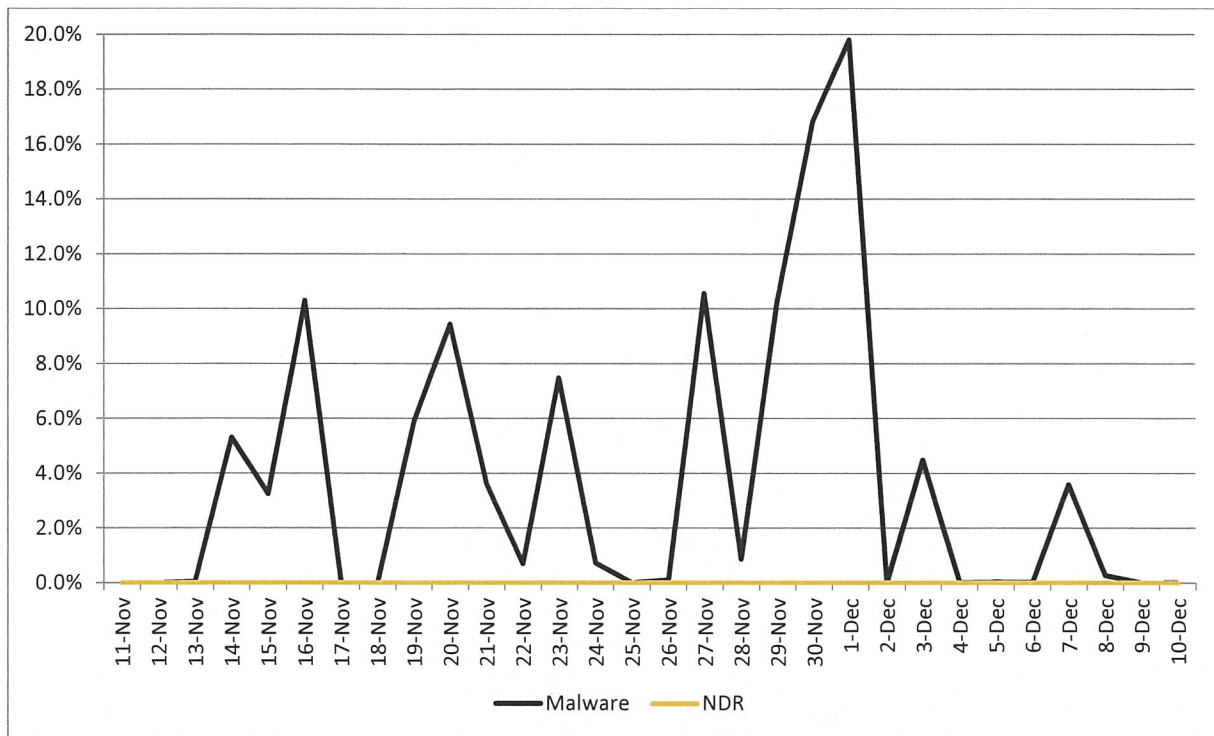
NDR spam, as shown in the chart above, is often as a result of widespread dictionary attacks during spam campaigns, where spammers make use of databases containing first and last names and combine them to generate random email addresses. A higher-level of activity is indicative of spammers that are seeking 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.
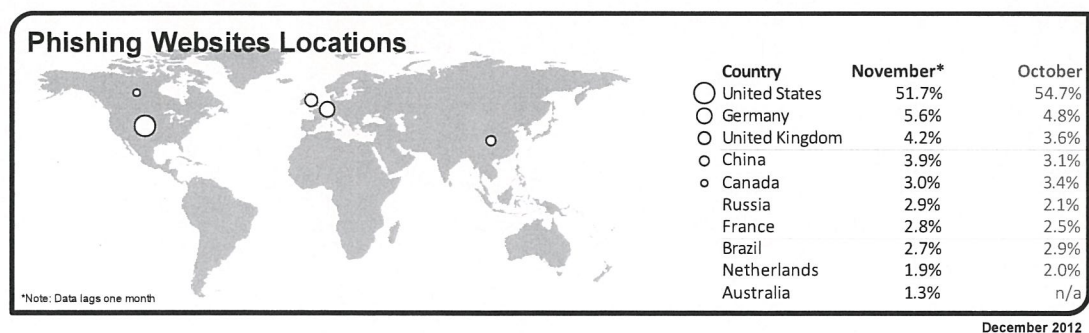
Symantec.™

Phishing Analysis

In December, the global phishing rate increased by 0.225 percentage points, taking the global average rate to one in 377.4 emails (0.27 percent) that comprised some form of phishing attack.

Phishing Rate					
1 in 377.4	1 in 81.4 Norway	1 in 134.7 Public Sector	1 in 221.7 1-250		
	1 in 84.2 South Africa	1 in 211.1 Marketing/Media	1 in 544.9 251-500		
	1 in 90.0 Spain	1 in 223.0 Agriculture	1 in 589.8 501-1000		
Last Month: 1 in 445.1	1 in 229.3 United Kingdom	1 in 230.9 Education	1 in 574.6 1001-1500		
	1 in 253.8 Singapore	1 in 258.0 Estate Agents	1 in 479.8 1501-2500		
Six MonthAvg.: 1 in 357.2	Top 5 Geographies	Top 5 Verticals	1 in 418.6 2501+		
			By Horizontal		

2006   2007   2008   2009   2010   2011   2012

1 in 377.4

Sources

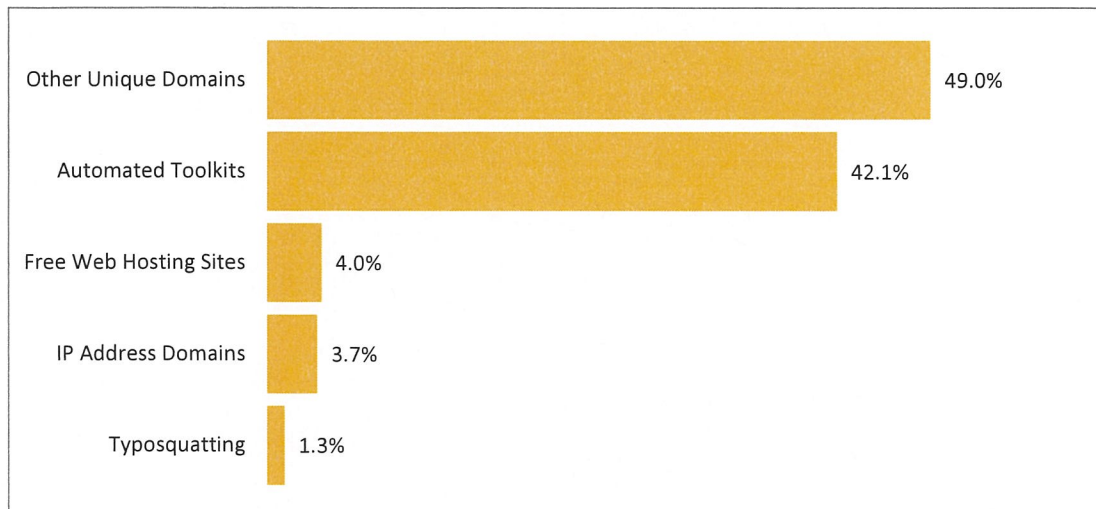|		
◯	United States	24.2%
◯	Norway	20.2%
◯	Spain	17.8%
◯	United Kingdom	16.3%
◦	Hong Kong	9.1%
	Korea, Republic of	3.8%
	Canada	1.9%
	Germany	1.5%
	France	0.9%
	Australia	0.9%

December 2012

Analysis of Phishing Websites

The overall phishing decreased by about 34 percent this month. Unique domains decreased by about 14 percent as compared to the previous month. Phishing websites that used automated toolkits decreased by 50 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 14 percent. Webhosting services comprised of 4 percent of all phishing, a decrease of 25 percent from the previous month. The number of non-English phishing sites increased by 7 percent. Among non-English phishing sites, French, Italian, Portuguese, and Chinese were highest in December.
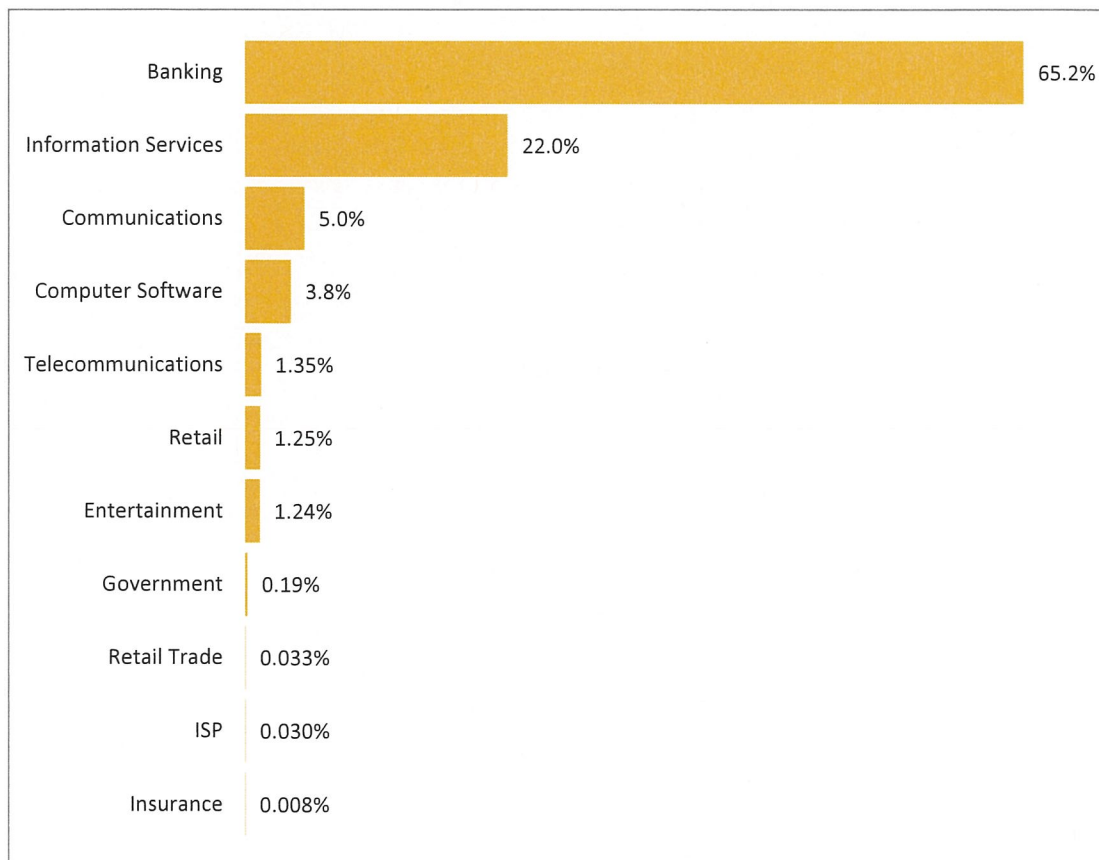
Geographic Location of Phishing Websites

Phishing Websites Locations

	Country	November*	October
◯	United States	51.7%	54.7%
◯	Germany	5.6%	4.8%
◯	United Kingdom	4.2%	3.6%
◦	China	3.9%	3.1%
◦	Canada	3.0%	3.4%
	Russia	2.9%	2.1%
	France	2.8%	2.5%
	Brazil	2.7%	2.9%
	Netherlands	1.9%	2.0%
	Australia	1.3%	n/a

*Note: Data lags one month

December 2012

✔Symantec™

Tactics of Phishing Distribution

Category	Percentage
Other Unique Domains	49.0%
Automated Toolkits	42.1%
Free Web Hosting Sites	4.0%
IP Address Domains	3.7%
Typosquatting	1.3%

Organizations Spoofed in Phishing Attacks, by Industry

Industry	Percentage
Banking	65.2%
Information Services	22.0%
Communications	5.0%
Computer Software	3.8%
Telecommunications	1.35%
Retail	1.25%
Entertainment	1.24%
Government	0.19%
Retail Trade	0.033%
ISP	0.030%
Insurance	0.008%

✓Symantec.

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 277.8 emails (0.36 percent) in December, a decrease of 0.03 percentage points since November.

In December, 27.2 percent of email-borne malware contained links to malicious websites, 13.0 percentage points higher than November.

Virus Rate	
1 in 277.8	
Last Month: **1 in 255.8**	
Six MonthAvg.: **1 in 258.0**	

Top 5 Geographies	
1 in 77.5	South Africa
1 in 94.0	Australia
1 in 177.3	United Kingdom
1 in 266.4	Italy
1 in 290.1	Canada

Top 5 Verticals	
1 in 69.4	Public Sector
1 in 125.5	Transport/Utilities
1 in 179.9	Recreation
1 in 207.3	Education
1 in 233.0	Marketing/Media

By Horizontal	
1 in 291.4	1-250
1 in 355.2	251-500
1 in 423.8	501-1000
1 in 129.9	1001-1500
1 in 305.9	1501-2500
1 in 278.1	2501+

1 in 277.8

Sources

United States	40.9%
United Kingdom	24.9%
Australia	9.1%
India	4.3%
Sweden	2.9%
Canada	2.5%
Brazil	2.1%
Netherlands	1.7%
Hong Kong	1.7%
France	1.6%

December 2012

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for December, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 46.9 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 0.9 percent of all email-borne malware blocked in December.
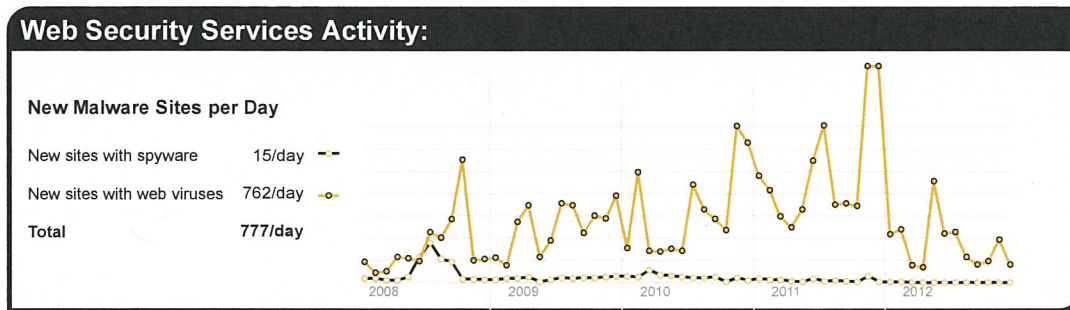
Malware Name	% Malware
Suspicious.JIT.a-SH	28.83%
Exploit/Link-generic-ee68	15.74%
W32/Exploit-Archive.Gen-SH	13.15%
Trojan.Gen-SH	5.21%
Suspicious.JIT.a-SH.dam	2.78%
W32/Exploit-Archive.Gen-SH.dam	2.57%
Exploit/SpoofBBB	2.40%
Exploit/Link-FakeACHUpdate	1.24%
Suspicious.JIT.a.dam	1.19%
ZIP/Generic.dam	1.17%

The top-ten list of most frequently blocked malware accounted for approximately 74.3 percent of all email-borne malware blocked in December.

✓Symantec.™

Web-based Malware Threats

In December, Symantec Intelligence identified an average of 762 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 58.7 percent since November. 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 39.6 percent of all malicious domains blocked were new in December; an increase of 7.1 percentage points compared with November. Additionally, 11.9 percent of all Web-based malware blocked was new in December; an increase of 0.3 percentage points since November.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware	15/day	- -
New sites with web viruses	762/day	-o-
Total	777/day	

The chart above shows the XXcreaseXX in the number of new spyware and adware websites blocked each day on average during December 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	
Advertisement and Popups	30.5%	Trojan.JS.Agent.GHF	17.8%	Dropped:Adware.Generic.299792	80.6%
Social Networking	28.6%	JS:Trojan.Script.AAL	7.0%	Application.DirectDownloade r.A	18.9%
Streaming Media	7.2%	Trojan.Swifi	6.4%	Dropped:Adware.Generic.262597	0.3%
Computing and Internet	4.0%	JS:Trojan.Crypt.KK	4.0%	Application:Android/Counterclank. A	0.03%
Peer-To-Peer	3.5%	JS:Trojan.Crypt.KA	2.9%	Adware:Android/AirPush. A	0.018%
Chat	3.1%	Trojan.Malscript!html	2.4%	Adware:W32/Baidu.gen!B	0.016%
Hosting Sites	2.8%	JS:Trojan.JS.Iframe.AM	2.4%	Adware.GoonSquad	0.014%
Games	2.0%	Trojan.Maljava	2.3%	Adware:Android/Ropin. A	0.013%
News	1.7%	Trojan.Malscript	2.2%	Adware.Adpopup	0.012%
Entertainment	1.5%	JS:Trojan.Crypt.JF	1.5%	Spyware.Ardakey	0.010%

December 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

Symantec.™

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[1]	% Malware
W32.Sality.AE	6.5%
W32.Ramnit!html	6.0%
W32.Downadup.B	4.9%
W32.Ramnit.B	4.9%
W32.Ramnit.B!inf	3.9%
W32.Almanahe.B!inf	2.4%
W32.Virut.CF	2.1%
W32.SillyFDC.BDP!lnk	1.9%
W32.Xpaj.B	1.1%
W32.Virut!html	1.0%

For much of 2012, variants of W32.Sality.AE[2] and W32.Ramnit[3] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 11.7% of all malware blocked at the endpoint in December, compared with 5.6 percent for all variants of W32.Sality.

Approximately 34.8 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.

---

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

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

[3] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99

✓Symantec.

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.