APRIL 2015
VOLUME 20

Symantec

ISTR20

INTERNET SECURITY THREAT REPORT

APPENDICES

CHARTS & TABLES

APPENDIX A: THREAT ACTIVITY TRENDS

Appendix A: Threat Activity Trends

Threat Activity Trends

The following section of the Symantec Global Internet Security Threat Report provides an analysis of threat activity, data breaches, and web-based attacks, as well as other malicious actions that Symantec observed in 2014. The malicious actions discussed in this section also include phishing, malicious code, spam zombies, bot-infected computers, and attack origins. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions of the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Source
- Malicious Web-Based Attack Prevalence
- Analysis of Malicious Web Activity by Attack Toolkits
- Analysis of Web-Based Spyware, Adware and Potentially Unwanted Programs
- Analysis of Web Policy Risks from Inappropriate Use
- Analysis of Website Categories Exploited to Deliver Malicious Code
- Bot-Infected Computers
- Analysis of Mobile Threats
- Data Breaches and Identity Theft

Malicious Activity by Source

Background

- Malicious activity usually affects computers that are connected to high-speed broadband Internet, because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than do other connection types, plus faster speeds, the potential for constantly connected systems, and typically a more stable connection. Symantec categorizes malicious activities as follows:
- Malicious code: This includes programs such as viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, and compromising the security or integrity of a victim's computer data.
- Spam zombies: These are remotely controlled, compromised systems specifically designed to send out large volumes of junk or unsolicited email messages. These email messages can be used to deliver malicious code and phishing attempts.
- Phishing hosts: Phishing hosts are computers that provide website services in order to illegally gather sensitive user information while pretending that the attempt is from a trusted, well-known organization by presenting a website designed to mimic the site of a legitimate business.
- Bot-infected computers: Malicious programs have been used to compromise computers to allow an attacker to control the targeted system remotely. Typically, a remote attacker controls a large number of compromised computers over a single reliable channel in a botnet, which can then be used to launch coordinated attacks.
- Network attack origins: These measure the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- Web-based attack origins: These measure attack sources that are delivered via the web or through HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Methodology

These metrics assess the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, namely malicious code reports, spam zombies, phishing hosts, bot-infected computers, network attack origins, and web-based attack origins. The proportion of each activity originating from each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question, and rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Geography	2014 World Rank	2014 Overall Average	2013 World Rank	2013 Overall Average	Change
United States	1	20.7%	1	20.3%	0.4%
China	2	10.6%	2	9.4%	1.2%
India	3	4.0%	3	5.1%	-1.1%
Netherlands	4	3.6%	4	3.5%	0.1%
Germany	5	3.3%	5	3.3%	0.0%
Taiwan	6	2.6%	9	2.5%	0.1%
United Kingdom	7	2.6%	7	2.6%	0.0%
Russia	8	2.5%	6	2.6%	-0.1%
Vietnam	9	2.4%	12	2.2%	0.2%
Brazil	10	2.3%	8	2.5%	-0.2%

Malicious Activity by Source: Overall Rankings, 2013-2014

Source: Symantec

Geography	2014 Malicious Code Rank	2014 Malicious Code %	2013 Malicious Code Rank	2013 Malicious Code %	Change
United States	1	19.8%	1	16.9%	2.9%
India	2	12.2%	2	15.3%	-3.1%
China	3	6.5%	3	5.9%	0.6%
Japan	4	3.8%	5	3.4%	0.4%
United Kingdom	5	3.5%	7	2.8%	0.7%
Netherlands	6	3.3%	8	2.8%	0.5%
Indonesia	7	3.2%	4	4.0%	-0.8%
Australia	8	3.0%	11	2.1%	0.9%
Germany	9	2.9%	9	2.7%	0.2%
Vietnam	10	2.4%	6	2.8%	-0.4%

Malicious Activity by Source: Malicious Code, 2013-2014

Source: Symantec

Geography	2014 Spam Rank	2014 Spam %	2013 Spam Rank	2013 Spam %	Change
Vietnam	1	10.1%	7	5.0%	5.1%
Netherlands	2	8.0%	2	8.2%	-0.2%
Iran	3	6.2%	5	5.3%	0.9%
Russia	4	6.2%	3	6.6%	-0.4%
Germany	5	5.8%	13	2.6%	3.2%
India	6	5.8%	1	9.8%	-4.0%
Argentina	7	5.1%	11	3.1%	2.0%
Spain	8	4.1%	12	2.9%	1.2%
United States	9	3.9%	9	4.3%	-0.4%
Taiwan	10	3.6%	4	5.5%	-1.9%

Malicious Activity by Source: Spam Zombies, 2013-2014

Source: Symantec

Geography	2014 Phishing Hosts Rank	2014 Phishing Hosts %	2013 Phishing Hosts Rank	2013 Phishing Hosts %	Change
United States	1	46.6%	1	39.4%	7.2%
Germany	2	5.4%	2	6.5%	-1.1%
United Kingdom	3	3.9%	3	3.8%	0.1%
Netherlands	4	3.2%	6	2.5%	0.7%
France	5	3.2%	5	2.6%	0.6%
Hong Kong	6	3.1%	19	1.1%	2.0%
Canada	7	2.5%	4	2.8%	-0.3%
Russia	8	2.5%	7	2.5%	0.0%
China	9	2.2%	9	2.2%	0.0%
Croatia	10	2.2%	70	0.1%	2.1%

Malicious Activity by Source: Phishing Hosts, 2013-2014

Source: Symantec

Geography	2014 Bots Rank	2014 Bots %	2013 Bots Rank	2013 Bots %	Change
China	1	16.5%	2	9.1%	7.3%
United States	2	16.1%	1	20.0%	-3.9%
Taiwan	3	8.5%	4	6.0%	2.5%
Italy	4	5.5%	3	6.0%	-0.5%
Hungary	5	4.9%	7	4.2%	0.6%
Brazil	6	4.3%	5	5.7%	-1.4%
Japan	7	3.4%	6	4.3%	-0.8%
Germany	8	3.1%	8	4.2%	-1.0%
Canada	9	3.0%	10	3.5%	-0.5%
Poland	10	2.8%	12	3.0%	-0.2%

Malicious Activity by Source: Bots, 2013-2014

Source: Symantec

Geography	2014 Web Attacking Countries Rank	2014 Web Attacking Countries %	2013 Web Attacking Countries Rank	2013 Web Attacking Countries %	Change
United States	1	21.1%	1	26.2%	-5.1%
China	2	6.6%	2	7.4%	-0.8%
Costa Rica	3	6.6%	68	0.03%	6.6%
Japan	4	3.2%	6	1.4%	1.8%
Netherlands	5	2.3%	3	2.8%	-0.5%
India	6	1.1%	4	1.6%	-0.5%
Philippines	7	1.1%	12	0.9%	0.2%
Brazil	8	1.0%	10	0.9%	0.1%
Korea, South	9	0.8%	7	1.4%	-0.6%
Germany	10	0.8%	5	1.6%	-0.8%

Malicious Activity by Source: Web Attack Origins, 2013-2014

Source: Symantec

Geography	2014 Network Attacking Countries Rank	2014 Network Attacking Countries %	2013 Network Attacking Countries Rank	2013 Network Attacking Countries %	Change
China	1	28.7%	1	26.6%	2.1%
United States	2	16.6%	2	15.2%	1.4%
Netherlands	3	4.2%	3	3.9%	0.3%
Russia	4	3.2%	5	3.1%	0.1%
United Kingdom	5	3.0%	4	3.3%	-0.3%
France	6	2.6%	7	2.6%	0.0%
Korea, South	7	2.4%	15	1.8%	0.6%
India	8	2.4%	9	2.4%	0.0%
Australia	9	2.2%	11	2.0%	0.2%
Japan	10	2.1%	10	2.2%	-0.1%

Malicious Activity by Source: Network Attack Origins, 2013-2014

Source: Symantec

Commentary

- In 2014, the United States and China remained the top two sources overall for malicious activity. The overall average proportion of attacks originating from the United States in 2014 increased by 0.4 percentage point compared with 2013, while the same figure for China saw an increase by 1.2 percentage points compared with 2013. Countries ranking in the top 10 for 2013 continued to appear in the same range in 2014.
- The United States remains in first position as a source of all activities except for spam zombies, bots, and network attacks. Vietnam remains in first position for spam zombies, and China remains primary for bots and network attacks.
- Of all bot activity, 16.5 percent originated in China: China was the main source of bot-infected computers, an increase of 7.3 percentage points compared with 2013.
- Of all web-based attacks, 21.1 percent originated in the United States: Web-based attacks originating from the United States decreased by 5.1 percentage points in 2014.
- Of all network attacks, 28.7 percent originated in China: China has the largest population of Internet users not only in the Asia region but also globally, which attributes to the high rates of attacks.
- Of all phishing websites, 46.6 percent were hosted in the United States: The United States is the second largest population of Internet users in the world, which could be one of the reasons that it accounts for highest number of phishing websites.

- Of all spam zombies, 10.1 percent were located in Vietnam, an increase of 5.1 percentage points compared with 2013. The proportion of spam zombies located in the United States dipped by 0.4 percentage point to 3.9 percent, resulting in the United States being ranked in ninth position in 2014, the same as in 2013.
- Of all malicious code activities, 19.8 percent originated from the United States, an increase of 2.9 percentage points compared with 2013, giving the country the same ranking as in 2013. With 12.2 percent of malicious activity originating in India, the country was ranked in second position.

Malicious Web-Based Attack Prevalence

Background

The circumstances and implications of web-based attacks vary widely. Web-based attacks may target specific businesses or organizations, or they may be widespread attacks of opportunity that exploit current events, zero-day vulnerabilities, or recently patched and publicized vulnerabilities that many users have yet to protect themselves against. While major attacks may have individual importance and often receive significant attention when they occur, examining web-based attacks overall provides insight into the threat landscape and how attack patterns may be shifting. Analysis of the underlying trend can provide insight into potential shifts in web-based attack usage and can assist in determining whether attackers are more or less likely to employ these attacks in the future. To see which vulnerabilities are being exploited by web-based attacks, see Appendix D: Vulnerability Trends.

Methodology

This metric assesses changes to the prevalence of web-based attack activity by comparing the overall volume of malicious activity in each month during the current and previous reporting periods. The data is obtained from Symantec Endpoint Protection and Norton Network Threat Protection IPS Signature detections.

Month	2014	2013
January	779,337	674,293
February	364,110	539,069
March	534,089	491,713
April	530,227	463,152
May	379,156	697,823
June	346,572	756,068
July	558,450	799,486
August	537,762	702,893
September	387,889	637,823
October	427,094	135,451
November	534,822	483,999
December	561,513	442,298

Malicious Website Activity, 2013-2014

Source: Symantec

Commentary

- The average number of malicious websites blocked each day dipped by approximately 12.7 percent, from approximately 568,700 in 2013 to 496,700 in 2014.
- The highest level of activity was in January, with approximately 779,300 blocks per day.
- The lowest rate of malicious activity was 346,600 blocks per day in June 2014.
- Further analysis of malicious code activity may be found in Appendix B: Malicious Code Trends, "Top Malicious Code Families."

Analysis of Malicious Web Activity by Attack Toolkits

Background

The increasing pervasiveness of web browser applications, along with increasingly common, easily exploited web browser application security vulnerabilities, has resulted in the widespread growth of web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers. Enterprises and consumers who visit mainstream websites hosting web attack toolkits are silently infected with a variety of malware. Symantec analyzes attack activity to determine which types of attacks and toolkits these predators are utilizing. This can provide insight into emerging web attack trends and may indicate the types of attacks with which attackers are having the most success.

Methodology

This metric assesses the top web-based attack activity grouped by exploit "web kit" families. These attacks originated from compromised legitimate sites and intentionally malicious sites set up to target Internet users in 2014. To determine this, Symantec ranked attack activity by the number of incidents associated with each toolkit.

Month	Sakura	Nuclear	Styx	OrangeKit	Blackhole	Others
January	9.48%	15.19%	25.09%	3.14%	10.08%	37.02%
February	14.43%	15.79%	21.85%	2.28%	8.23%	37.43%
March	21.48%	15.24%	4.77%	1.53%	5.01%	51.98%
April	12.76%	8.81%	5.27%	1.04%	4.42%	67.69%
May	16.45%	19.95%	6.22%	2.72%	5.60%	49.06%
June	28.04%	12.47%	9.14%	5.18%	8.14%	37.03%
July	34.21%	10.10%	3.45%	9.07%	5.35%	37.83%
August	38.86%	9.06%	1.71%	8.24%	4.70%	37.44%
September	29.38%	8.30%	1.89%	6.99%	2.54%	50.90%
October	37.85%	4.31%	2.73%	11.33%	1.65%	42.12%
November	19.31%	1.93%	1.44%	3.82%	1.03%	72.48%
December	19.72%	1.05%	2.03%	9.37%	3.36%	64.48%

Malicious Website Activity: Attack Toolkit Trends, 2014

Source: Symantec

Toolkit	% of Attacks
Sakura	22.76%
Nuclear	9.98%
Styx	7.23%
OrangeKit	5.27%
Blackhole	5.07%
Other	49.70%

Malicious Website Activity: Overall Frequency of Major Attack Toolkits, 2014

Source: Symantec

Commentary

- G01 Pack Exploit Kit virtually disappeared from the detections of web attack kits in 2014, though ranked first in 2013 with 23 percent of total attacks blocked. Sakura ranked first in 2014, with 23 percent of attacks blocked. The Nuclear toolkit that didn't appear in the top five in 2013 ranked second in 2014, with 10 percent.
- Blackhole has reappeared, ranking fifth in 2014.

Analysis of Web-Based Spyware, Adware and Potentially Unwanted Programs

Background

One of the main goals of a drive-by web-based installation is the deployment of malicious code, but often a compromised website is also used to install spyware or adware code. This is because the cybercriminals pushing the spyware and adware in this way are being paid a small fee for each installation. Most adware vendors, such as those providing add-in toolbars for web browsers, are not aware of how their code came to be installed on users' computers; the expectation is that it is with the permission of the end user, but this is typically not the case in a drive-by installation and may be in breach of the vendors' terms and conditions of use.

Methodology

This metric assesses the prevalence of web-based spyware and adware activity by tracking the trend in the average number of spyware- and adware-related websites blocked each day by users of Symantec.cloud web security services. Underlying trends observed in the sample data provide a reasonable representation of overall malicious web-based activity trends.

Rank	Spyware Name	Percent
1	Adware.Adpeak.E	23.6%
2	Application.SearchProtect.R	10.4%
3	Adware.Crossid	9.6%
4	Application.Downloader.SS	7.5%
5	Adware.Adpeak.C	6.5%
6	Adware.SwiftBrowse.E	3.5%
7	Application.SearchProtect.AD	2.9%
8	Adware.NewNextMe.A	2.5%
9	Adware.Multiplug.DH	2.4%
10	Adware.BrowseFox.U	2.4%

Potentially Unwanted Programs: Spyware and Adware Blocked, 2014

Source: Symantec.cloud

Commentary

- It is sometimes the case that "potentially unwanted programs" are legitimate programs that have been installed as part of a drive-by download and the installation is performed without the permission of the user. This is typically when the third party behind the installation is being rewarded for the number of installations of a particular program, irrespective of whether the user has granted permission. It is often without the knowledge of the original vendor and may be in breach of its affiliate terms and conditions.
- The most frequently blocked installation of potentially unwanted programs in 2014 was for the adware Adpeak.E.
- In 2014, seven of the top 10 potentially unwanted programs were classified as adware, compared with nine in 2013.
- In 2014, 31.6 percent of spyware and adware was detected using generic techniques, compared with 1.8 percent in 2013.

Analysis of Web Policy Risks from Inappropriate Use

Background

Many organizations implement an acceptable usage policy to limit employees' use of Internet resources to a subset of websites that have been approved for business use. This enables an organization to limit the level of risk that may arise from users' visiting inappropriate or unacceptable websites, such as those containing sexual images and other potentially illegal or harmful content. Often there will be varying degrees of granularity imposed on such restrictions, with some rules being applied to groups of users, while other rules may apply only at certain times of the day. For example, an organization may wish to limit employees' access to video-sharing websites to Friday lunchtime only but may also allow any member of the PR and marketing teams access at any time during the week. This enables an organization to implement and monitor its acceptable usage policy and reduce its exposure to certain risks that may also expose the organization to legal difficulties.

Methodology

This metric assesses the classification of prohibited websites blocked by users of Symantec. cloud web security services. The policies are applied by the organization from a default selection of rules that may also be refined and customized. This metric provides an indication of the potential risks that may arise from uncontrolled use of Internet resources.

Rank	Category	2014	2013	Change
1	Social Networking	37.4%	39.0%	-1.5%
2	Advertisement & Popups	23.8%	24.4%	-0.5%
3	Computing & Internet	4.6%	4.5%	0.1%
4	Streaming Media	4.0%	5.2%	-1.2%
5	Hacking	3.4%	0.0%	3.4%
6	Hosting Sites	3.1%	3.7%	-0.6%
7	Portal	2.5%	0.8%	1.7%
8	Chat	1.7%	2.9%	-1.2%
9	Search	1.2%	2.8%	-1.6%
10	Entertainment	1.2%	1.1%	0.1%

Web Policies That Triggered Blocks, 2013-2014

Source: Symantec.cloud

Commentary

- The most frequently blocked traffic was categorized as social networking, and it accounted for 37 percent of policy-based filtering activity that was blocked, equivalent to approximately one in every 2.5 websites blocked. Many organizations allow access to social networking websites but in some cases implement policies to permit access only at certain times of the day. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.
- Twenty-four percent of web activity blocked through policy controls was related to advertisements and pop-ups. Web-based advertisements pose a potential risk through the use of "malvertisements," or malicious advertisements. These may occur as the result of a legitimate online ad provider's being compromised or a banner ad's being used to serve malware on an otherwise harmless website.
- Activity related to streaming media policies resulted in 4 percent of policy-based filtering blocks in 2014. 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 figure was likely to have been higher in 2012 due to the staging of the Olympics in London.

Analysis of Website Categories Exploited to Deliver Malicious Code

Background

As organizations seek to implement appropriate levels of control in order to minimize risk levels from uncontrolled web access, it is important to understand the level of threat posed by certain classifications of websites and categories. This provides insight on the types of legitimate websites that may be more susceptible to being compromised and therefore could expose users to greater levels of risk.

Methodology

This metric assesses the classification of malicious websites blocked by users of Norton Safe Web[1] technology. Data is collected anonymously from customers voluntarily contributing to this technology, including through Norton Community Watch. Norton Safe Web is processing billions of rating requests each day and monitoring millions of daily software downloads.

This metric provides an indication of the levels of infection of legitimate websites that have been compromised or abused for malicious purposes. The malicious URLs identified by the Safe Web technology were classified by category using the Symantec RuleSpace[2] technology. RuleSpace proactively categorizes websites into nearly 100 categories in 30 languages.

Rank	Top 10 Most Frequently Exploited Categories of Websites	% of Total Number of Infected Websites
1	Technology	21.5%
2	Hosting	7.3%
3	Blogging	7.1%
4	Business	6.0%
5	Anonymizer	5.0%
6	Entertainment	2.6%
7	Shopping	2.5%
8	Illegal	2.4%
9	Placeholder	2.2%
10	Virtual Community	1.8%

Malicious Web Activity: Categories That Delivered Malicious Code, 2014

Source: Symantec

Rank	Top-10 Most Frequently Exploited Categories of Websites	Average Number of Threats Found on Infected Website	Top 3 Threat Types Detected		
1	Technology	1.4	Virus: 50%	Browser Exploit: 37%	Phish: 6%
2	Hosting	1.2	Browser Exploit: 52%	Virus: 34%	Phish: 9%
3	Blogging	1.4	Virus: 57%	Browser Exploit: 36%	Phish: 3%
4	Business	1.5	Browser Exploit: 68%	Phish: 17%	Virus: 8%
5	Anonymizer	6.5	Security Risk: 58%	Virus: 39%	Browser Exploit: 3%
6	Entertainment	1.8	Browser Exploit: 69%	Virus: 13%	Phish: 11%
7	Shopping	1.7	Browser Exploit: 60%	Virus: 17%	Phish: 14%
8	Illegal	2.1	Virus: 40%	Browser Exploit: 35%	Phish: 16%
9	Placeholder	2.1	Browser Exploit: 50%	Virus: 16%	Security Risk: 5%
10	Virtual Community	1.2	Virus: 89%	Browser Exploit: 9%	Phish: 1%

Malicious Web Activity: Malicious Code by Number of Infections per Site for Top-10 Most Frequently Exploited Categories, 2014

Source: Symantec.cloud

Commentary

- Of all malicious website activity, 21.5 percent was classified in the technology category.
- Websites classified as Anonymizers were found to host the greatest number of threats per site among all categories, with an average of 6.5 threats per website, the majority of which related to security risks (58 percent).
- The Illegal category includes sites that fall into the following subcategories: activist groups, cyberbullying, malware accomplice, password cracking, potentially malicious software and unwanted programs, remote access programs, and several other types of phishing- and spam-related content.
- The Placeholder category refers to any domain name that is registered but may be for sale or has recently expired and is redirected to a domain parking page.
- Anonymizers are sites that provide anonymous access to websites through a PHP or CGI proxy, allowing users to gain access to websites blocked by corporate and school proxies as well as parental control filtering solutions. Examples include:
  - Transparent proxy servers
  - Elite, disguised, distorting, and high-anonymity proxy servers
  - Websites explaining how to surf the web anonymously

Bot-Infected Computers

Background

Bot-infected computer programs, or bots, are programs that are covertly installed on a user's machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet Relay Chat (IRC), peer to peer (P2P), or Hypertext Transfer Protocol (HTTP). These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality, and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft—all of which can lead to serious financial and legal consequences. Attackers favor bot-infected computers with a decentralized command and control model because they are difficult to disable and allow the attackers to hide in plain sight among the massive amounts of unrelated traffic occurring over the same communication channels, such as P2P. Most important, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate.

Methodology

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; a single such computer can be active on a number of different days. A distinct bot-infected computer is one that was active at least once during the period. The bot-infected computer activities that Symantec tracks can be classified as active attacker bots or bots that send out spam (that is, spam zombies).

Distributed denial-of-service (DDoS) campaigns may not always be indicative of bot-infected computer activity. DDoS activity can occur without the use of bot-infected computers. For example, the use of publicly available software such as Low Orbit Ion Cannon (LOIC), when used in a coordinated effort and in sufficiently large numbers, may disrupt some businesses' website operations.

The following analysis reveals the average life span of a bot-infected computer for the highest populations of bot-infected computers. To be included in the list, the geography must account for at least 0.1 percent of the global bot population.

Rank	Geography	Average Life Span of Bot (Days) - 2014	% of World Bots - 2014	Average Life Span of Bot (Days) - 2013	% of World Bots - 2013
1	Romania	23	0.2%	20	0.2%
2	United States	21	16.1%	13	20.0%
3	Indonesia	15	0.2%	15	0.1%
4	Pakistan	14	0.1%	15	0.1%
5	Iran	14	0.1%	9	0.1%
6	New Zealand	13	0.1%	10	0.2%
7	Israel	13	0.9%	8	1.0%
8	Bulgaria	13	0.2%	14	0.1%
9	Korea, South	13	1.2%	9	1.0%
10	Denmark	12	0.1%	7	0.2%

Top-10 Bot Locations by Average Lifespan of Bot, 2013-2014

Source: Symantec

Commentary

- Bots located in Romania were active for an average of 23 days in 2014, compared with 20 days in 2013; 0.2 percent of bots were located in Romania, compared with 0.19 percent in 2013.
- Although it still takes longer to identify and clean a bot-infected computer in Romania than it does in the United States, the number of infections in the United States is more than 100 times greater than that in Romania. One factor contributing to this disparity may be a low level of user awareness of the issues involved, combined with the lower availability of remediation guidance and support tools in the Romanian language.
- In the United States, which was home to 16 percent of the world's bots in 2014, the average life span of a bot was 21 days.
- All other countries outside the top 10 had bot life spans of 12 days or less. The overall global average bot life span was 7.5 days, slightly higher than in 2013, when it was six days.

Analysis of Mobile Threats

Background

Since the first smartphone arrived in the hands of consumers, speculation about threats targeting these devices has abounded. While threats targeted early "smart" devices such as those based on Symbian and Palm OS in the past, none of these threats ever became widespread and many remained proof of concept. Recently, with the growing uptake of smartphones and tablets and their increasing connectivity and capability, there has been a corresponding increase in attention, from both threat developers and security researchers.

While the number of immediate threats to mobile devices remains relatively low in comparison to threats targeting PCs, there have been new developments in the field, and as malicious code for mobile begins to generate revenue for malware authors, there will be more threats created for these devices, especially as people increasingly use mobile devices for sensitive transactions such as online shopping and banking.

As with desktop computers, the exploitation of a vulnerability can be a way for malicious code to be installed on a mobile device.

Methodology

In 2014, there was an increase in the number of vulnerabilities reported that affected mobile devices. Symantec documented 168 vulnerabilities in mobile device operating systems in 2014, compared with 127 in 2013 and 416 in 2012.

Symantec tracks the number of threats discovered against mobile platforms by tracking malicious threats identified by Symantec's own security products and confirmed vulnerabilities documented by mobile vendors.

Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile application ("app") marketplaces in the hope that users will download and install them, often trying to pass themselves off as legitimate apps or games. Attackers have also taken popular legitimate applications and added supplementary code to them. Symantec has classified these threats into a variety of categories based on their functionality.

Month	2014	2013
January	3	4
February	2	1
March	4	7
April	2	5
May	3	4
June	4	9
July	4	8
August	2	2
September	3	7
October	5	4
November	8	2
December	6	4

Android Mobile Threats: Newly Discovered Malicious Code, 2013-2014

Source: Symantec

Month	2014	2013
January	46	53
February	60	133
March	41	107
April	80	44
May	53	78
June	40	56
July	7	20
August	7	107
September	25	36
October	204	48
November	22	93
December	3	33

Android Mobile Threats: Average Number of Malware Variants per Family, 2013–2014

Source: Symantec

Platform	Number of Threats	Percent of Threats
Android	45	94%
Symbian	0	0%
Windows	0	0%
iOS	3	6%

Mobile Threats: Malicious Code by Platform, 2014

Source: Symantec

High-level Risk Categories	Track User	Steal Information	Send Content	Traditional Threats	Reconfigure Device	Adware/ Annoyance
Percent of Actions Found in Threats (2014)	22%	21%	11%	26%	13%	7%
Percent of Actions Found in Threats (2013)	30%	23%	8%	20%	10%	9%

Mobile Threats: Malicious Code Actions in Malware, 2013-2014

Source: Symantec

Detailed Threat Categories	Percent Found in Threats, 2014	Percent Found in Threats, 2013
Steals Device Data	36%	17%
Spies On User	36%	28%
Sends Premium SMS	16%	5%
Downloader	18%	8%
Back door	18%	12%
Tracks Location	9%	3%
Modifies Settings	20%	8%
Spam	7%	3%
Steals Media	0%	3%
Elevates Privileges	7%	2%
Banking Trojan	7%	3%
SEO Poisoning	0%	0%
Adware/ Annoyance	13%	9%
DDOS Utility	0%	0%
Hacktool	0%	0%

Mobile Threats: Malicious Code Actions—Additional Detail, 2013-2014

Source: Symantec

Platform	Documented Vulnerabilities	Percent
Apple iOS/iPhone/iPad	140	84%
Android	19	11%
BlackBerry	7	4%
Windows Mobile	1	1%

Mobile Threats: Documented Mobile Vulnerabilities by Platform, 2014

Source: Symantec

Month	Documented Vulnerabilities
January	2
February	6
March	28
April	19
May	1
June	29
July	6
August	1
September	53
October	7
November	16
December	0

Mobile Threats: Documented Mobile Vulnerabilities by Month, 2014

Source: Symantec

The following are specific definitions of each subcategory:

- Steals device data—gathers information that is specific to the functionality of the device, such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), operating system, and phone configuration data
- Spies on user—intentionally gathers information from the device to monitor a user, such as phone logs and SMSs, and sends it to a remote source
- Sends premium SMSs—sends SMSs to premium-rate numbers that are charged to the user's mobile account
- Downloader—can download other risks onto the compromised device
- Back door—opens a back door on the compromised device, allowing attackers to perform arbitrary actions
- Tracks location—gathers GPS information from the device specifically to track the user's location
- Modifies settings—changes configuration settings on the compromised device
- Spam—sends spam email messages from the compromised device
- Steals media—sends media, such as pictures, to a remote source
- Elevates privileges—attempts to gain privileges beyond those laid out when installing the app bundled with the risk
- Banking Trojan—monitors the device for banking transactions, gathering sensitive details for further malicious actions
- SEO poisoning—periodically sends the phone's browser to predetermined URLs in order to boost search rankings

Apps with malicious intentions can present serious risks to users of mobile devices. These metrics show the different functions that these bad apps performed during the year. The data was compiled by analyzing the key functionality of malicious apps.

Symantec has identified five primary mobile risk types:

- Steal information—Most common among bad apps is the collection of data from the compromised device. This is typically done with the intent to carry out further malicious activities, in much the way an information-stealing Trojan might. This includes both device- and user-specific data, ranging from configuration data to banking details. This information can be used in a number of ways, but for the most part it is fairly innocuous, with IMEI and IMSI numbers taken by attackers as a way to uniquely identify a device. More concerning is data gathered about the device software, such as operating system (OS) version or applications installed, to carry out further attacks (say, by exploiting a software vulnerability). Rarer but of greatest concern is when user-specific data, such as banking details, is gathered in an attempt to make unauthorized transactions. While this category covers a broad range of data, the distinction between device and user data is given in more detail in the subcategories below.
- Track user—The next most common purpose is to track a user's personal behavior and actions. These apps take data specifically in order to spy on the individual using the phone. This is done by gathering up various communication data, such as SMSs and phone call logs, and sending it to another computer or device. In some instances they may even record phone calls. In other cases these apps track GPS coordinates, essentially keeping tabs on the location of the device (and its user) at any given time. Gathering pictures taken with the phone also falls into this category.

- Send content—The third largest in the group of risks is apps that send out content. These risks are different from the first two categories because their direct intent is to make money for the attacker. Most of these apps will send a text message to a premium SMS number, ultimately appearing on the mobile bill of the device's owner. Also within this category are apps that can be used as email spam relays, controlled by the attackers and sending unwanted emails from addresses registered to the device. Another example in this category is constantly sent HTTP requests in the hope of bumping up certain pages within search rankings.
- Traditional threats—The fourth group contains more traditional threats, such as back doors and downloaders. Attackers often port these types of apps from PCs to mobile devices.
- Change settings—Finally, there are a small number of apps that focus on making configuration changes. They attempt to elevate privileges or simply modify various settings within the OS. The goal for this final group seems to be to perform further actions on the compromised devices.

Commentary

- Forty-six new Android malware families were identified in 2014, compared with 57 in 2013.
- The average number of variants per family in 2014 was 48, compared with 57 in 2013. Similar to the overall number of new mobile malware families, the number of variants for each family is also lower in 2014 compared with the previous year.
- As we have seen in previous years, a high number of vulnerabilities for a mobile OS do not necessarily lead to malware that exploits those vulnerabilities. Overall, there were 168 mobile vulnerabilities published in 2014, compared with 127 in 2013, an increase of 32 percent.
- Further analysis of mobile malware and spyware indicated the most common type of activity undertaken on a compromised device was done to spy on the user, at 36 percent in 2014 compared with 28 percent in 2013. Thirty-six percent of malicious mobile activity was designed to steal data in 2014, compared with 17 percent in 2013.

Data Breaches and Identity Theft

Background

Hacking continued to be the primary cause of data breaches in 2014. In 2014, there were four data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 145 million identities. Comparatively, there were eight breaches in 2013 of more than 10 million identities. As a result, the overall average number of identities exposed has decreased, from 2,181,891 identities per breach in 2013 to 1,116,767 in 2014.

As the overall average size of a breach has decreased, the median number of identities stolen has slightly increased, from 6,777 in 2013 to 7,000 in 2014. Using the median can be helpful in this scenario since it ignores the extreme values caused by the notable, rare events that resulted in the largest numbers of identities' being exposed. In this way, the median may be more representative of the underlying trend. While the number of incidents has increased, the number of identities exposed is still in the order of thousands, but there were fewer incidents that resulted in extremely large volumes of identities' being exposed in 2014 than in the previous year.

Hacking was the chief cause of most data breaches in 2014, and it consequently received a great deal of media attention. Hacking can undermine institutional confidence in a company, exposing its attitude toward security. The loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 49 percent of data breaches in 2014, according to Norton Cybercrime Index (CCI) data. As data breach notification legislation becomes more commonplace, we are likely to see the number of data breaches rise. Such legislation is often used to regulate the responsibilities of organizations after a data breach has occurred and may help mitigate against the potential negative impact on the individuals concerned.

The healthcare, retail, and education sectors were ranked highest for the number of data breach incidents in 2014; the top three accounted for 58 percent of all data breaches. However, the retail, computer software, and financial sectors accounted for 92 percent of all the identities exposed in 2014.

Methodology

The information analyzed regarding data breaches that could lead to identity theft is procured from the Norton CCI. The Norton CCI is a statistical model that measures daily the levels of threats, including malicious software, fraud, identity theft, spam, phishing, and social engineering. Data for the CCI is primarily derived from the Symantec Global Intelligence Network, one of the industry's most comprehensive sources of intelligence about online threats, along with certain other data from ID Analytics.[3] The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information, including names, addresses, Social Security numbers, credit card numbers, and medical histories. Using publicly available data, the Norton CCI determines the sectors that were most often affected by data breaches and the most common causes of data loss.

The sector that experienced the loss, along with the cause of the loss that occurred, is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

The data also reflects the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data. An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach. Data may include names, government-issued identification numbers, credit card information, home addresses, or email information. A data breach is considered deliberate when the

cause of the breach is due to hacking, insider intervention, or fraud. A data breach is considered to be caused by hacking if data related to identity theft is exposed by attackers' (external to an organization) gaining unauthorized access to computers or networks.

It should be noted that some sectors may need to comply with more stringent reporting requirements for data breaches than may others. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[4] Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are neither required nor encouraged to report data breaches may be underrepresented in this data set.

Date	Identities Exposed	Incidents
January	8,100,970	22
February	3,238,996	33
March	1,743,522	34
April	58,745,468	27
May	147,621,411	31
June	1,213,567	27
July	77,979,705	26
August	31,563,950	24
September	10,194,376	25
October	1,136,601	26
November	6,484,574	23
December	408,016	14

Timeline of Data Breaches Showing Identities Breached in 2014, Global

Source: Symantec

- There were 312 data breach incidents recorded by the Norton Cybercrime Index for 2014 and a total of 348 million identities exposed as a result.
- The average number of identities exposed per incident was 1,116,767, compared with 2,181,891 in 2013 (a decrease of more than 49 percent).
- The median number of identities exposed was 7,000, compared with 6,777 in 2013. The median is a useful measure, as it eliminates extreme values caused by the most notable incidents, which may not necessarily be typical.
- The number of incidents that resulted in 10 million or more identities' being exposed was four, compared with eight in 2013.

Rank	Sector	Number of Incidents	% of Incidents
1	Healthcare	116	37.2%
2	Retail	34	10.9%
3	Education	31	9.9%
4	Government and Public Sector	26	8.3%
5	Financial	19	6.1%
6	Computer Software	13	4.2%
7	Hospitality	12	3.8%
8	Insurance	11	3.5%
9	Transportation	9	2.9%
10	Arts and Media	6	1.9%

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

Rank	Sector	Number of Identities Exposed	% of Identities Exposed
1	Retail	205,446,276	59.0%
2	Financial	79,465,597	22.8%
3	Computer Software	35,068,405	10.1%
4	Healthcare	7,230,517	2.1%
5	Government and Public Sector	7,127,263	2.0%
6	Social Networking	4,600,000	1.3%
7	Telecom	2,124,021	0.6%
8	Hospitality	1,818,600	0.5%
9	Education	1,359,190	0.4%
10	Arts and Media	1,082,690	0.3%

Top 10 Sectors Breached by Number of Identities Exposed

Source: Symantec

- Healthcare, retail, and education were ranked highest for the number of data breach incidents in 2014; the top three accounted for 58 percent of all data breaches.
- The retail, computer software, and financial sectors accounted for 92 percent of all the identities exposed in 2014.
- This highlights that sectors involved in the majority of data breaches don't necessarily result in the largest caches of stolen identities, with the exception of retail.

Cause of Breach	Average Identities per Incident
Administration and human resources	9,090
Agriculture	5,480
Community and non-profit	193,722
Computer hardware	52,876
Computer software	2,697,570
Education	43,845
Financial	4,182,400
Government	274,126
Healthcare	62,332
Hospitality	151,550
Insurance	13,240
Internet service provider	212,500
Retail	6,042,538
Social networking	1,533,333
Telecom	424,804
Transportation	91,671
Arts and media	180,448
Manufacturing	2,492
Business consulting	19,154
Architectural	52,660

Average Number of Identities Exposed per Data Breach by Notable Sector

Source: Symantec

- The highest average number of identities exposed per breach in 2014 was in the retail and financial sectors, with between 4 million and 6 million identities exposed in each breach, on average.
- The largest breach incident in 2014 occurred in the retail sector, with an incident resulting in 145 million identities' reportedly being exposed.

Cause of Breach	Number of Incidents	% of Incidents
Attackers	153	49.0%
Accidentally made public	67	21.5%
Theft or loss of computer or drive	66	21.2%
Insider theft	26	8.3%

Top Causes for Data Breaches by Number of Breaches

Source: Symantec

Cause of Breach	Number of Identities Exposed	% of Identities Exposed
Attackers	286,398,409	82.2%
Accidentally made public	60,019,573	17.2%
Theft or loss of computer or drive	1,049,498	0.3%
Insider theft	963,676	0.3%

Top Causes for Data Breaches by Number of Identities Exposed

Source: Symantec

Cause of Breach	Average Identities per Incident
Hackers	1,871,885
Accidentally made public	895,815
Theft or loss	15,901
Insider theft	37,064

Average Number of Identities Exposed per Data Breach, by Cause

Source: Symantec

- Hacking was the leading cause of reported identities exposed in 2014: Hackers were also responsible for the largest number of identities exposed, as well as for 49 percent of the incidents and 82 percent of the identities exposed in data breach incidents during 2014.
- The average number of identities exposed per data breach for hacking incidents was approximately 1.8 million.

Type of Information	Number of Incidents	% of Data Types
Real Names	215	68.9%
Gov ID numbers (Soc Sec)	140	44.9%
Home Address	134	42.9%
Financial Information	110	35.3%
Birth Dates	109	34.9%
Medical Records	105	33.7%
Phone Numbers	66	21.2%
Email Addresses	61	19.6%
User names & Passwords	40	12.8%
Insurance	35	11.2%
Driver's licenses	16	5.1%

Types of Personal Information Exposed in Data Breach Incidents

Source: Symantec

- The most common type of personal information exposed in data breaches during 2014 was real names, where 69 percent of the incidents in 2014 included this type of information's being exposed.
- Government ID numbers (including Social Security numbers) were identified in 45 percent of the identity breaches during 2014, compared with birth dates in 35 percent and user names and passwords in 13 percent.

APPENDIX B: MALICIOUS CODE TRENDS

Appendix B: Malicious Code Trends

Malicious Code Trends

Symantec collects malicious code information from our large global customer base through a series of opt-in anonymous telemetry programs, including Norton Community Watch, Symantec Digital Immune System, and Symantec Scan and Deliver technologies. Millions of devices, including client devices, servers, and gateway systems, actively contribute to these programs. New malicious code samples, as well as detection incidents from known malicious code types, are reported back to Symantec. These resources give Symantec's analysts unparalleled sources of data to identify, analyze, and provide informed commentary on emerging trends in malicious code activity in the threat landscape. Reported incidents are considered potential infections if infections could have occurred in the absence of security software to detect and eliminate threats.

Malicious code threats are classified into four main types—back doors, viruses, worms, and Trojans:

- Back doors allow an attacker to remotely access compromised computers.
- Viruses propagate by infecting existing files on affected computers with malicious code.
- Worms are malicious code threats that can replicate on infected computers or in a manner that facilitates their being copied to another computer (such as via USB storage devices).
- Trojans are malicious code that users unwittingly install onto their computers, most commonly through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.

Many malicious code threats have multiple features. For example, a back door will always be categorized in conjunction with another malicious code feature. Typically, back doors are also Trojans; however, many worms and viruses also incorporate back door functionality. In addition, many malicious code samples can be classified as both worms and viruses due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.

The following malicious code trends were analyzed for 2014:

- Top Malicious Code Families
- Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
- Propagation Mechanisms
- Targeted Attacks Intelligence: Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Top Malicious Code Families

Background

Symantec analyzes new and existing malicious code families to determine attack methodologies and vectors that are being employed in the most prevalent threats. This information also allows system administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

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 new threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may be deployed, such as gateway or cloud-based filtering.

Methodology

A malicious code family initially consists of a distinct malicious code sample. As variants to the sample are released, the family can grow to include multiple variants. Symantec determines the most prevalent malicious code families by collating and analyzing anonymous telemetry data gathered for the reporting period.

Malicious code is classified into families based on variants in the signatures assigned by Symantec when the code is identified. Variants appear when attackers modify or improve existing malicious code to add or change functionality. These changes alter existing code enough that antivirus sensors may not detect the threat as an existing signature.

Overall, the top 10 list of malicious code families accounted for 33 percent of all potential infections blocked in 2014.

Rank	Name	Type	Propagation Mechanisms	Impacts/Features	% Overall
1	W32.Ramnit	Virus/ Worm	Executable files and removable drives	Infects various file types, including executable files, and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	10.4%
2	W32.Sality	Virus/ Worm	Executable files and removable drives	Uses polymorphism to evade detection. Once running on an infected computer it infects executable files on local, removable and shared network drives. It then connects to a P2P botnet, downloads and installs additional threats. The virus also disables installed security software.	5.9%
3	W32.Almanahe	Virus/ Worm	CIFS/mapped drives/ removable drives/ executables	Disables security software by ending related processes. It also infects executable files and copies itself to local, removable, and shared network drives. The worm may also download and install additional threats.	4.0%
4	W32.Downadup	Worm/ Back door	P2P/CIFS/remote vulnerability	The worm disables security applications and Windows Update functionality and allows remote access to the infected computer. Exploits vulnerabilities to copy itself to shared network drives. It also connects to a P2P botnet and may download and install additional threats.	3.9%
5	W32.SillyFDC	Worm	Removable drives	Downloads additional threats and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	3.4%
6	W32.Virut	Virus/ Back door	Executables	Infects various file types including executable files and copies itself to local, removable, and shared network drives. It also establishes a back door that may be used to download and install additional threats.	2.3%
7	W32.Chir	Worm	SMTP engine	Searches across the network and accesses files on other computers. However, due to a bug, these files are not modified in any way.	1.3%
8	W32.Imaut	Worm	IM	Downloads and installs additional threats as well as disables security software by ending security related processes. Sends instant messages containing a malicious URL that, if clicked, will trigger an attack on the recipient and install a copy of the worm.	0.8%
9	W32.Mabezat	Virus/Worm	SMTP/CIFS/ removable drives	Copies itself to local, removable, and shared network drives. Infects executables and encrypts various file types. It may also use the infected computer to send spam email containing infected attachments.	0.7%
10	W32.Changeup	Worm	Removable and mapped drives/ File sharing programs/Microsoft Vulnerability	The primary function of this threat is to download more malware on to the compromised computer. It is likely that the authors of the threat are associated with affiliate schemes that are attempting to generate money through the distribution of malware.	0.2%

Overall Top Malicious Code Families, 2014

Source: Symantec

Rank	Malware	% of Email Malware	Equivalent Ratio in Email
1	Trojan.Zbot	6.0%	1 in 16.8
2	Trojan.Zbot-SH	4.3%	1 in 23.0
3	Exploit/Link.G	3.2%	1 in 31.1
4	VBS.Downloader.Trojan	2.5%	1 in 40.0
5	Exploit/Link.D	1.5%	1 in 67.5
6	Court.Fakeavlock	0.9%	1 in 107.2
7	Exploit/Link-Downloader	0.9%	1 in 113.9
8	Trojan.Dropper	0.9%	1 in 116.3
9	JS/Selfaltering.dam	0.6%	1 in 164.2
10	W97M.Downloader	0.5%	1 in 185.4

Relative Proportion of Top 10 Malicious Code Blocked in Email Traffic by Symantec.cloud in 2014, by Percentage and Ratio

Source: Symantec.cloud

Commentary

- Ramnit overtook Sality again to become the most prevalent malicious code family in 2014.[5] Ranked first in 2011, 2012, and 2013, it was the top malicious code family by volume of potential infections again in 2014.
- Samples of the Ramnit family of malware were responsible for significantly more potential infections (10.4 percent) than was the second-ranked malicious code family in 2014, Sality[6] (5.9 percent).
- First discovered in 2010, W32.Ramnit has remained a prominent feature of the threat landscape.
- Ramnit spreads by encrypting and then appending itself to DLL, EXE, and HTML files. It can also spread by copying itself to the recycle bin on removable drives and creating an AUTORUN.INF file so that the malware is potentially automatically executed on other computers. This can occur when an infected USB device is attached to a computer. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Ramnit and Sality (as well as SillyFDC[7] and others) effective vehicles for installing additional malicious code on computers.
- The Sality family of malware remains attractive to attackers because it uses polymorphic code that can hamper detection. Sality is also capable of disabling security services on affected computers. These two factors may lead to a higher rate of successful installations for attackers. Sality propagates by infecting executable files and copying itself to removable drives such as USB devices. Similar to Ramnit, Sality also relies on AUTORUN.INF functionality to potentially execute when those drives are accessed.

- Overall in 2014, 1 in 244 emails was identified as malicious, compared with 1 in 196 in 2013; 12 percent of email-borne malware contained hyperlinks that referenced malicious code, in contrast with malware that was contained in an attachment to the email. This figure was 25.4 percent in 2013, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.
- In 2014, 13.9 percent of malicious code detected that year was identified and blocked using generic detection technology. 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 family, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.
- Trojan.Zbot was the most frequently blocked malware in email traffic by Symantec.cloud in 2014, with Trojan.Zbot-SH taking the second position. It was the reverse ranking in 2013.

Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size

Background

Malicious code activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace, which can drive down prices, thereby increasing adoption rates. There may be other factors at work based on the local economic conditions. Similarly, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. Small and medium businesses (SMBs) may find themselves the targets of malicious attacks by virtue of the relationships they have with other organizations. For example, a company may be subjected to an attack because it is a supplier to a larger organization, and attackers may seek to take advantage of this relationship in forming the social engineering behind subsequent attacks on the main target, using the SMB as a springboard for these later attacks. SMBs are perceived to be softer targets, as they are less likely to have the same levels of security as larger organizations, which have larger budgets applied to their security countermeasures.

Methodology

Analysis of malicious code activity by geography, industry, and size is based on the telemetry analysis from Symantec.cloud clients for threats detected and blocked against those organizations in email traffic during 2014.

This analysis looks at the profile of organizations being subjected to malicious attacks, not the source of the attacks.

Industry	2014	2013
Public Administration	1 in 88.9	1 in 95.4
Agriculture, forestry & fishing	1 in 149.5	1 in 415.5
Services – Professional	1 in 171.2	1 in 396.5
Services – Non-Traditional	1 in 186.2	1 in 401.8
Finance, insurance & Real Estate	1 in 204.0	1 in 426.8
Nonclassifiable Establishments	1 in 213.9	1 in 460.2
Construction	1 in 217.7	1 in 471.8
Wholesale	1 in 223.2	1 in 435.0
Transportation & Communication	1 in 289.0	1 in 480.5
Mining	1 in 427.3	1 in 426.8

Proportion of Email Traffic Identified as Malicious by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1-250	1 in 142.3	1 in 332.1
251-500	1 in 135.2	1 in 359.4
501-1000	1 in 203.3	1 in 470.3
1001-1500	1 in 180.6	1 in 356.9
1501-2500	1 in 218.4	1 in 483.5
2501+	1 in 284.7	1 in 346.5

Proportion of Email Traffic Identified as Malicious by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
United Kingdom	1 in 78.6	1 in 198.9
Saudi Arabia	1 in 167.8	1 in 869.1
Kenya	1 in 177.4	1 in 1011.7
Hong Kong	1 in 180.3	1 in 440.7
Nigeria	1 in 193.9	1 in 970.3
Austria	1 in 197.1	1 in 300.7
Ireland	1 in 199.5	1 in 440.6
South Africa	1 in 214.7	1 in 272.8
Hungary	1 in 221.5	1 in 306.8
Thailand	1 in 227.7	1 in 929.2

Proportion of Email Traffic Identified as Malicious by Geographic Location, 2014

Source: Symantec.cloud

Commentary

- The rate of malicious attacks carried out by email has increased for four of the top 10 geographies being targeted, and six new countries appeared in the top 10 list in 2014: Saudi Arabia, Kenya, Hong Kong, Nigeria, Ireland, and Thailand.
- Businesses in the United Kingdom were subjected to the highest average ratio of malicious email-borne threats in 2014, with 1 in 78.6 emails blocked as malicious, compared with 1 in 198.9 in 2013.
- Globally, organizations in the government and public sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 88.9 emails blocked as malicious in 2014, compared with 1 in 95.4 in 2013.
- Malicious email threats have increased for all sizes of organizations, with 1 in 284.7 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2014, compared with 1 in 346.5 in 2013.
- One in 142.3 emails was blocked as malicious for SMBs with 1–250 employees in 2014, compared with 1 in 332.1 in 2013.

Propagation Mechanisms

Background

Worms and viruses use various means to spread from one computer to another. These means are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), Simple Mail Transfer Protocol (SMTP), common Internet file system (CIFS),[8] peer-to-peer (P2P) file transfers, and remotely exploitable vulnerabilities.Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a back door server and using it to upload and install itself.

Methodology

This metric assesses the prominence of propagation mechanisms used by malicious code. To determine this, Symantec analyzes the malicious code samples that propagate and ranks associated propagation mechanisms according to the related volumes of potential infections observed during the reporting period.[9]

Rank	Propagation Mechanisms	2014 Percentage	Change	2013 Percentage
1	Executable file sharing The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	65%	-5%	70%
2	File transfer, CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within. Malicious code creates copies of itself on shared directories to affect other users who have access to the share.	31%	-1%	32%
3	Remotely exploitable vulnerability The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	22%	-1%	23%
4	File transfer, email attachment The malicious code sends spam email that contains a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	7%	-1%	8%
5	File transfer, non-executable file sharing The malicious code infects non-executable files.	4%	+1%	3%
6	Peer to Peer file sharing	2%	-1%	3%
7	SQL The malicious code accesses SQL servers, by exploiting a latent SQL vulnerability or by trying default or guessable administrator passwords, and copies itself to the server.	1%	+0%	1%
8	File Transfer, Instant Messenger The malicious code sends or modifies instant messages that contains a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	1%	+0%	1%
9	File transfer, HTTP, embedded URI, email message body The malicious code sends spam email containing a malicious URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	<1%	=	<1%
10	File transfer, MMS attachment. The malicious code sends an MMS attachment, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	<1%	=	<1%

Propagation Mechanisms

Source: Symantec

Commentary

As malicious code continues to become more sophisticated, many threats employ multiple mechanisms:

- Executable file sharing activity decreases: In 2014, 65 percent of malicious code propagated as executables, a small decrease from 70 percent in 2013. This propagation mechanism is typically employed by viruses and some worms to infect files on removable media. For example, variants of Ramnit and Sality use this mechanism, and both families of malware were significant contributing factors in this metric, as they were ranked as the two most common potential infections blocked in 2014.
- Remotely exploitable vulnerabilities decrease: At 22 percent, the percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2014 was 1 percentage point lower than in 2013. Examples of attacks employing this mechanism include Downadup, which gained some momentum and is still a major contributing factor to the threat landscape, but was ranked fourth in 2013.
- File transfer using CIFS is in decline: The percentage of malicious code that propagated through CIFS file transfer fell by 1 percentage point between 2013 and 2014, a similar decline as between 2012 and 2013. Fewer attacks exploited CIFS as an infection vector in 2014.
- File transfer via email attachments also decreased: It is worth noting that file transfer via email attachments slightly decreased in 2014 compared with 2013, with 1 in 244 emails being identified as malicious in 2014, compared with 1 in 196 in 2013. In 2014, 12 percent of email attacks used malicious URLs, compared with 25 percent in 2013, showing an overall decrease in malicious emails.

Targeted Attacks Intelligence: Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Over the year 2014, Symantec could identify about 26,000 spear phishing emails that were deemed targeted by our threat analysts. However, this does not mean that we were facing the same number of attackers. Intuitively, we can easily imagine that some of these targeted attacks or intrusions may originate from the same hackers or threat group. Some of these threat actors may have different skills, exhibit various behaviors, and pursue different goals. To get a better understanding of this threat landscape, it is important to be able to differentiate between them and identify series of related attacks that might have been sourced by the same (group of) attackers. This will help us get a better understanding of attackers' tactics, techniques, and procedures (TTPs) and their motivation, which can ultimately be used to proactively detect them when attackers are coming back with new exploits or if they use slightly adapted techniques to attempt to compromise other customers.

However, finding groups of related attacks and attributing them to a specific threat actor or hacker group, based solely on intrusion activity or logging data, are challenging. The main reason is that skilled attackers can and do obviously update at least part of their attack tools and methodology in order to maximize their chances of successfully compromising the organization(s) they are targeting. While changing all aspects of their attack tools or exploit kits might have a prohibitive cost, chances are that they will adapt their methods over time by investing their resources into developing new exploits and adapting their intrusion tools.

As a result, it might be challenging for us, as defenders, to determine whether two spear phishing attacks were conducted by the same person, by different people who are collaborating, or by two unrelated hackers who decide independently to compromise the same company or even the same computer. Nevertheless, with enough information, analytical experience, and the technological tools to piece it all together, it might be possible to reconstruct attack campaigns from raw email data and additional meta-data on the malware or the exploit crafted together with the email. Consider an analogy with a serial killer in the real world, who leaves behind traces of his crime at different crime scenes. While individual crimes may vary in many details (such as the crime location, the victim's gender and age, the weapon or vehicle used, the various signs left at the crime scene, and how the crime scene was framed by the criminal), investigators might be able to collect different pieces of evidence that, when put together appropriately, could enable them to reconstruct the whole puzzle and ultimately identify which criminal was behind a series of crimes, based on the identified modus operandi and through the combination of all available pieces of evidence.

How Symantec is able to differentiate between distinct targeted attack campaigns using advanced TRIAGE technology

Symantec advanced TRIAGE data analytics technology aims at reproducing, in an automated fashion, a forensics methodology similar to the one performed by crime investigators, yet in the digital world. This framework has been designed to help analysts answer fundamental questions about cyberattacks, such as:

- Campaign analysis: Which series of attacks might be related to each other, even though they may be targeting different organizations—on the same or different dates—and using different malware or different exploits?
- What are the attackers' TTPs? How many different groups of attackers can we identify based on their modus operandi?
- What are the characteristics and dynamics of attack campaigns run by the same hacker groups? For example, what is their prevalence, size, and scale, or their sophistication?

Symantec uses the term attack campaign to refer to a series of spear phishing emails (or email intrusions) that:

1. Show clear evidence that the subject and target have been deliberately selected
2. Contain at least 3–4 strong correlations to other emails, such as the email topic, sender address, recipient domain, source IP address, attachment MD5, etc.

Attack campaigns may be sent on a single day or spread across multiple days; however, emails within the same campaign are always linked by a number of similar traits and thus form a sort of "chain of attacks."

One of the challenges to identifying such attack campaigns is that intrusions sourced by the same attackers (group) may have varying degrees of correlation. Without knowing in advance which features or indicators one should use to correlate attacks, this makes it very tedious for analysts to identify groups of related attacks. Figure 1 illustrates graphically this challenge of varying correlations between three different intrusions that were identified as parts of the same campaign. For example, intrusions 1 and 2 are linked by a different set of email features than are intrusions 2 and 3. This means that attackers may change any one feature when targeting different companies over time. Since we don't know in advance what their next move is, we have to rely on advanced correlation mechanisms that enable us to identify groups of related attacks (for example, originating from a specific threat group) without knowing which set of features should be used to associate these attacks with a particular group.

Phase	Email feature	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	**Recipient**	[user1]@org1.**gov.xy**	[user2]@**org2.gov.xy**	[user3]@**org2.gov.xy**
Weaponization	**Attach_name**	**Global Pulse Project***.pdf**		Agenda - G20***.pdf
	Attach MD5	**dd2ed3f7dea d4a[***]**		2e36081dd7f62e[***]
Delivery	**Date**	2011-05-13	2011-05-14	2011-07-02
	From addr.	[Att1]@domain1.com	[Att2]@domain2.com	
	Sender IP	**74.125.83.*** **		74.125.82.***
	Subject	FW:Project Document	Project Document	G20 Ds Finance Key Info – Paris July 2011
	Email body	[body1]		[body2]
Exploitation	**AV signature**	**CVE-2011-0611.C**		
Persistence	**C&C domains**	www.webserver.***		[N/A]

Figure 1: Illustration of varying correlations between different intrusions of the same campaign

By leveraging our TRIAGE data analytics technology, we can automatically group targeted attacks based on common elements likely reflecting the same root cause. As a result, we are able to identify complex patterns showing various types of relationships among series of targeted attacks, giving insight into the manner by which attack campaigns are orchestrated by various threat actors. The TRIAGE approach is illustrated in Figure 2.

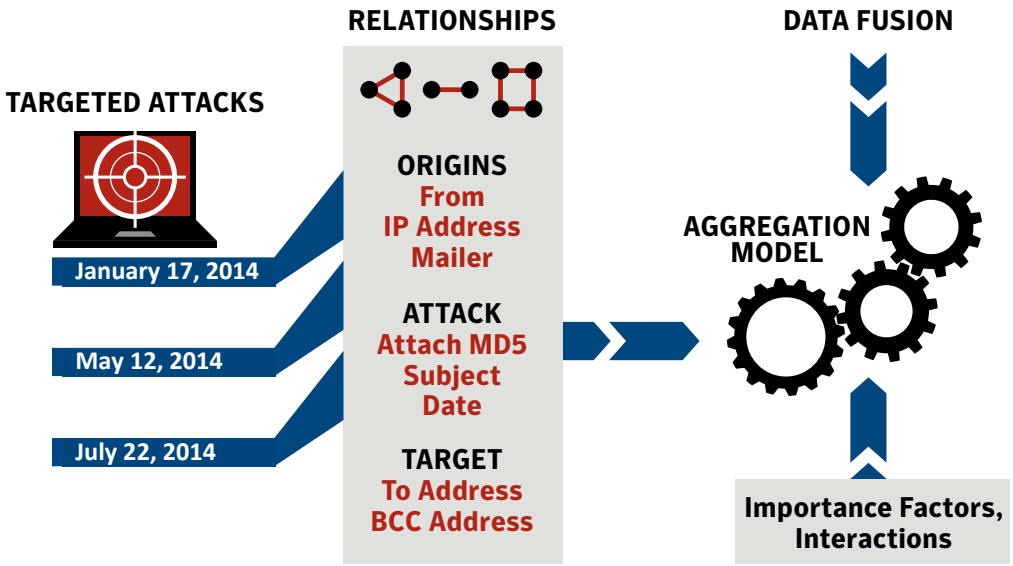


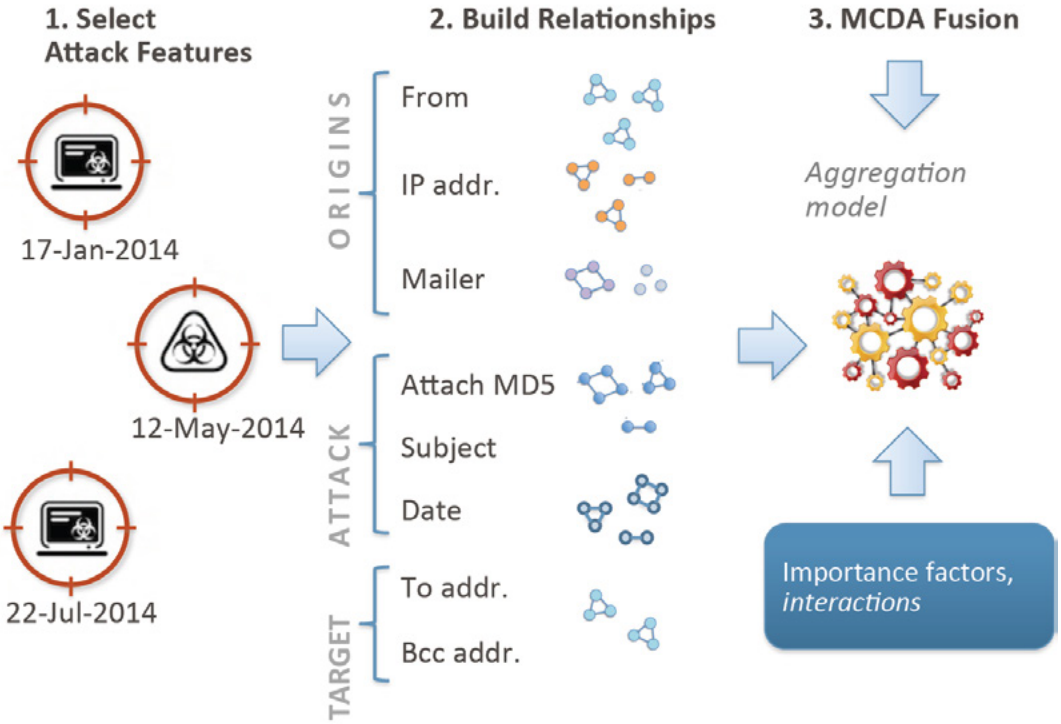
Figure 2: Illustration of TRIAGE methodology

It is worth mentioning that our TRIAGE framework was recently enhanced with novel visualizations thanks to VIS-SENSE,[10] a European research project aimed at developing visual analytics technologies for network security applications. Since its original conception, TRIAGE has been successfully used to analyze the behavior of cybercriminals involved in various types of Internet attack activities, such as rogue antivirus websites,[11] spam botnets operations,[12] scam campaigns,[13] spam campaigns launched from hijacked networks,[14] and targeted attacks performed via spear phishing emails.[15,16]

Insights into targeted attack campaigns

In 2014 Symantec's TRIAGE technology identified 841 clusters of spear phishing attacks (hereafter called attack campaigns, as defined previously), which quite likely reflect different waves of attacks launched by the same groups of individuals. Indeed, within the same cluster, attacks are linked by at least 3–4 characteristics among the following ones:

- The origins of the attack (like the email "From" address and source IP address used by the attacker)
- The attack date
- The characteristics of the malicious file attached to the email (for example, MD5 checksum; AV signature; file name; some meta-data coming from both static and dynamic analysis, such as document type or domains and IPs contacted by the malware)
- The email subject
- The targeted recipient (To" or "BCC" address fields in the email)

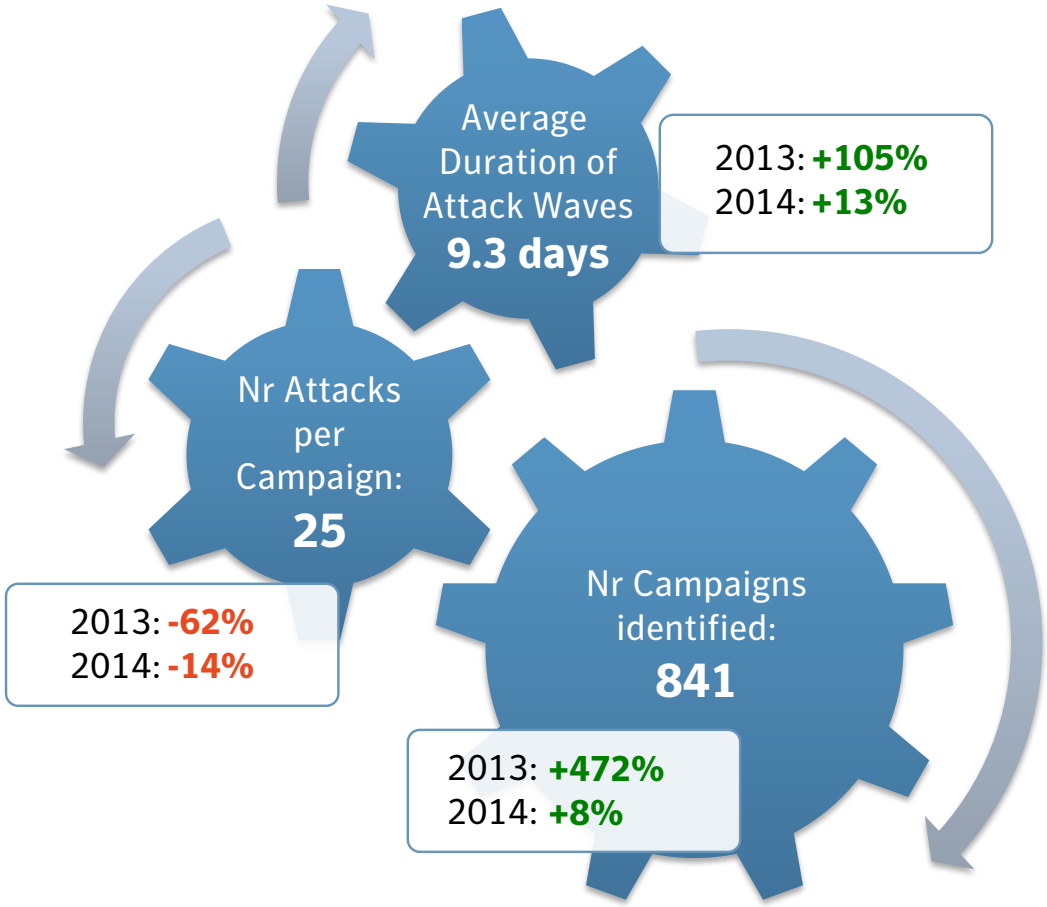


- *Figure 3: Illustration of Symantec's TRIAGE methodology*

Figure 4 and Figure 5 highlight some global metrics calculated across all attack campaigns identified by TRIAGE. To give more perspective to these figures, we compare them with statistics calculated in the past two years (since 2013), which can generate some insights about the characteristics and evolution of spear phishing campaigns. More specifically, we can clearly identify the following new trends:

- Spear phishing email campaigns have been increasingly prevalent since 2011, with a slight increase (8 percent) in the number of spear phishing campaigns compared with 2013! Considering the 16 percent decrease in the number of observed (individual) spear phishing emails since 2013, the increased number of spear phishing campaigns indicates that spear phishing emails have become a more prevalent technique among cybercriminal groups to launch targeted attacks. As companies and organizations have become more and more aware of the importance of securing their networks and systems against the wide range of Internet attacks, more cybercriminal groups appear to be leveraging spear phishing emails to infiltrate networks.
- Because the average number of attacks per campaign has significantly decreased, we can say they are performed at a smaller scale, likely in an effort by attackers to remain as stealthy as possible and not to raise too much suspicion. Because of the way TRIAGE identifies campaigns of spear phishing emails, we can also say that campaigns are more diverse in terms of the attackers perpetrating them, the companies or organizations that are targeted, the content of attacks (for example, the email, the exploit[s] used, the contacted C&C server[s], etc.), or a combination thereof.

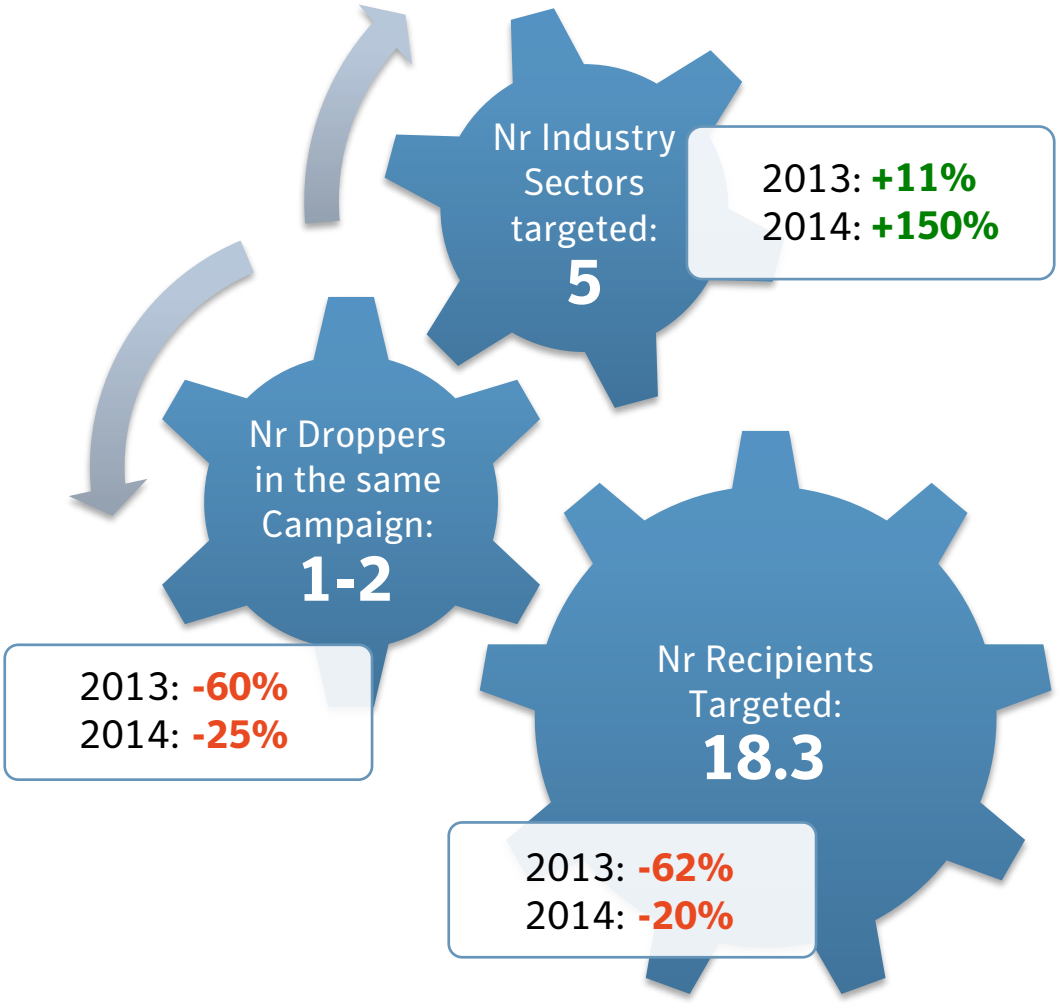
- We observe also that the average duration of a spear phishing campaign has increased a lot (9.3 days on average), which suggests that these campaigns have been increasingly persistent over the past few years (attackers won't give up after the first attempt! On the contrary, they will persist much longer to try to penetrate the premises of a company or an organization). The decreased number of attacks per campaign combined with the longer average duration of campaigns also likely indicates the will of attackers to remain under the radar by launching fewer attacks over a longer period of time.



- *Figure 4: Global metrics calculated across all identified campaigns (1)*

Figure 5 further highlights other interesting aspects of these targeted attack campaigns:

- If we look now at the average number of recipients targeted during the same campaign, this number has dropped significantly compared with 2013. This means that spear phishing campaigns are more and more focused, targeting fewer individuals, and conducted over a long period of time!
- Similarly, we observed that the average number of distinct droppers used in the same campaign has dropped by 25 compared with 2013. This tends to show that campaigns are usually tied to very few attacks (one or two on average) used against many targets. This makes spear phishing campaigns more consistent attack-wise and thus slightly less stealthy. Note that different droppers may sometimes contain the very same exploit, which was simply repacked in different documents (pdf, doc, xls, etc). The availability of and easy access to these exploits (for example, via tools like Metasploit) for a wide range of vulnerabilities (including zero-day vulnerabilities) then make targeted attacks via spear phishing emails a method of choice for attackers to breach a company's or organization's network.
- Finally, the average number of different industries targeted during the same campaign has increased by 150 compared with 2013, showing a significant broader diversification in spear phishing attacks!



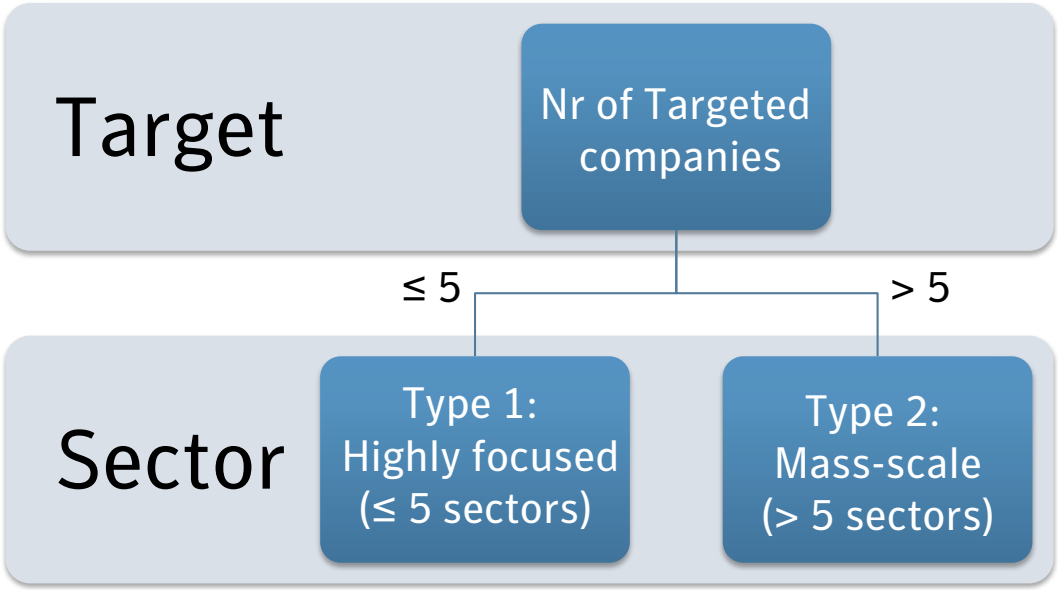
- *Figure 5: Global metrics calculated across all identified campaigns (2)*

Highly Focused versus Mass-Scale Campaigns

The 841 distinct campaigns of spear phishing attacks were then further classified into two groups:

- Type 1: Highly focused and targeted campaigns
- Type 2: Mass-scale organizational targeted attacks (MOTAs)

To this end, we used a combination of two criteria: the number of targeted companies and the number of distinct industry sectors associated with them. Type 1 campaigns were defined as spear phishing campaigns that targeted five (or fewer) distinct companies in five (or fewer) different sectors. Spear phishing campaigns not matching these criteria were deemed Type 2 campaigns (that is, they fit the profile of MOTAs) because they targeted a more significant set of different industries having very different lines of business.



- *Figure 6: Criteria used to classify targeted attack campaigns according to their scale*

Based on the classification defined previously, we found that in 2014 about three-fifths of spear phishing campaigns were highly focused and targeted a smaller number of companies active in the same or closely related sectors. The other two-fifths of the campaigns were still targeted (in the sense of being in low-copy number and showing some evidence of a selection of a subject in relation with the recipient activity), but these campaigns involved more large-scale attacks, in the sense that they were targeting more companies and organizations active in different sectors.

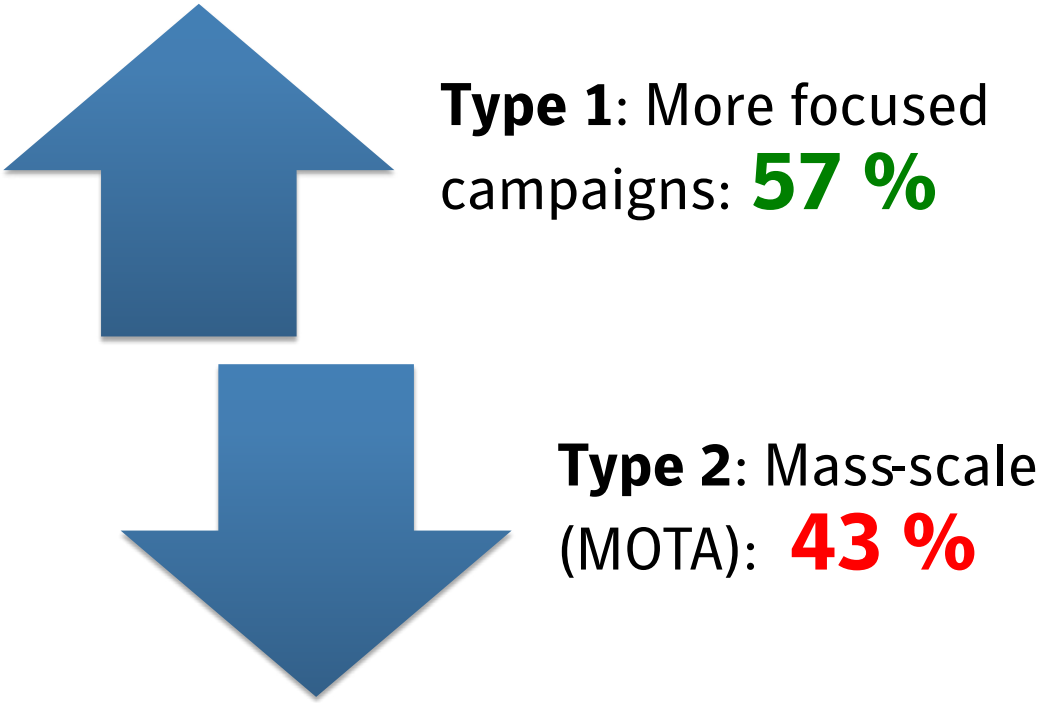


Figure 7: Types of campaigns

Type 1 – highly targeted campaigns

Campaign against an intergovernmental organization on October 8, 2014

As we have seen, 57 percent of spear phishing attacks are forming rather small campaigns, meaning they are organized on a relatively small scale and tend to focus on specific targets. A first example of such a campaign took place on October 8, 2014, and targeted an intergovernmental organization. As illustrated in Figure 8, spear phishing emails were sent to nine different recipients within the organization but from only three different email addresses. All emails had the same subject line—"Situation Report about Afghan"—a topic relevant to the targeted recipients and that turns out to also be the name of the attached file. The attached file ("Situation Report about Afghan.doc"; md5=ed9f9814a9fd661ec00392171133a4cc) was carrying a malicious payload exploiting an old vulnerability in Microsoft Office (CVE-2012-1058), allowing arbitrary code, such as code to install a back door or any other piece of malicious code, to be executed by the attacker. Although the vulnerability was patched shortly after it was disclosed (CVE-2012-1058), in February 2012, it seemed to have been widely used by cybercriminals in numerous targeted attack campaigns. Evidence also shows the attacks likely originated from Russia (domain names in source email addresses ended with .ru top-level domain and were hosted in Russia).

As far as we know, Symantec customers have been protected against the exploitation of the CVE-2012-1058 vulnerability since its disclosure.[17]

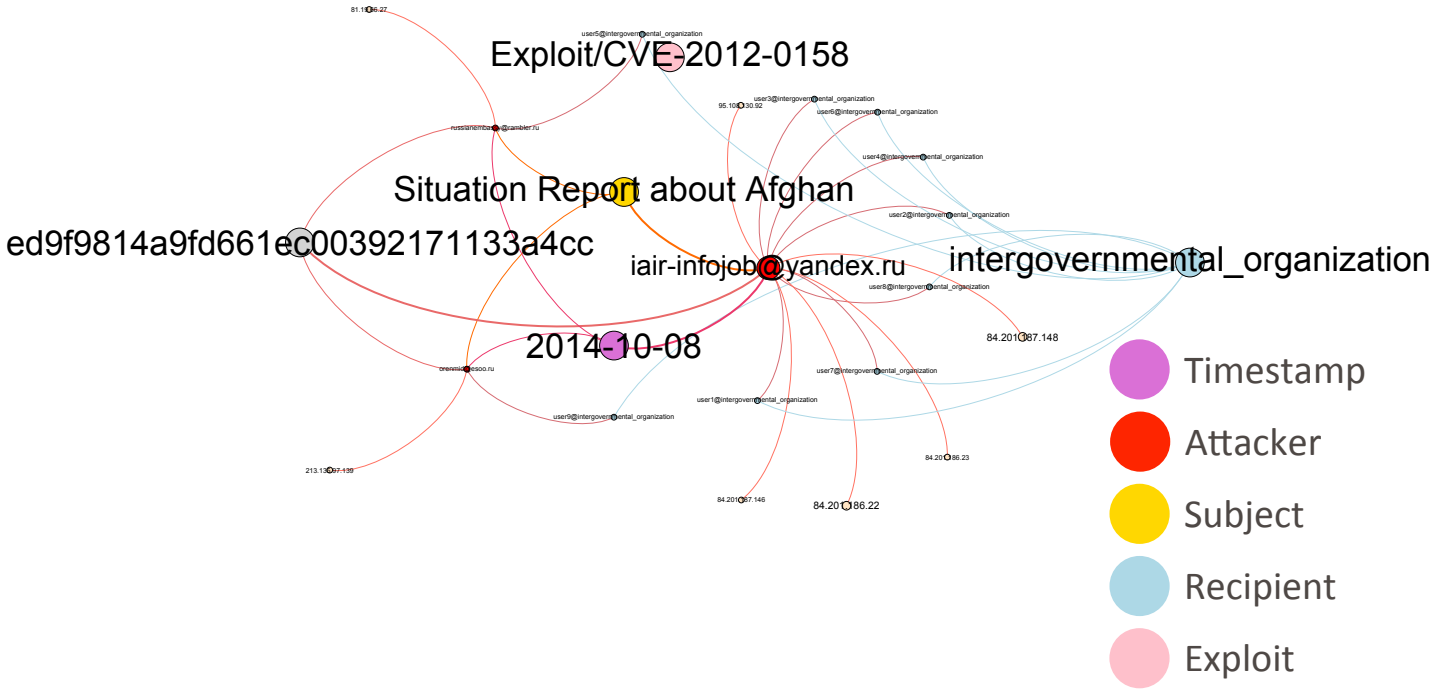


Figure 8: Spear phishing email campaign against an intergovernmental organization

Campaign against a major energy company between February 8, 2014, and February 22, 2014

Another highly targeted spear phishing email campaign took place between February 8, 2014, and February 22, 2014, and targeted an American company active in the energy sector. During this campaign, nine spear phishing emails were sent to a single recipient in the company but from eight different email addresses. On some days and during the 15 days this campaign lasted, up to two emails per day were sent. This campaign is illustrated in Figure 8. All emails included a different subject line (such as "Fortune 100 Loyalty Incentives Program," "Trade Monitoring Report as at 14th February"). While the name of the attached file remained the same throughout the campaign ("script.au3"), the content of the file varied a lot, possibly due to a single piece of malware repacked several times, thus producing apparently different files. We do not know whether the attacks were successful or what the objective of the attacker(s) was, for instance, using the infected system as a pivot to infiltrate other systems in the corporate network, stealing sensitive information from the infected system directly). We believe the attacks all originated from within the United States (domain names in source email addresses were hosted in the United States). Finally, the duration and highly targeted aspect of this campaign show that attackers nowadays can be perseverant and determined to attack a given company or, in this case, a given individual within that company.

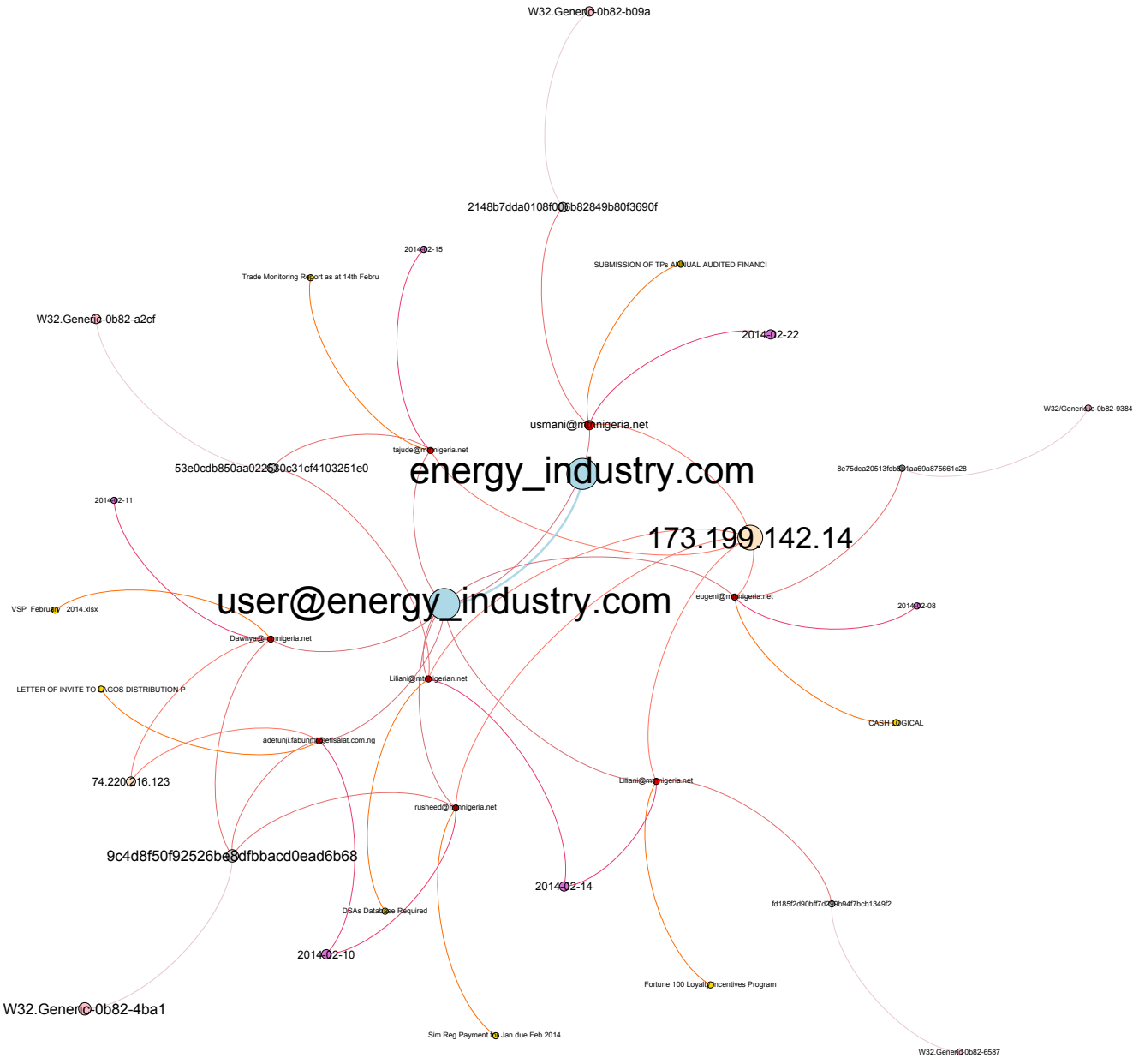


Figure 9: Spear phishing email campaign against a major energy company

Type 2: Mass-scale Organizational Targeted Attacks (MOTAs)

About two-fifths of targeted attacks identified in 2014 were organized on a larger scale and fit the profile of a MOTA. MOTAs target a large number of people in multiple organizations, working in different sectors, over multiple days. As described earlier, we used a threshold of five different companies, active in five completely different sectors, to classify attack campaigns and label them as MOTA versus highly focused. Most of the large-scale campaigns are quite well resourced, with up to 17 different exploits used during the same campaign.

The Bagle mass-mailer worm campaign between January 1, 2014, and April 29, 2014

A first example of such a campaign, illustrated in Figure 10, took place between January 1, 2014, and April 29, 2014; targeted no less than 12 companies located in Europe, Asia, and Australia; and was active in seven different industry sectors, including public administration, finance and insurance, and transportation. A total of 155 emails were sent over a period of about four months. This campaign thus appears loosely focused.

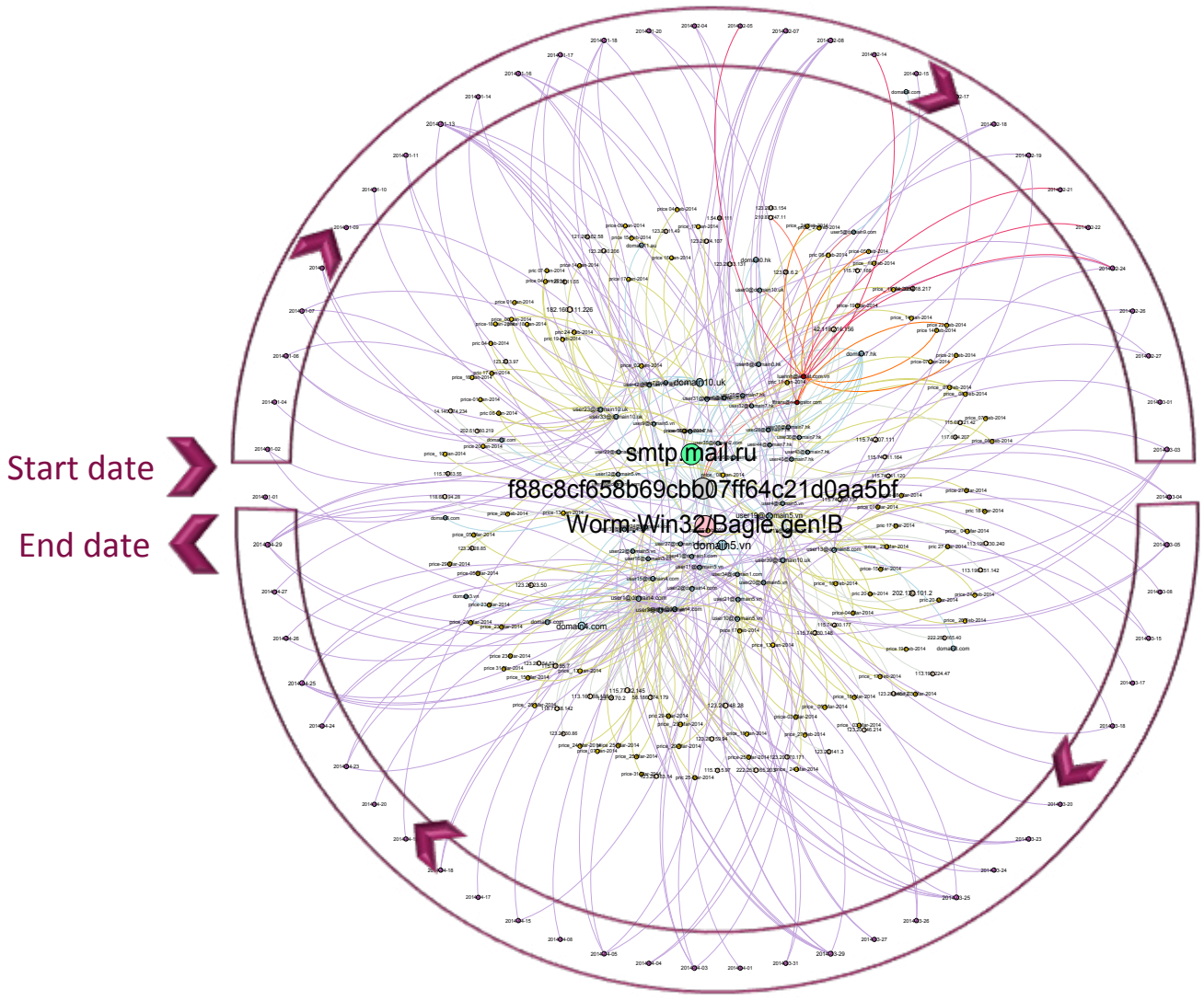


Figure 10: The Bagle mass-mailer worm campaign

When looking at the file attached to the emails, we can see that all emails were carrying a variant of the Bagle worm (Worm:Win32/Bagle.gen!B), which is a piece of code that replicates itself automatically by sending copies of itself via an attached file in an email.[18] Although the attached file name (pattern: "[8-12 characters].exe") was different in almost every spear phishing email, the content of the file was identical throughout the campaign (md5=f88c8cf658b69cbb07ff64c-21d0aa5bf). Moreover, the subject line included in the emails varied with the attachment file name and always followed the pattern "price[-_][date in the format dd-mm-yyyy]." Also, we found that the instance of the Bagle worm observed in this campaign used the free Russian mail service mail.ru to send the emails through which it replicated itself.

As far as we know, Symantec customers were protected against these attacks.

The Ebola campaign on October 27–28, 2014

Another interesting example of a mass-scale spear phishing email campaign took place on October 27–28, 2014, and consisted of 80 emails that targeted about 50 different companies active in 10 different industry sectors around the world. All emails included a subject line referring to the Ebola virus that dominated the news headlines in 2014.

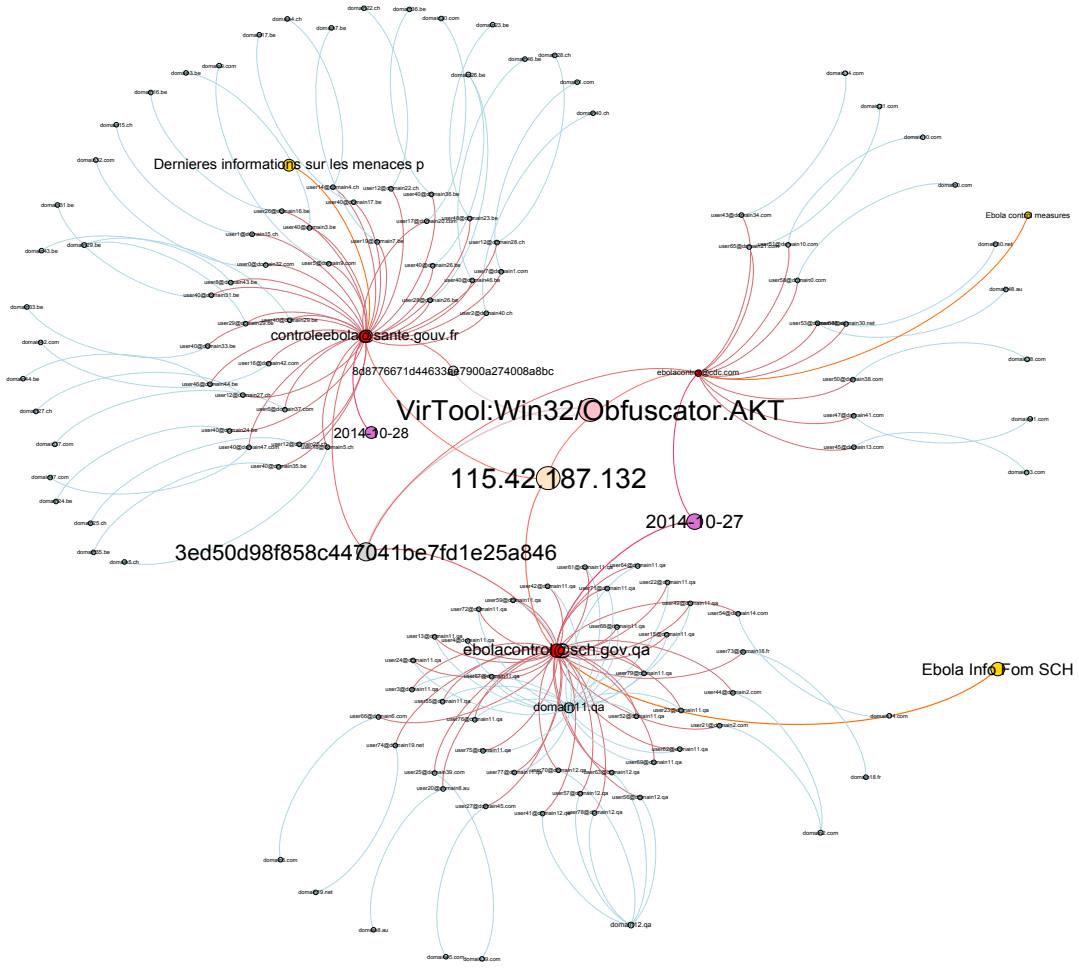


Figure 11: The Ebola campaign

In this campaign, illustrated in Figure 11, all emails were carrying two apparently different instances of an obfuscated piece of malware (VirTool:Win32/Obfuscator.AKT, md5=3ed50d98f-858c447041be7fd1e25a846; 8d8776671d44633ae7900a274008a8bc). The obfuscation of the attached malware hindered the detection and identification of the underlying piece of malicious code. However, the attached piece of code was apparently dropping a Trojan. All emails were sent using only three different source email addresses, but all three could be tracked to a single source IP address (115[.]42[.]187[.]132). We identified two waves in the campaign: (1) one taking place on October 27 and (2) one taking place on October 28.

1. In the first wave, emails were sent from two source email addresses. Two different subject lines—one for each source address—were used for the emails. The set of recipients varied with the source email address used.
2. In the second wave, emails were sent from a single source email address. A singular aspect of this wave is that it appeared to target a French-speaking audience, with emails (including the subject line) translated into French and apparently originating from the French Ministry of Health (@sante.gouv.fr source email address). Of course, the source email address was likely spoofed by the attacker(s). Email recipients were also mostly located in France, Belgium, and Switzerland.

APPENDIX C: SPAM & FRAUD ACTIVITY TRENDS

Appendix C: Spam & Fraud Activity Trends

Spam and Fraud Activity Trends

This section covers phishing and spam trends. It also discusses activities observed on underground economy-type servers, as this is where much of the profit is made from phishing and spam attacks.

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they can then use to commit fraudulent acts. Phishing generally requires victims to provide their credentials, often by duping them into filling out an online form. This is one of the characteristics that distinguish phishing from spam-based scams (such as the widely disseminated "419 scam"[19] and other social engineering scams).

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver Trojans, viruses, and phishing attacks. Spam can also include URLs that link to malicious sites that, without the user's being aware of it, attack a user's system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email services.

This section includes the following metrics:

- Analysis of Spam Activity Trends
- Analysis of Spam Activity by Geography, Industry Sector, and Company Size
- Analysis of Spam Delivered by Botnets
- Analysis of Phishing Activity by Geography, Industry Sector, and Company Size
- Whois attacking you? Beware of malicious BGP hijacks!

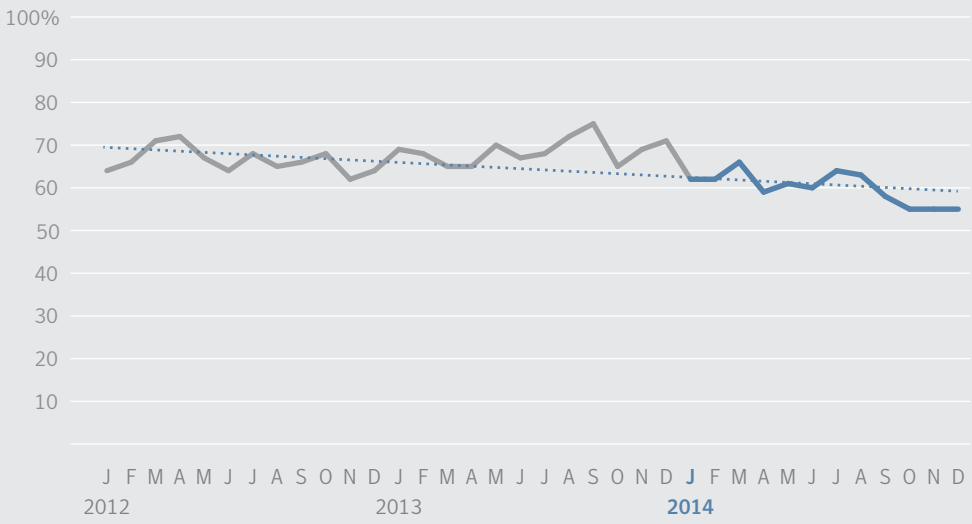
Analysis of Spam Activity Trends

Background

This section discusses the patterns and trends relating to spam message volumes and the proportion of email traffic identified as spam during 2014.

Methodology

The analysis for this section is based on global spam and overall email volumes for 2014. Global values are determined based on the statistically representative sample provided by Symantec Messaging Gateway[20] operations, and the spam rates include spam blocked by Symantec.cloud.



Global Spam Rate, 2012–2014

Source: Symantec

Commentary

- Approximately 28 billion spam emails were in circulation worldwide each day in 2014, compared with 29 billion in 2013, representing a decrease of 3.3 percent in global spam volume.
- Overall for 2014, 60 percent of email traffic was identified as spam, compared with 66.4 percent in 2013, representing a decrease of 6.4 percentage points.

Analysis of Spam Activity by Geography, Industry Sector, and Company Size

Background

Spam activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace, which can drive down prices, thereby increasing adoption rates. There may also be other factors at work based on the local economic conditions. Similarly, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. Small and medium businesses (SMBs) may find themselves the targets of spam attacks because they are perceived to be softer targets than larger organizations. They are likely to have less stringent security countermeasures than larger organizations, which can apply greater resources to their antispam and security countermeasures.

Methodology

Analysis of spam activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2014.

Industry	2014	2013
Mining	56.8%	60.0%
Manufacturing	56.2%	66.0%
Construction	56.2%	60.5%
Services – Non-Traditional	55.6%	60.4%
Services – Professional	55.5%	65.2%
Finance, Insurance & Real Estate	55.4%	73.0%
Agriculture, Forestry & Fishing	55.3%	65.4%
Public Administration	55.0%	65.5%
Wholesale	54.8%	65.1%
Nonclassifiable Establishments	54.5%	65.4%

Proportion of Email Traffic Identified as Spam by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1–250	55.2%	70.4%
251–500	55.5%	65.4%
501–1000	55.2%	65.2%
1001–1500	54.9%	65.6%
1501–2500	55.4%	65.6%
2501+	55.4%	65.6%

Proportion of Email Traffic Identified as Spam by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
Serbia	90.3%	65.8%
Ukraine	89.0%	65.3%
Burundi	79.3%	61.3%
Chile	76.6%	61.1%
Bulgaria	73.2%	62.9%
Zimbabwe	72.5%	63.7%
Sri Lanka	68.6%	75.7%
Northern Mariana Islands	66.3%	61.9%
Bahamas	66.3%	61.6%
Azerbaijan	64.4%	61.5%

Proportion of Email Traffic Identified as Spam by Geographic Location, 2014

Source: Symantec.cloud

Commentary

- The spam rate decreased across all top 10 geographies in 2014. The highest rate of spam was for organizations in Serbia, with an overall average spam rate of 90.3 percent.
- The spam rate decreased across all top 10 industry sectors in 2014, with mining on the top, with 56.8 percent. But in 2013, finance was subjected to the highest spam rate, with 73.0 percent.
- The spam rate decreased for all sizes of organizations in 2014.
- Of all emails sent to large enterprises with more than 2,500 employees in 2014, 55.4 percent were identified as spam, compared with 65.6 percent in 2013.

Analysis of Spam Delivered by Botnets

Background

This section discusses botnets and their use in sending spam. Similar to how ballistic analysis can reveal the gun used to fire a bullet, botnets can be identified by common features within the structure of email headers and corresponding patterns during the Simple Mail Transfer Protocol (SMTP) transactions. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis reviews only botnets involved in sending spam and does not look at botnets used for other purposes, such as financial fraud or distributed denial-of-service attacks.

Methodology

Symantec.cloud spam honeypots collects millions of spam emails each day. These were classified according to a series of heuristic rules applied to the SMTP conversation and the email header information.

A variety of internal and external IP reputation lists were also used in order to classify known botnet traffic based on the source IP address of the sending machine. Information is shared with other security experts to ensure the data is up to date and accurate.

Location of Botnet Activity	% of Botnet Spam
United States	7.7%
Spain	6.9%
Argentina	5.2%
Germany	4.9%
Italy	4.5%
Vietnam	4.3%
Russia	4.0%
Brazil	3.5%
India	2.7%
Romania	2.7%

Top Sources of Botnet Spam by Location, 2014

Source: Symantec.cloud

Commentary

- In 2014, approximately 74 percent of spam email was distributed by spam-sending botnets, compared with 76 percent in 2013. Ongoing actions to disrupt a number of botnet activities during the year contributed to this gradual decline.
- The top spam botnet, Kelihos, was responsible for 51.6 percent of spam, generating an estimated 1 billion spam emails each day, compared with 10 billion in 2013.
- The United States was at the top of the spam-sending botnet table in 2014 and was the source of approximately 7.7 percent of global botnet spam, 0.8 percentage point higher than Spain, in second place.

Analysis of Phishing Activity by Geography, Industry Sector, and Company Size

Background

Phishing activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. For example, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. SMBs may find themselves the targets of spam attacks because SMBs are perceived to be softer targets, as they are less likely to have the same levels of defense in depth as larger organizations, which tend to have greater budgetary expenditure applied to antispam and security countermeasures.

Methodology

Analysis of phishing activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2014.

Industry	2014	2013
Agriculture, Forestry & Fishing	1 in 833.4	1 in 1,173.6
Public Administration	1 in 838.9	1 in 216.4
Nonclassifiable Establishments	1 in 946.2	1 in 1,294.5
Services – Professional	1 in 1,193.2	1 in 1,155.4
Services – Non-Traditional	1 in 1,554.8	1 in 1,567.7
Construction	1 in 1,625.6	1 in 1,368.8
Finance, Insurance & Real Estate	1 in 1,630.5	1 in 767.7
Mining	1 in 1,931.6	1 in 1,355.4
Wholesale	1 in 2,074.0	1 in 1,533.1
Transportation, Communications, Electric, Gas & Sanitary Services	1 in 2,172.9	1 in 2,226.1

Proportion of Email Traffic Identified as Phishing by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1–250	1 in 1,401.5	1 in 689.5
251–500	1 in 1,253.5	1 in 1,075.9
501–1000	1 in 1,248.4	1 in 1,574.6
1001–1500	1 in 1,639.6	1 in 1,309.8
1501–2500	1 in 1,621.2	1 in 1,709.3
2501+	1 in 1,685.4	1 in 844.7

Proportion of Email Traffic Identified as Phishing by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
South Africa	1 in 568.0	1 in 419.8
Canada	1 in 765.6	1 in 1,059.3
Austria	1 in 805.8	1 in 1,049.0
New Zealand	1 in 961.5	1 in 1,784.7
United Kingdom	1 in 1,072.4	1 in 454.1
Netherlands	1 in 1,162.5	1 in 1,115.9
Belgium	1 in 1,312.2	1 in 1,935.4
Switzerland	1 in 1,462.6	1 in 1,917.7
Germany	1 in 1,472.7	1 in 1,901.1
Singapore	1 in 1,521.9	1 in 2,600.7

Proportion of Email Traffic Identified as Phishing by Geographic Location, 2014

Source: Symantec.cloud

Commentary

- The highest average rate for phishing activity in 2014 was for organizations in South Africa, with an overall average phishing rate of 1 in 568.0, compared with 1 in 419.8 in 2013.
- Organizations in the agriculture sector were subjected to the highest level of phishing activity in 2014, with 1 in 833.4 emails identified and blocked as a phishing attack. In 2013 the sector with the highest average phishing rate was government and public sector, with a phishing rate of 1 in 216.4.
- The phishing rate decreased for all sizes of organization in 2014. Of all emails sent to large enterprises with more than 2,500 employees in 2014, 1 in 1,685.4 was identified and blocked as a phishing attack, compared with 1 in 844.7 in 2013.
- Of all emails sent to businesses with up to 250 employees in 2014, 1 in 1,401.5 was identified and blocked as a phishing attack, compared with 1 in 689.5 in 2013.

"Whois" attacking you? Beware of malicious BGP hijacks!

Background

What is BGP hijacking?

The Internet is divided into thousands of smaller networks called autonomous systems (ASes), each of them belonging to a single entity (for example, an Internet service provider, a company, a university). Routing between ASes is achieved using the Border Gateway Protocol (BGP), which allows ASes to advertise to others the addresses of their network and receive the routes to reach other ASes.

Each AS implicitly trusts the peer ASes it exchanges routing information with. BGP hijacking is an attack against the routing protocol that consists of taking control of blocks of IP addresses owned by a given organization, without its authorization. This enables the attacker to perform other malicious activities (for example, spamming, phishing, malware hosting) using hijacked IP addresses belonging to somebody else.

In the volumes 17 and 19 of the Symantec Internet Security Threat Report we highlighted a phenomenon where so-called fly-by spammers temporarily steal (or hijack) blocks of network IP addresses and use them to send spam and hinder their traceability. We presented several real-world case studies involving very sophisticated spammers who briefly hijacked other people's networks in order to originate spam from them and successfully circumvented traditional spam IP blacklists. Although at the time we presented a limited number of cases of spammers behaving this way, we envision that such a phenomenon will become more prevalent.

Why is it important to detect BGP hijacking attacks?

It is important to detect and mitigate malicious BGP hijacks for the following reasons:

- Oftentimes when facing an attack, network operators use services such as whois to determine the individual or organization responsible for the offending IP address(es). However, BGP hijack attacks can lead to misattributing other attacks, such as denial-of-service attacks or spam, launched from hijacked networks due to hijackers' stealing the IP identity of the victim network owner. Correctly attributing attacks is critical when responding with possible legal actions.
- Many security systems protecting networks and systems rely on IP reputation as a first layer of defense. For example, spam filters heavily use IP blacklists to filter out emails coming from known spam senders. An attacker can thus defeat such protections by hijacking a network with a good reputation and then using the available IP addresses to launch devious attacks.

Methodology

How is Symantec able to identify malicious BGP hijacks using SpamTracer[21] technology?

Identifying malicious BGP hijacks involves (i) identifying networks originating nefarious network traffic, such as spam; and (ii) determining whether these networks have been stolen (or hijacked) from their legitimate owner. A tool called SpamTracer has been developed within Symantec Research Labs to track such attacks. SpamTracer monitors the routes toward networks seen originating cyberattacks to detect when the attackers manipulate the Internet routing to steal (or hijack) IP addresses used in these cyberattacks.

Data and commentary

In 2014, Symantec research identified, using SpamTracer, no less than 2,655 network IP address blocks that were hijacked from their legitimate owner. While hijacked, networks were used to send spam and host scam websites.

Malicious BGP hijack signature?

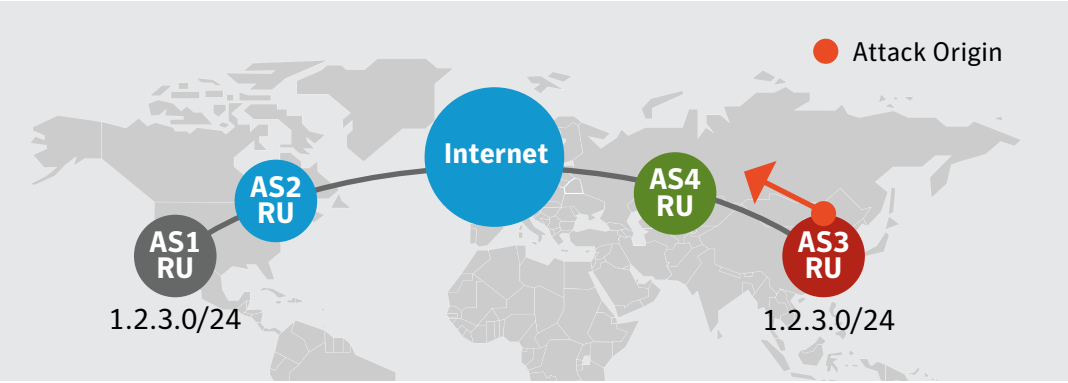
Looking at how the network IP address blocks were announced in BGP by the attackers, we were able to determine the modus operandi used to abuse the Internet routing and hijack the networks.

Hijacked network IP address blocks were:

- Not announced/used by their legitimate owner prior to being hijacked (that is, they were "dormant")
- Advertised by the attackers either (i) by a rogue origin AS (prefix hijack) or (ii) by the valid origin AS but via a rogue upstream provider (AS hijack)

In a prefix hijack, illustrated in Figure 1, the attacker (AS3) typically advertises the hijacked IP prefix (for example, 1.2.3.0/24, normally owned by AS1) using a rogue origin AS number (AS3). In our example, AS3 is said to be a rogue origin AS because the address block 1.2.3.0/24 is normally advertised by AS1, not AS3.

Prefix hijacks accounted for 92 percent (2,443 out of 2,655) of hijacks identified by Symantec in 2014.



- *Figure 1: Prefix hijack*

In an AS hijack, illustrated in Figure 2, the attacker (AS3) typically advertises the hijacked IP prefix (for example, 1.2.3.0/24, normally owned by AS1) using the AS number of the legitimate owner (AS1) but via a rogue upstream provider (AS3). In our example, AS3 is said to be a rogue upstream provider for AS1 because AS1 is normally connected (or a peer) with AS2, not AS3.

AS hijacks accounted for 8 percent (212 out of 2,655) of hijacks identified by Symantec in 2014.

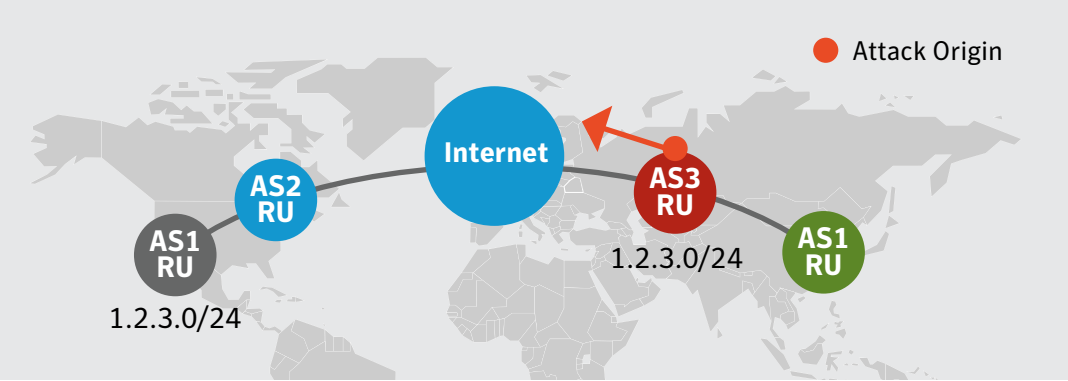


Figure 2: AS hijack

How long do hijacks last?

An important aspect of hijacks is their duration. The shorter a hijack attack lasts, the harder it is to detect and mitigate it. Attackers are more likely to be successful and evade protections, such as spam IP blacklists, if they use hijacked networks for a short period of time, because by the time a network is identified as "bad" by these protections, the attacker has already moved to another network. We identified two main hijack phenomena: short lived (from a few minutes to one week) and long lived (from one week to several months).

Out of the 2,655 hijacks uncovered during 2014, 98.7 percent were short lived (that is, they lasted at most one week). Moreover, 85.5 percent lasted less than 24 hours. Such short-lived hijacks clearly show that attackers are willing to remain as stealthy as possible and raise as little attention as possible.

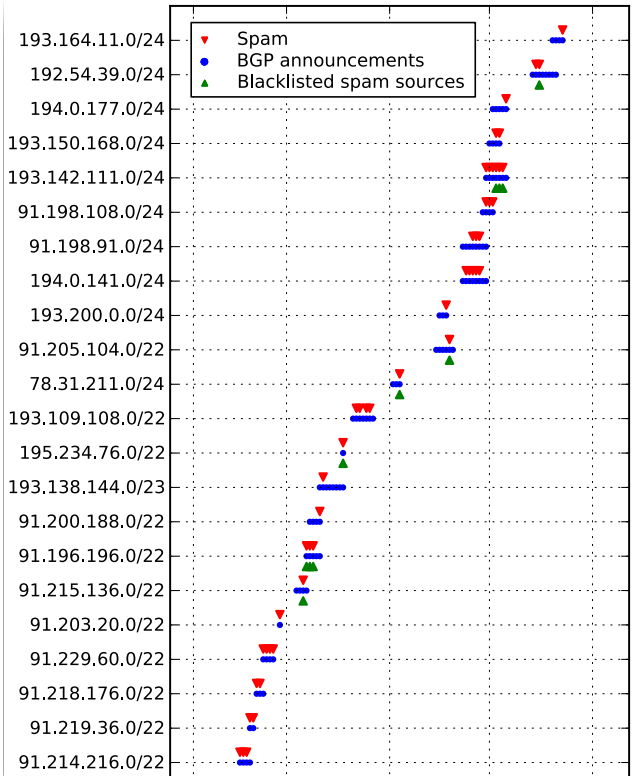
How effective is this spamming technique?

In the volumes 17 and 19 of the Symantec Internet Security Threat Report we reported evidence of spammers abusing the Internet routing to send spam in a stealthy way and prevent any traceback. The main objective of these sophisticated spammers is to circumvent spam IP black-lists by sending spam from a clean, "reputable" network until it starts appearing on blacklists and its reputation is degraded.

Out of the 2,655 IP address blocks identified as having been hijacked during 2014, 64 of them sent spam to spam traps set up by Symantec.cloud. Spam traps are decoy domains or email accounts used for the sole purpose of collecting all emails addressed to them since they are all spam. Out of these 64 hijacked networks that we know have been used for spamming, only 13 ended up being blacklisted by Spamhaus (SBL), Uceprotect, or Manitu. The remaining 51 network blocks never appeared to be blacklisted even though we observed spam emails sent from them. Figure 3 shows the BGP announcements, spam, and blacklisted spam sources related to a sample of 25 out of 64 short-lived hijacked IP prefixes. The figure highlights:

- The strong temporal correlation between BGP announcements and spam
- The low number of IP address blocks (7 out of 64) blacklisted before the end of the hijack

A total of 4,149 spam emails were received from these 64 hijacked IP address blocks. We extracted from this spam all advertised URLs that were pointing to 1,174 unique domain names, resolving to IP addresses belonging to the same hijacked IP address blocks, showing that some IP addresses were used in parallel to send spam and host the advertised scam websites. From whois information, we observed that these domain names were usually created within a few days before the networks were hijacked. This shows that attackers, very likely, control the entire IP address blocks and take full advantage of them.



- *Figure 3: Correlation between BGP announcements, spam emails, and blacklisted spam sources related to hijacked IP address ranges*

What about those not used for sending spam?

While examining hijacks that did not send spam to Symantec.cloud, we uncovered an intriguing phenomenon. This phenomenon is significant since it includes 2,562 short-lived hijacks, representing 97.8 percent of all short-lived hijacks identified. Figure 4 depicts a sample of 87 (out of 2,562) hijacks that occurred in June 2014 and shows that:

- All hijacks are actually performed by groups of two to four prefixes, starting and ending at the same time.
- During the 13-month period there were always, at any point in time, at least two IP prefixes hijacked.

Although only part of the phenomenon is depicted, it is recurrent and persistent over the complete year of 2014. This strongly indicates that the hijacks may have been performed with the same modus operandi. The fact that some groups of hijacks start only seconds after the end of previous groups further suggests that they might be carried out in an automated way, possibly also relying on some automated process to find target network address blocks to hijack.

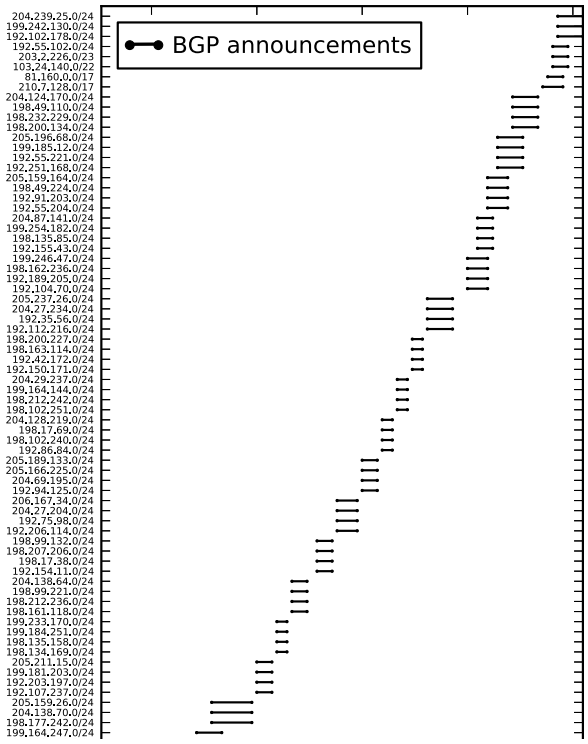


Figure 4: Intriguing hijack phenomenon in which hijacks are performed by groups of at least two IP prefixes (for the sake of conciseness, only a sample of 87 [out of 2,562] IP address ranges hijacked in June 2014 are depicted)

How many attackers are we facing?

While identifying malicious BGP hijacks is an important first step in the mitigation of these attacks, we wanted to gain more insight into the cybercriminal organizations behind such sophisticated attacks. In particular, we wanted to determine whether we could observe spammers repeatedly hijacking blocks of IP addresses for a short period of time to send spam using these hijacked (or stolen) IP addresses. We leveraged Symantec's advanced TRIAGE data analytics technology to identify spam campaigns launched from the 64 hijacked networks that sent spam to Symantec. cloud spam traps. We applied TRIAGE to the approximately 5,000 spam emails sent from hijacked networks. TRIAGE identified 30 different spam campaigns, from which we uncovered three key modi operandi of hijacking spammers: (i) 10 campaigns (out of 30) involved a single hijacked IP prefix that was not abused elsewhere in any other campaign; (ii) 17 campaigns involved a single hijacked IP prefix, yet the hijacked prefix was abused concurrently in different spam campaigns; and (iii) three campaigns were observed abusing multiple hijacked IP prefixes sequentially over a longer period of time. While the first two phenomena actually confirmed our intuition about the behavior of this class of spammers, the latter phenomenon is the most interesting, as it confirms the existence of BGP spectrum agility in the form of campaigns of BGP hijacks orchestrated by the same spammers. Indeed, it highlights the existence of a more agile and sophisticated modus operandi of spammers capable of hijacking and abusing multiple IP prefixes, and subsequently hopping from one hijacked IP prefix to another to distribute spam. This agility enables them to send spam in a stealthier manner and thus stay undetected "under the radar."

The graph in Figure 5 describes a campaign of spam emails sent from network IP address blocks that have been hijacked (or stolen) from their legitimate owner.[22] It illustrates the BGP spectrum agility phenomenon,[23] in which spammers temporarily hijack blocks of IP addresses to send spam. By repeatedly hijacking new blocks of IP addresses and sending spam from them for a short period of time, they manage to circumvent IP blacklists. We can distinguish in the figure below the 12 different hijacked IP address blocks (yellow nodes) involved in this spam campaign. Over 660 spam emails were sent from these network blocks. Each of them was used to distribute spam using a large number of one-time URLs, with most of them including domain names (blue nodes) registered at ENOM (large pink node) and using privacy-protected email addresses provided by whoisprivacyprotect.com (red nodes). The spam-advertised content (domain URLs) was hosted on one of the six shared server IP addresses (light gray nodes). The campaign had a lifetime of 84 days, with only 24 active days (purple nodes laid out in a clockwise fashion) during which spammers were hopping from one hijacked IP prefix to another, in an effort to circumvent IP-based spam filters and reputation systems.

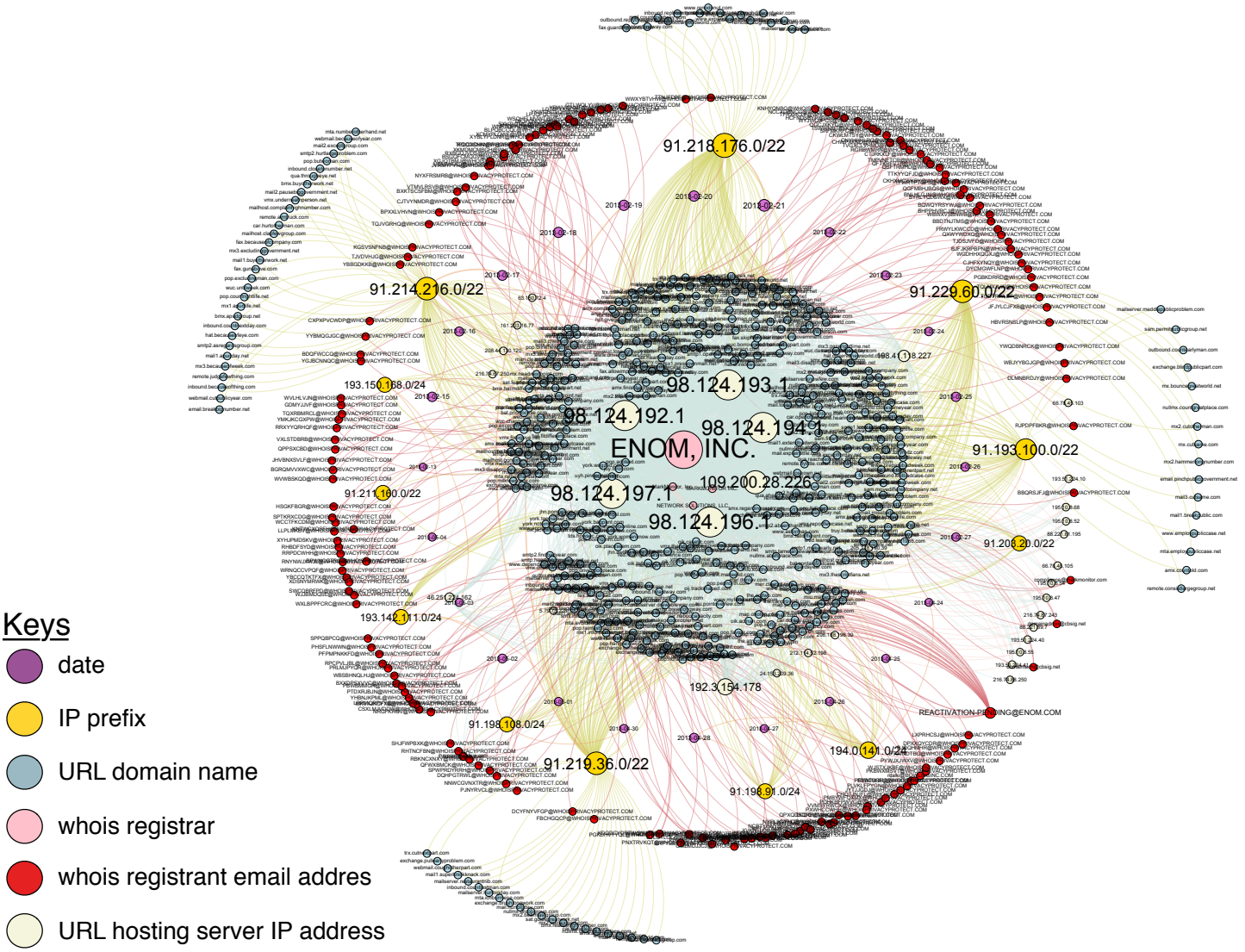


Figure 5: An example of a large-scale spam campaign involving multiple hijacked IP prefixes (the nodes are laid out in a clockwise fashion to reflect the timeline of the campaign)

Effectiveness of countermeasures?

BGP hijacking is a well-known attack against the Internet routing infrastructure. Recently, network operators have started to adopt and deploy a framework, commonly referred to as RPKI, meant to secure BGP and prevent address hijacking. RPKI works as a security extension to the routing protocol (BGP) by ensuring the authenticity and integrity of the messages exchanged between networks (ASes) using cryptography. The framework is divided into two modules that would prevent any hijacking attack. However, the first module protects BGP against prefix hijacks only, which accounted for 92 percent of the hijacks identified by Symantec in 2014. While the first module is already being deployed, it has been adopted by only about 4 percent of the Internet. The second module (BGPsec), which is required to mitigate AS hijacks (8 percent of the identified hijacks in 2014), is not yet being deployed and has not even been standardized yet.

Interestingly we found that none of the 2,655 hijacks we identified were detected by the RPKI system. The adoption and deployment of the first RPKI module by all networks on the Internet could have prevented no less than 2,442 (92 percent) hijacks.

Conclusion

It has been more than two years since our first report of malicious BGP hijacking attacks being carried out by cybercriminals on the Internet. In 2014 the scale and prevalence of these attacks reached unprecedented levels, with more than 2,000 confirmed attacks (up 875 percent compared with 2013). Using SpamTracer, a system developed within Symantec Research Labs, we have documented the existence of persistent and stealthy campaigns of malicious BGP hijacks. We have also shown that today's BGP hijack mitigation systems, such as the RPKI system, are easily defeated by the sophisticated hijack attacks we've observed. By identifying confirmed cases of spammers performing BGP hijacks to send spam from stolen networks, we also confirmed the increased prevalence of sophisticated spammers willing to remain stealthy and hinder their traceability. We found that all network IP address blocks we identified as having been hijacked were dormant blocks (that is, they were not publicly announced by their legitimate owner when they were hijacked). As of today, as much as 20 percent of the all the available IPv4 addresses are currently allocated to some organization but not publicly announced, which makes them potentially vulnerable to such malicious BGP hijacks.

Disclaimer

In this article, for the sake of conciseness, we discuss hijacks and attackers instead of candidate hijacks and likely attackers even though we have no bulletproof evidence of their wrongdoing. IP address blocks and ASes were likely abused in hijacks between January 2014 and December 2014 and, therefore, might now be legitimately used.

APPENDIX D: VULNERABILITY TRENDS

Appendix D: Vulnerability Trends

Vulnerability Trends

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security.

Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities being identified in the threat landscape because early detection and patching will minimize the chances of being exploited. This section discusses selected vulnerability trends, providing analysis and discussion of the trends indicated by the data.

The following metrics are included:

- Total Number of Vulnerabilities
- Zero-Day Vulnerabilities
- Web Browser Vulnerabilities
- Web Browser Plug-In Vulnerabilities
- ICS Vulnerabilities

Total Number of Vulnerabilities

Background

The total number of vulnerabilities for 2014 is based on research from independent security experts and vendors of affected products. The yearly total also includes zero-day vulnerabilities that attackers uncovered and that were subsequently identified post-exploitation. The Symantec DeepSight Intelligence vulnerability database tracks vulnerabilities reported in major, well-known applications that are in common business use and in applications that customers have specifically requested be tracked. For example, DeepSight does not track vulnerabilities in all open-source projects and consumer products, such as video games.

Symantec gathers information on all of these vulnerabilities as part of its DeepSight vulnerability database and alerting services. Examining these trends also provides further insight into other topics discussed in this report. Calculating the total number of vulnerabilities provides insight into vulnerability research being conducted in the threat landscape. There are many motivations for conducting vulnerability research, including security, academic, promotional, and software quality assurance, as well as, of course, the malicious motivations that drive attackers.

Discovering vulnerabilities can be advantageous to both sides of the security equation. Legitimate researchers may learn how better to defend against attacks by analyzing the work of attackers who uncover vulnerabilities; conversely, cybercriminals can capitalize on the published work of legitimate researchers to advance their attack capabilities. The vast majority of vulnerabilities that are exploited by attack toolkits are publicly known by the time they are exploited.

Methodology

Information about vulnerabilities is made public through a number of sources. These include mailing lists, vendor advisories, and detection in the wild. Symantec gathers this information and analyzes various characteristics of the vulnerabilities, including technical information and ratings, in order to determine the severity and impact of the vulnerabilities. This information is stored in the DeepSight vulnerability database, which houses approximately 66,400 distinct vulnerabilities spanning a period of over 20 years, from more than 21,300 vendors representing over 62,300 products.

As part of the data gathering process, Symantec scores the vulnerabilities according to version 2.0 of the community-based Common Vulnerability Scoring System (CVSS).[24] Symantec adopted version 2.0 of the scoring system in 2008. The total number of vulnerabilities is determined by counting all of the vulnerabilities published during the reporting period.

All vulnerabilities are included, regardless of severity or whether or not the vendor that produced the vulnerable product confirmed them.

Year	Total Number of Vulnerabilities
2014	6,549
2013	6,787
2012	5,291
2011	4,989
2010	6,253
2009	4,814
2008	5,562
2007	4,644
2006	4,842

Total Vulnerabilities Identified, 2006–2014

Source: Symantec

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2014	591	556	568	528	601	445	447	625	619	471	617	481	6,549
2013	565	515	695	481	582	547	607	493	598	658	579	467	6,787

Total Vulnerabilities Month by Month, 2013–2014

Source: Symantec

Commentary

- The actual number of new vulnerabilities reported is down, and the trend is still up: The total number of new vulnerabilities reported in 2014 stood at 6,549. This figure amounts to approximately 126 new vulnerabilities a week. Compared with the 6,787 new vulnerabilities reported in 2013, it represents a decrease of 4 percent, yet the overall trend is still on an upward trajectory.
- One thing to note is that websites hosting malicious toolkits often contain multiple exploits that can be tried against the visitor. In some cases, the kit will attempt to use all exploits at its disposal in a non-intelligent fashion, whereas in more modern advanced kits, the website code will attempt to fingerprint the software installed on the computer before deciding which exploit(s) to send to maximize the success rate.

Zero-Day Vulnerabilities

Background

Zero-day vulnerabilities are vulnerabilities against which the vendor has not released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases this type of threat can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

Methodology

Zero-day vulnerabilities are a subset of the total number of vulnerabilities documented over the reporting period. A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the affected vendor prior to exploitation, and at the time of the exploit activity, the vendor had not released a patch. The data for this section consists of the vulnerabilities that Symantec has identified that meet the above criteria.

Year	Count
2014	24
2013	23
2012	14
2011	8
2010	14
2009	12
2008	9
2007	15
2006	13

Volume of Zero-Day Vulnerabilities, 2006–2014

Source: Symantec

CVE Identifier	Description
CVE-2014-0493	Adobe Acrobat And Reader CVE-2014-0493 Remote Code Execution Vulnerability
CVE-2014-0495	Adobe Acrobat and Reader CVE-2014-0495 Remote Code Execution Vulnerability
CVE-2014-0496	Adobe Acrobat And Reader CVE-2014-0496 Remote Code Execution Vulnerability
CVE-2014-0491	Adobe Flash Player And AIR CVE-2014-0491 Remote Security Bypass Vulnerability
CVE-2014-0492	Adobe Flash Player and AIR CVE-2014-0492 Information Disclosure Vulnerability
CVE-2014-0497	Adobe Flash Player CVE-2014-0497 Remote Code Execution Vulnerability
CVE-2014-0322	Microsoft Internet Explorer CVE-2014-0322 Use-After-Free Remote Code Execution Vulnerability
CVE-2013-7331	Microsoft XMLDOM ActiveX Control Multiple Information Disclosure Vulnerabilities
CVE-2014-0502	Adobe Flash Player and AIR CVE-2014-0502 Remote Code Execution Vulnerability
CVE-2014-0502	Adobe Flash Player and AIR CVE-2014-0502 Remote Code Execution Vulnerability
CVE-2014-0498	Adobe Flash Player and AIR CVE-2014-0498 Remote Stack Overflow Vulnerability
CVE-2014-0324	Microsoft Internet Explorer CVE-2014-0324 Memory Corruption Vulnerability
CVE-2014-1761	Microsoft Word CVE-2014-1761 Remote Memory Corruption Vulnerability
CVE-2014-1776	Microsoft Internet Explorer CVE-2014-1776 Remote Code Execution Vulnerability
CVE-2014-0515	Adobe Flash Player CVE-2014-0515 Buffer Overflow Vulnerability
CVE-2014-0517	Adobe Flash Player and AIR CVE-2014-0517 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0518	Adobe Flash Player and AIR CVE-2014-0518 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0520	Adobe Flash Player and AIR CVE-2014-0520 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0519	Adobe Flash Player and AIR CVE-2014-0519 Unspecified Remote Security Bypass Vulnerability
CVE-MAP-NOMATCH	Linux Kernel 'ptrace' Function Call Local Privilege Escalation Vulnerability
CVE-2014-0546	Adobe Acrobat and Reader CVE-2014-0546 Unspecified Security Bypass Vulnerability
CVE-2014-4114	Microsoft Windows CVE-2014-4114 OLE Package Manager Remote Code Execution Vulnerability
CVE-2014-6352	Microsoft Windows CVE-2014-6352 OLE Remote Code Execution Vulnerability
CVE-2014-9163	Adobe Flash Player CVE-2014-9163 Unspecified Stack Based Buffer Overflow Vulnerability

Zero-Day Vulnerabilities Identified in 2014

Source: Symantec

Commentary

With 24 new zero-day vulnerabilities disclosed in 2014, this represents the highest number since 2006.

- There was a 4 percent increase in vulnerabilities in 2014 compared with 2013. However, the number of vulnerabilities in 2014 was magnified due to an increase in the number of published vulnerabilities for Adobe products. In 2014 there were 14 Adobe-related vulnerabilities, compared with seven in 2013.
- As the number of zero-day vulnerabilities increased, attacks using these vulnerabilities were also on the rise. Some of these vulnerabilities were leveraged in targeted attacks, through the use of watering-hole-based attacks. Adobe Flash Player and Microsoft Windows ActiveX Control vulnerabilities were widely used in such targeted attacks, and Microsoft-related products and technologies accounted for more than a third of the zero-day vulnerabilities disclosed in 2014.
- Many attack scenarios were planned in such a way that an attacker would craft a malicious webpage to exploit the vulnerability, and email or other similar means would be used to entice unsuspecting users to visit it. Once the page was viewed, the attacker-supplied malicious code would potentially be run undetected.

Web Browser Vulnerabilities

Background

Web browsers are ubiquitous components for both enterprise and individual users on desktop and mobile devices. Vulnerabilities in web browser are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and adware. In addition, web browsers are exposed to a greater amount of potentially untrusted or hostile content than are most other applications and are particularly targeted by multi-exploit attack kits.

Web-based attacks can originate from malicious websites and from legitimate websites that have been compromised to serve malicious content. Some content, such as media files or documents, are often presented in browsers via browser plug-in technologies. While browser functionality is extended by the inclusion of various plug-ins, the addition of a plug-in component also results in a wider potential attack surface for client-side attacks.

Methodology

Browser vulnerabilities are a subset of the total number of vulnerabilities cataloged by Symantec throughout the year. To determine the number of vulnerabilities affecting browsers, Symantec considers all vulnerabilities that have been publicly reported, regardless of whether they have been confirmed by the vendor. While vendors do confirm the majority of browser vulnerabilities that are published, not all vulnerabilities may have been confirmed at the time of writing. Vulnerabilities that are not confirmed by a vendor may still pose a threat to browser users and are therefore included in this study.

This metric examines the total number of vulnerabilities affecting the following popular web browsers:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox
- Opera

Year	Apple Safari	Google Chrome	Microsoft Internet Explorer	Mozilla Firefox	Opera	Total
2014	86	155	282	109	7	639
2013	54	219	148	157	13	591
2012	343	268	60	186	34	891

Browser Vulnerabilities, 2012–2014

Source: Symantec

Commentary

- Five popular browsers had 639 reported vulnerabilities in total in 2014, which is a slight increase from 591 in 2013. This is due to a reduction in the number of disclosed vulnerabilities for Chrome, Firefox, and Opera.

Web Browser Plug-In Vulnerabilities

Background

This metric examines the number of vulnerabilities affecting plug-ins for web browsers. Browser plug-ins are technologies that run inside the web browser and extend its features, such as allowing additional multimedia content from webpages to be rendered. Although plug-ins are often run inside the browser, some vendors have started to use sandbox containers to execute plug-ins in order to limit the potential harm of vulnerabilities. Unfortunately, web browser plug-ins continue to be one of the most exploited vectors for web-based attacks and drive-by downloads that silently infect consumer and enterprise users.

Many browsers now include various plug-ins in their default installation and also provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of web browsers and are often required in order to use many commercial sites. Vulnerabilities affecting plug-ins are an increasingly favored vector for a range of client-side attacks, and the exploits targeting these vulnerabilities are commonly included in attack kits. Web attack kits can exploit many different browser and browser plug-in vulnerabilities at one time, enabling full access to download any malware to affected computers.

Some plug-in technologies include automatic update mechanisms that aid in keeping software up to date, which may aid in limiting exposure to certain vulnerabilities. Enterprises that choose to disable these updating mechanisms, or continue to use vulnerable out-of-date versions, will continue to put their organizations at considerable risk of silent infection and exploitation. Through a variety of drive-by web attacks, exploits against browser plug-in vulnerabilities continue to be a favored infection vector for hackers and malware authors to breach enterprises and consumer systems. To help mitigate the risk, some browsers have started to check for the version of installed third-party plug-ins and inform the user if there are any updates available for install. Enterprises should also check to determine whether every browser plug-in is needed and consider removing or disabling potentially vulnerable software.

Methodology

Web browser plug-in vulnerabilities comprise a subset of the total number of vulnerabilities cataloged by Symantec over the reporting period. The vulnerabilities in this section cover the entire range of possible severity ratings and include those that are both unconfirmed and confirmed by the affected product's vendor. Confirmed vulnerabilities consist of security issues that the vendor has publicly acknowledged, either by releasing an advisory or otherwise making a public statement to concur that the vulnerability exists. Unconfirmed vulnerabilities are vulnerabilities that are reported by third parties—usually security researchers—and have not been publicly confirmed by the vendor. That a vulnerability is unconfirmed does not mean that the vulnerability report is not legitimate but only that the vendor has not released a public statement confirming the existence of the vulnerability.

Symantec identified the following popular browser plug-ins as having the most reported vulnerabilities in 2014:

- Adobe Reader
- Adobe Flash Player
- Apple QuickTime
- Microsoft ActiveX
- Mozilla Firefox extensions
- Oracle Sun Java Platform, Standard Edition (Java SE)

Year	Adobe Acrobat Reader	Adobe Flash	Active X	Apple QuickTime	Firefox Extension	Oracle Sun Java	Total
2014	46	76	72	23	0	119	**336**
2013	68	56	54	13	0	184	375

Browser Plug-In Vulnerabilities, 2013–2014

Source: Symantec

Commentary

- In 2014, 336 vulnerabilities affecting browser plug-ins were documented by Symantec, a decrease compared with the 375 vulnerabilities in 2013.
- The number of published Java vulnerabilities decreased significantly in 2014. This caused the reduction seen in the total count for 2014.

ICS Vulnerabilities

Background

This metric examines all the vulnerabilities with industrial control systems (ICS) technologies. ICS is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other smaller control system configurations such as programmable logic controllers (PLCs) often found in the industrial sectors and in critical infrastructure. ICSs are typically used in industries such as electrical, water, oil, and gas. Based on data received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices.

SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes, but is not limited to, power generation, manufacturing, oil and gas, water treatment, and waste management. The security of SCADA technologies and protocols is a national security concern because the disruption of related services can result in, among other things, the failure of infrastructure and potential loss of life.

Methodology

This discussion is based on data surrounding publicly known vulnerabilities affecting ICS technologies. Due to the potential for disruption of critical infrastructure services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks, representing a concern for both governments and enterprises involved in the sector. While this metric provides insight into public ICS/SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure it is likely that private security research is conducted by ICS technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

BID	Title	Published
64941	Multiple WellinTech Products ActiveX Remote Code Execution Vulnerability	January 14, 2014
64938	Multiple WellinTech Products Information Disclosure Vulnerability	January 14, 2014
64972	Ecava IntegraXor Stack Buffer Overflow Vulnerability	January 16, 2014
65262	Schneider Electric Telvent SAGE 3030 RTUs Remote Denial of Service Vulnerability	January 30, 2014
65337	Rockwell Automation RSLogix 5000 CVE-2014-0755 Security Bypass Vulnerability	February 4, 2014
65635	Multiple Schneider Electric Products Remote Denial of Service Vulnerability	February 18, 2014
65706	Iconics GENESIS32 ActiveX Control CVE-2014-0758 Remote Code Execution Vulnerability	February 20, 2014
66500	Multiple Schneider Electric Products Stack Buffer Overflow Vulnerability	March 27, 2014
66554	Ecava IntegraXor Account Information Disclosure Vulnerability	April 1, 2014
66709	WellinTech KingSCADA CVE-2014-0787 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66732	Advantech WebAccess CVE-2014-0768 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66742	Advantech WebAccess CVE-2014-0773 Security Bypass Vulnerability	April 8, 2014
66722	Advantech WebAccess CVE-2014-0765 Stack Based Buffer Overflow Vulnerability	April 8, 2014
66740	Advantech WebAccess CVE-2014-0763 SQL Injection Vulnerability	April 8, 2014
66725	Advantech WebAccess CVE-2014-0766 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66728	Advantech WebAccess CVE-2014-0767 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66750	Advantech WebAccess CVE-2014-0771 Information Disclosure Vulnerability	April 8, 2014
66718	Advantech WebAccess CVE-2014-0764 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66733	Advantech WebAccess CVE-2014-0770 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66749	Advantech WebAccess CVE-2014-0772 Information Disclosure Vulnerability	April 8, 2014
66934	Progea Movicon CVE-2014-0778 Information Disclosure Vulnerability	April 15, 2014
67056	InduSoft Web Studio CVE-2014-0780 Directory Traversal Vulnerability	April 24, 2014
68717	Advantech WebAccess CVE-2014-2366 Remote Information Disclosure Vulnerability	July 15, 2014
68716	Advantech WebAccess CVE-2014-2367 Remote Authentication Bypass Vulnerability	July 15, 2014
68718	Advantech WebAccess CVE-2014-2365 Remote Code Execution Vulnerability	July 18, 2014
68715	Advantech WebAccess CVE-2014-2368 Unsafe ActiveX Control Remote Security Weakness	July 18, 2014
68714	Advantech WebAccess CVE-2014-2364 Multiple Remote Stack Based Buffer Overflow Vulnerabilities	July 18, 2014
68872	Siemens SIMATIC WinCC and PCS 7 CVE-2014-4685 Local Privilege Escalation Vulnerability	July 23, 2014
68880	Siemens SIMATIC WinCC and PCS7 Database Server Remote Privilege Escalation Vulnerability	July 23, 2014
68875	Siemens SIMATIC WinCC and PCS7 CVE-2014-4686 Privilege Escalation Vulnerability	July 23, 2014
68879	Siemens SIMATIC WinCC And PCS7 CVE-2014-4683 Remote Privilege Escalation Vulnerability	July 23, 2014
68876	Siemens SIMATIC WinCC And PCS7 WebNavigator Server Information Disclosure Vulnerability	July 24, 2014
70193	Multiple Schneider Electric Products CVE-2014-2732 Directory Traversal Vulnerability	September 30, 2014
71239	Multiple Siemens Products CVE-2014-8551 Remote Code Execution Vulnerability	November 21, 2014
71240	Multiple Siemens SIMATIC Products CVE-2014-8552 Information Disclosure Vulnerability	November 21, 2014

ICS Vulnerabilities, 2014

Source: Symantec

Commentary

- The number of ICS vulnerabilities increased slightly in 2014, with 35 publicly disclosed vulnerabilities, compared with the 39 vulnerabilities disclosed in 2013.

Footnotes

01 For more details about Norton Safe Web, please visit http://safeweb.norton.com

02 For more details about Symantec RuleSpace, please visit http://www.symantec.com/theme.jsp?themeid=rulespace

03 http://www.idanalytics.com

04 For example, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) of California. For more on this act, please see: http://www.privacyrights.org/fs/fs6a-facta.htm. Another example is the Health Insurance Portability and Accountability Act of 1996. For more information, see http://www.cms.hhs.gov/HIPAAGenInfo/.

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

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

07 http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

08 CIFS is a file-sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.

09 Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

10 http://www.vis-sense.eu/

11 Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. An Analysis of Rogue AV Campaigns. In Proc. of the 13th International Conference on Recent Advances in Intrusion Detection (RAID), 2010.

12 O. Thonnard, M. Dacier. A Strategic Analysis of Spam Botnets Operations. CEAS'11, Perth, WA, Australia, Sep 2011.

13 Jelena Isacenkova, Olivier Thonnard, Andrei Costin, Davide Balzarotti, Aurelien Francillon. Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. International Workshop on Cyber Crime (IWCC 2013), IEEE S&P Workshops, 2013.

14 P.-A. Vervier, O. Thonnard, and M. Dacier. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In Proc. of the Network and Distributed System Security (NDSS) Symposium. IEEE, 2015.

15 Olivier Thonnard, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, Martin Lee. Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat. In Proc. of the 15th International Conference on Research in Attacks, Intrusions, and Defenses (RAID), 2012.

16 Symantec Internet Security Threat Report (ISTR), Volume 17, April 2012.

17 Symantec product detections for Microsoft monthly Security Advisories—February 2012. http://www.symantec.com/business/support/index?page=content&id=TECH181344

18 Worm:Win32/Bagle.gen!B. http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Worm%3aWin32%2fBagle.gen%21C#tab=1

19 http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam

20 http://www.symantec.com/messaging-gateway/

21 P.-A. Vervier and O. Thonnard. Spamtracer: How Stealthy Are Spammers? In IEEE International TMA Workshop, pages 453–458, 2013.

22 P.-A. Vervier, O. Thonnard, and M. Dacier. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In Network and Distributed System Security (NDSS) Symposium, 2015.

23 A. Ramachandran and N. Feamster. Understanding the Network-Level Behavior of Spammers. In SIGCOMM, pages 291–302, 2006.

24 http://www.first.org/cvss/cvss-guide.html

25 SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more on this, please see http://www.sec.gov/

26 http://www.digitalenvoy.net/

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

04/15 21347931