Symantec

2013 Trends, Volume 19, Published April 2014

ISTR

INTERNET SECURITY THREAT REPORT
APPENDIX ⌖ 2014

CONTENTS

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 2013. 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 for 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
- Denial of Service Attacks
- Analysis of Mobile Threats
- Quantified Self – A Path to Self-Enlightenment or Just Another Security Nightmare?
- Data Breaches That Could Lead to Identity Theft
- Threat of the Insider
- Gaming Attacks
- The New Black Market

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 other connection types, including faster speeds, the potential of constantly connected systems, and a typically 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 purpose of malicious code includes 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:** A phishing host is a computer that provides 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:** This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- **Web-based attack origins:** This measures 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 in 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 the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Fig. A.1

Malicious Activity by Source: Overall Rankings, 2012–2013

Source: Symantec

Country/Region	2013 World Rank	2013 Overall Average	2012 World Rank	2012 Overall Average	Change
United States	1	20.3%	1	22.7%	-2.4%
China	2	9.4%	2	11.0%	-1.6%
India	3	5.1%	3	6.5%	-1.4%
Netherlands	4	3.5%	7	2.7%	0.8%
Germany	5	3.3%	6	3.4%	-0.2%
Russia	6	2.6%	11	2.2%	0.4%
United Kingdom	7	2.6%	9	2.4%	0.2%
Brazil	8	2.5%	5	4.0%	-1.5%
Taiwan	9	2.5%	10	2.3%	0.1%
Italy	10	2.3%	8	2.4%	-0.1%

Fig. A.2

Malicious Activity by Source: Malicious Code, 2012–2013

Source: Symantec

Country/Region	2013 Malicious Code Rank	2013 Malicious Code Percentage	2012 Malicious Code Rank	2012 Malicious Code Percentage	Change
United States	1	16.9%	1	17.2%	-0.3%
India	2	15.3%	2	16.2%	-0.9%
China	3	5.9%	3	6.1%	-0.1%
Indonesia	4	4.0%	4	3.9%	0.1%
Japan	5	3.4%	5	3.4%	0.0%
Vietnam	6	2.8%	6	3.0%	-0.1%
United Kingdom	7	2.8%	8	2.7%	0.1%
Netherlands	8	2.8%	12	2.1%	0.7%
Germany	9	2.7%	10	2.5%	0.3%
Brazil	10	2.6%	7	2.9%	-0.2%

Fig. A.3

Malicious Activity by Source: Spam Zombies, 2012–2013

Source: Symantec

Country/Region	2013 Spam Rank	2013 Spam Percentage	2012 Spam Rank	2012 Spam Percentage	Change
India	1	9.8%	1	17.1%	-7.4%
Netherlands	2	8.2%	3	6.5%	1.7%
Russia	3	6.6%	10	2.7%	3.8%
Taiwan	4	5.5%	17	2.2%	3.2%
Iran	5	5.3%	18	1.5%	3.7%
China	6	5.1%	9	3.1%	2.0%
Vietnam	7	5.0%	13	2.5%	2.5%
Peru	8	4.5%	12	2.6%	1.9%
United States	9	4.3%	5	4.2%	0.1%
Italy	10	3.2%	20	1.5%	1.8%

Fig. A.4

Malicious Activity by Source: Phishing Hosts, 2012–2013

Source: Symantec

Country/Region	2013 Phishing Hosts Rank	2013 Phishing Hosts Percentage	2012 Phishing Hosts Rank	2012 Phishing Hosts Percentage	Change
United States	1	39.4%	1	50.0%	-10.6%
Germany	2	6.5%	2	6.2%	0.3%
United Kingdom	3	3.8%	3	3.9%	-0.1%
Canada	4	2.8%	6	2.9%	-0.1%
France	5	2.6%	7	2.7%	-0.1%
Netherlands	6	2.5%	9	2.3%	0.2%
Russia	7	2.5%	8	2.4%	0.1%
Brazil	8	2.2%	4	3.6%	-1.4%
China	9	2.2%	5	3.2%	-1.1%
Poland	10	1.8%	10	1.6%	0.2%

Fig. A.5

Malicious Activity by Source: Bots, 2012–2013

Source: Symantec

Country/Region	2013 Bots Rank	2013 Bots Percentage	2012 Bots Rank	2012 Bots Percentage	Change
United States	1	20.0%	1	15.3%	4.7%
China	2	9.1%	2	15.0%	-5.9%
Italy	3	6.0%	5	7.6%	-1.6%
Taiwan	4	6.0%	3	7.9%	-1.9%
Brazil	5	5.7%	4	7.8%	-2.1%
Japan	6	4.3%	6	4.6%	-0.3%
Hungary	7	4.2%	8	4.2%	0.0%
Germany	8	4.2%	9	4.0%	0.1%
Spain	9	3.9%	10	3.2%	0.7%
Canada	10	3.5%	11	2.0%	1.5%

Fig. A.6

Malicious Activity by Source: Web Attack Origins, 2012–2013

Source: Symantec

Country/Region	2013 Web-Attacking Countries Rank	2013 Web Attacking Countries Percentage	2012 Web Attacking Countries Rank	2012 Web Attacking Countries Percentage	Change
United States	1	26.2%	1	34.4%	-8.2%
China	2	7.4%	3	9.4%	-2.0%
Netherlands	3	2.8%	6	2.4%	0.3%
India	4	1.6%	7	1.7%	0.0%
Germany	5	1.6%	5	2.6%	-1.0%
Japan	6	1.4%	8	1.6%	-0.2%
Korea, South	7	1.4%	4	3.0%	-1.6%
United Kingdom	8	1.0%	10	1.5%	-0.4%
Russia	9	0.9%	9	1.5%	-0.6%
Brazil	10	0.9%	11	1.3%	-0.4%

Fig. A.7

Malicious Activity by Source: Network Attack Origins, 2012–2013

Source: Symantec

Country/Region	2013 Network Attacking Countries Rank	2013 Network Attacking Countries Percentage	2012 Network Attacking Countries Rank	2012 Network Attacking Countries Percentage	Change
China	1	26.6%	1	29.2%	-2.6%
United States	2	15.2%	2	14.9%	0.3%
Netherlands	3	3.9%	6	2.6%	1.3%
United Kingdom	4	3.3%	4	3.1%	0.2%
Russia	5	3.1%	3	3.7%	-0.6%
Vietnam	6	2.7%	23	0.8%	1.9%
France	7	2.6%	10	2.3%	0.4%
Brazil	8	2.6%	5	3.0%	-0.4%
India	9	2.4%	8	2.4%	0.0%
Japan	10	2.2%	7	2.4%	-0.2%

Commentary

- **In 2013, 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 2013 decreased by 2.4 percentage points compared with 2012, while the same figure for China saw a decrease by 1.6 percentage points compared with 2012. Countries ranking in the top-ten for 2012 continued to appear in the same range in 2013.
- The United States remains ranked in first position for the source of all activities except for spam zombies and network attacks. India remains in first position for spam zombies and China remains primary for network attacks.
- **20 percent of bot activity originated in the United States:** The United States was the main source of bot-infected computers, an increase of 4.7 percentage points compared with 2012. The US population are avid users of the Internet, with 78 percent Internet penetration, and undoubtedly their keen use of the Internet contributes to their popularity with malware authors.
- **26.2 percent of Web-based Attacks originated in the United States:** Web-based attacks originating from the United States decreased by 8.2 percentage points in 2013.
- **26.6 percent of network attacks originated in China.** China has the largest population of Internet users in the Asia region, with its Internet population growing to approximately 618 million Internet users by the end of 2013[1], 81 percent of which connecting via mobile, making it the country with the largest Internet population in the world.
- **39.4 percent of phishing websites were hosted in the United States.** In 2013, with approximately 256 million Internet users[2], the United States was has the second largest population of Internet users in the world.
- **9.8 percent of spam zombies were located in India,** a decrease of 7.4 percentage points compared with 2012. The proportion of spam zombies located in the United States rose by 0.1 percentage points to 4.3 percent, resulting in the United States being ranked in 9th position in 2013, compared with 5th position in 2012.
- **16.9 percent of all malicious code activities originated from the United States,** a decrease of 0.3 percentage points compared with 2012, overtaking India as the main source of malicious code activity in 2013. With 15.3 percent of malicious activity originating in India, the country was ranked in second position. India has approximately 205 million Internet users,[3] with the third largest population of Internet users in the world.

Malicious Web-Based Attack Prevalence

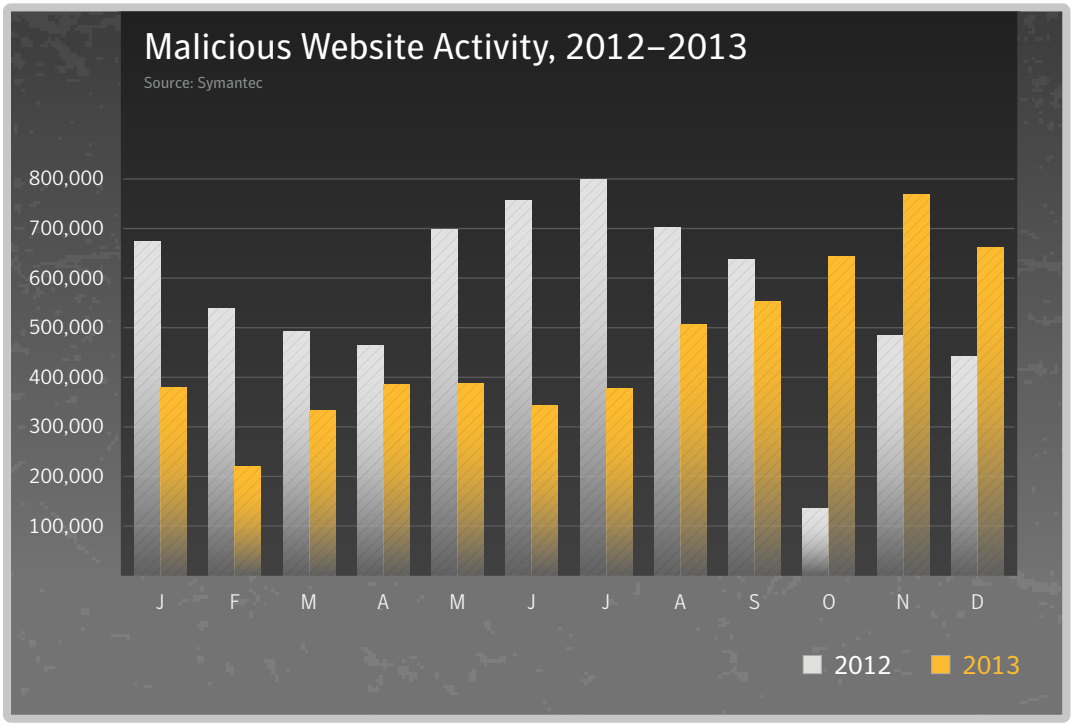
Background

The circumstances and implications of web-based attacks vary widely. They 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 overall web-based attacks 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.

Fig. A.8



Commentary

- The average number of malicious websites blocked each day rose by approximately 22.5 percent from approximately 464,100 in 2012 to 568,700 in 2013.
- The highest level of activity was in July, with approximately 799,500 blocks per day.
- The lowest rate of malicious activity was 135,450 blocks per day in October 2013; this is likely to have been connected to the arrest in Russia of "Paunch," the alleged author of the Blackhole and Cool Exploit web attack toolkits. Blackhole operates as a software-as-a-service toolkit, which is maintained in the cloud. With no one around to update it, it quickly became less effective, leaving a space for other operators to move in.
- 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

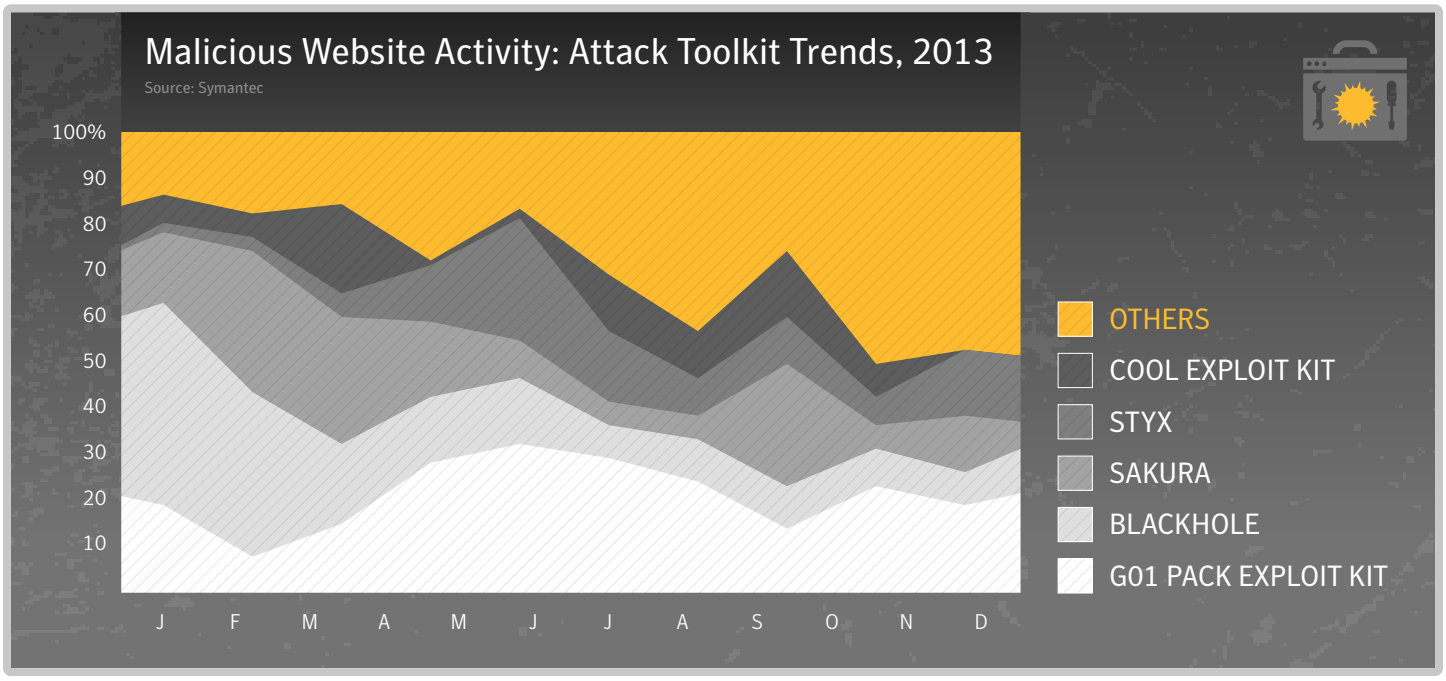
Background

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. These attacks work by infecting enterprises and consumers that visit mainstream websites hosting web attack toolkits, and silently infect them with a variety of malware. Symantec analyzes attack activity to determine which types of attacks and attack toolkits attackers 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 2013. To determine this, Symantec ranked attack activity by the number of associated incidents associated with each given web kit.

Fig. A.9



Commentary

- Blackhole virtually disappears from the detections of web attack kits in 2013, while ranked first in 2013 with 44.3 percent of total attacks blocked. G01 Pack Exploit Kit ranked first in 2013 with 23 percent of attacks blocked. The Sakura toolkit that ranked second in 2012, accounting for 22 percent of attacks is seen third place in 2013 with 14 percent.
- Many of the more common attack toolkits were updated in 2013 to include exploits for the Java Runtime Environment, including CVE-2013-0422, CVE-2013-2465 and CVE-2013-1493 and the Microsoft Internet Explorer vulnerability CVE-2013-2551.

Fig. A.10

Malicious Website Activity: Overall Frequency of Major Attack Toolkits, 2013

Source: Symantec

Toolkit	Percentage of Attacks
G01 PACK EXPLOIT KIT	22.7%
BLACKHOLE	18.8%
SAKURA	14.0%
STYX	9.9%
COOL EXPLOIT KIT	7.5%
OTHERS	27.0%

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. However, most adware vendors, such as those providing add-in toolbars for web browsers, are not always aware how their code came to be installed on users' computers; the expectation is that it is with the permission of the end-user, when 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.

Fig. A.11

Potentially Unwanted Programs: Spyware and Adware Blocked, 2013

Source: Symantec.cloud

Rank	Name	Percent
1	Adware.Singalng	56.5%
2	Adware.DealPly	19.2%
3	Adware.Adpeak.E	13.6%
4	Adware.BHO.WVF	3.8%
5	Adware.Adpeak.C	2.6%
6	Adware.Adpeak.F	1.0%
7	Adware.GoonSquad	0.7%
8	Adware.Gamevance.AV	0.6%
9	Adware.BHO.BProtector.E	0.2%
10	Application:Android/Counterclank.A	0.2%
	Total spyware detected generically	1.8%

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 their affiliate terms and conditions.
- The most frequently blocked installation of potentially unwanted programs in 2013 was for the adware Singalng.
- In 2013, nine of the top-ten potentially unwanted programs were classified as adware, compared with four in 2012.
- 1.8 percent of spyware and adware was detected using generic techniques compared with 80.9 percent in 2012.

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 Web sites, 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 only apply at certain times of the day; for example, an organization may wish to limit employees access to video sharing websites to only Friday lunchtime, but may also allow any member of the PR and Marketing teams access at any time of the day. 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.

Fig. A.12

Web Policies that Triggered Blocks, 2012–2013

Source: Symantec.cloud

Rank	Category	2013	2012	Change
1	Social Networking	39.0%	24.1%	14.9%
2	Advertisement & Popups	24.4%	31.8%	-7.4%
3	Streaming Media	5.2%	9.0%	-3.8%
4	Computing & Internet	4.5%	4.0%	0.5%
5	Hosting Sites	3.7%	2.8%	0.9%
6	Chat	2.9%	4.7%	-1.8%
7	Search	2.8%	1.7%	1.1%
8	Peer-To-Peer	2.7%	3.3%	-0.6%
9	Games	2.6%	1.9%	0.7%
10	News	1.3%	1.7%	-0.4%

Commentary

- The most frequently blocked traffic was categorized as **Social Networking, and accounted for 39 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 only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.
- **24 percent of web activity blocked through policy controls was related to advertisement and popups.** Web-based advertisements pose a potential risk though the use of "malvertisements," or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless website.
- **Activity related to streaming media policies resulted in 9 percent of policy-based filtering blocks in 2012.** 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 London Olympics.

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 helps provide a better understanding of the types of legitimate websites that may be more susceptible to being compromised, that would potentially expose users to greater levels of risk.

Methodology

This metric assesses the classification of malicious websites blocked by users of Norton Safe Web[4] 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 Norton Safe Web technology were classified by category using the Symantec Rulespace[5] technology. RuleSpace proactively categorizes websites into nearly 100 categories in 30 languages.

Fig. A.13

Malicious Web Activity: Categories that Delivered Malicious Code, 2013

Source: Symantec.cloud

Rank	Top-Ten Most Frequently Exploited Categories of Websites	Percentage of Total Number of infected Websites	2012	Change
1	Technology	9.9%	24.1%	14.9%
2	Business	6.7%	31.8%	-7.4%
3	Hosting	5.3%	9.0%	-3.8%
4	Blogging	5.0%	4.0%	0.5%
5	Illegal	3.8%	2.8%	0.9%
6	Shopping	3.3%	4.7%	-1.8%
7	Entertainment	2.9%	1.7%	1.1%
8	Automotive	1.8%	3.3%	-0.6%
9	Educational	1.7%	1.9%	0.7%
10	Virtual Community	1.7%	1.7%	-0.4%

Fig. A.14

Malicious Web Activity: Malicious Code By Number of Infections per Site for Top-Five Most Frequently Exploited Categories, 2013

Source: Symantec.cloud

Rank	Top-Five Most Frequently Exploited Categories of Websites	Average Number of Threats Found on Infected Website	Top 3 Threat Types Detected		
1	Technology	1.9	Malware: 38%	Malicious Site: 17%	Fake AV: 14%
2	Business	2.1	Malware: 42%	Fake AV: 27%	Malicious Site: 14%
3	Hosting	1.4	Scam: 35%	Malicious Site: 21%	Malware: 19%
4	Blogging	1.6	Browser Exploit: 25%	Scam: 17%	Web Attack: 17%
5	Illegal	1.3	Malicious Site: 51%	PHISH: 25%	Malware: 6%

Fig. A.15

Malicious Web Activity: Malicious Code by Number of Infections per Site, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites	Average Number of Threats Found on Infected Website	Major Threat Type Detected
1	Automated Web Application	3.4	Malware: 82%
2	Placeholder	2.9	Pay Per Click: 68%
3	Automotive	2.9	Pay Per Click: 63%
4	Kids	2.8	Malware: 67%
5	Cult	2.6	Fake Antivirus: 49%
6	Military	2.5	Malware: 60%
7	Hate	2.4	Malware: 54%
8	Humor	2.3	Malware: 31%
9	Forums	2.2	Scam: 28%
10	Weapons	2.2	Fake Antivirus: 38%

Fig. A.16

Malicious Web Activity: Fake Antivirus by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Fake Antivirus	Percent of Threats Found Within Same Category	Percent of Fake AV Attacks Found Within Top-Ten Categories
1	Art and Museums	50%	4%
2	Cult	49%	0.2%
3	Alcohol	40%	2%
4	Religion	39%	9%
5	Weapons	38%	1%
6	Shopping	37%	42%
7	Drugs	36%	0.2%
8	Entertainment	35%	34%
9	Glamour	34%	2%
10	Food and Restaurants	33%	7%

- The fake antivirus (fake AV) threat has been explicitly analyzed and the above top-ten website categories have been generated and ranked based on the percentage of fake AV threats that each of them account for.
- Art and Museum websites rank at the top with 50 percent of all threats being fake AV. But this website category accounts to only 4 percent of this threat when compared with other categories in the top-ten list.
- It shows that the majority of threats from Art and Museum websites are fake AV but the volume of such threats is very low. Entertainment has the highest volume of fake AV threats.

Fig. A.17

Malicious Web Activity: Browser Exploits by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Browser Exploits	Percentage of Threats Found Within Same Category	Percentage of Browser Exploits Found Within Top-Ten Categories
1	Anonymizer	73%	21%
2	Blogging	27%	67%
3	Dynamic	20%	4%
4	Violence	11%	0.005%
5	Filesharing	10%	2%
6	Portal	10%	1%
7	Humor	10%	0.1%
8	Pornography	8%	4%
9	Hacking	7%	0.1%
10	Automated Web Application	7%	0.01%

- The browser exploit threat has been explicitly analyzed and the above top-ten website categories have been generated and ranked based on the percentage of browser exploit threats that each of them account for.
- Websites catergorized as Anonymizer rank at the top with 73 percent of all threats being browser exploits. But this website category accounts for only 21 percent of this threat when compared with other categories in the top-ten list.
- It shows that the majority of threats from anonymizer type websites are browser exploits, although the volume of such threats is not the highest. Blogging has the highest volume of browser exploit threats.

Fig. A.18

Malicious Web Activity: Social Networking Attacks by Category, 2013

Source: Symantec.cloud

Rank	Top-Ten Potentially Most Harmful Categories of Websites - Social Networking	Percentage Used To Deliver Social Networking Attacks
1	Blogging	17%
2	Hosting	4%
3	Illegal	3%
4	Technology	2%
5	News	1%

Commentary

- Approximately 67 percent of websites used to distribute malware were identified as legitimate but compromised websites, an increase of four percentage points compared with 2012. This figure excluded URLs that contained just an IP address and did not include general domain parking and pay-per-click websites.
- 9.9 percent of malicious website activity was classified in the Technology category.
- Websites classified as automated web application were found to host the greatest number of threats per site than other categories, with an average of 3.4 threats per website, the majority of which related to Malware (82 percent).
- Analysis of websites that were used to deliver drive-by fake AV attacks revealed that 4 percent of fake AV threats were found on compromised Art and Museum sites. Additionally, 50 percent of threats found on compromised Art and Museum sites were fake AV. 42 percent of threats found on compromised Shopping sites were also fake AV.
- Analysis of websites that were used to deliver attacks using browser exploits revealed that 21 percent of threats found on compromised anonymizer sites were related to browser exploits. 73 percent of browser exploit attacks were found on compromised anonymizer sites. 67 percent of attacks found on compromised blogging sites involved browser exploits.
- 17 percent of attacks on social networking sites were related to malware hosted on compromised blogging sites. This is where a URL hyperlink for a compromised website is shared on a social network. Websites dedicated to the discussion of hosting accounted for 4 percent of social networking attacks.
- The Dynamic category is used to classify websites that have been found to contain both appropriate and inappropriate user-generated content, such as social networking or blogging websites. Also, websites in which the page content changes based on how the user is interacting with it (for example, an Internet search).
- The Illegal category includes sites that fall into the following sub-categories: Activist Groups, Cyberbullying, Malware Accomplice, Password Cracking, Potentially Malicious Software and Unwanted Programs, Remote Access Programs, and several other 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.
- The Automated Web Application category refers to sites which allow a computer to automatically open an HTTP connection for various reasons including checking for operating system or application updates.

Bot-Infected Computers

Background

Bot-infected computers, 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), P2P, or hyper-text 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 (DoS) 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 —all of which can lead to serious financial and legal consequences. Attackers favor bot-infected computers with a decentralized C&C[6] 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 importantly, 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 a distinct computer that was active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they can be classified as active attacker bots or bots that send out spam, i.e. 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 publically available software such as "Low Orbit Ion Cannon" (LOIC) when used in a coordinated effort may disrupt some businesses' website operations if used in sufficiently large numbers.

The following analysis reveals the average lifespan 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.

Fig. A.19

Top-Ten Bot Locations by Average Lifespan of Bot, 2012–2013

Source: Symantec.cloud

Rank	Country/Region	Average Lifespan of Bot (Days) - 2013	Average Lifespan of Bot (Days) - 2012	Percentage of World Bots - 2013	Percentage of World Bots - 2012
1	Romania	20	24	0.19%	0.16%
2	Indonesia	15	12	0.12%	0.12%
3	Bulgaria	14	17	0.12%	0.10%
4	United States	13	13	20.01%	15.34%
5	Egypt	11	10	0.11%	0.11%
6	Colombia	11	6	0.10%	0.12%
7	Switzerland	10	8	0.31%	0.28%
8	Philippines	10	10	0.16%	0.16%
9	New Zealand	10	6	0.15%	0.16%
10	Ukraine	9	10	0.15%	0.15%

Commentary

- Bots located in Romania were active for an average of 20 days in 2013, compared with 24 days in 2012; 0.19 percent of bots were located in Romania, compared with 0.16 percent in 2012.
- 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 a hundred times greater than that of 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 20 percent of the world's bots in 2013, the average lifespan for a bot was still 13 days, unchanged from 2012.
- Additionally, in China, which was ranked second for bot activity in 2013 and was host for 9 percent of the world's bots, the average lifespan for a bot was 5 days.
- All other countries outside the top-ten had a lifespan of 9 days or less. The overall global average lifespan was 6 days, unchanged from 2012.

Botnets, which are large networks of malware-infected computers, continued to be a significant feature of the threat landscape in 2013. By pooling the power of infected computers, attackers have a powerful tool that allows them to engage in activities such as Distributed Denial of Service (DDoS) attacks, click fraud or Bitcoin mining.

Symantec actively initiates and supports clean-up actions against botnets. However, botnets are becoming resilient against takedowns. We believe that even if a takedown operation does not remove a botnet completely, it does at least make it harder for cybercriminals. It might lead to arrests and they are forced to rebuild, losing revenue in the process.

During 2013, Symantec struck a major blow against the ZeroAccess botnet. With 1.9 million computers under its control, it is one of the larger botnets in operation at present. ZeroAccess has been largely used to engage in click fraud to generate profits for its controllers. The gang also experimented with a Bitcoin-mining module, but appear to have deemed it not profitable and removed it again.

One of the key features of the ZeroAccess botnet is that it uses a peer-to-peer (P2P) framework for its command and control (C&C) architecture. This makes ZeroAccess highly resilient. Because there is no central C&C, the botnet cannot be disabled by simply targeting C&C servers.

While analyzing the ZeroAccess malware Symantec discovered a weakness in the protocol used by the botnet and put in place plans for a takedown operation. When ZeroAccess' controllers started to address this weakness by updating their software, Symantec immediately began sinkholing computers while the opportunity lasted. Roughly half a million computers were liberated from the botnet during the operation.

A number of other botnet takedowns and sinkhole initiatives took place in 2013. Among them was a combined Microsoft/FBI attempt to disrupt the Citadel botnet and the takedown of the Bamital botnet by Symantec and Microsoft. This might explain part of the reduction in the number of bots we observed. The number of infected computers decreased from 3.4 million in 2012 to 2.3 million in 2013 (a reduction of 32.8 percent). However, newer forms of botnets also emerged in 2013, utilizing low-powered devices such as routers, and other hardware.

Denial of Service Attacks

The size of denial of service attacks underwent a dramatic increase in 2013, with one attack in particular reaching over 300Gbps. This increase is due in part to changes in the techniques used by attackers, with old tricks that worked well in the past seeing a resurgence. Internet access and quality is constantly improving and reaching previously unconnected or poorly connected parts of the globe. This new access also brings with it poorly configured infrastructure and computers with little or no security, which is good news for malicious actors who see commodities waiting to be utilized.

The number of attacks is increasing year over year, with Akamai seeing 250 attacks in 2011, compared to 768 in 2012.[7] With their final quarterly report for 2013 still to be released, Akamai have so far seen 807 attacks,[8] a clear sign that DDoS attacks are an increasingly popular method of attack.

Throughout 2012 the size of DDoS attacks, in terms of bandwidth, averaged in the realm of double digits. That all changed in 2013, when the triple digit mark of 100Gbps was not only reached but was exceeded more than threefold. In March the anti-spam organization Spamhaus was targeted with a DDoS attack that peaked at over 300Gbps. An attack of this magnitude was made possible by a method known as DNS reflection, also known as DNS amplification. In this type of attack, an attacker sends a request with a spoofed source IP address matching that of the target to a large number of recursive DNS resolvers. The resolvers then respond to the request, but the response is much larger in size, which means the attacker can effectively amplify their attack to many times that of the bandwidth they have available. DNS reflection attacks are made possible by poorly configured domain name servers that have recursion enabled and will respond to anyone, these are referred to as open resolvers or open DNS recursors. There are millions of open resolvers[9] online that need to be locked down and secured, and until this problem is addressed DNS reflection attacks will not only continue but increase in size.

Network Time Protocol (NTP) reflection attacks also saw a significant increase last year with December seeing a major spike in activity.[10] NTP is used to sync time between computers on the Internet and, if not updated, can be used in DDoS attacks. As with DNS reflection attacks, an attacker can send a small packet of data to an NTP server which then sends a large amount of data to the target IP address. The recent attacks against the servers of several well-known online games[11] used this technique, and it seems set to continue to be used by attackers in 2014, with one major NTP reflection attack this year already reported to have reached 400Gbps.[12]

Use of reflection attack methodology means there may be less need for tools such as the Low Orbit Ion Cannon or large botnets with DDoS capabilities because fewer individual computers are now needed to undertake larger attacks.

The increased use of reflection attacks doesn't mean that other methods have disappeared. An attack against one the world's largest Bitcoin exchanges - the cryptocurrency being a prime target for DDoS attacks in 2013 - used a SYN flood attack and still reached over 100Gbps. Rather than using a huge botnet of compromised computers for this attack, it is believed those responsible used a network of compromised servers. This is another tactic that is becoming increasingly popular. Compromising unsecured servers gives hackers access to far more bandwidth than they would get from even a modest size botnet with DDoS functionality.

The increase in DDoS size also means an increase in severity, reflected by the reported slowdown of the Internet due to the Spamhaus attack in March. Denial of service attacks are one of the largest threats to the Internet. As we become more reliant on devices that are connected to the Internet,

these attacks will not only increasingly threaten governments, organizations, and businesses, but also individuals using the Internet for their everyday activities. A prime example of this was the attack against the Chinese registry,[13] which caused many .cn websites to go offline for several hours.

Mobile devices are becoming alternative tools for launching DDoS attacks. Symantec detected several mobile applications that allow the user to simply enter the target information and, at the press of a button, start the attack. Users can join large DDoS groups and pool their efforts, making this similar to older computer-based tools such as the LOIC. It is predicted that close to one billion smartphones[14] were sold in 2013. That is a huge number of potential recruits for DDoS attacks.

Approximately 45 percent of the world's population is now covered by a 3G mobile network[15] and the cost of mobile data is continually falling, with unlimited data plans becoming commonplace. It was forecasted that 4G/LTE networks will account for 1 in 5 mobile broadband subscriptions in 2017,[16] compared to 1 in 25 in 2012. LTE networks will increase connection speeds dramatically with an estimated average speed of 3,898kbps projected by 2017,[17] compared to 189kbps in 2010. Attacks emanating from mobile devices will likely increase in 2014 as more people migrate to mobile devices and networks around the world continue to improve connection speeds and reduce the cost of mobile data.

DDoS as a service

It is now easier than ever to carry out a DDoS attack regardless of someone's technical knowledge. DDoS as a service is sold online on underground hacking forums and attacks of varying sizes can be organized for the right price. Websites or businesses that offer DDoS as a service, referred to as stressers, can be found online with relative ease. These services are commonly offered in the gaming community to temporarily get rid of competing players during critical gaming sessions.

While some services say their business is only for "stress testing your own website" others are more blatant about what they are offering.

Prices range from US$5 to over $1,000 depending on the length and magnitude of the attack.

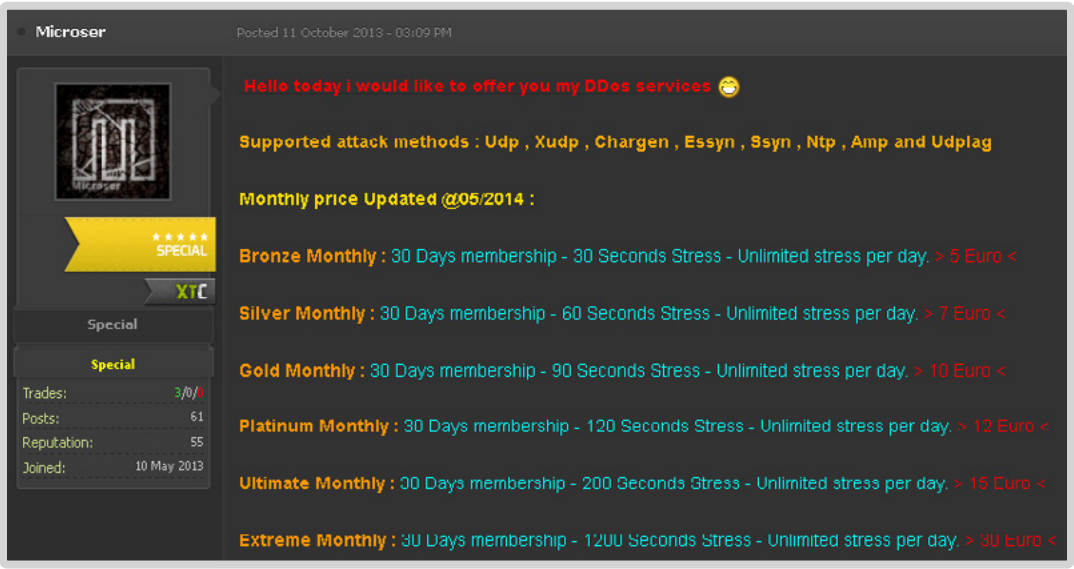


Fig. A.20 DDoS Service options

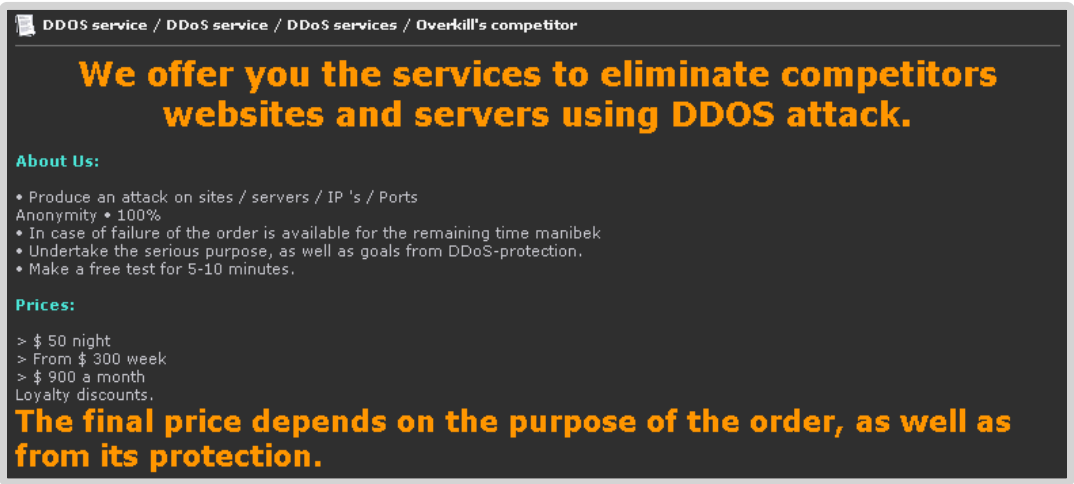


Fig. A.21 DDoS Service example

Hacktivism

Improved Internet access can help people who may not have been heard in the past to voice their opinions and political views. Unfortunately, some individuals and groups feel that cybercrime is a better way to get their message across. When discussing hacktivist collectives, one of the largest and best-known is Anonymous. While this loosely associated network of individuals and groups is still making its mark, its campaigns are failing to create the impact they once did. The second assault against Israel in April 2013, which promised to "wipe Israel off the map of the Internet", failed to cause much disruption. The same was true for other campaigns such as #OpUSA. While attacks under the Anonymous banner still pose a major risk, it is another hacktivist group that has taken the limelight recently.

Rise of the SEA

The pro-Bashar al-Assad hacktivist collective the Syrian Electronic Army (SEA), was quite prolific throughout 2013.

Although active since 2011, the SEA became increasingly active in 2013, compromising a multitude of high-profile websites and social media accounts. The SEA is usually happy with posting political messages on hacked social media accounts or websites by defacement or redirection, but it has also been known to steal information. However this does not seem to be its preferred modus operandi. Whether or not data breaches by the SEA will become more common in 2014 remains to be seen.

When it comes to security the SEA know that the weakest link in the chain is often users themselves and the hacktivist group uses this to its advantage. Phishing attacks are used to obtain the login credentials for social media accounts of target organizations, and due to many users within an organization having access to the same accounts it greatly improves the chances of getting the credentials in this manner. Often the same credentials are used for more than one account, so a successful phishing attack can grant attackers access to several accounts. The global phishing rate reflects the popularity of this method of attack; it has increased from 2012, when 1 in 414 emails per day were actual phishing attacks, to 1 in 392.4 emails being phishing attempts in 2013.

The widespread use of social media by companies and organizations has made it an ideal target for hacktivists and this will no doubt continue in 2014. The 2013 Norton Report[18] revealed that 12 percent of social media users admit to having their accounts hacked and a staggering 25 percent of people shared their account credentials with others. While two-factor authentication (2FA) is slowly becoming commonplace, it is often not practical for companies that share social media accounts across several geographical regions. For instance, if a social media account allows only one mobile phone number to be registered for 2FA purposes, it will limit the authentication to one region. This type of restriction means that enterprises with shared accounts are often less secure than individual users. If at all possible, users must take advantage of 2FA and other security measures, such as single sign-on technology[19] and multiple permission levels, before social media hacking is placed out of the reach of hackers like the SEA.

While some may view defacement attacks by hacktivist groups as relatively harmless, this was not the case when in April 2013 the Twitter account belonging to a well-known news agency was hacked. The SEA tweeted that two explosions had gone off in the White House. This news caused the US stock market to panic and the Dow Jones to drop by 143 points. The news agency quickly reported the hack and the stock market recovered but this highlights the power that social media hacking can wield in today's world.

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 in smartphones and tablets, and their increasing connectivity and capability, there has been a corresponding increase in attention, both from 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 2013, there was a decrease in the number of vulnerabilities reported that affected mobile devices. Symantec documented 132 vulnerabilities in mobile device operating systems in 2013, compared to 416 in 2012 and 315 in 2011; a decrease of 68 percent.

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 the types of threats into a variety of categories based on their functionality.

Fig. A.22

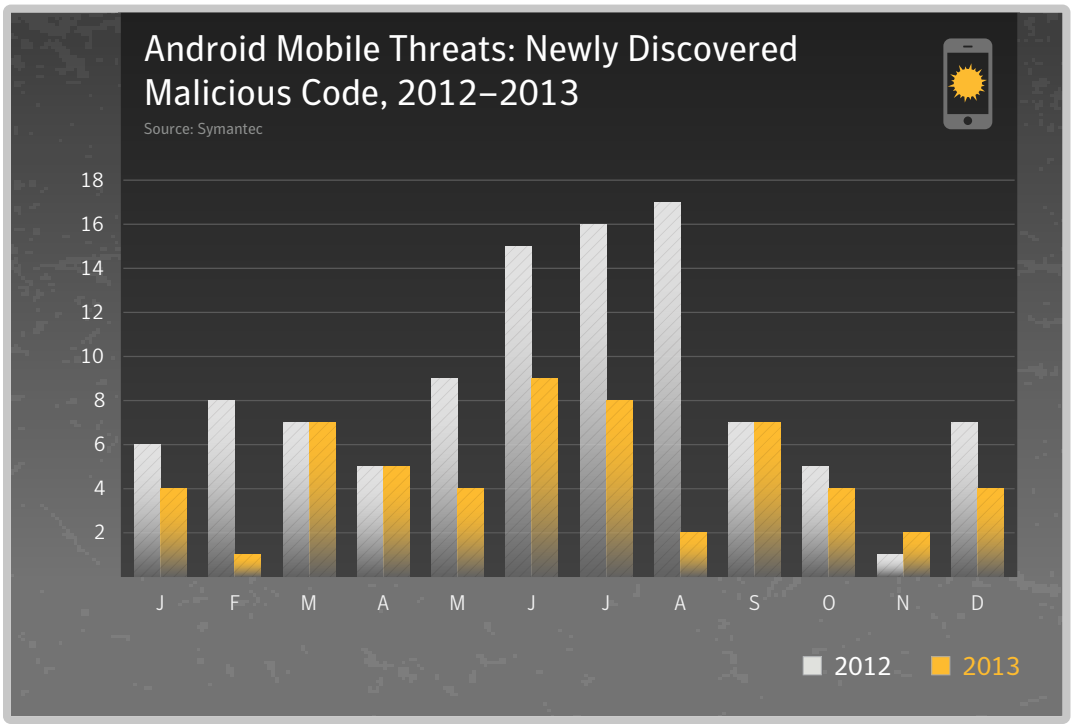


Fig. A.23

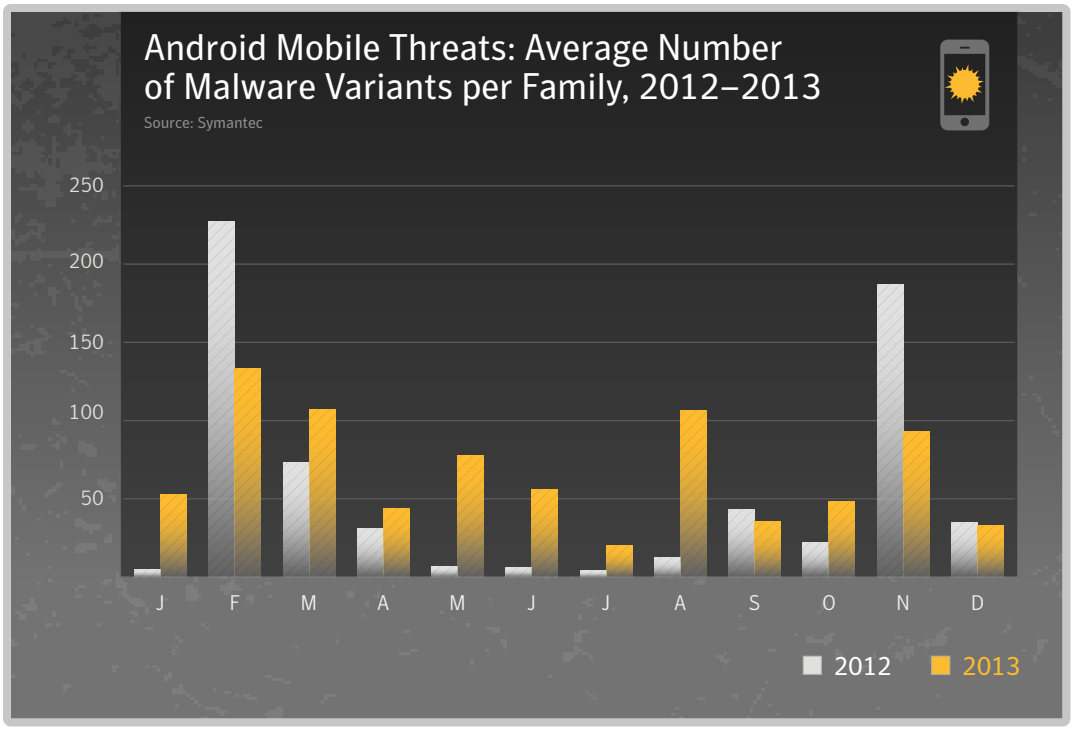


Fig. A.24

Mobile Threats: Malicious Code by Platform, 2013

Source: Symantec

Platform	Number of Threats	Percent of Threats
Android	57	97%
Symbian	1	2%
Windows	1	2%
iOS	0	0%

Fig. A.25

Mobile Threats: Malicious Code Actions in Malware, 2012–2013

Source: Symantec

High-level Risk Categories	Track User	Steal Information	Send Content	Traditional Threats	Reconfigure Device	Adware/ Annoyance
Percentage of actions found in threats (2012)	15%	32%	13%	25%	8%	8%
Percentage of actions found in threats (2013)	30%	23%	8%	20%	10%	9%

Fig. A.26

Mobile Threats: Malicious Code Actions – Additional Detail, 2012–2013

Source: Symantec

Detailed Threat Categories	Percent Found in Threats, 2013	Percent Found in Threats, 2012
Steals Device Data	17%	27%
Spies On User	28%	12%
Sends Premium SMS	5%	11%
Downloader	8%	11%
Back door	12%	13%
Tracks Location	3%	3%
Modifies Settings	8%	5%
Spam	3%	2%
Steals Media	3%	2%
Elevates Privileges	2%	3%
Banking Trojan	3%	2%
Adware/ Annoyance	9%	8%
DDOS Utility	0%	1%
Hacktool	0%	1%

Fig. A.27

Mobile Threats: Documented Mobile Vulnerabilities by Platform, 2013

Source: Symantec

Platform	Documented vulnerabilities	Percentage
Apple iOS/iPhone/iPad	108	82%
Android	17	13%
BlackBerry	1	1%
Nokia	1	1%

Fig. A.28

Mobile Threats: Documented Mobile Vulnerabilities by Month, 2013

Source: Symantec

Month	Documented Vulnerabilities
January	16
February	4
March	9
April	7
May	22
June	5
July	4
August	3
September	45
October	5
November	7
December	1

The following are specific definitions of each subcategory:

- **Steals Device Data**—gathers information that is specific to the functionality of the device, such as IMEI, 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 SMS messages, and sends them to a remote source.
- **Sends Premium SMS**—sends SMS messages to premium-rate numbers that are charged to the user's mobile account.
- **Downloader**—can download other risks on to the compromised device.
- **Backdoor**—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.

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

Symantec has identified five primary mobile risk types:

Steal Information. Most common among bad mobile apps was the collection of data from the compromised device. This was 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[20] and IMSI[21] 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 was to track a user's personal behavior and actions. These risks take data specifically in order to spy on the individual using the phone. This is done by gathering up various communication data, such as SMS messages and phone call logs, and sending them to another computer or device. In some instances they may even record phone calls. In other cases these risks track GPS coordinates, essentially keeping tabs on the location of the device (and their 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 risks 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 risks that can be used as email spam relays, controlled by the attackers and sending unwanted emails from addresses registered to the device. One threat in this category constantly sent HTTP requests in the hope of bumping certain pages within search rankings.

Traditional Threats. The fourth group contains more traditional threats, such as backdoors and downloaders. Attackers often port these types of risks from PCs to mobile devices.

Change Settings. Finally there are a small number of risks that focus on making configuration changes. These types 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

- There were 57 new Android malware families identified in 2013, compared with 103 in 2012
- The average number of variants per family in 2013 was 57, compared with 38 in 2012. Although the overall number of new mobile malware families was much lower than in the previous year, the number of variants for each family is now much higher. This is likely to be a result of mobile malware toolkits allowing the attackers to repackage and customize their malware variants more easily, and in so doing using them much more widely.
- 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 127 mobile vulnerabilities published in 2013, compared with 416 in 2012, a decrease of 69 percent.
- Further analysis of mobile malware and spyware indicated the highest type of activity undertaken on a compromised device was to spy on the user, 28 percent in 2013 compared with 12 percent in 2012. 17 percent of malicious mobile activity was designed to steal data in 2013, compared with 27 percent in 2012.

Quantified Self – A Path to Self-Enlightenment or Just Another Security Nightmare?

In recent years, the idea of collecting and analysing data about a person's activities and status has really taken off. A new term had been coined for this activity and it is known as the concept of the Quantified Self[22] (QS) – also known as life tracking.

At its core, the QS describes the notion of collection and analysis of all types of data about a person on an ongoing and often real-time basis. The goal is usually some high-minded aspiration such as to live better or improve oneself in some shape or form. While we are hearing a lot more about QS these days, it is not a new concept by any means. In the past, this type of monitoring was something that was mostly done by professional athletes to enhance training and performance or medical patients for managing life-threatening conditions. Today, improved technology, innovative startups and lower costs are all driving forward the current wave of the QS movement at breakneck speed and creating a tsunami of data in its wake.

It's Personal Data, But Not as We've Known It

We are all familiar with the collection and use of the traditional types of personal information in the form of the name, address, date of birth, and so on. We as users have been sharing this type of information with businesses for decades. When we talk of "personal information" this is typically what we think of. But now, new technologies enable us to collect much more information at a deeper and more personal level. Data generated by quantified self devices and services (also known as first-party data) is highly personal and could reveal a lot more about ourselves to others than we may like.

The types of data typically generated by QS applications include:

- GPS location
- Heart rate
- Height/weight
- Calorie/alcohol intake
- Mood
- Sleep times/patterns
- Body temperature

Users need to understand what's being collected, how it is being stored and shared, and be comfortable with this fact and its implications and potential applications before proceeding.

A Burgeoning Sector

Despite the many potential security landmines in the field of QS, public interest in it has mushroomed in the past year few years. One indicator of this interest is in the amount of startup business activity in this area. According to CB Insights, funding for QS related startups reached US$318 million[23] in 2013, up 165 percent from 2012. Businesses in this category track nearly every aspect of human activity. A lot of the data that is collected will be done with active user consent – the person will install the app, then sign up and consent for services that collect and analyze the data. But there will also be cases where data may be collected without user consent or knowledge, and we as users of these new technologies and services will have to proceed with caution.

Data Breaches that could lead to Identity Theft

Background

Hacking continued to be the primary cause of data breaches in 2013. In 2013, there were eight data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 150 million identities. In contrast, 2012 saw only one breach larger than 10 million identities. As a result the overall average number of identities exposed has increased significantly, from 604,826 identities per breach in 2012 to 2,181,891 in 2013.

As the overall average size of a breach has increased, the median number of identities stolen has actually fallen from 8,350 in 2012 to 6,777 in 2013. 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 is rising, the number of identities exposed is still in in the order of thousands, but there were also more incidents that resulted in extremely large volumes of identities being exposed in 2013 than in the previous year.

Hacking was the chief cause of most data breaches in 2013, and consequently received a great deal of media attention. Hacking can undermine institutional confidence in a company, exposing its attitude to security. The loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 34 percent of data breaches in 2013 according to the Norton Cybercrime Index data.[24] As data breach notification legislation becomes more commonplace, we are likely to see the number of data breaches rising. Such legislation is often used to regulate the responsibilities of organizations after a data breach has occurred and may help to mitigate against the potential negative impact on the individuals concerned.

The Healthcare, Education, and the Public Sector were ranked highest for the number of data breach incidents in 2013; the top three accounted for 58 percent of all data breaches. However, the Retail, Computer Software and Financial sectors accounted for 77 percent of all the identities exposed in 2013.

Methodology

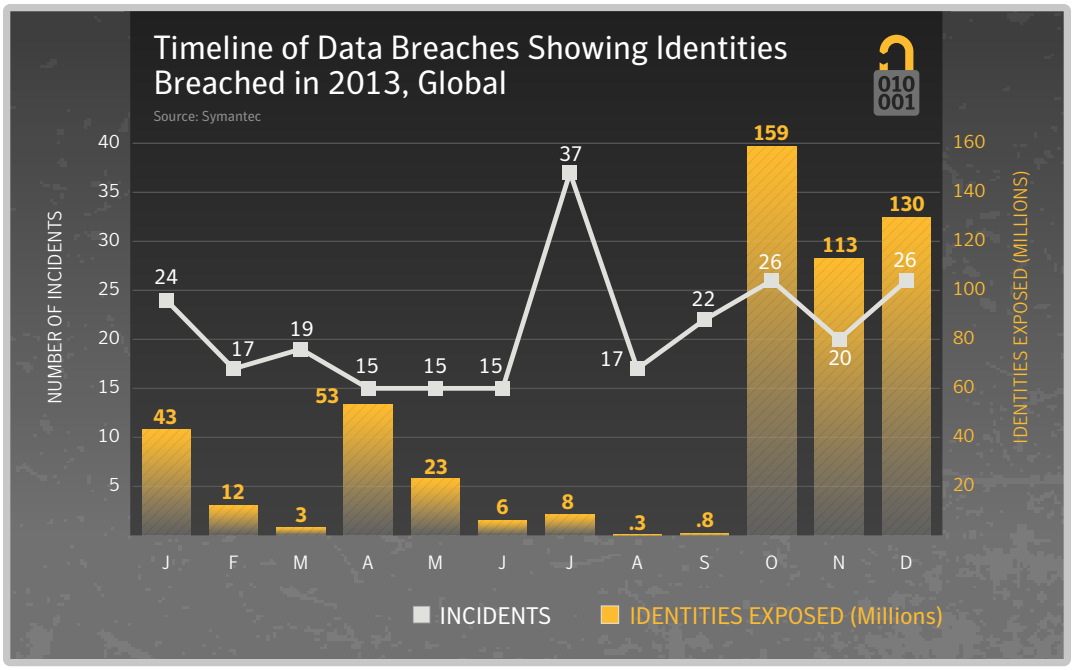
The information analysed regarding data breaches that could lead to identity theft is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model which measures the levels of threats including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. Data for the CCI is primarily derived from Symantec Global Intelligence Network and for certain data from ID Analytics.[25] The majority of the Norton CCI's data comes from Symantec's Global Intelligence Network, one of the industry's most comprehensive sources of intelligence about online threats. 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 name, address, Social Security numbers, credit card numbers, and medical history. Using publicly available data the Norton CCI determines the sectors that were most often affected by data breaches, as well as the most common causes of data loss.

The sector that experienced the loss, along with the cause of 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 was 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 others do. 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.[26] 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 under-represented in this data set.

Fig. A.29



- There were 253 data breach incidents recorded by the Norton Cybercrime Index for 2013 and a total of 552,018,539 identities exposed as a result.
- The average number of identities exposed per incident was 2,181,891 compared with 604,826 in 2012 (an increase of more than 2.6 times).
- The median number of identities exposed was 6,777 compared with 8,350 in 2012. 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 eight, compared with only one in 2012.

Fig. A.30

Data Breach Incidents by Sector, 2013

Source: Norton Cybercrime Index

Industry Sector	Number of Incidents	Percentage of Incidents
Healthcare	93	36.8%
Education	32	12.6%
Government and Public Sector	22	8.7%
Retail	19	7.5%
Accounting	13	5.1%
Computer software	12	4.7%
Hospitality	10	4.0%
Insurance	9	3.6%
Financial	9	3.6%
Transportation	6	2.4%
Information technology	5	2.0%
Telecom	4	1.6%
Law enforcement	4	1.6%
Social networking	3	1.2%
Agriculture	2	0.8%
Community and non-profit	2	0.8%
Administration and human resources	2	0.8%
Military	2	0.8%
Construction	1	0.4%
Utilities and energy	1	0.4%
Computer hardware	1	0.4%

Fig. A.31

Identities Exposed by Sector, 2013

Source: Norton Cybercrime Index

Industry Sector	Identities Exposed	Percentage of Identities Exposed
Retail	165,154,040	29.9%
Computer software	153,134,178	27.7%
Financial	106,958,000	19.4%
Social networking	48,250,000	8.7%
Information technology	22,501,152	4.1%
Hospitality	20,342,323	3.7%
Telecom	12,117,143	2.20%
Accounting	8,760,912	1.6%
Healthcare	6,279,270	1.1%
Education	3,208,557	0.6%
Government and Public Sector	2,197,646	0.4%
Transportation	1,460,340	0.3%
Insurance	1,032,973	0.2%
Administration and human resources	301,300	0.1%
Computer hardware	100,000	0.02%
Agriculture	74,000	0.01%
Community and non-profit	69,228	0.01%
Military	53,000	0.01%
Law enforcement	4,477	0.001%

- Healthcare, Education, and the Public Sector were ranked highest for the number of data breach incidents in 2013; the top three accounted for 58 percent of all data breaches
- The Retail, Computer Software and Financial sectors accounted for 77 percent of all the identities exposed in 2013.
- This highlights that sectors involved in the majority of data breaches don't necessarily result in the largest caches of stolen identities.

Fig. A.32

Average Number of Identities Exposed per Data Breach by Notable Sector

Source: Norton Cybercrime Index

Cause of Breach	Average Identities per Incident
Accounting	673,916
Administration and human resources	150,650
Agriculture	37,000
Community and non-profit	34,614
Computer hardware	100,000
Computer software	12,761,182
Education	100,267
Financial	11,884,222
Government	99,893
Healthcare	67,519
Hospitality	2,034,232
Information technology	4,500,230
Insurance	114,775
Law enforcement	1,119
Military	26,500
Retail	8,692,318
Social networking	16,083,333
Telecom	3,029,286
Transportation	243,390
Construction	20,000

- The highest average number of identities exposed per breach in 2013 was in the Social Networking and Computer Software categories, with between 16 million and 12 million identities exposed in each breach, on average.
- The largest breach incident in 2013 occurred in the Computer Software sector, with an incident resulting in 15 million identities reportedly exposed.

Fig. A.33

Top Causes for Data Breach by Number of Breaches

Source: Norton Cybercrime Index

Cause of Breach	Number of Incidents	Percentage of Incidents
Hackers	87	34.4%
Accidentally made public	72	28.5%
Theft or loss of computer or drive	69	27.3%
Insider theft	15	5.9%
Unknown	6	2.4%
Fraud	4	1.6%

Fig. A.34

Top Causes for Data Breaches by Number of Identities Exposed

Source: Norton Cybercrime Index

Cause of Breach	Number of Identities Exposed	Percentage of Identities Exposed
Hackers	408,432,788	74.0%
Insider theft	112,435,788	20.4%
Accidentally made public	22,350,376	4.1%
Theft or loss of computer or drive	6,231,790	1.1%
Fraud	2,417,320	0.4%
Unknown	150,477	0.03%

Fig. A.35

Average Number of Identities Exposed per Data Breach, by Cause

Source: Norton Cybercrime Index

Cause of Breach	Average Identities per Incident
Hackers	4,694,630
Insider theft	7,495,719
Accidentally made public	310,422
Theft or loss	90,316
Fraud	604,330
Unknown	25,080

- **Hacking was the leading cause of reported identities exposed in 2013:** Hackers were also responsible for the largest number of identities exposed, responsible for 34 percent of the incidents and 74 percent of the identities exposed in data breach incidents during 2013.
- The average number of identities exposed per data breach for Hacking incidents was approximately 4.7 million.

Fig. A.36

Types of Information Exposed, by Data Breach

Source: Norton Cybercrime Index

Type of Information	Number of Incidents	Percentage of Data Types
Real Names	181	71.5%
Birth Dates	109	43.1%
Government ID numbers (incl. Social Security)	100	39.5%
Home Address	95	37.5%
Medical Records	85	33.6%
Phone Numbers	48	19.0%
Financial Information	45	17.8%
Email Addresses	39	15.4%
Usernames & Passwords	30	11.9%
Insurance	15	5.9%

- The most common type of personal information exposed in data breaches during 2013 was real names, where 84 percent of the incidents in 2013 included this type of information being exposed
- Birth dates were identified in 51 percent of the identity breaches during 2013, compared with usernames and passwords, which were exposed in 14 percent of incidents
- Government ID numbers, including social security numbers, were exposed in 47 percent of breach incidents during 2013

Threat of the Insider

For many companies, the leaked NSA documents have shown how an insider can easily gain access to confidential information and the damage that leaked information can cause. This issue was further highlighted when three South Korean credit card firms announced that they suffered a major data breach that affected tens of millions of customers. The cause of the breach, which is believed to be the largest ever recorded in South Korea, was due to one employee at a company that produces credit scores. This insider stole names, resident registration numbers (a Government identification number), and credit card details simply by copying this data to a USB stick which was then sold on to marketing firms.

Unlike external attackers, insiders may already possess privileged access to sensitive customer information, meaning they don't have to go to the trouble of stealing login credentials from someone else. They also have knowledge of the inner workings of a company, so if they know that their firm has lax security practices, they may believe that they will get away with data theft unscathed. Our recent research conducted with the Ponemon Institute suggests that 51 percent of employees claim it's acceptable to transfer corporate data to their personal computers, as their companies don't strictly enforce data security policies. Insiders could earn a lot of money by selling customer details, which may be sufficient motivation to risk their careers.

Outside of leaking information for the insider's personal gain, insider data breaches may also be the result of an accident. There were several cases last year in which company laptops were lost, potentially exposing personal information. Employees may not have had adequate data-handling training, meaning that they may have stored or shared data on insecure channels.

Accidental data breaches were most prevalent in 2013. We estimate that 28.5 percent of all data breaches were cases where records were accidently made public. This was the second biggest cause of data breaches all year.

German companies are the most likely to experience a malicious or criminal attack, according to our recent research with the Ponemon Institute, followed by Australia and Japan. Brazilian companies were most likely to experience data breaches caused by human error. All companies should be aware that, in addition to protecting their data from outsider threats, they should also keep an eye on those on the inside and strengthen their data protection policies in light of this.

Gaming Attacks

While gaming services may not seem like an obvious target for cybercriminals, account information such as usernames and passwords are valuable in themselves. In addition to this, in-game items have a real world value, making them a target for theft.

A console game vendor in Asia had 24,000 accounts relating to its reward program broken into by a brute force attack which involved around 5 million login attempts. One week later a similar attack against a Japanese computer game vendor resulted in 35,000 accounts being compromised. In this case, four million password guesses were required.

It would appear that it took around 160 password guesses on average per account to guess the password. This is a clear indication that many users still use easy-to-guess passwords.

In addition to this, attackers are re-using data from data breaches on other services. At least three large online game vendors fell victim to such breaches in 2013, revealing millions of account records. These events helped motivate some gaming companies to move to two-factor authentication for their login process.

The attackers behind gaming Trojans have also begun to expand their focus and move outside of the gaming sector. For example, Trojan.Grolker is a common gaming Trojan that has now started to target customers of a major South Korean bank.

Attacks are not just motivated by account theft. In some instances the attacker just wants to disrupt the game. For example, during the Christmas holiday, a group of attackers used NTP amplification DDoS attacks to bring down a handful of popular online games. On Twitter the group said they were doing it just for fun.

DDoS attacks require relatively little technical expertise to mount and the main obstacle for the attacker is finding enough bots or an amplifier to use. A new development is the emergence of DDoS services customized for gamers. Those so called “booter” services start at around US$2.50 for short-burst attacks.

Online games can also suffer from vulnerabilities like any other software. Researchers have found[27] multiple vulnerabilities such as buffer overflows in many of the popular game engines. Successful exploitation could lead to the compromise of the gaming server or even to remote code execution on all connected clients.

The gaming sector has also not been immune to the attention of state-sponsored attackers. Leaks to the media have revealed that a number of popular online gaming platforms were monitored by intelligence agencies, who were fearful that in-game communication tools were being used by terrorists for covert communications.

The New Black Market

One of the most notable developments of 2013 was the emergence of new underground markets for drugs and other illegal goods. The oldest and best known of these marketplaces is Silk Road. Launched in 2001, it maintained a relatively low profile until last year, when it emerged into the public's consciousness and gathered significant media attention before it was temporarily shut down by the US Federal Bureau of Investigation (FBI) in October.

Silk Road epitomizes the growing professionalization of the cybercrime underground. It borrows the business model of legitimate e-commerce marketplaces such as Amazon and eBay, incorporating features such as vendor feedback, escrow payments and dispute resolution.

Where Silk Road and other sites differ is in the degree of anonymity they afford their users. Most of these sites operate on Tor, a network designed to facilitate anonymous access to the Internet. Transactions are conducted through virtual currency Bitcoin, which is largely unregulated.

If these measures led users to believe that they could operate with impunity, that illusion was shattered by the FBI raids in October. A man alleged to be the founder of the website was arrested and Bitcoins worth more than US$28 million were seized.

Law enforcement moves have yet to deter the online narcotics trade completely. In the aftermath of the raid, business moved to a number of copycat marketplaces such as Black Market Reloaded and Sheep. Before the end of the year Silk Road itself was re-launched by former administrators of the original site.

These developments indicate that the new black market has a high degree of resilience. While the original Silk Road employed numerous measures to preserve the anonymity of its users, its alleged founder did make several mistakes that allowed the FBI to discover his identity. A new generation of black marketeers may be more careful about guarding their identity. If so, other marketplaces will prove more difficult to dismantle.

The evolution of the new black market model closely resembles the growth of online music and video piracy. Early ad hoc sales were followed by the construction of a trading platform. When the original marketplace falls foul of the law, it is succeeded by a host of copycat services, each seeking to perfect the business model and enhance security.

On this basis, it would appear that the new black market is still in its infancy and could prove to be a persistent threat for years to come. While such marketplaces in themselves do not represent an information security threat, they have the potential to facilitate other criminal activity, such as providing further income for cybercrime gangs or acting as a platform for scams and fraud.

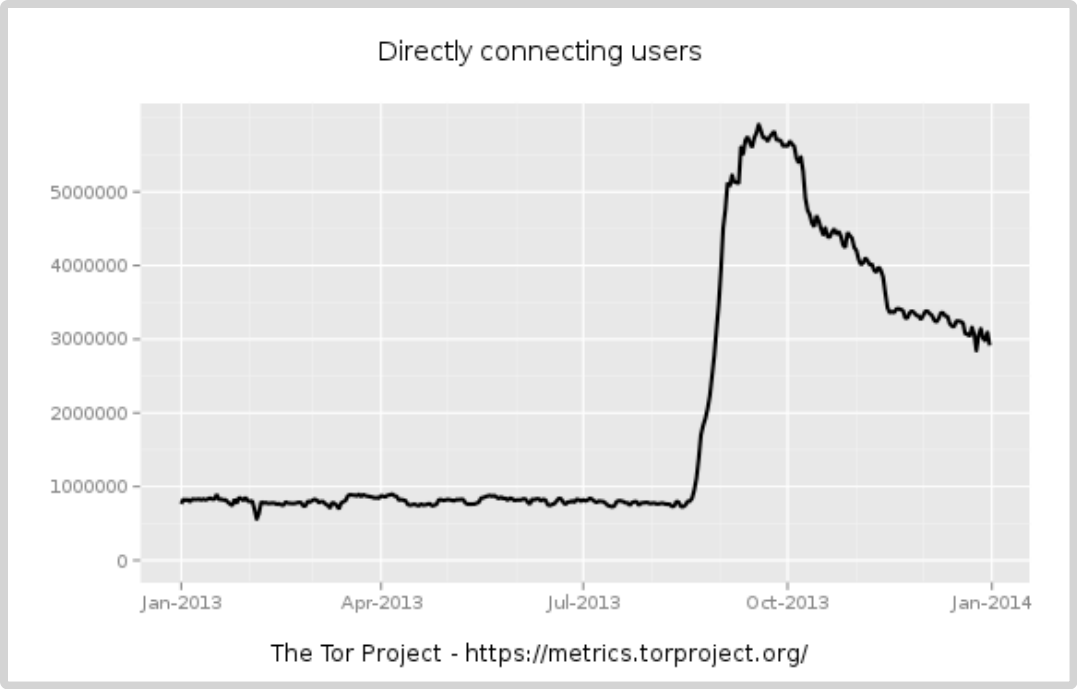


Fig. A.37 *Directly connected Tor users in 2013.*

The narcotics trade has traditionally been controlled by powerful and violent criminal gangs. If these new online marketplaces continue to gain popularity, it is likely that these gangs will not easily cede their market share to new arrivals, leading to potential for conflict and violence.

Tor is the most popular means of accessing these underground sites, but other networks like I2P or Freenet also became popular in 2013. The Tor network was more popular than ever, promoted as the best way to stay anonymous on the Internet. In August the number of active users grew from 1 million to 5 million in just two weeks. But some of that growth might have been related to the botnet Backdoor.Mevede,[28] which switched to use Tor as its command infrastructure.

Footnotes

01 http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201401/P020140116395418429515.pdf

02 http://data.worldbank.org/indicator/IT.NET.USER.P2 and http://www.prb.org/DataFinder/Topic/Rankings.aspx?ind=14

03 http://www.iamai.in/PRelease_detail.aspx?nid=3222&NMonth=11&NYear=2013

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

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

06 Command and control

07 http://www.akamai.com/dl/whitepapers/akamai_soti_q412.pdf?curl=/dl/whitepapers/akamai_soti_q412.pdf&solcheck=1&

08 http://www.akamai.com/dl/akamai/akamai-soti-q313.pdf?WT.mc_id=soti_Q313

09 http://openresolverproject.org

10 http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

11 http://arstechnica.com/security/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol

12 http://www.informationweek.com/security/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787

13 http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend

14 https://www.gartner.com/login/loginInitAction.do?method=initialize&TARGET=http://www.gartner.com/document/2622821

15 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/b#3g-or-better

16 http://www.gsmamobileeconomy.com/GSMA Mobile Economy 2013.pdf

17 http://www.gsmamobileeconomy.com/GSMA_ME_Report_2014_R2_WEB.pdf

18 http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

19 http://en.wikipedia.org/wiki/Single_sign-on

20 International Mobile Equipment Identity

21 International Mobile Subscriber Identity

22 http://en.wikipedia.org/wiki/Quantified_Self

23 http://www.cbinsights.com/blog/trends/quantified-self-venture-capital

24 http://www.nortoncybercrimeindex.com

25 http://www.idanalytics.com

26 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

27 http://revuln.com/files/ReVuln_Game_Engines_0days_tale.pdf

28 http://www.symantec.com/security_response/writeup.jsp?docid=2013-090611-2333-99

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 clients, 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 an infection could have occurred in the absence of security software to detect and eliminate the threat.

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

- Backdoors 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 them 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 backdoor will always be categorized in conjunction with another malicious code feature. Typically, backdoors are also Trojans, however many worms and viruses also incorporate backdoor functionality. In addition, many malicious code samples can be classified as both worm and virus 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 2013:

- Top Malicious Code Families
- Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
- Propagation Mechanisms
- Email Targeted Spear-Phishing Attacks Intelligence

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 is initially comprised 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-ten list of malicious code families accounted for 40.1 percent of all potential infections blocked in 2013.

Fig. B.1

Overall Top Malicious Code Families, 2013

Source: Symantec

Rank	Name	Type	Propagation Mechanisms	Impacts/Features	Percent 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.	15.4%
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.	7.4%
3	W32.Downadup	Worm/Backdoor	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.	4.5%
4	W32.Virut	Virus/Backdoor	Executables	Infects various file types including executable files and copies itself to local, removable, and shared network drives. It also establishes a backdoor that may be used to download and install additional threats.	3.4%
5	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.	3.3%
6	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.	2.9%
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.	1.4%
8	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.	1.2%
9	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.	0.4%
10	W32.Xpaj	Virus	Executables/removable, mapped, and network drives	Infects .dll, .exe, .scr, and .sys files on the compromised computer.	0.2%

Fig. B.2

Relative Proportion of Top-Ten Malicious Code Blocked in Email Traffic by Symantec.cloud in 2013, by Percentage and Ratio

Source: Symantec.cloud

Rank	Malware	Percentage of Email Malware	Equivalent Ratio in Email	Percentage Overall
1	Trojan.Zbot-SH	24%	1 in 4.2	15.4%
2	Trojan.Zbot	11%	1 in 8.7	7.4%
3	Exploit/Link.D	3%	1 in 33.2	4.5%
4	Exploit/Link-Downloader	2%	1 in 41.1	3.4%
5	Exploit/LinkAlias	2%	1 in 42.8	3.3%
6	w32/NewMalware-30e9	2%	1 in 50.6	2.9%
7	Exploit/LinkAlias.fu	1%	1 in 71.7	1.4%
8	Exploit/Link.G	1%	1 in 81.6	1.2%
9	Exploit/Link-30e9	1%	1 in 85.1	0.4%
10	Exploit/MimeBoundary003	1%	1 in 105.8	0.2%

Fig. B.3

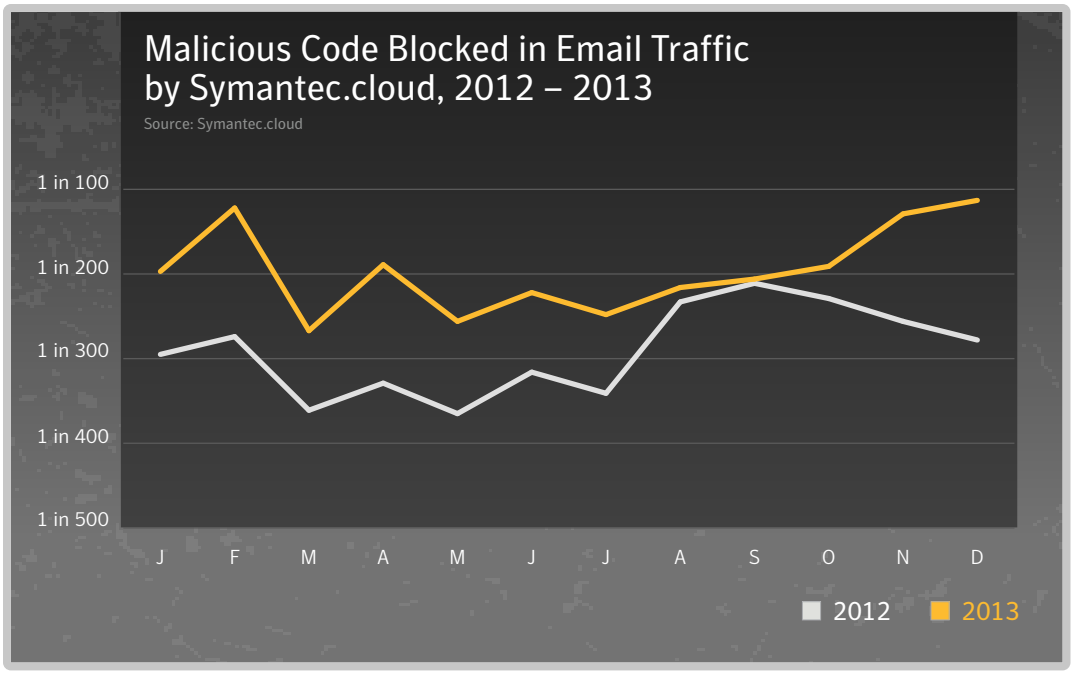


Fig. B.4

Relative Proportion of Top-Ten Malicious Code Blocked in Web Traffic by Symantec.cloud in 2013, by Percentage and Ratio

Source: Symantec.cloud

Rank	Malware Name	Percentage of Web Malware	Equivalent Ratio
1	Trojan.Iframe.BMY	5.6%	1 in 17.8
2	Bloodhound.Exploit.281	2.4%	1 in 42.1
3	Trojan.Malscript	1.8%	1 in 56.8
4	EML/Worm.AA.dam	1.7%	1 in 58.1
5	URL.Malware	1.1%	1 in 87.6
6	Trojan.Maljava	1.0%	1 in 96.0
7	IFrame.Exploit	1.0%	1 in 96.5
8	Trojan.HTML.Redirector.CH	0.6%	1 in 165.0
9	JS:Trojan.JS.Iframe.AM	0.6%	1 in 166.0
10	JS:Trojan.Crypt.KA	0.6%	1 in 181.6

Commentary

- Ramnit overtook Sality again to become the most prevalent malicious code family in 2013. Ranked first in 2011 and 2012, it was the top malicious code family by volume of potential infections again in 2013.[1]
- Samples of the Ramnit family of malware were responsible for significantly more potential infections (15.4 percent) than the second ranked malicious code family in 2013, Sality[2] (7.4 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[3] 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.
- Downadup gains some momentum: Downadup (a.k.a. Conficker) was ranked in third position in 2013 and 2012. Downadup propagates by exploiting vulnerabilities in order to copy itself to network shares.
- Overall in 2013, 1 in 196.4 emails was identified as malicious, compared with 1 in 291 in 2012; 25.4 percent of email-borne malware comprised hyperlinks that referenced malicious code, in contrast with malware that was contained in an attachment to the email. This figure was 22.5 percent in 2012, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.

- In 2013, 10.5 percent of malicious code detected in 2013 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 families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.
- Trojan.Zbot-SH was the most frequently blocked malware in email traffic by Symantec.cloud in 2013, with Trojan.Zbot taking the second position.
- Trojan.Iframe.BMY was the most frequently blocked malicious activity in web traffic filtered by Symantec.cloud in 2013, accounting for 5.6 percent. Detection for a malicious IFrame is triggered in HTML files that contain hidden HTML IFrame elements with JavaScript code that attempts to perform malicious actions on the computer; for example, when visiting a malicious web page, the code attempts to quietly direct the user to a malicious URL while the current page is loading.
- Bloodhound.Exploit.281 ranks second with 2.4 percent of detections.
- Trojan.Malscript ranks third with a detection of 1.8%.

Data Ownership: Targeting the User's Information Directly

Many people believe that only after they hand over their data to a company for purposes such as social networking and shopping, this data is under threat. If we continue with this logic, it could lead us to assume that, as long as a person does not give any of their personal data to third-party services, they're safe. However, this is not necessarily the case. There are several forms of malware that specifically target data that resides on the user's computer.

Stealing Information Directly

Infostealer malware, as the name implies, specifically focuses on stealing information directly from the user's computer. This malware could log keystrokes or take screenshots to steal login credentials, financial information and other personally identifiable information.

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 that can drive down prices, increasing adoption rates. There may be other factors at work based on the local economic conditions that present different risk factors. Similarly, the industry sector may also have an influence on an organization's risk factor, where 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 their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a malicious attack by virtue of the relationships they have with other organizations; for example, a company may be subjected to an attack because they are a supplier to a larger organization, and attackers may seek to take advantage of this relationship in forming the social engineering behind subsequent attacks to the main target using the SMB as a springboard for these later attacks. SMBs are perceived to be a softer target as they are less likely to have the same levels of security as a larger organization, which is likely to have a larger budget applied to their security countermeasures.

Methodology

Analysis of malicious code activity on geography, industry, and size are based on the telemetry analysis from Symantec.cloud clients for threats detected and blocked against those organizations in email traffic during 2013.

This analysis looked at the profile of organizations being subjected to malicious attacks, in contrast to the source of the attack.

Fig. B.5

Proportion of Email Traffic Identified as Malicious by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013	2012
Public Sector	1 in 95.4	1 in 72.2
Education	1 in 233.0	1 in 163.1
Accommodation and Catering	1 in 247.3	1 in 236.4
Marketing/Media	1 in 291.8	1 in 234.6
Non-Profit	1 in 328.4	1 in 272.3
Estate Agents	1 in 360.2	1 in 291.4
Recreation	1 in 370.8	1 in 315.1
Prof Services	1 in 396.5	1 in 315.1
Agriculture	1 in 415.5	1 in 329.7
Finance	1 in 426.8	1 in 218.3

Fig. B.6

Proportion of Email Traffic Identified as Malicious by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013	2012
1-250	1 in 332.1	1 in 299.2
251-500	1 in 359.4	1 in 325.4
501-1000	1 in 470.3	1 in 314.2
1001-1500	1 in 356.9	1 in 295.0
1501-2500	1 in 483.5	1 in 401.9
2501+	1 in 346.5	1 in 252.1

Fig. B.7

Proportion of Email Traffic Identified as Malicious by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013	2012
United Kingdom	1 in 198.9	1 in 163.2
South Africa	1 in 272.8	1 in 178.1
Austria	1 in 300.7	1 in 262.9
Hungary	1 in 306.8	1 in 289.8
Italy	1 in 370.3	1 in 385.3
Netherlands	1 in 379.5	1 in 108.0
China	1 in 380.8	1 in 358.0
Australia	1 in 399.6	1 in 245.9
United Arab Emirates	1 in 420.6	1 in 462.3
Germany	1 in 429.2	1 in 196.1

Commentary

- The rate of malicious attacks carried out by email has increased for two of the top-ten geographies being targeted and decreased for the other eight; malicious email threats fell in 2013 for organizations in United Kingdom, South Africa, Austria, Hungary, Netherlands, China, Australia and Germany.
- Businesses in the United Kingdom were subjected to the highest average ratio of malicious email-borne threats in 2013, with 1 in 198.9 emails blocked as malicious, compared with 1 in 163.2 in 2012.
- Globally, organizations in the Government and Public sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 95.4 emails blocked as malicious in 2013, compared with 1 in 72.2 for 2012.
- Malicious email threats have decreased for all sizes of organizations, with 1 in 346.5 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2013, compared with 1 in 252.1 in 2012.
- 1 in 332.1 emails were blocked as malicious for small to medium-sized businesses with between 1-250 employees in 2013, compared with 1 in 299.2 in 2012.

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), peer-to-peer file transfers (P2P), and remotely exploitable vulnerabilities.[4] Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a backdoor 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.[5]

Fig. B.8

Propagation Mechanisms

Source: Symantec

Rank	Propagation Mechanisms	2013	Change	2012
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.	70%	-1%	71%
2	**File transfer, CIFS:** 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.	32%	-1%	33%
3	**Remotely exploitable vulnerability:** The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	23%	-3%	26%
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.	8%	+0%	8%
5	**File transfer, HTTP, embedded URI, instant messenger:** The malicious code sends or modifies instant messages with an embedded URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	3%	+0%	3%
6	**File transfer, non-executable file sharing:** The malicious code infects non-executable files.	3%	+0%	3%
7	**Peer-to-peer file sharing**	3%	+0%	3%
8	**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%	+2%	1%
9	**File transfer, instant messenger:** The malicious code sends or modifies instant messages that contain 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%
10	**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%

Commentary

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

- Executable file-sharing activity decreases: In 2013, 70 percent of malicious code propagated as executables, a small decrease from 71 percent in 2012. 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 2013.
- Remotely exploitable vulnerabilities decrease: The percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2013 at 23 percent was 3 percentage points lower than in 2012. Examples of attacks employing this mechanism include Downadup, which gained some momentum and is still a major contributing factor to the threat landscape, ranked in third position in 2012.
- File transfer using CIFS is in decline: The percentage of malicious code that propagated through CIFS file transfer fell by 1 percentage point between 2012 and 2013, a smaller decline than that seen in 2012. Fewer attacks exploited CIFS as an infection vector in 2013.
- File transfer via email attachments remains the same: It is worth noting that file transfer via email attachments remains the same in 2013 compared to 2012. This is justified by 1 in 196.4 emails being identified as malicious in 2013, compared with 1 in 291 in 2012. In 2013, 25.4 percent of email attacks used malicious URLs, compared with 22.5 percent in 2012, which is also an increase.

Email-Targeted Spear-Phishing Attacks Intelligence

Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Over the year 2013, Symantec identified about thirty-thousand spear-phishing emails that were deemed targeted by our threat analysts. Some of these originate from malicious actors that 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 them and identify series of related attacks that might have been sourced by the same (group of) attackers. This will help get a better understanding of attackers' tactics, techniques and procedures (TTPs) as well as their motivation, which can ultimately be used to proactively detect or predict when attackers are coming back with new exploits, or if they use slightly adapted techniques in attempts 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, is challenging. The main reason is that skilled attackers can and will update at least part of their attack tools and methodology in order to maximize their chance of successfully compromising the organizations they are targeting. While changing all aspects of their attack tools or exploit kits might have a prohibitive cost, there is a strong chance that they will adapt their methods over time by investing resources in developing new exploits and adapting their intrusion tools.

As a result it can be challenging for us, as defenders, to determine whether any two spear-phishing attacks were conducted by the same person, by different persons who are collaborating, or by two unrelated hackers who decided independently to compromise the same company or computer. Nevertheless, with enough information, analytical experience, and technological tools to piece it all together, it is possible to reconstruct attack campaigns from raw email data and additional metadata 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 gender and age, the weapon or vehicle used, the various signs left on the crime scene and how it was framed by the criminal), investigators might be able to collect different pieces of evidence which, when put together appropriately, can 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 Distinct Targeted Attack Campaigns Using the Advanced TRIAGE Technology

Symantec advanced TRIAGE[6] data analytics technology aims at reproducing, in an automated fashion, a forensics methodology similar to the one performed by crime investigators, but in the digital world. This framework has been designed to help analysts answer fundamental questions about cyber-attacks, such as:

- *Campaign analysis:* which series of attacks might be related with each other, even though they may be targeting different organizations – on the same or different dates – and use different malware or different exploits?
- What are the attackers' tactics, techniques and procedures (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? Example, what is their prevalence, their 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 has been deliberately selected.
2. Contain at least 3 to 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 "chain of attacks".

One of the challenges in identifying such attack campaigns is that intrusions sourced by the same attackers (or group) may have varying degrees of correlation. Without knowing in advance which features or indicators one should use to correlate attacks, it can be very tedious for analysts to identify groups of related attacks. Figure B.9 illustrates graphically this challenge of varying correlations between three different intrusions that were identified as part of the same campaign. For example, intrusions 1 and 2 are linked by a different set of email features than 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 might be the next move, we have to rely on advanced correlation mechanisms that enable us to identify groups of related attacks (i.e. originating from a specific threat group) without knowing which set of features should be used to associate these attacks to 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	**dd2ed3f7dead4a[***]**		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]

Fig. B.9 Illustration of varying correlations between different intrusions of the same campaign

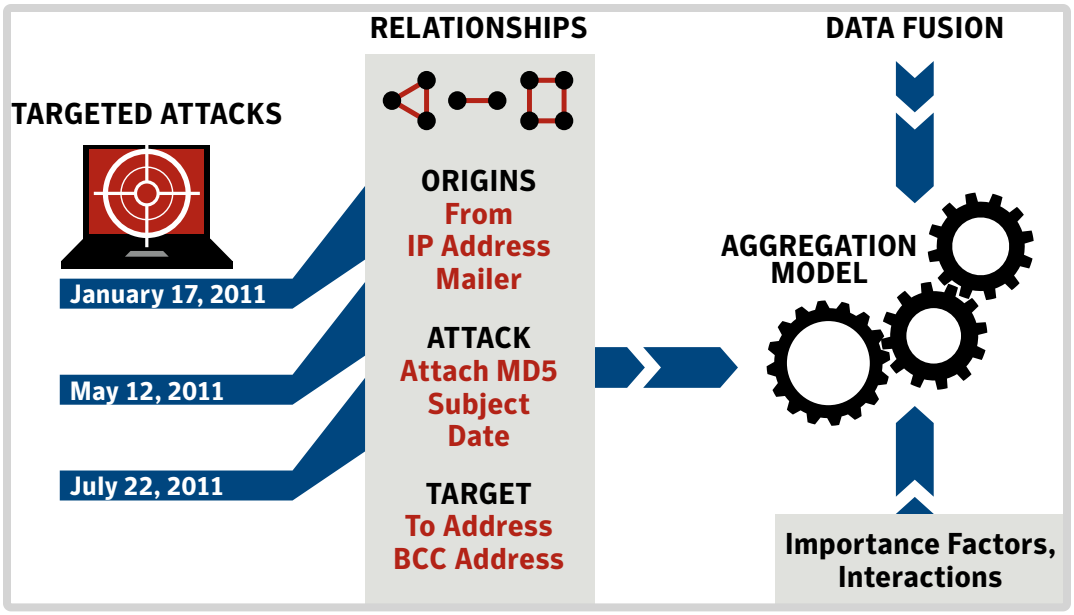


Fig. B.10 Illustration of TRIAGE methodology

By leveraging our TRIAGE data analytics technology, targeted attacks can be automatically grouped together based upon common elements which are likely to reflect 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 insights into the manner by which attack campaigns are orchestrated by various threat actors. The TRIAGE approach is illustrated in Figure B.10.

It is worth mentioning that our TRIAGE framework was recently enhanced with novel visualizations thanks to VIS-SENSE,[7] a European research project aiming 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,[8] spam botnet operations,[9] scam campaigns,[10] and targeted attacks performed via spear-phishing emails[11,12].

Insights into targeted attack campaigns

In 2013 Symantec's TRIAGE technology has identified 779 clusters of spear-phishing attacks (named hereafter "attack campaigns", as defined previously), which are quite likely to reflect different waves of attacks launched by the same groups of individuals. Indeed, within the same cluster, attacks are linked by at least 3 to 4 characteristics among the following:

- 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 (MD5 checksum, AV signature, file name and some metadata coming from both static and dynamic analysis, such as document type or domains and IP addresses contacted by the malware).
- The email subject.
- The targeted recipient ('To:' or 'Bcc:' address fields in the email).

Figure B.11 and Figure B.12 highlight some global metrics calculated across all attack campaigns identified by TRIAGE. To give more perspective to these figures, we compare them to statistics calculated in the past two years (2011-2012), which can generate some insight concerning the characteristics and evolution of spear-phishing campaigns. More specifically, we can clearly identify the following new trends:

- Spear-phishing campaigns seem to be more widespread, with a significant increase in the number of distinct campaigns compared to 2011-2012.
- The average number of attacks per campaign has significantly decreased, which suggests campaigns are becoming more diverse, and possibly more automated. While we have not gathered conclusive evidence about this aspect, we anticipate that attackers are increasingly relying on exploit toolkits such as the Social Engineering Toolkit (SET), the Metasploit framework, and also the large availability of exploit codes on the Internet, which enable more threat groups to leverage this attack vector (spear-phishing emails).
- We observe also that the average duration of a spear-phishing campaign has increased (8.2 days on average), which suggests that these campaigns are much more persistent.

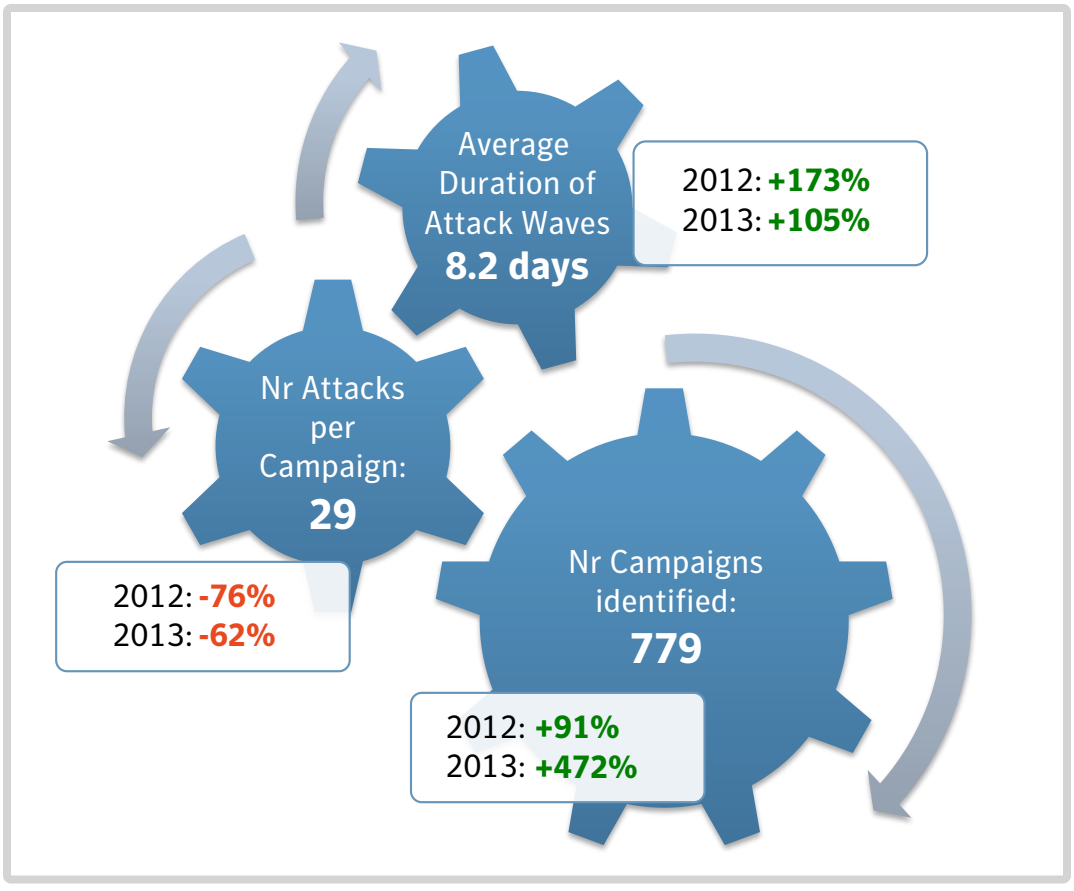


Fig. B.11 Global metrics calculated across all identified campaigns (1)

Figure B.12 highlights other interesting aspects of these targeted attack campaigns:

- The average number of recipients targeted during the same campaign has dropped significantly compared to 2011-2012. This means the vast majority of spear-phishing campaigns are now more focused, and targeted specifically at a small set of companies and individuals.
- Similarly, we observed that the average number of distinct droppers used in the same campaign has decreased by 84 and 60 percent compared to 2012 and 2011, respectively. This suggests that attackers try to be stealthier, and avoid sending attacks in large volumes during the same campaign. On average they will use only two different droppers in the same campaign. However, note that these two different droppers may sometimes contain the very same exploit, which was simply re-packed in two different documents (pdf, doc, xls, etc.)
- Finally, looking at the average number of different industries[13] targeted during the same campaign, we note that this number has increased by 33 and 11 percent compared to 2012 and 2011 respectively, showing an increased prevalence and broader diversification in spear-phishing attacks.

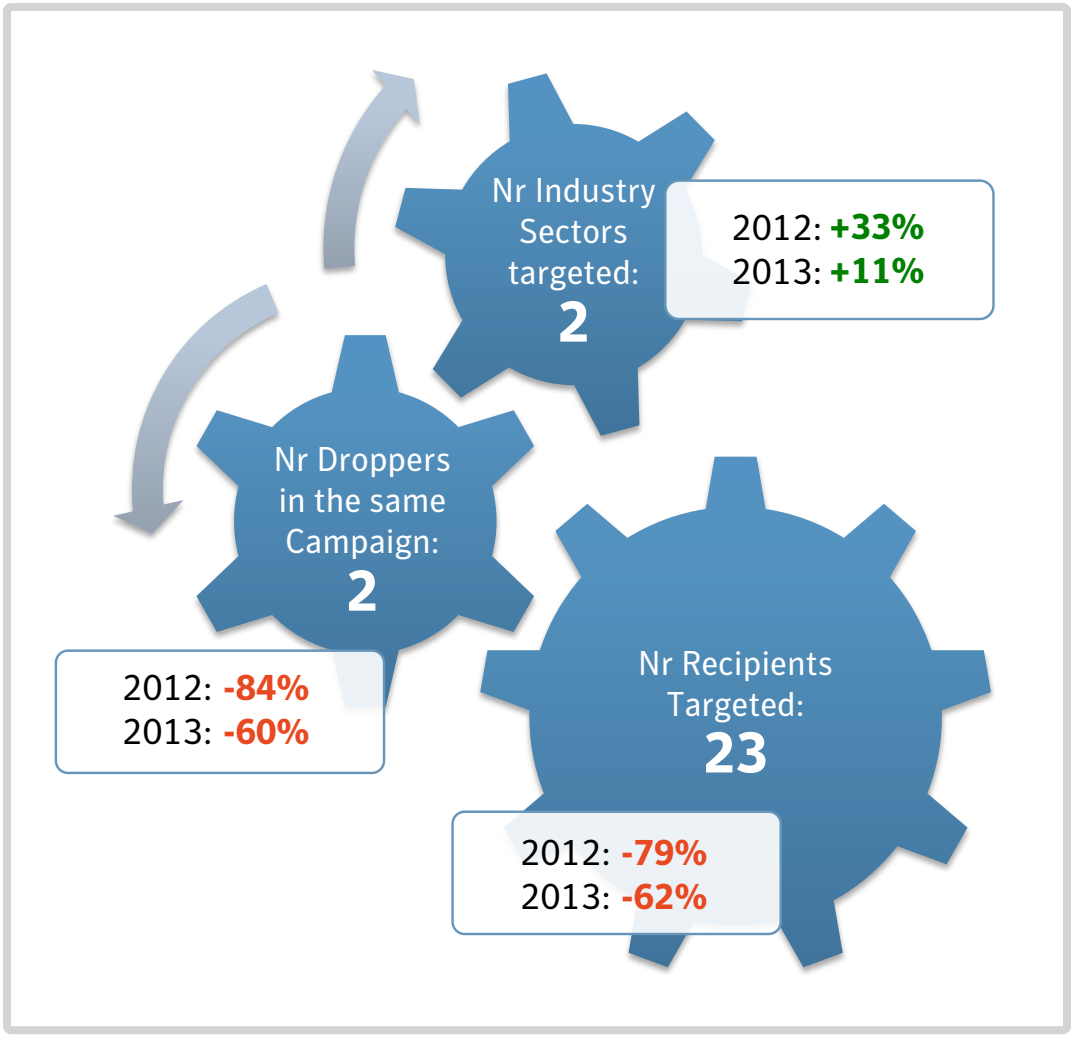


Fig. B.12 Global metrics calculated across all identified campaigns (2)

Highly focused versus Mass-scale campaigns

The 779 distinct campaigns of spear-phishing attacks were then classified into two groups:

- **Type 1:** Highly focused and targeted campaigns
- **Type 2:** Mass-scale Organizational Targeted Campaigns (MOTA)

To this end, we used a combination of two criteria on the number of targeted companies and the number of distinct industry sectors associated to them. Type 1-campaigns are defined as spear-phishing campaigns that had targeted five (or less) distinct companies, in five (or less) different sectors. Spear-phishing campaigns not matching these criteria were deemed as 'Type 2" campaigns, i.e., they fit the profile of so-called *Mass-scale Organizational Targeted Campaigns* (MOTA) because they target a more significant set of different industries having very different lines of business.

Based on the classification defined previously, we found that in 2013 about two-thirds of spear-phishing campaigns were highly focused and targeted a reduced set of companies active in the same or closely related sectors. The other one-third 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 instead involved more large-scale attacks, in the sense that they were targeting a more significant number of companies and organizations active in different sectors.

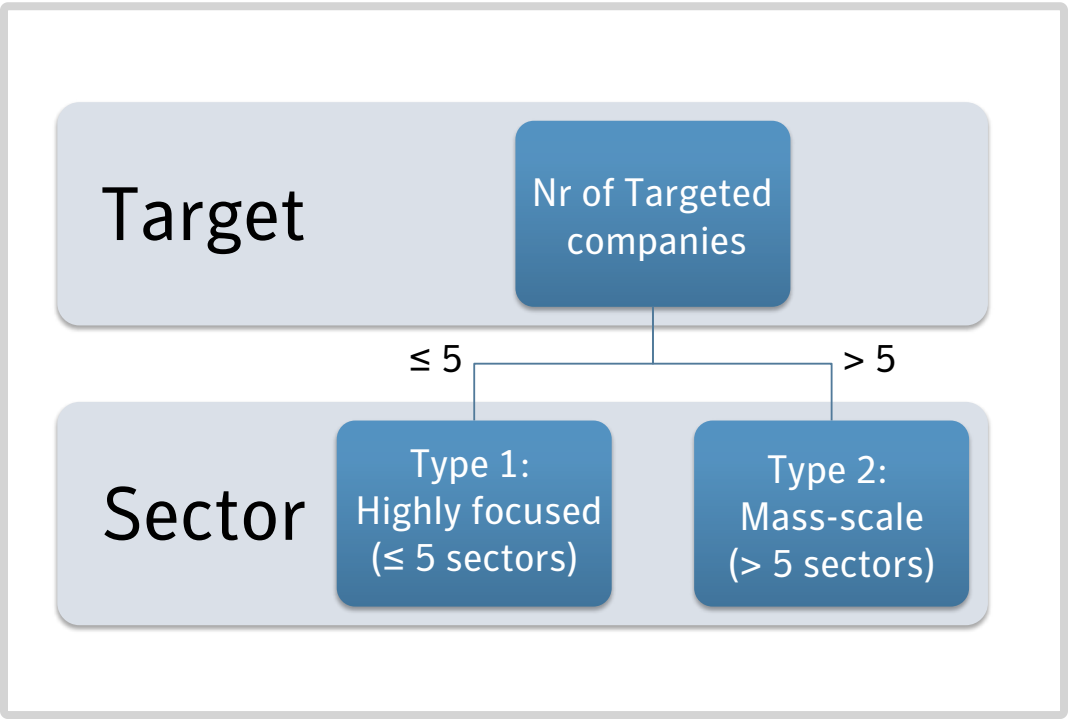


Fig. B.13 Criteria used to classify targeted attack campaigns according to their scale

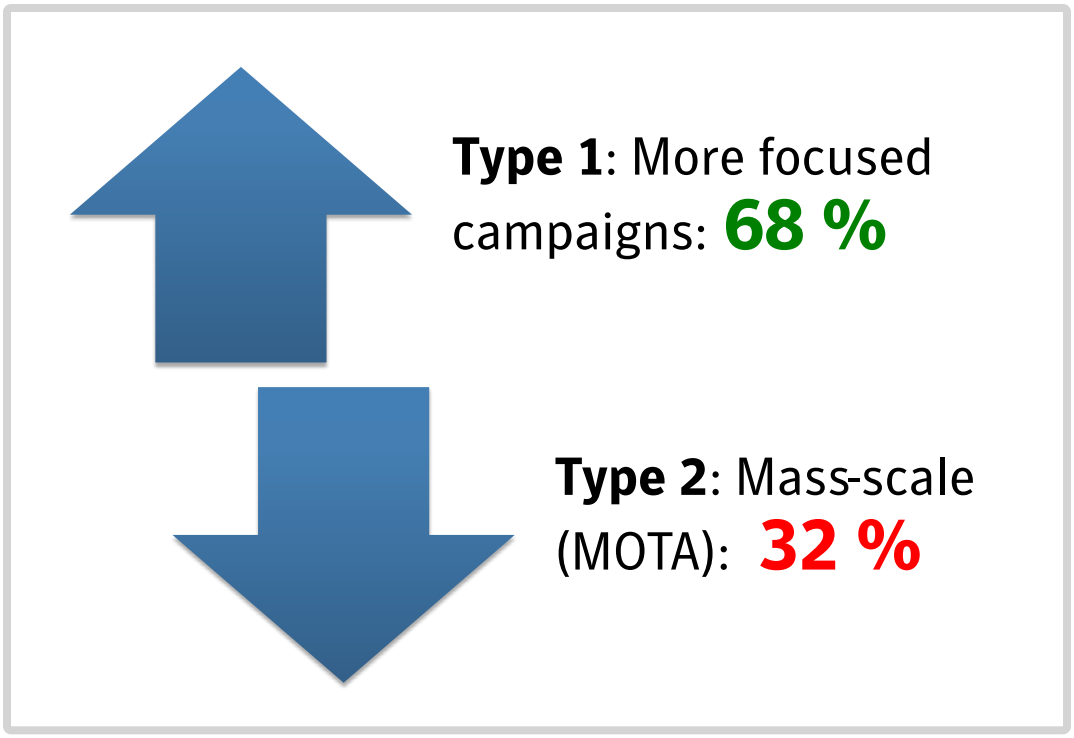


Fig. B.14 Types of campaigns

Type 1 – Highly targeted campaigns

As we have seen, 68 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. One example of such campaigns took place on January 1, 2013 and targeted a global energy research company – hence dubbed the "New Year campaign". As illustrated in Figure B.15, a first wave of spear-phishing emails was sent from two distinct Freemailer accounts to 291 individuals at the targeted company. All receiving email addresses started with a letter between G and R, covering half of the alphabet. Whether there was a second wave of emails using the other half of the alphabet or whether the attackers only got their hands on part of the address book remains unknown.

All emails had either the subject line "2013,Obama QE4! Merry Christmas !" or "2013,Obama QE4!". It is common to see spear-phishing attacks take place around holidays, as people are receiving more emails during these times and are less likely to perform due diligence while opening them. All of the emails contained the same Trojan.Dropper disguised as an attachment with the filename AVP.dll.

The malware itself drops a malicious Downloader "clbcatq.dll" into a newly created "wuauclt" directory, posing as Windows update and taking advantage of the DLL search order hijack weakness in order to load the malicious code in Windows. The same family of dropper was used in previous targeted attacks against other sectors, indicating that a group with multiple interests is behind the attacks. The backdoor provided full access to the compromised computers.

A week later, on January 7, 2013, the group attacked the same company again with another wave of spear-phishing emails (which appears quite clearly in the graph diagram in Figure B.15). Seventy emails were sent to 58 individuals using either "2012-13 NFL Playoffs Schedule" or "Re: 2012-13 NFL Playoffs Schedule" as a subject line. In this wave, the attackers used a similar AVP.dll to the one used before. In some of the emails, an additional CHM file with an old exploit was used in an effort to maximize the chances of a successful infection.

After this second wave, the attack ceased. It is unknown whether the attackers successfully retrieved the information they were seeking, if they installed other backdoor Trojans or gained passwords that allowed them to directly access the computers, or if they had given up on the target. Nevertheless, this "New-Year campaign" illustrates quite well how persistent and determined attackers can be in this type of focused, highly targeted campaign.

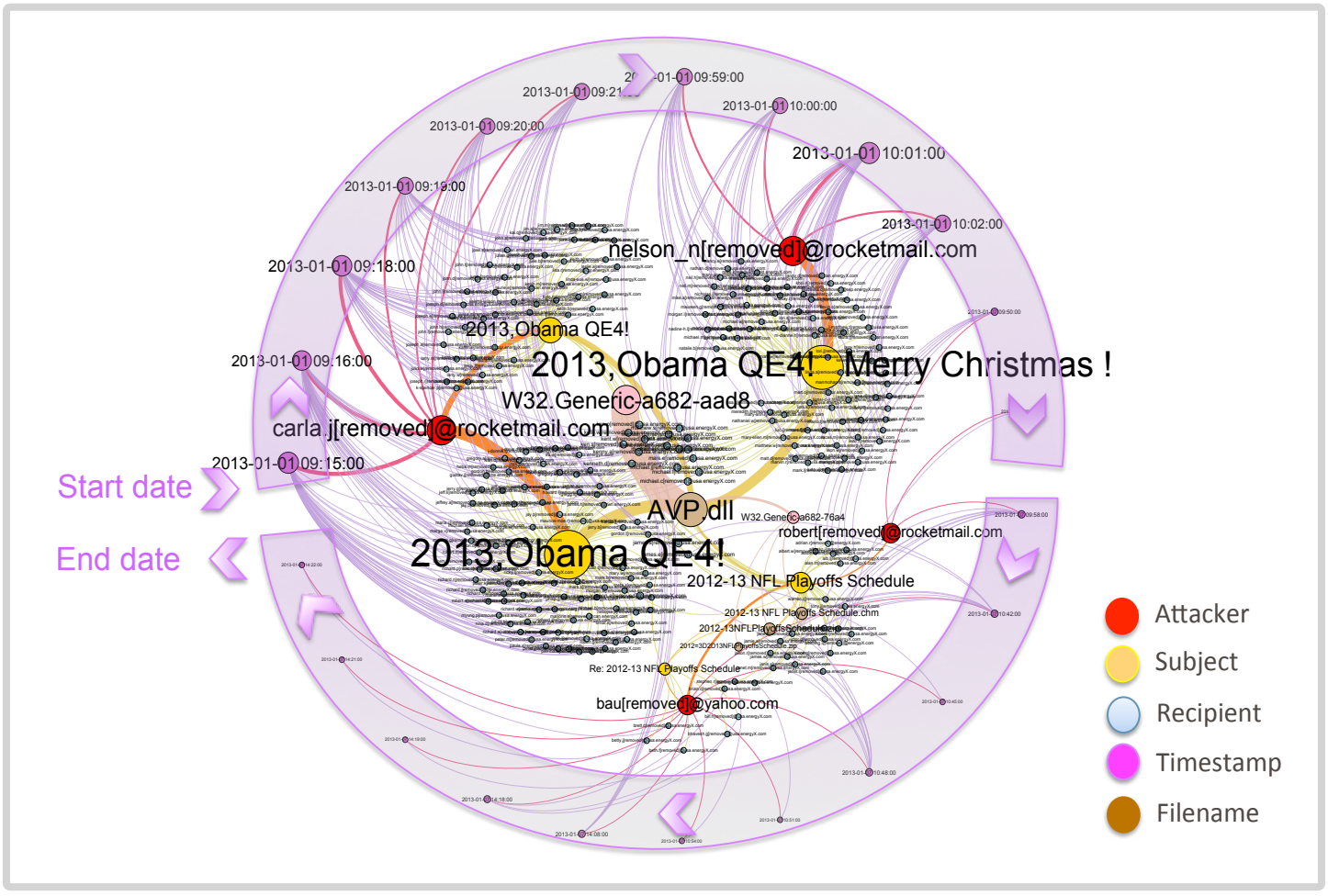


Fig. B.15 The New Year campaign, targeting a large energy research company (zoom for detail)

The Miniduke Campaign – February 20-21, 2013

Another good example of a highly focused attack campaign consisted of a series of targeted attacks launched in February 2013 against governments, which was dubbed "Miniduke" by security experts. The Miniduke campaign targeted dozens of computer systems at government agencies across Europe, in a series of attacks that exploited an Adobe Reader zero-day exploit (subsequently identified as CVE-2013-0640) which was used to drop a previously unknown, advanced piece of malware. An in-depth analysis revealed that this downloader was unique in that every compromised system contained a customized backdoor written in Assembler, suggesting that the authors possessed advanced technical skills. At system boot, the downloader then generated a unique fingerprint on every compromised computer, which was used later to uniquely encrypt the communications with the attacker's servers. An advanced C2 infrastructure had been set up by Miniduke creators, by which all communications between the malware and the C2 servers were initially proxied via Twitter accounts using encoded tweets (or Google searches as a fall-back mechanism); probably as an attempt to fly under the radar, but also to ensure the resilience of their C&C infrastructure.

To compromise their victims, attackers used extremely effective social engineering techniques that involved sending malicious PDF documents with highly relevant topics and well-crafted content informing the victims about a human rights seminar (ASEM), Ukraine's foreign policy, EU-Armenia relationships and NATO membership plans. A sample of email subjects and associated documents and MD5s used in this series of attacks are shown in Figure B.16.

The origins of the attacks (email senders) were identified as being mainly from Armenia, Ukraine, and Korea. Figure B.17 depicts graphically the Miniduke campaign as identified by Symantec's TRIAGE technology. About 208 spear-phishing emails were grouped together and identified as

Fig. B.16

Miniduke Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
Emb of RSA: The 13th Informal ASEM Seminar on Human Rights	ASEM_Seminar.pdf	6945e1fbef586468a6d4f0c4f184af8b ae52908370dcdf6c150b6e2ad3d8b11b 86cc193d9a47fd6a039453159ff35628 a7c89d433f737b3fdc45b9ffbc947c4d
State administration Ukraine: Meeting of the NATO-Ukraine commission	action_plan.pdf	ef90f2927421d61875751a7fe3c7a131 3668b018b4bb080d1875aee346e3650a 151add98eec006f532c635ea3fc205ce ef90f2927421d61875751a7fe3c7a131
MFA of the Republic of Armenia: EU-Armenia Partnership	EUAG_report.pdf	3f301758aa3d5d123a9ddbad1890853b cf5a5239ada9b43592757c0d7bf66169
Armenian MFA: 2013 Economic Meeting in Armenia	The 2013 Armenian Economic Association.pdf	668aaf324ebe42b18e507234281aa772 9c572606a22a756a1fcc76924570e92a cb633268f82f7047c9afa05d1e7f9b19 5ada55c4a39e3280e320b7b6703492dc

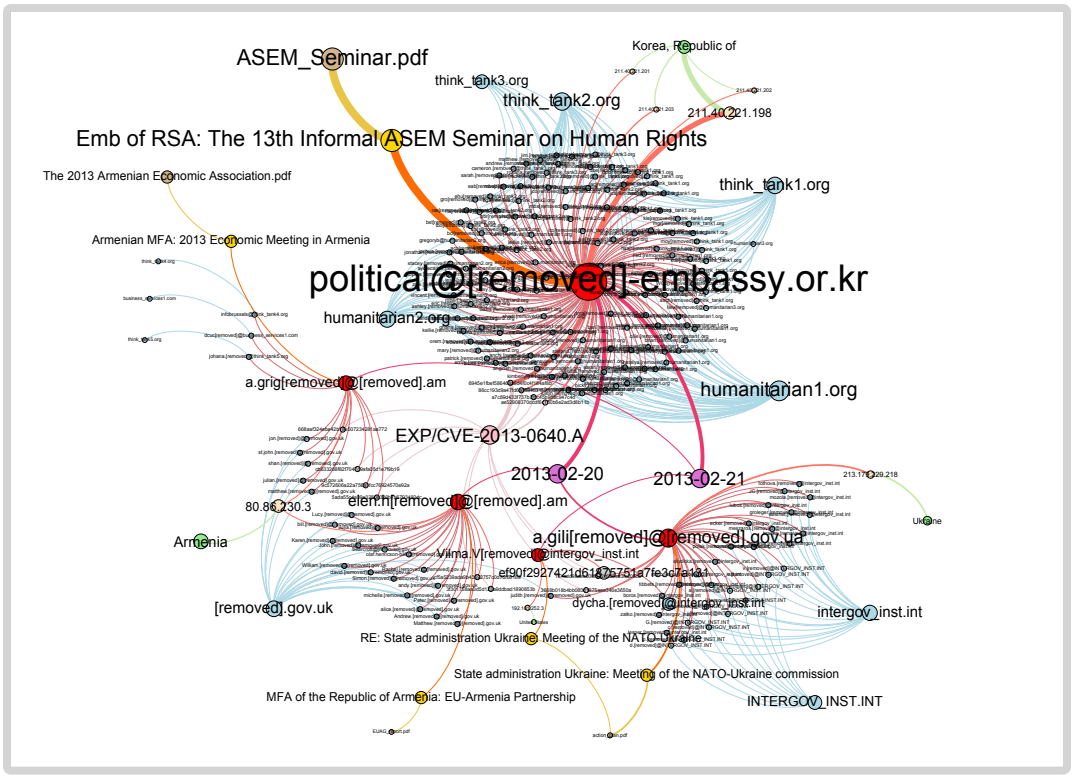


Fig. B.17 The Miniduke campaign (zoom for detail)

being associated with Miniduke. The diagram clearly shows that the bulk of the campaign was sent from a fake email account political@***-embassy.or.kr (whose IP address was mapped to Republic of Korea), targeting 3 different think-tanks and a humanitarian organization using a pdf document containing information on the ASEM human rights seminar.

At least 4 other email accounts (usually spoofed sender addresses) were used by the same group of attackers to target international and governmental institutions on the very same dates (Feb 20-21), this time from IP addresses located in Ukraine and Armenia and using other PDF documents discussing NATO-Ukraine and EU-Armenia political relations.

While we have no visibility into the attacker's ultimate goal, the Miniduke malware was quite likely designed for cyber-espionage and information stealing, just like many other targeted attacks of this kind. However, the sophistication of this cyber attack (in particular the customized malware written in Assembler, and the use of Twitter accounts and Google searches as part of the C2 infrastructure) makes it unusual and quite unique, indicating a type of threat actor that was not observed recently and shows technical traces reminiscent of old-school hackers from the late 1990s. While we can only speculate at this stage regarding the real identity of the authors, the technical indicators[14] and sophistication level of this cyber-attack could very well reflect the involvement, or at least sponsorship, of a nation-state.

As far as we know, Symantec customers have been fully protected from this fairly advanced malware campaign, as the spear-phishing emails sent by Miniduke attackers have been blocked between reaching the mailboxes of their targets.

The Elderwood Campaign: "Focused" does not Always Mean "Small" in Size

While highly targeted cyber-attack campaigns are usually focusing on a limited number of targets, it does not always mean that such campaigns are small in terms of the number of compromise attempts or spear-phishing emails sent by attackers. Unveiled by Symantec in April 2012, the Elderwood project was a good example of an advanced threat group that was capable of launching highly focused, yet large and persistent campaigns. In April 2012, we observed nearly 2,000 spear-phishing emails being sent by the Elderwood attackers within the same campaign to a large number of recipients who were employees of two major defense industries.

The "Elderwood Project"[15] was the name given to the group of attackers behind these targeted attacks, and comes from the exploit communication platform used in some of the attacks. The attack platform developed by this gang also enables them to quickly deploy zero-day exploits.

We have been monitoring the activities of the threat group behind the Elderwood platform for a few years now, which dates back as far as 2009 with the high profile attacks associated with the Hydraq[16] (Aurora) Trojan horse. The Elderwood attackers have consistently targeted a number of industries, and systematically used a number of zero-day exploits against not just the intended target organization, but also on the supply chain manufacturers that service the company in their cross-hairs. The attacking methodology has always used spear-phishing emails, but since 2012 we have observed an increased adoption of watering-hole attacks (compromising certain websites likely to be visited by individuals associated with the target organization) used in combination with spear-phishing emails as additional attack vectors used by the same attackers probably to maximize their success rate.

Serious zero-day vulnerabilities which are exploited in the wild and affect a widely used piece of software are relatively rare. However, the Elderwood attackers were able to exploit no less than four such zero-day vulnerabilities within the same cyber-attack campaign. Although there are other threat groups utilizing zero-day exploits (for example, the Miniduke, Sykipot,[17] Nitro,[18] or even Stuxnet[19] attacks), we have seen no other group use so many. The number of zero-day exploits used indicates access to a high level of technical capability.

Figure B.19 illustrates visually the Elderwood spear-phishing campaign identified by Symantec's advanced TRIAGE technology, which was blocked by Symantec in April 2012. In this campaign, a large number of email accounts (depicted with red nodes) were used by the attackers to send about 1,800 spear-phishing emails (whose subjects are depicted with yellow nodes) to the same amount of employees of two different organizations involved in the defense industry (represented with blue nodes). Only a few different MD5's were used as email attachments to try to compromise the targets, but all documents were dropping the same backdoor connecting to the same C&C servers (denoted with green nodes in the diagram). Interestingly, a large proportion of emails were sent apparently from the same mailer software (Foxmail 6). All email subjects (yellow nodes laid out on the external side of the visualization) were customized to every recipient (by adding his/her user name). The overall patterns visualized in Figure B.19 strongly suggest that attackers were able to automate the sending process of this series of cyber attacks. A sample of email subjects and associated documents and MD5s used in this Elderwood campaign are shown below in Figure B.18.

Fig. B.18

Elderwood Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
Wage Data 2012	page 1-2.doc	c0c83fe9f21560c3be8dd13876c11098
London 2012 Medal Top-Ten	MedalTop10.doc	919708b75b1087f863b6b49a71eb133d
Message from Anne regarding *** Organizational Announcement!	Message_from_PerInge.doc	8b47310c168f22c72a263437f2d246d0
The *** is in the unpromising situation after acquisition by ***	create.doc	4525759c6452f2855ca815277f519684
Hi, [REM]. I heard about the consolidation of ***, is that true?	Consolidation Schedule.doc	78c3d73e2e2bba6d8811c5dc39edd600
Invitation Letter to LED Industry Summit 2012.	[REM] Invitation Letter to LED Industry Summit 2012.doc	4525759c6452f2855ca815277f519684 84a1405c9e96c037a9d332def39f2d29

A few striking elements are standing out in Figure B.19, where we can identify some less volatile email features, such as:

- Mailer software used by attackers (which in most cases was Foxmail 6, 14, 103, 30 [cn], but also in a limited number of attacks, KooMail 5.41 [En] was also used to send emails).
- Domain name and IP address used as part of the C&C infrastructure (green nodes in the center).
- Limited number of email accounts (webmail1.com[20]) used to send attack emails in separate batches to subsets of recipients.

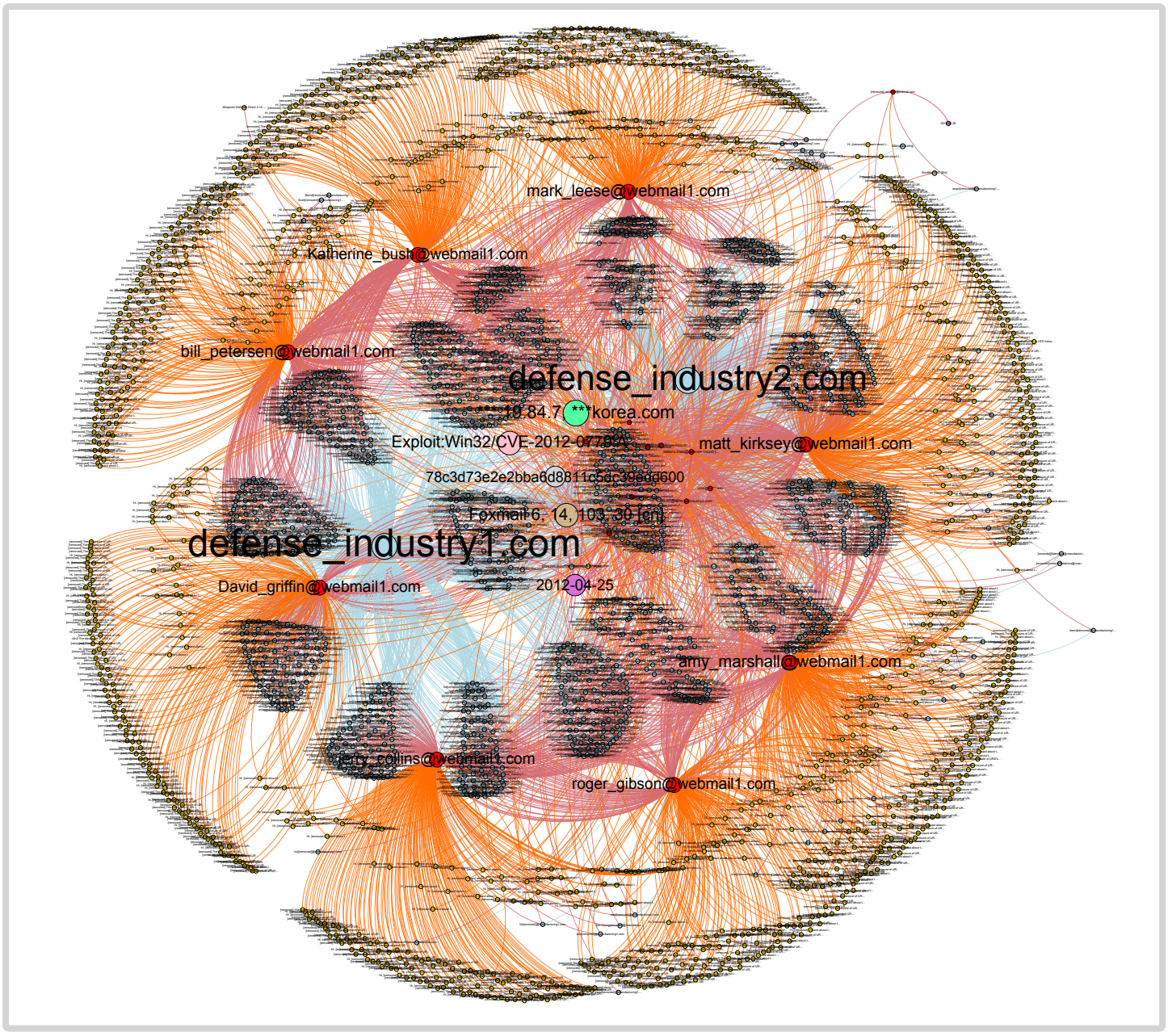


Fig. B.19 The Elderwood campaign: A highly focused campaign but large in size and likely automated (zoom for detail)

Type 2 – Mass-scale Organizational Targeted Attacks (MOTA)

One third of targeted attacks are organized on a larger-scale and fit the profile of what we call a Mass-scale Organizationally Targeted Attack (MOTA): they 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 "Mass-scale" (MOTA) versus "highly focused". Most of the large-scale campaigns are very well resourced, with up to four different exploits used during the same campaign.

One example of attacker group that is typically responsible for organizing MOTA-like campaigns is APT1, also known as "CommentCrew". An example of a campaign attributed to CommentCrew is visualized in Figure B.20. During this campaign, about 1,200 attack emails were sent from 44 email accounts (red nodes) to 191 different recipients (blue nodes) who are employees working in more than 20 different companies, active mainly in sectors such as Aerospace, Defense, Engineering, Satellite communications and Governmental organizations. Attack emails were sent on 10 different dates, however the whole campaign lasted for more than two months in April/May 2012. During this timeframe CommentCrew attackers were able to craft a significant number of very diverse phishing emails, all of them containing malicious documents exploiting various vulnerabilities in MS Office or Adobe software, in attempts to compromise their victims. A sample of email subjects and associated documents and MD5s used in this series of attacks are shown below in Figure B.21.

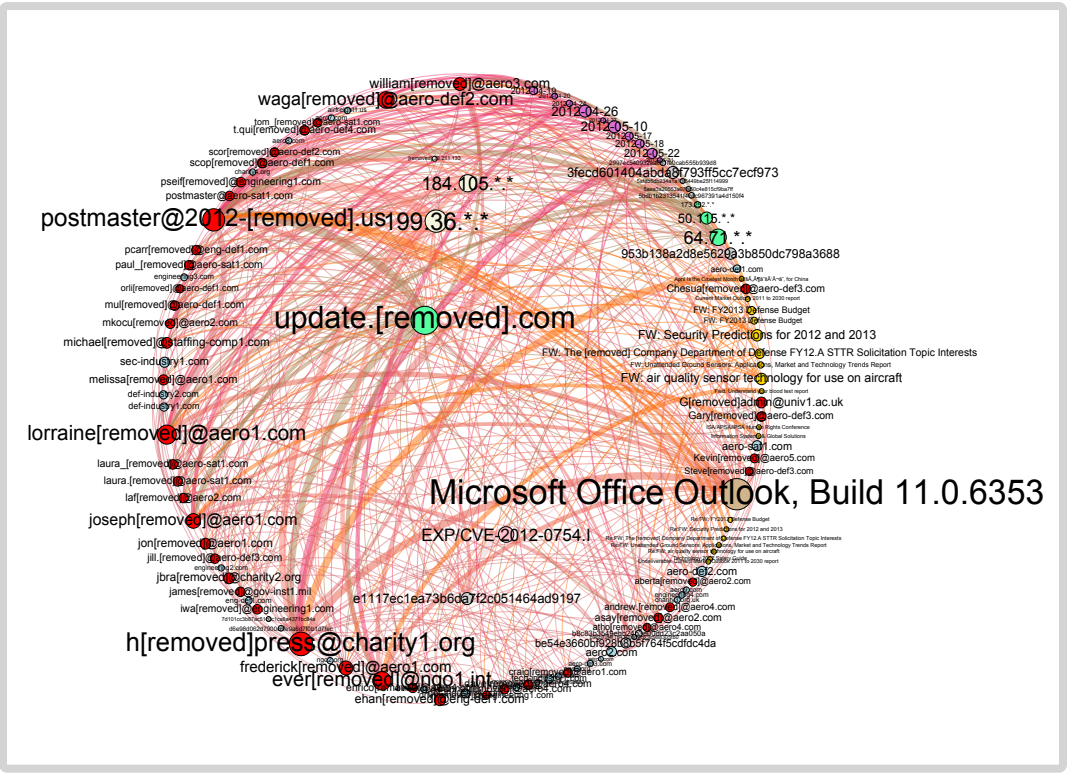


Fig. B.20 A campaign of attacks attributed to the CommentCrew group (April-May 2012) (zoom for detail)

Fig. B.21

APT1 Sample of Email Subjects, Documents, and MD5s

Source: Symantec.cloud

Subjects	Documents	Associated MD5's
April Is the Cruelest Month … for China	April Is the Cruelest Month.pdf	5afdb5db234a1a13f5449be25f114999 2997ec540932ea6b1fe0cab555b939d8
FW: air quality sensor technology for use on aircraft	sensor environments.doc	3fecd601404abda8f793ff5cc7ecf973
FW: Security Predictions for 2012 and 2013	Security Predictions for 2012 and 2013.pdf	e1117ec1ea73b6da7f2c051464ad9197 d795292ea23217480ad92939daf6dd22
FW: FY2013 Defense Budget	FY2013_Budget_Request_Overview_Book.pdf	953b138a2d8e5629a3b850dc798a3688
Fwd: Understand your blood test report	Understand your blood test report.pdf	5aea3a20553a07fa50c4e815cf9ba7ff
Information Systems & Global Solutions	Schedule_list.pdf	b96b79f4f1b4306ac2c63fc988305fb0
FW: The *** Company Department of Defense FY12.A STTR Solicitation Topic Interests	Dept of Defense FY12 A STTR Solicitation Topics of Interest to <aerospace comp>.pdf	be54e3660bf928b8b5f764f5cdfdc4da
Current Market Outlook 2011 to 2030 report	[REM]_Current_Market_Outlook_2011_to_2030.pdf	d6e98d062d7900c6fe9a6d7f0b1d7fec
Technology 2012 Salary Guide	RHT_SalaryGuide_2012.pdf	5bdb1b2313541f4cdc967391a4d150f4
ISA/APSA/IPSA Human Rights Conference	HR 2012 Conference Program .doc	7d101cc3b87ac51c0c1ca8a4371bc84a
Re:FW: air quality sensor technology for use on aircraft	sensor environments.doc	3fecd601404abda8f793ff5cc7ecf973

Symantec's TRIAGE technology also identified another spear-phishing campaign attributed to CommentCrew, which took place on January 16, 2013, and is illustrated in Figure B.22. This attack campaign occurred a few weeks before the release by Mandiant of a report exposing Comment-Crew's multi-year, enterprise-scale computer espionage campaigns, in which they investigated computer security breaches made by the CommentCrew group at hundreds of organizations around the world. According to many experts, CommentCrew is one of the most prolific cyber-espionage groups in terms of the sheer quantity of information stolen.

Although our visibility of CommentCrew's activities is likely to be incomplete, we could analyze a number of intrusions that this threat group conducted against more than 30 companies just in the last 2 years. Figure B.22 shows one of the last series of targeted attacks performed by the group that we could observe just before the publication of Mandiant's report on their espionage activities. About 77 victims working in 16 different companies were targeted using the very same document (*Global_A&D_outlook_2012.pdf - 578de4091ed0b2752012668d59828fe2*) and similar email topics (*FW:2012 Global aerospace and defense industry outlook*). However, CommentCrew attackers have used different fake email accounts to conduct their attacks, as shown in the diagram in Figure B.22.

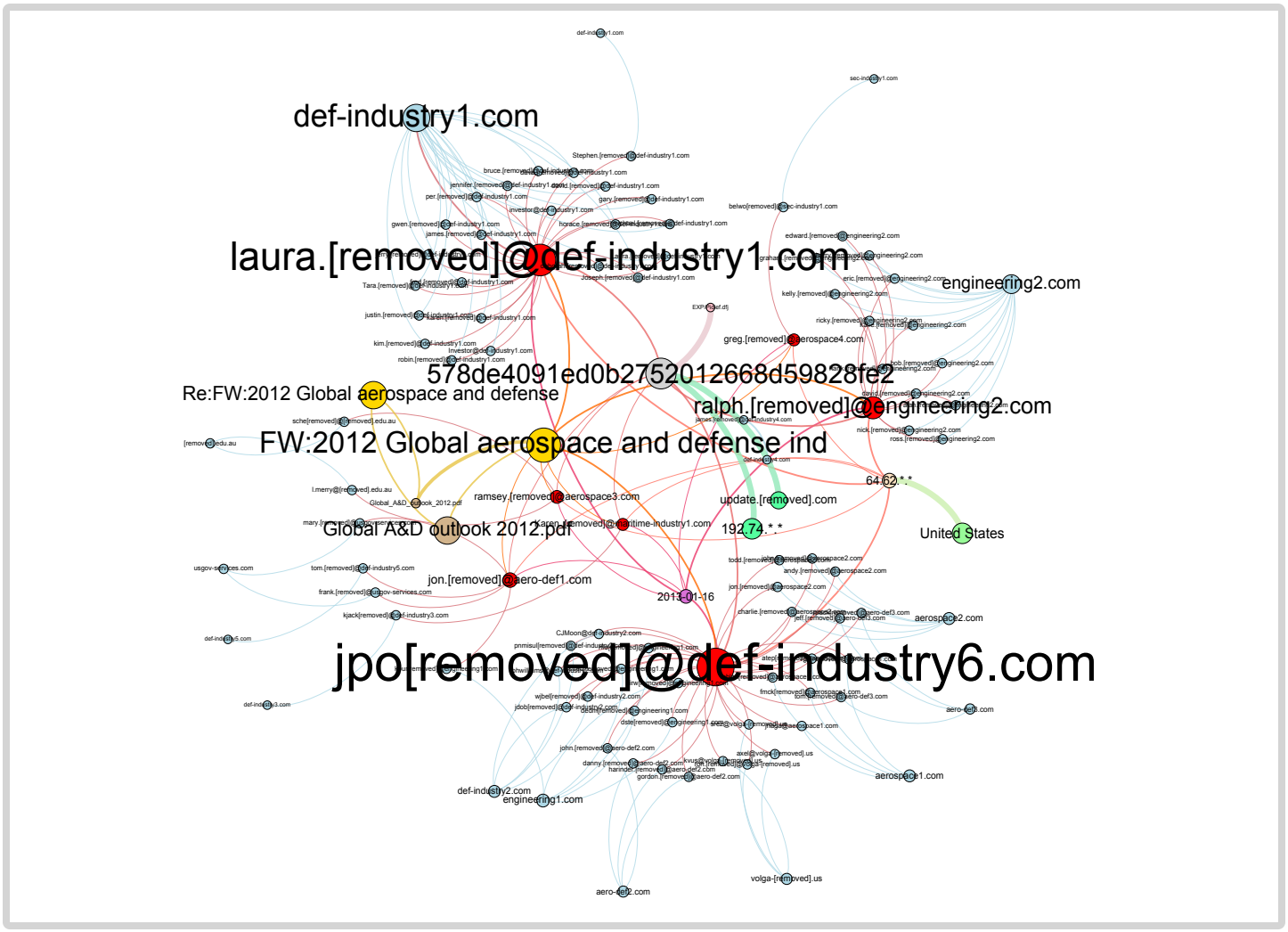


Fig. B.22 CommentCrew campaign identified in January 2013. (zoom for detail)

Footnotes

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

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

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

04 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.

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

06 Developed by Symantec in the context of the European funded WOMBAT research project (http://www.wombat-project.eu), TRIAGE is a novel attack attribution method based on a multi-criteria decision algorithm. TRIAGE is currently improved and enriched with Visual Analytics technologies in the context of another European funded research project named VIS-SENSE (http://www.vis-sense.eu), in which Symantec collaborates with five other partners.

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

08 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.

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

10 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.

11 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.

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

13 Targeted recipients and domains were mapped to industry sectors based on the SIC taxonomy. This allows us to collect statistics on the prevalence of targeted attacks in various industry sectors.

14 http://www.symantec.com/security_response/writeup.jsp?docid=2013-030119-2820-99

15 http://www.symantec.com/connect/blogs/elderwood-project

16 http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99

17 http://www.symantec.com/security_response/writeup.jsp?docid=2010-031015-0224-99

18 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

19 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

20 Domain names have been anonymized or obfuscated for privacy reasons.

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"[1] 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 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
- Significant Spam Tactics
- Analysis of Spam by Categorization
- Phishing Activity Trends
- Analysis of Phishing Activity by Geography, Industry Sector, and Company Size
- New Spam Trend: BGP Hijacking

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 2013.

Methodology

The analysis for this section is based on global spam and overall email volumes for 2013. Global values are determined based on the statistically representative sample provided by Symantec Messaging Gateway[2] operations, and the spam rates include spam blocked by Symantec.cloud.

Commentary

- There were approximately 29 billion spam emails in circulation worldwide each day in 2013, compared with 30 billion in 2012; a decrease of 3.3 percent in global spam volume.
- Overall for 2013, 66.4 percent of email traffic was identified as spam, compared with 68.5 percent in 2012; a decrease of 1.9 percentage points.

Fig. C.1

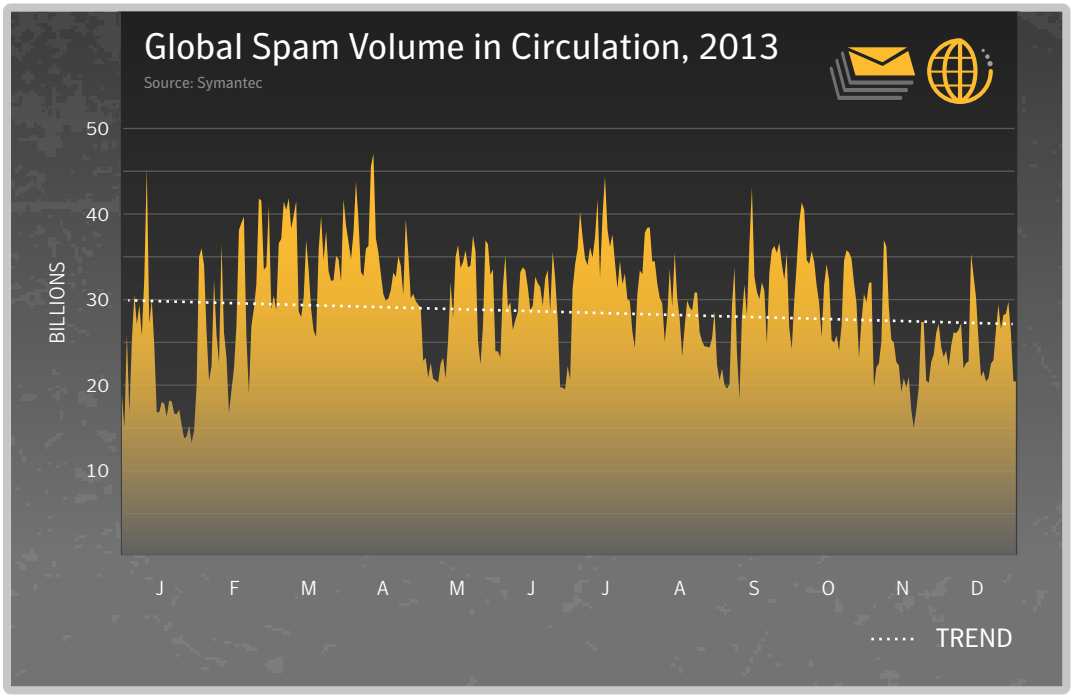
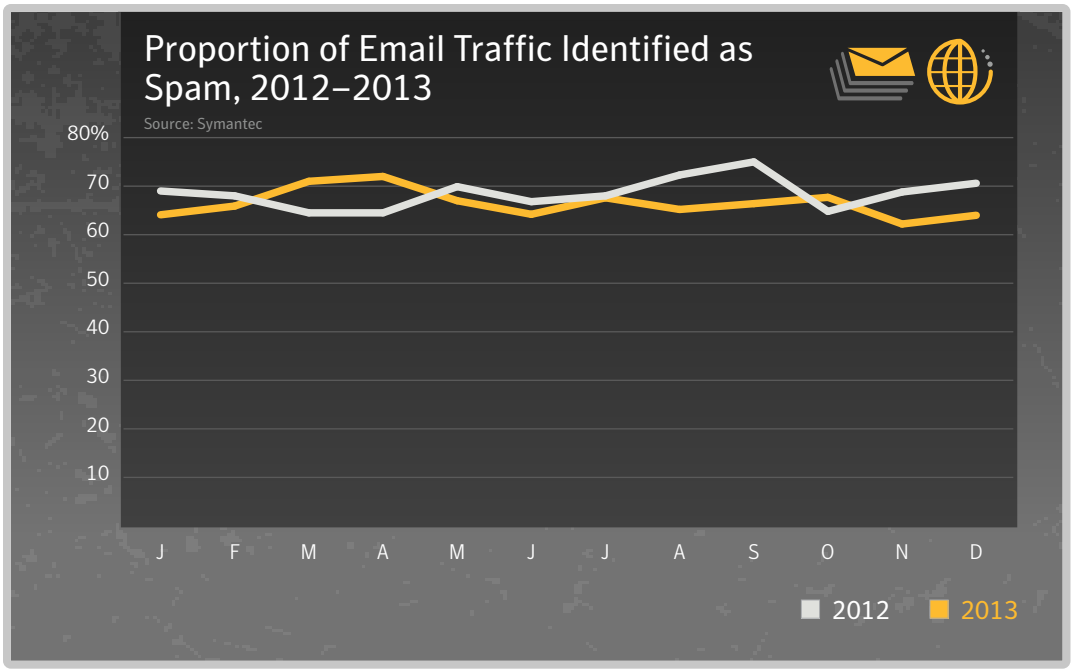


Fig. C.2


Proportion of Email Traffic Identified as Spam, 2012–2013
Source: Symantec
80%
70
60
50
40
30
20
10
J
F
M
A
M
J
J
A
S
O
N
D
2012
2013

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 that can drive down prices, increasing adoption rates. There may also be other factors at work, based on the local economic conditions that present different risk factors. Similarly the industry sector may also have an influence on an organization's risk factor, where 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 their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a spam attack because they are perceived to be a softer target than larger organizations. They are likely to have less-stringent security countermeasures than larger organizations, which are more likely to apply greater resources to their anti-spam and security countermeasures.

Methodology

Analysis of spam activity based on geography, industry and size is determined from the patterns of spam activity for Symantec. cloud clients for threats during 2013.

Fig. C.3

Proportion of Email Traffic Identified as Spam by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013 Spam	2012 Spam
Finance	73.0%	67.8%
Education	67.4%	70.5%
Chem/Pharm	66.5%	68.5%
Non-Profit	66.4%	69.6%
Manufacturing	66.0%	69.1%
Marketing/Media	65.9%	69.3%
Accom/Catering	65.9%	68.7%
Recreation	65.7%	69.0%
Gov/Public Sector	65.5%	68.9%
Agriculture	65.4%	68.9%

Fig. C.4

Proportion of Email Traffic Identified as Spam by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013 Spam	2012 Spam
1-250	70.4%	68.4%
251-500	65.4%	68.2%
501-1000	65.2%	68.3%
1001-1500	65.6%	68.8%
1501-2500	65.6%	68.9%
2501+	65.6%	68.4%

Fig. C.5

Proportion of Email Traffic Identified as Spam by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013 Spam	2012 Spam
Saudi Arabia	78.2%	79.1%
Sri Lanka	75.7%	73.1%
China	71.3%	73.3%
Hungary	71.1%	74.2%
Qatar	69.9%	72.6%
Brazil	69.7%	72.5%
Ecuador	69.6%	71.2%
Greece	68.9%	67.7%
Poland	68.6%	71.2%
India	68.5%	70.4%

Commentary

- The spam rate decreased across all top-ten geographies in 2013. The highest rate of spam is for organizations in Saudi Arabia, with an overall average spam rate of 78.2 percent. In 2012 the highest rate was also in Saudi Arabia, with an overall average spam rate of 79.1 percent.
- The spam rate decreased across all top-ten industry sectors in 2013 except for Finance, in which organizations were subjected to the highest spam rate of 73.0 percent. In 2012, the Marketing/Media sector had the highest spam rate of 69.3 percent.
- The spam rate decreased for all sizes of organization in 2013, except for small to medium-sized businesses with 1-250 employees. These organizations accounted for 70.4 percent of spam compared to 68.4 percent in 2012.
- 65.6 percent of emails sent to large enterprises with more than 2,500 employees in 2013 were identified as spam, compared with 68.4 percent in 2012.

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 SMTP[3] transactions. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis only reviews botnets involved in sending spam, and does not look at botnets used for other purposes such as financial fraud or DDoS attacks.

Methodology

Symantec.cloud spam honeypots collected approximately 15 million spam emails each day during 2013. 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.

Fig. C.6

Top Sources of Botnet Spam by Location, 2013

Source: Symantec.cloud

Location of Botnet Activity	Percentage of Botnet Spam
India	6.6%
United States	5.9%
Spain	5.2%
Argentina	5.1%
Peru	4.4%
Italy	3.9%
Iran	3.1%
Russia	2.9%
Colombia	2.9%
Vietnam	2.7%

Fig. C.7

Analysis of Spam-Sending Botnet Activity at the End of 2013

Source: Symantec.cloud

Botnet Name	Percentage of Botnet Spam	Est. Spam Per Day	Top Sources of Spam From Botnet		
KELIHOS	46.90%	10.41BN	Spain 8.4%	United States 7.2%	India 6.6%
CUTWAIL	36.33%	8.06BN	India 7.7%	Peru 7.5%	Argentina 4.8%
DARKMAILER	7.21%	1.60BN	Russia 12.4%	Poland 8.3%	United States 8.1%
MAAZBEN	2.70%	598.12M	China 23.6%	United States 8.2%	Russia 4.8%
DARKMAILER3	2.58%	573.33M	United States 18.2%	France 10.4%	Poland 7.5%
UNCLASSIFIED[4]	1.17%	259.03M	China 35.1%	United States 10.0%	Russia 7.5%
FESTI	0.81%	178.89M	China 21.9%	Russia 5.8%	Ukraine 4.7%
DARKMAILER2	0.72%	158.73M	United States 12.6%	Belarus 8.3%	Poland 6.6%
GRUM	0.53%	118.00M	Russia 14.5%	Argentina 6.9%	India 6.9%
GHEG	0.35%	76.81M	Poland 17.4%	Vietnam 12.1%	India 11.5%

Commentary

- In 2013, approximately 76 percent of spam email was distributed by spam-sending botnets, compared with 79 percent in 2012. Ongoing actions to disrupt a number of botnet activities during the year helped to contribute to this gradual decline.
- The takedown of ZeroAccess Botnet resulted in the disruption of over half a million bots controlled by the botmaster.[5]
- The top two spam botnets, Kelihos and Cutwail were responsible for more than 83 percent of spam, generating an estimated 10 billion and 8 billion spam emails each day, respectively.
- India was top of the spam-sending botnet table in 2013, and was the source of approximately 6.6 percent of global botnet spam, 0.7 percentage points higher than the United States.

Significant Spam Tactics

Background

This section discusses significant spam tactics used throughout 2013, including the size of spam messages and the languages used in spam emails.

Fig. C.8

Frequency of Spam Messages by Size, 2013

Source: Symantec

Size	<5KB	5KB-10KB	10KB-50kb	50KB-100KB	>100KB
Percentage of Spam	32.8%	29.5%	27.0%	0.8%	1.0%

Fig. C.9

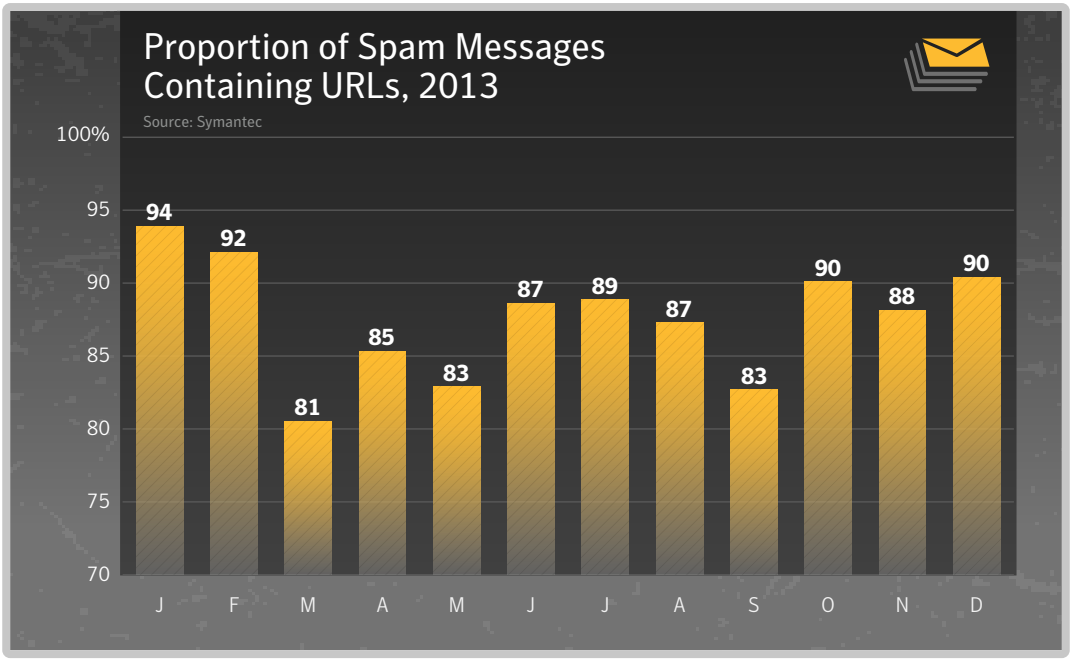


Fig. C.10

Analysis of Top-Level Domains Used in Spam URLs, 2013

Source: Symantec

Domains	Spam Percentage
.com	33.3%
.ru	22.9%
.pl	35.5%
.info	10.2%
.net	6.5%

Commentary

- In 2013, 32.8 percent of spam messages were less than 5KB in size. For spammers, smaller file sizes mean more messages can be sent using the same resources.
- Increased sizes are often associated with malicious activity, where email attachments contain malicious executable code.
- In 2013, 87.3 percent of spam messages contained at least one URL hyperlink, compared with 86.1 percent in 2012.
- In 2013, 35.5 percent of spam URLs were domains registered in the .pl top-level domain (TLD).
- The second most frequently used TLD was .com, which accounted for approximately 33.3 percent of all spam URL domains.
- The third most frequently used TLD was .ru, which is the top-level country code domain for Russia and accounted for approximately 22.9 percent of all spam URL domains.

Analysis of Spam by Categorization

Background

Spam is created in a variety of different styles and complexities. Some spam is plain text with a URL, while others are cluttered with images and/or attachments. Some are constructed with very little in terms of text, perhaps only a URL. And, of course, spam is distributed in a variety of different languages. It is also common for spam to contain "Bayes poison" – random text added to messages that has been haphazardly scraped from websites, with the purpose of "polluting" the spam with words bearing no relation to the intent of the spam message itself. Bayes poison is used to thwart spam filters that typically try to deduce spam based on a database of words that are frequently repeated in spam messages.

Any automated process to classify spam into categories needs to overcome this randomness issue. For example, the word "watch" may appear in the random text included in a pharmaceutical spam message, posing a challenge whether to classify the message as pharmaceutical spam or in the watches/jewelry category. Another challenge occurs when a pharmaceutical spam contains no words with an obvious relation to pharmaceuticals, but instead only contain an image and a URL.

Spammers attempt to get their messages through to recipients without revealing too many clues that the message is spam. Clues found in the plain text content of the email can be examined using automated anti-spam techniques. A common way to overcome automated techniques is by using random text. An equally effective way is to include very little in the way of extra text in the spam, instead including a URL in the body of the message.

Spam detection services often resist classifying spam into different categories because it is difficult to do (for the reasons above), and because the purpose of spam detection is to determine whether the message is spam and to block it rather than to identify its subject matter. In order to overcome the ambiguity faced by using automated techniques to classify spam, the most accurate way to do it is to have someone classify unknown spam manually. While time-consuming, this process provides much more accurate results. An analyst can read the message, understand the context of the email, view images, follow URLs, and visit websites in order to gather the bigger picture around the spam message.

Methodology

Once per month, several thousand random spam samples are collected and classified by Symantec.cloud using a combination of electronic and human analysis into one of the following categories:

- Casino/Gambling
- Degrees/Diplomas
- Diet/Weight Loss
- Jobs/Money Mules
- Malware
- Mobile Phones
- Pharmaceutical
- Phishing
- Scams/Fraud/419s
- Sexual/Dating
- Software
- Unknown/Other
- Unsolicited Newsletters
- Watches/Jewelry

Fig. C.11

Spam by Category, 2013

Source: Symantec.cloud

Category	2013	2012	Change (percentage points)
Pharmaceutical	17.7%	21.1%	-3.4
Watches/Jewelry	2.8%	9.2%	-6.4
Sexual/Dating	69.7%	54.6%	+15.1
Unsolicited Newsletters	0.1%	7.4%	-7.3
Casino/Gambling	0.6%	1.6%	-1.0
Diet/Weight Loss	1.1%	1.0%	+0.1
Malware	0.1%	1.9%	-1.8
Unknown/Other	1.0%	2.4%	-1.4%
Scams/Fraud/419s	0.2%	0.4%	-0.2
Software	0.9%	2.1%	-1.2
Jobs/Money Mules	6.2%	4.4%	+1.8
Degrees/Diplomas	0.1%	0.3%	-0.1
Mobile Phones	0.4%	0.6%	-0.2
Phishing	0.2%	0.4%	-0.2

Commentary

- Adult Spam dominated in 2013, with more than two-thirds (69.7 percent) of all spam related to adult spam, an increase of 15.1 percentage points compared with 2012. These are often email messages inviting the recipient to connect to the scammer through instant messaging, or a URL hyperlink where they are then typically invited to a pay-per-view adult-content webcam site. Often any IM conversation would be handled by a bot responder, or a person working in a low-pay, offshore call center.
- A category with a low percentage still means millions of spam messages. Although it is difficult to be certain what the true volume of spam in circulation is at any given time, Symantec estimates that approximately 29 billion spam emails were sent globally each day in 2013. Where some of the categories listed earlier represent 0.4 percent of spam, this figure equates to more than 120 million spam emails in a single day.
- Spam related to Watches/Jewelry, Casino/Gambling, Unsolicited Newsletters and Scams/Fraud all decreased.

Phishing Activity Trends

Background

This section discusses the proportion of malicious email activity that is categorized as phishing attacks and looks more closely at emerging trends, particularly social engineering techniques and how attackers can automate the use of RSS news feeds to incorporate news and current affairs stories into their scams.

Methodology

The data for this section is based on the analysis of email traffic collected from Symantec.cloud global honeypots, and from the analysis of malicious and unwanted email traffic data collected from customers worldwide. The analysis of phishing trends is based on emails processed by Symantec.cloud Skeptic™ technology[6] and emails collected in spam honeypots. Symantec.cloud spam honeypots collected approximately 15 million spam emails each day during 2013.

Fig. C.12

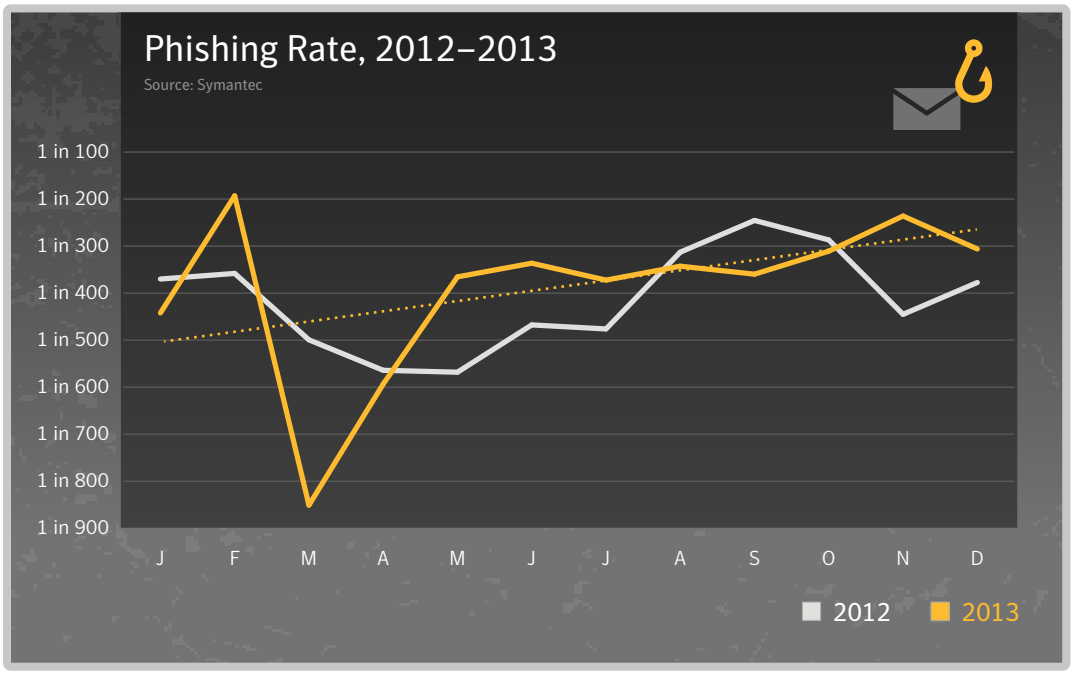


Fig. C.13

Phishing Category Types, Top 200 Organizations, 2013

Source: Symantec.cloud

Sectors	Phishing Percentage
Financial	71.7%
Information Services	21.0%
Others	7.0%
Government	0.2%

Others	Phishing Percentage
Telecommunications	5.2%
Retail	47.0%
Communications	10.7%
Retail Trade	0.6%
Security	0.1%
ISP	0.4%
Insurance	0.4%
Aviation	0.1%
Computer Software	25.5%
Entertainment	6.4%
Electronics	0.0%
Energy	3.3%

Fig. C.14

Tactics of Phishing Distribution, 2013

Source: Symantec.cloud

Attack Type	Phishing Percentage
Typosquatting	1.1%
Free Web Hosting Sites	3.7%
IP Address Domains	4.9%
Other Unique Domains	41.0%
Automated Toolkits	49.3%

Commentary

- Overall for 2013, 1 in 392.4 emails was identified and blocked as a phishing attack, compared with 1 in 414.3 in 2012.
- 70.9 percent of phishing attacks in 2013 related to spoofed financial organizations, compared with 67.3 percent in 2012
- Phishing attacks on organizations in the Information Services sector accounted for 21.8 percent of phishing attacks in 2013
- Phishing URLs spoofing banks attempt to steal a wide variety of information that can be used for identity theft and fraud. Attackers seek information such as names, government-issued identification numbers, bank account information, and credit card numbers. Cybercriminals are more focused on stealing financial information that can make them large amounts of money quickly versus goods that require a larger time investment, such as scams.
- 49.3 percent of phishing attacks were conducted through the use of phishing toolkits.
- In 2013 there was an increase in phishing activity spoofing energy companies, and mimicking vendors of online loyalty point schemes such as those collected whilst travelling long-haul flights. The reported increase in phishing activity against energy companies was relatively new, and was not reflected in the detailed analysis above. However, this will present a worrying trend if it continues to rise, since some energy companies may incentivize its customers to switch to paperless billing, and a successful phishing attack against an online account may then provide the attacker with enough information to open a false finance account using an online energy bill as proof of identity.

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, where 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 their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a spam attack because SMBs are perceived to be a softer target as they are less likely to have the same levels of defense-in-depth as a larger organization, who tend to have greater budgetary expenditure applied to anti-spam and security countermeasures.

Methodology

Analysis of phishing activity based on geography, industry and size is determined from the patterns of spam activity for Symantec.cloud clients for threats during 2013.

Fig. C.15

Proportion of Email Traffic Identified as Phishing by Industry Sector, 2013

Source: Symantec.cloud

Industry	2013	2012
Public Sector	1 in 216.4	1 in 95.4
Education	1 in 568.8	1 in 222.8
Accom/Catering	1 in 594.5	1 in 297.4
Marketing/Media	1 in 752.1	1 in 355.2
Finance	1 in 767.7	1 in 211.1
Non-Profit	1 in 780.6	1 in 362.3
Estate Agents	1 in 977.9	1 in 448.6
Prof Services	1 in 1,155.4	1 in 510.9
Agriculture	1 in 1,173.6	1 in 450.8
General Services	1 in 1,185.0	1 in 397.7

Fig. C.16

Proportion of Email Traffic Identified as Phishing by Organization Size, 2013

Source: Symantec.cloud

Company Size	2013	2012
1-250	1 in 689.5	1 in 293.8
251-500	1 in 1,075.9	1 in 500.8
501-1000	1 in 1,574.6	1 in 671.1
1001-1500	1 in 1,309.8	1 in 607.0
1501-2500	1 in 1,709.3	1 in 739.1
2501+	1 in 844.7	1 in 346.0

Fig. C.17

Proportion of Email Traffic Identified as Phishing by Geographic Location, 2013

Source: Symantec.cloud

Country/Region	2013	2012
South Africa	1 in 419.8	1 in 176.6
United Kingdom	1 in 454.1	1 in 190.6
Italy	1 in 873.5	1 in 520.0
Australia	1 in 906.4	1 in 426.0
Austria	1 in 1,049.0	1 in 611.6
Canada	1 in 1,059.3	1 in 400.2
Netherlands	1 in 1,115.9	1 in 123.1
Brazil	1 in 1,761.3	1 in 735.2
Denmark	1 in 1,768.6	1 in 374.3
New Zealand	1 in 1,784.7	1 in 740.0

Commentary

- The phishing rate has significantly decreased for all of the top-ten geographies in 2013. The highest average rate for phishing activity in 2013 was for organizations in South Africa, with an overall average phishing rate of 1 in 419.8. In 2012, the highest rate was for Netherlands, with an overall average phishing rate of 1 in 123.1.
- The phishing rate has decreased across all of the top-ten industry sectors in 2013. Organizations in the Government and Public Sector were subjected to the highest level of phishing activity in 2013, with 1 in 216.4 emails identified and blocked as phishing attacks. In 2012 the sector with the highest average phishing rate was also the Government and Public Sector, with a phishing rate of 1 in 95.4.
- The phishing rate has decreased for all sizes of organization in 2013. 1 in 844.7 emails sent to large enterprises with more than 2,500 employees in 2013 were identified and blocked as phishing attacks, compared with 1 in 346.0 in 2012.
- 1 in 689.5 emails sent to businesses with up to 250 employees in 2013 were identified and blocked as phishing attacks, compared with 1 in 293.8 in 2012.

New Spam Trend: BGP Hijacking

Background

The Internet is divided into thousands of smaller networks called Autonomous Systems (ASes), each of them belonging a single entity (e.g., 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 the 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 in taking control of blocks of IP addresses owned by a given organization without its authorization. This enables the attacker to perform other malicious activities (e.g. spamming, phishing, malware hosting) using hijacked IP addresses belonging to somebody else.

In the Symantec Internet Security Threat Report 2012[7] we introduced a new 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 a real-world case study involving a very sophisticated spammer who hijacked someone else's network for several months in 2011 before the victim network owner eventually noticed and regained control over his network. Although at that time we presented only one confirmed case of spammers behaving this way, we envisioned that such phenomenon would become more prevalent.

It is important to detect such malicious BGP hijacks. First, such attacks can lead to misattributing other attacks, such as denial of service attacks, launched from hijacked networks due to hijackers stealing IP identity. Correctly attributing attacks is critical when responding with possible legal action. Second, spam filters heavily rely on IP reputation systems, such as spam sender blacklists, to filter out emails coming from known spam networks. Sending spam from a hijacked network with a good reputation can thus defeat such protections.

Methodology

Studying fly-by spammers' operations involves (1) identifying spam-emitting networks and (2) 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 and study fly-by spammers. SpamTracer monitors the routes towards spam networks identified by Symantec.cloud, to detect when spammers manipulate the Internet routing to steal (or hijack) network IP addresses and launch spam campaigns using those addresses.

Commentary

A detailed analysis of data collected by SpamTracer between January and July 2013 led to identification of 29 hijacked network IP address blocks. We further examined these cases and uncovered a common *modus operandi* used by spammers to hijack the networks.

Fly-by spammers ***modus operandi*****:** Spammers hijacked dormant network IP address blocks, i.e. by the time the networks were hijacked they had been left idle by their owner. This situation can result, for example, from an organization going out of business without properly returning its assigned network addresses leaving them in a dormant state. Spammers also advertised the hijacked IP address blocks in BGP using the AS of their legitimate owner in an effort not to raise suspicion and to remain stealthy. Finally, hijacks were short-lived, lasting from several minutes to a few days.

We can see through this *modus operandi* that fly-by spammers really try not to raise suspicion, remaining stealthy. First, they hijack dormant networks allowing them to avoid any disruption that would result from hijacking a network actively used by its owner. Second, they advertise the hijacked networks in BGP in a way that appears to be advertised by their legitimate owner. Finally, they hijack networks for a short period of time to send spam using the stolen addresses and quickly disappear afterwards.

Below we describe in more details some key characteristics of fly-by spammers.

Duration of hijacks: Figure C.18 depicts the duration of the identified hijacks. The minimum duration is 30 minutes and the maximum duration is 20 days. Most hijacks (20 out of 29) lasted at most 4 days. Overall fly-by spammers appear to perform short-lived hijacks, likely in an effort to remain stealthy. Such hijacks really contrast with the hijack case study we presented in our Internet Security Threat Report 2012, which lasted five months. As shown later in this document, short-lived hijacks are very effective at defeating known spam protections, such as spam sender blacklists.

Duration of network idle period: Figure C.19 depicts the duration of the period during which networks were left idle/dormant before being hijacked. Fly-by spammers appear to hijack more networks (23 out of 29) that have been dormant for a very long time, i.e. more than one year, possibly to ensure their owner has permanently left them idle.

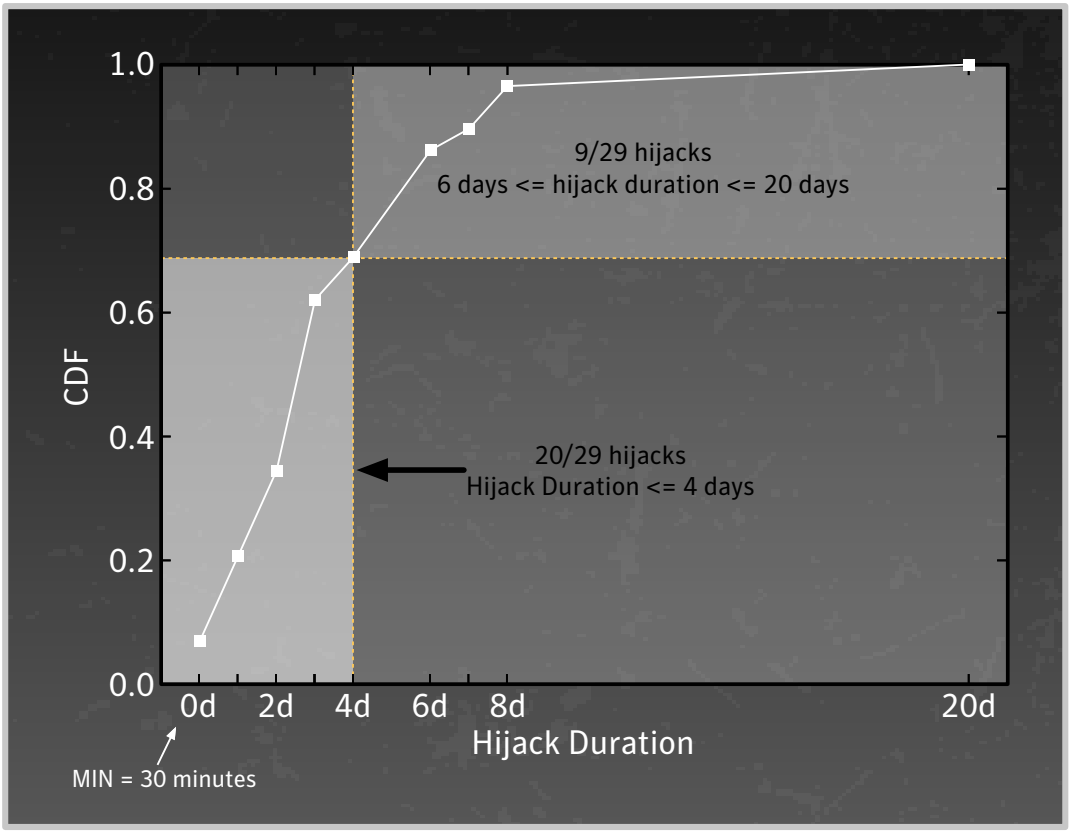


Fig. C.18 Duration of hijacks

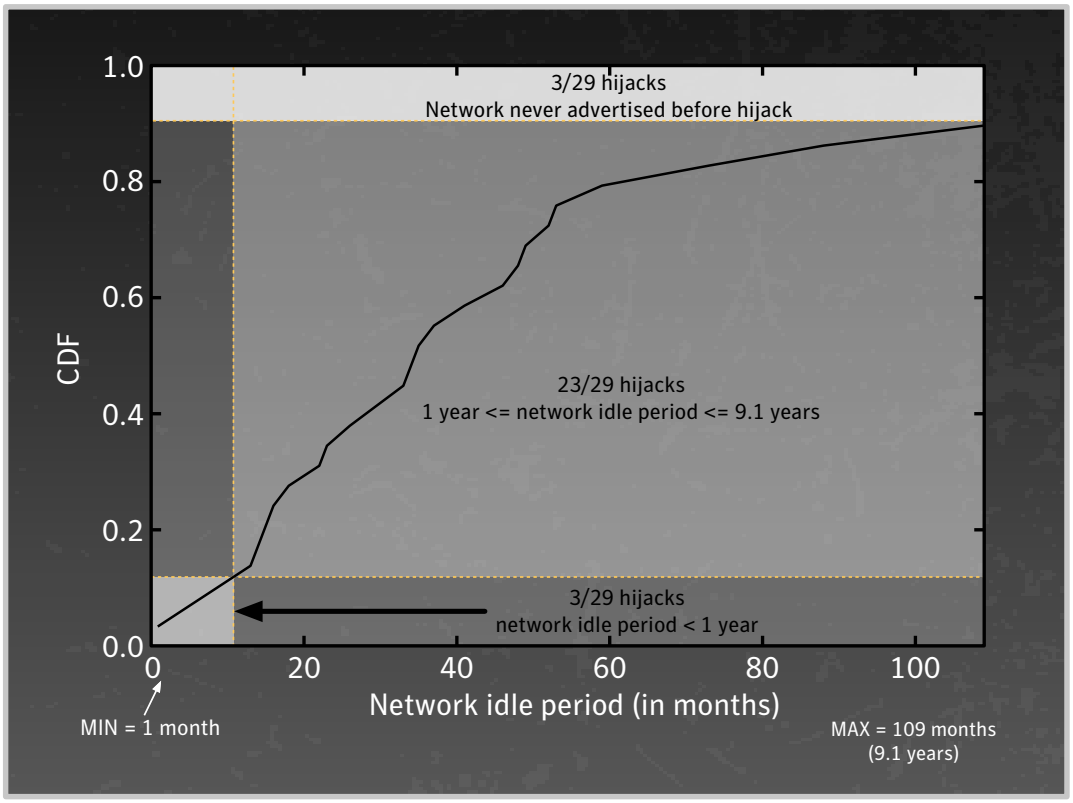


Fig. C.19 Duration of network Idle period

Routing and spamming behavior: To further illustrate the routing and spamming behavior of fly-by spammers, we consider some case studies. Figure C.20 shows the temporal correlation between the BGP advertisements for network IP address blocks and spam received from those networks at Symantec.cloud spamtraps. For example, the address block on the top of the figure was advertised in BGP (and hijacked) for only one day during which about 2,000 spam emails were received from it. The figure really highlights the strong temporal correlation between BGP advertisements and spam and the short-lived nature of the hijacks.

In order to assess the impact of spam from short-lived hijacks on spam sender blacklists, we extracted records for the hijacked networks in the Uceprotect[8], Manitu[9] and Spamhaus SBL and DROP[10] blacklists. Figure C.20 shows that out of the ten address blocks considered in these case studies only two had spam sources listed in those blacklists.

Finally, we also observed that a lot of scam websites advertised in the received spam emails were hosted on the hijacked networks, indicating that spammers took full advantage of the address blocks under their control.

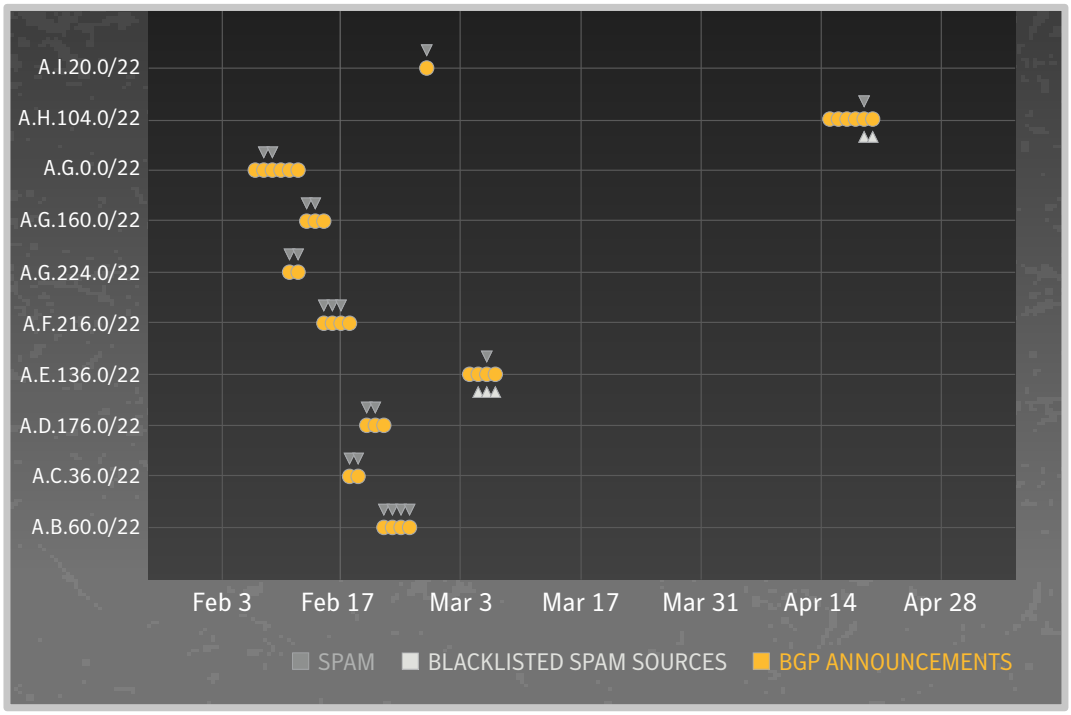


Fig. C.20 Temporal correlation between BGP advertisements and spam for hijacked networks

Effectiveness of fly-by spammers' spamming technique: Of the 29 hijacked network address blocks we observed only 13 (45 percent) of them were blacklisted either in Uceprotect, Manitu or Spamhaus SBL and DROP. Interestingly, Spamhaus' DROP (Don't Route Or Peer) is supposed to list hijacked networks, but little is known about how this list is actually built. Spam sent from short-lived hijacked networks thus appear to be very effective at defeating spam sender blacklists.

It is also noteworthy that none of the 29 hijacks were reported on any specialized mailing list, such as the North American Network Operators' Group mailing list, or published elsewhere. Finally, spammers never hijacked the same network twice showing that they not only perform short-lived hijacks but they also never reuse previously hijacked networks, likely in an effort to remain stealthy.

From these observations, fly-by spammers seem able to remain under the radar.

Networks targeted by fly-by spammers: We further looked at the organizations whose network address blocks were hijacked and found that:

- All hijacked address blocks were properly registered to an organization at the time they were hijacked. Moreover, they all belonged to different organizations.
- Of the 29 organizations, 12 of them were no longer in business while the remaining 17 were likely still in business.

These observations lead us to the conclusion that fly-by spammers seem to simply target dormant network IP address blocks regardless of their owner still being in business or not.

How to prevent fly-by spammers: BGP relies on the concept of trust among interconnect ASes exchanging routing information. This makes BGP insecure by design. An architecture[11] for securing BGP by relying on cryptography to ensure the authenticity and integrity of the routing information exchanged has been in development for many years now and is the most promising solution. However, the current state of the deployment of this architecture does not fully secure BGP and can consequently not prevent fly-by spammers using the *modus operandi* we presented. As a result, the only solution to prevent fly-by spammers for now is to use tools to detect such spammers and mitigate their effect, for example, by leveraging identified hijacked networks in spam filters to block emails that originate there.

Conclusion: Using SpamTracer, a system developed within Symantec Research Labs, we identified several confirmed attack cases where fly-by spammers temporarily stole (or hijacked) blocks of IP address and used them to send spam. We demonstrated that this technique for sending spam is very effective at defeating known protections, such as spam sender IP-based blacklisting. Finally we provided some insight into the *modus operandi* of these sophisticated spammers. This analysis confirms the first observations of fly-by spammers reported in our Internet Security Threat Report 2012 and shows the increasing prevalence of this phenomenon. By identifying confirmed cases of spammers performing BGP hijacks to send spam from stolen networks we also witnessed how spammers managed to evolve and become even more sophisticated, allowing them to send spam while remaining stealthy and hindering their traceability. Finally, this demonstrates the importance of securing the routing infrastructure of the Internet and studying the constantly evolving behavior of attackers to help improve current protections.

Footnotes

01 http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam
02 http://www.symantec.com/security_response/landing/spam
03 SMTP – Simple Mail Transfer Protocol
04 An as-yet unnamed spam-sending botnet.
05 http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet
06 http://www.symanteccloud.com/sv/se/globalthreats/learning_center/what_is_skeptic
07 http://www.symantec.com/threatreport/topic.jsp?id=spam_fraud_activity_trends&aid=future_spam_trends
08 http://www.uceprotect.net
09 http://www.dnsbl.manitu.net
10 http://www.spamhaus.org
11 http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-2/142_bgp.html

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
- Web Attack Toolkits
- SCADA Vulnerabilities

Total Number of Vulnerabilities

Background

The total number of vulnerabilities for 2013 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 were subsequently identified post-exploitation. Symantec's DeepSight vulnerability database tracks vulnerabilities reported in major well-known applications that are in common business use and applications that customers have specifically requested to be tracked. For example, DeepSight does not track vulnerabilities in all open source projects or in all consumer products such as video games.

Symantec gathers information on all the aforementioned 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, software quality assurance, and 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 60,000 distinct vulnerabilities spanning a period of over 20 years. As part of the data gathering process, Symantec scores the vulnerabilities according to version 2.0 of the community-based CVSS (Common Vulnerability Scoring System[1]). 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 who produced the vulnerable product confirmed them.

Fig. D.1

Total Vulnerabilities Identified 2006–2013

Source: Symantec

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

Fig. D.2

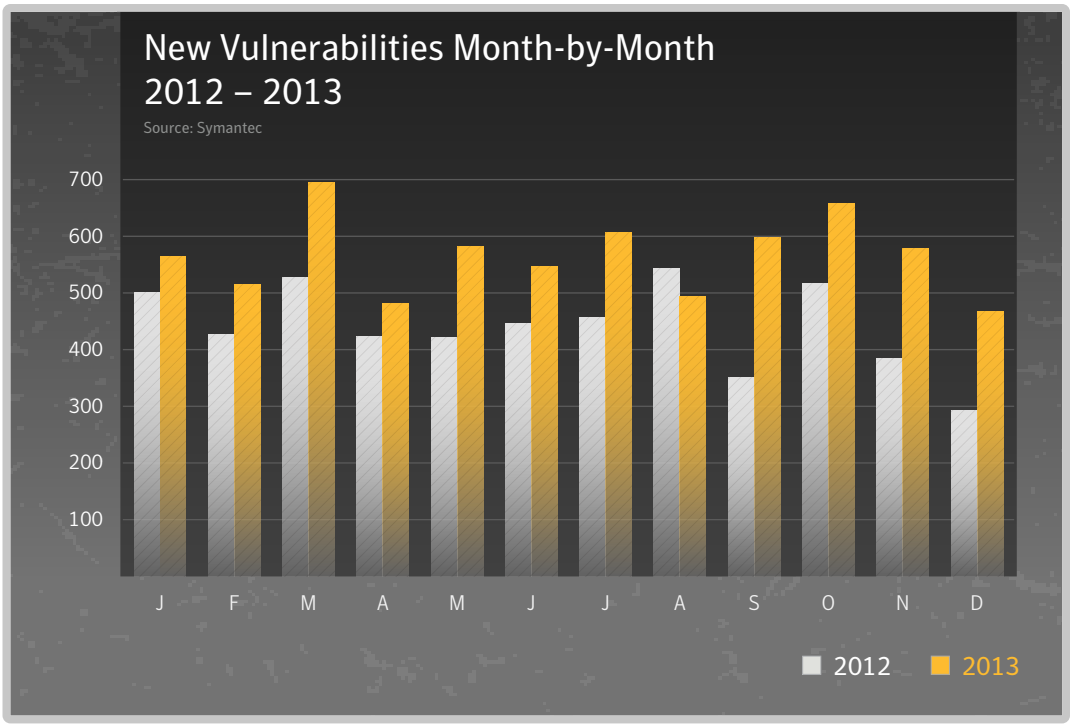


Fig. D.3

Most Frequently Attacked Vulnerabilities, 2013

Source: Symantec

BID	Number of Detections	Title
BID 31874	54,451,440	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
BID 8234	3,829,870	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
BID 10127	3,829,357	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
BID 6005	3,829,356	Microsoft Windows RPC Service Denial of Service Vulnerability
BID 10121	3,829,356	Microsoft Windows Object Identity Network Communication Vulnerability

Commentary

- **Actual number of new vulnerabilities reported is up, and trend is still upwards:** The total number of new vulnerabilities reported in 2013 stood at 6,787. This figure amounts to approximately 131 new vulnerabilities each week. Compared with the 5,291 new vulnerabilities reported in 2012, it represents an increase of 22 percent and the overall trend is still on an upward trajectory.
- **The most often exploited vulnerabilities are not the newest:** From observation of in-field telemetry, we can see that the most frequently used vulnerability in attacks is not the newest. Our data shows that the most commonly attacked component by a wide margin is the Microsoft Windows RPC component. The attacks against this component are mostly using the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874[2]). This vulnerability was first reported back in October 2008 and Symantec blocked 54.5 million attempts to exploit it in 2013. This figure represents 18 times the volume of the second most exploited vulnerability, the Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability (BID 8234[3]), from July 2003.
- The next two most often used vulnerabilities are the Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability (BID 10127[4]), dating from April 2004 and the Microsoft Windows RPC Service Denial of Service Vulnerability (BID 6005[5]), from October 2002.
- Finally the fifth most exploited vulnerability is the Microsoft Windows Object Identity Network Communication Vulnerability (BID 10121[6]), reported in April 2004.
- **All of the top five vulnerabilities are several years old with patches available:** So why are they used so often even several years after patches are available? There are several reasons why this is the case:
    - Trading of vulnerabilities[7] either through legitimate or clandestine channels has given exploitable vulnerabilities a significant monetary value. Because of the restricted information available on some of these new vulnerabilities, criminals may not be able to take advantage of them unless they are willing to pay the often substantial asking prices. If they are unable or unwilling to pay, they may resort to existing, widely available vulnerabilities that are tried and tested to achieve their goals, even if it may potentially be less effective.
    - For those willing to pay, they will want to ensure maximum return on their investment. This could mean they will use it discretely and selectively rather than making a big splash and arousing the attention of security vendors and other criminal groups looking for new vulnerabilities to use.
    - Older vulnerabilities have a more established malware user base, and so account for a greater amount of traffic. For example, widespread and well-established malware threats, such as W32.Downadup[8] and its variants, use the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), which continues to register over 150,000 hits each day. Because these threats use vulnerabilities to spread in an automated fashion, the number of attacks they can launch would generally be far higher than for targeted attacks.
    - For various reasons, not all of the user population apply security patches quickly or at all. This means older vulnerabilities can often still be effective, even years after patches are available. Because of this, there will always be a window of opportunity for criminals to exploit, and they are all too aware of this.
- One thing to note, 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 no vendor has 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 these threats 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 sub-set 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.

Fig. D.4

Volume of Zero-Day Vulnerabilities, 2006–2013

Source: Symantec

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

Fig. D.5

Zero-Day Vulnerabilities Identified, 2013

Source: Symantec

CVE Identifier	Description
CVE-2013-0422	Oracle Java Runtime Environment CVE-2013-0422 Multiple Remote Code Execution Vulnerabilities
CVE-2012-3174	Oracle Java Runtime Environment CVE-2012-3174 Remote Code Execution Vulnerability
CVE-2013-0634	Adobe Flash Player CVE-2013-0634 Remote Memory Corruption Vulnerability
CVE-2013-0633	Adobe Flash Player CVE-2013-0633 Buffer Overflow Vulnerability
CVE-2013-0640	Adobe Acrobat And Reader CVE-2013-0640 Remote Code Execution Vulnerability
CVE-2013-0641	Adobe Acrobat And Reader CVE-2013-0641 Remote Code Execution Vulnerability
CVE-2013-0643	Adobe Flash Player CVE-2013-0643 Unspecified Security Vulnerability
CVE-2013-0648	Adobe Flash Player CVE-2013-0648 Remote Code Execution Vulnerability
CVE-2013-1493	Oracle Java SE CVE-2013-1493 Remote Code Execution Vulnerability
CVE-2013-2423	Oracle Java Runtime Environment CVE-2013-2423 Security Bypass Vulnerability
CVE-2013-1347	Microsoft Internet Explorer CVE-2013-1347 Use-After-Free Remote Code Execution Vulnerability
CVE-2013-1331	Microsoft Office PNG File CVE-2013-1331 Buffer Overflow Vulnerability
CVE-2013-3163	Microsoft Internet Explorer CVE-2013-3163 Memory Corruption Vulnerability
CVE-MAP-NOMATCH	vBulletin '/install/upgrade.php' Security Bypass Vulnerability
CVE-2013-3893	Microsoft Internet Explorer CVE-2013-3893 Memory Corruption Vulnerability
CVE-2013-3897	Microsoft Internet Explorer CVE-2013-3897 Memory Corruption Vulnerability
CVE-2013-3906	Multiple Microsoft Products CVE-2013-3906 Remote Code Execution Vulnerability
CVE-2013-3918	Microsoft Windows 'icardie.dll' ActiveX Control CVE-2013-3918 Remote Code Execution Vulnerability
CVE-MAP-NOMATCH	vBulletin Unspecified Security Vulnerability
CVE-MAP-NOMATCH	Microsoft Windows Kernel 'NDProxy.sys' Local Privilege Escalation Vulnerability
CVE-MAP-NOMATCH	Adobe Flash Player and AIR Type Confusion Remote Code Execution Vulnerability
CVE-2013-2463	Oracle Java SE CVE-2013-2463 Remote Code Execution Vulnerability
CVE-2013-3660	Microsoft Windows Kernel 'Win32k.sys' CVE-2013-3660 Local Privilege Escalation Vulnerability

Commentary

- 2013 saw an increase in number of zero-day vulnerabilities compared to 2012. There was a 39 percent increase in vulnerabilities in 2013 compared with 2012. However the number of vulnerabilities from 2013 was inflated due to Microsoft Oracle vulnerabilities, while in 2013 there were seven Adobe vulnerabilities, compared with only three in 2012.
- While the overall number of zero-day vulnerabilities is up, attacks using these vulnerabilities continue to be successful. Some of these vulnerabilities are leveraged in targeted attacks. Adobe Flash Player and Microsoft Windows ActiveX Control vulnerabilities are widely used in targeted attacks and Microsoft technologies accounted for almost a third of the zero-day vulnerabilities seen in 2013.
- Most of the attack scenarios are planned in such a way that an attacker crafts a malicious webpage to exploit the issue, and uses email or other means to distribute the page and entices an unsuspecting user to view it. When the victim views the page, the attacker-supplied code is run.

Web Browser Vulnerabilities

Background

Web browsers are ever-present components for computing for both enterprise and individual users on desktop and on mobile devices. Web browser vulnerabilities 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 most other applications and are particularly targeted by multi-exploit attack kits.

Web-based attacks can originate from malicious websites as well as 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 often 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 sub-set 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.

Commentary

- This metric examines the total number of vulnerabilities affecting the following web browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Opera
- All vulnerabilities decreased in 2013, except Microsoft Internet Explorer which saw an increase of 59 percent, compared to 2012.
- These five browsers had 591 reported vulnerabilities in total in 2013, which is a significant decrease from 891 in 2012. This drop is due to a dramatic reduction in vulnerabilities seen in Safari, Chrome and Firefox.

Fig. D.6

Browser Vulnerabilities, 2011–2013

Source: Symantec

	Apple Safari	Google Chrome	Microsoft Internet Explorer	Mozilla Firefox	Opera	Total
2013	54	219	148	157	13	591
2012	343	268	60	186	34	891
2011	117	62	48	98	26	351

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 web pages to be rendered. Although this is 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 silently infecting 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 up to 25 different browser and browser plug-in vulnerabilities at one time, enabling full access to download any malware to the endpoint system.

Some plug-in technologies include automatic update mechanisms that are designed to keep 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 enterprises 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 if every browser plug-in is needed and consider removing or disabling potentially vulnerable software.

Methodology

Web browser plug-in vulnerabilities comprise a sub-set 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 vulnerabilities that are both unconfirmed and confirmed by the vendor of the affected product. Confirmed vulnerabilities consist of security issues that the vendor has publicly acknowledged, by either 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, which have not been publicly confirmed by the vendor. That a vulnerability is unconfirmed does not mean that the vulnerability report is not legitimate; only that the vendor has not released a public statement to confirm the existence of the vulnerability.

Fig. D.7

Browser Plug-In Vulnerabilities, 2012–2013

Source: Symantec

	Adobe Acrobat Reader	Adobe Flash	Active X	Apple Quicktime	Firefox Extension	Oracle Sun Java	Total
2012	32	70	118	28	0	64	312
2013	68	56	54	13	0	184	375

Commentary

- Symantec identified the following plug-in technologies as having the most reported vulnerabilities in 2013:
  - Adobe Reader
  - Adobe Flash Player
  - Apple QuickTime
  - Microsoft ActiveX
  - Mozilla Firefox extensions
  - Oracle Sun Java Platform Standard Edition (Java SE)
- In 2012, 375 vulnerabilities affecting browser plug-ins were documented by Symantec, an increase compared to the 312 vulnerabilities affecting browser plug-ins in 2012.
- ActiveX vulnerabilities decreased in 2013.
- Java vulnerabilities increased in 2013. This trend was already visible in 2012 and grew again. This is also reflected in the vulnerability usage in attack toolkits which have focused around Adobe Flash Player, Adobe PDF Reader and Java in 2013.

Web Attack Toolkits

Web attack toolkits are a collection of scripts, often PHP or JavaScript files, which are used to create malicious websites that exploit vulnerabilities in order to infect visitors. There are a few dozen known families used in the wild. Many toolkits are traded or sold on underground forums for USD$100-$1000.

Some are actively developed with new vulnerabilities added over time, and some web attack toolkits employ a subscription model that operates rather like a Software-as-a-Service (SaaS) model. The exploit code is kept away from the criminals who are renting the toolkit, so that they may not steal the toolkit author's intellectual property. However, the attacker will include code that links to the actual toolkit. This may be further hidden behind fast-flux DNS in order to further obfuscate the attack code.

Since many toolkits regularly use the same exploits, it is often difficult to identify the specific attack toolkit behind each infection attempt. An attack toolkit may contain many different exploits, each focusing on a variety of browser-independent plug-in vulnerabilities. In general, older exploits are not removed from the toolkits, since some systems may still be unpatched and these may often be tried first, in order to keep the newer attacks below the radar. This is perhaps why many of the toolkits still contain an exploit for the old Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability (BID 17462) from 2006. The malicious script will test all possible exploits in sequence until one succeeds. This may magnify the attack numbers seen for older vulnerabilities, even if they were unsuccessful.

For more information on Web attack toolkits, please read Appendix A: Threat Activity Trends - Analysis of Malicious Web Activity by Attack Toolkits.

SCADA Vulnerabilities

Background

This metric will examine the SCADA (Supervisory Control and Data Acquisition) security threat landscape. 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 concern related to national security 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 SCADA technologies. The purpose of the metric is to provide insight into the state of security research in relation to SCADA systems. To a lesser degree, this may provide insight into the overall state of SCADA security. Vulnerabilities affecting SCADA systems may present a threat to critical infrastructure that relies on these systems. Due to the potential for disruption of critical services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks. This is a concern for both governments and enterprises involved in the critical infrastructure sector. While this metric provides insight into public SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure it is likely that private security research is conducted by SCADA technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

Fig. D.8

SCADA Vulnerabilities Identified, 2013

Source: Symantec

BugTraq#	Description	Published
57438	Rockwell Automation ControlLogix CVE-2012-6442 Denial of Service Vulnerability	11 January 2013
57309	Rockwell Automation ControlLogix CVE-2012-6436 Remote Denial of Service Vulnerability	11 January 2013
57651	Rockwell Automation ControlLogix CVE-2012-6437 Security Bypass Vulnerability	11 January 2013
57311	Rockwell Automation ControlLogix CVE-2012-6435 Denial of Service Vulnerability	11 January 2013
58917	Rockwell Automation ControlLogix CVE-2012-6439 Denial of Service Vulnerability	11 January 2013
57435	Rockwell Automation ControlLogix CVE-2012-6440 Replay Security Bypass Vulnerability	11 January 2013
59703	Rockwell Automation ControlLogix CVE-2012-6438 Remote Denial of Service Vulnerability	11 January 2013
59709	Rockwell Automation ControlLogix CVE-2012-6441 Information Disclosure Vulnerability	14 January 2013
62936	Schneider Electric Software Update Remote Arbitrary Code Execution Vulnerability	16 January 2013
62635	Schneider Electric Products Multiple Security Vulnerabilities	16 January 2013
57317	Schneider Electric Accutech Manager Heap Buffer Overflow Vulnerability	21 January 2013
64351	Schneider Electric Ethernet Modules CVE-2013-2761 Denial of Service Vulnerability	23 January 2013
59708	Ecava IntegraXor CVE-2012-4700 ActiveX Control Remote Buffer Overflow Vulnerability	05 February 2013

Fig. D.8

SCADA Vulnerabilities Identified, 2013 (cont.)

Source: Symantec

BugTraq#	Description	Published
62419	WellinTech KingView CVE-2012-4711 Memory Corruption Vulnerability	12 February 2013
57909	Multiple Schneider Electric Products 'ModbusDrv.exe' Local Buffer Overflow Vulnerability	11 March 2013
61598	Mitsubishi MX Component ActiveX Control 'ActUWzd.dll' Remote Buffer Overflow Vulnerability	25 March 2013
57306	RSLinx Enterprise 'Logger.dll' CVE-2012-4695 Denial of Service Vulnerability	05 April 2013
58950	Invensys Wonderware Information Server CVE-2013-0688 Cross Site Scripting Vulnerability	07 May 2013
62878	Invensys Wonderware Information Server CVE-2013-0685 Denial of Service Vulnerability	07 May 2013
57308	Invensys Wonderware Information Server CVE-2013-0686 Information Disclosure Vulnerability	07 May 2013
57767	Invensys Wonderware Information Server CVE-2013-0684 SQL Injection Vulnerability	07 May 2013
64684	Multiple Schneider Electric Products XML External Entity Information Disclosure Vulnerability	16 July 2013
62880	ClearSCADA Web Requests Remote Denial of Service Vulnerability	01 August 2013
61968	Schneider Electric Multiple Trio J-Series Radio Devices CVE-2013-2782 Security Bypass Vulnerability	22 August 2013
57315	WellinTech KingView ActiveX Controls Multiple Insecure Method Vulnerabilities	04 September 2013
57307	Invensys Wonderware InTouch XML External Entities Information Disclosure Vulnerability	20 September 2013
62879	RSLinx Enterprise 'LogReceiver.exe' Integer Overflow Denial of Service Vulnerability	07 October 2013
59704	RSLinx Enterprise 'LogReceiver.exe' Integer Overflow Denial of Service Vulnerability	07 October 2013
57310	RSLinx Enterprise 'LogReceiver.exe' Out-of-bounds Remote Denial of Service Vulnerability	07 October 2013
62660	InduSoft Thin Client 'novapi7.dll' ActiveX Control Buffer Overflow Vulnerability	08 October 2013
58999	Ecava IntegraXor Project Directory Information Disclosure Vulnerability	15 December 2013
58692	Schneider Electric Accutech Manager RFManagerService SQL Injection Vulnerablity	18 December 2013

Commentary

- The number of SCADA vulnerabilities decreased in 2013: In 2013, there were 32 public SCADA vulnerabilities, a decrease compared with the 52 vulnerabilities disclosed in 2012

Footnotes

01 http://www.first.org/cvss/cvss-guide.html
02 http://www.securityfocus.com/bid/31874
03 http://www.securityfocus.com/bid/8234
04 http://www.securityfocus.com/bid/10127
05 http://www.securityfocus.com/bid/6005
06 http://www.securityfocus.com/bid/10121
07 http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/231900575/more-exploits-for-sale-means-better-security.html
08 http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99

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 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Security Response Publications: http://www.symantec.com/security_response/publications/
- Internet Security Threat Report Resource Page: 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/

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.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

04/14 21284438-2