2012 Trends, Volume 18, Published April 2013

ISTR

INTERNET SECURITY THREAT REPORT
APPENDIX ⌖ 2013

CONTENTS

APPENDIX :: A THREAT ACTIVITY TRENDS

Threat Activity Trends

The Symantec Global Internet Security Threat Report provides an analysis of threat activity, as well as other malicious activity, data breaches, and Web-based attacks that Symantec observed in 2012. The malicious activity discussed in this section not only includes threat activity, but also 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 covers the following metrics and provides analysis and discussion of the trends indicated by the data:

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

Malicious Activity by Source

Background

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, 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 purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, or 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 these 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

This metric assesses 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.

Data

Figure A.1. **Malicious Activity by Source: Overall Rankings, 2011–2012**

Source: Symantec

Geography	2012 World Rank	2012 Overall Average	2011 World Rank	2011 Overall Average	Change
United States	1	22.7%	1	21.1%	1.6%
China	2	11.0%	2	9.2%	1.8%
India	3	6.5%	3	6.2%	0.3%
Brazil	4	4.0%	4	4.1%	-0.1%
Germany	5	3.4%	5	3.9%	-0.5%
Netherlands	6	2.7%	20	1.1%	1.6%
Italy	7	2.4%	9	2.7%	-0.3%
United Kingdom	8	2.4%	7	3.2%	-0.8%
Taiwan	9	2.3%	8	3.0%	-0.7%
Russia	10	2.2%	6	3.2%	-1.0%

Figure A.2. **Malicious Activity by Source: Malicious Code, 2011–2012**

Source: Symantec

Geography	2012 Malicious Code Rank	2012 Malicious Code %	2011 Malicious Code Rank	2011 Malicious Code %	Change
United States	1	17.2%	2	13.3%	3.9%
India	2	16.2%	1	15.3%	0.9%
China	3	6.1%	4	5.1%	0.9%
Indonesia	4	3.9%	3	8.0%	-4.1%
Japan	5	3.4%	11	2.2%	1.2%
Vietnam	6	3.0%	6	3.8%	-0.8%
Brazil	7	2.9%	8	2.8%	0.0%
United Kingdom	8	2.7%	5	4.0%	-1.3%
Egypt	9	2.6%	7	3.4%	-0.8%
Germany	10	2.5%	15	1.5%	1.0%

Figure A.3. **Malicious Activity by Source: Spam Zombies, 2011–2012**

Source: Symantec

Geography	2012 Spam Zombies Rank	2012 Spam Zombies %	2011 Spam Zombies Rank	2011 Spam Zombies %	Change
India	1	17.1%	1	17.5%	-0.3%
Saudi Arabia	2	7.0%	19	1.5%	5.6%
Netherlands	3	6.5%	27	0.7%	5.8%
Brazil	4	5.5%	5	6.0%	-0.5%
United States	5	4.2%	15	1.8%	2.4%
Spain	6	4.0%	21	1.4%	2.6%
Argentina	7	3.8%	12	2.2%	1.6%
Germany	8	3.6%	23	1.2%	2.4%
China	9	3.1%	9	2.6%	0.5%
Russia	10	2.7%	3	7.8%	-5.0%

Figure A.4. **Malicious Activity by Source: Phishing Hosts, 2011–2012**

Source: Symantec

Geography	2012 Phishing Hosts Rank	2012 Phishing Hosts %	2011 Phishing Hosts Rank	2011 Phishing Hosts %	Change
United States	1	50.0%	1	48.5%	1.4%
Germany	2	6.2%	2	6.8%	-0.6%
United Kingdom	3	3.9%	3	3.6%	0.2%
Brazil	4	3.6%	8	2.3%	1.3%
China	5	3.2%	5	3.1%	0.2%
Canada	6	2.9%	4	3.3%	-0.4%
France	7	2.7%	7	2.4%	0.3%
Russia	8	2.4%	9	2.3%	0.0%
Netherlands	9	2.3%	6	2.4%	-0.1%
Poland	10	1.6%	12	1.6%	-0.1%

Figure A.5. **Malicious Activity by Source: Bots, 2011–2012**

Source: Symantec

Geography	2012 Bots Rank	2012 Bots %	2011 Bots Rank	2011 Bots %	Change
United States	1	15.3%	1	12.6%	2.8%
China	2	15.0%	6	6.6%	8.4%
Taiwan	3	7.9%	2	11.4%	-3.5%
Brazil	4	7.8%	3	8.9%	-1.1%
Italy	5	7.6%	4	8.3%	-0.7%
Japan	6	4.6%	8	4.6%	0.0%
Poland	7	4.4%	7	5.4%	-1.0%
Hungary	8	4.2%	9	4.3%	-0.1%
Germany	9	4.0%	5	7.0%	-2.9%
Spain	10	3.2%	11	2.6%	0.6%

Figure A.6. **Malicious Activity by Source: Web Attack Origins, 2011–2012**

Source: Symantec

Geography	2012 Web Attacking Countries Rank	2012 Web Attacking Countries %	2011 Web Attacking Countries Rank	2011 Web Attacking Countries %	Change
United States	1	34.4%	1	33.5%	0.9%
China	2	9.4%	2	11.0%	-1.6%
Korea, South	3	3.0%	3	4.4%	-1.4%
Germany	4	2.6%	4	3.5%	-0.9%
Netherlands	5	2.4%	8	2.0%	0.5%
India	6	1.7%	14	1.0%	0.6%
Japan	7	1.6%	6	2.2%	-0.6%
Russia	8	1.5%	7	2.1%	-0.6%
United Kingdom	9	1.5%	5	2.3%	-0.8%
Brazil	10	1.3%	11	1.3%	0.0%

Figure A.7. **Malicious Activity by Source: Network Attack Origins, 2011–2012**

Source: Symantec

Geography	2012 Network Attacking Countries Rank	2012 Network Attacking Countries %	2011 Network Attacking Countries Rank	2011 Network Attacking Countries %	Change
China	1	29.2%	1	26.9%	2.3%
United States	2	14.9%	2	16.9%	-1.9%
Russia	3	3.7%	5	3.4%	0.3%
United Kingdom	4	3.1%	3	4.1%	-0.9%
Brazil	5	3.0%	6	3.2%	-0.2%
Netherlands	6	2.6%	21	0.8%	1.8%
Japan	7	2.4%	8	2.5%	0.0%
India	8	2.4%	11	2.0%	0.4%
Italy	9	2.4%	7	2.8%	-0.4%
France	10	2.3%	10	2.1%	0.2%

Commentary

- **In 2012, corresponding with their large Internet populations, 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 2012 increased by 1.6 percentage points compared with 2011, while the same figure for China saw an increase by 1.8 percentage points compared with 2011. Malicious activity in the Netherlands also increased by 1.6 percentage points, resulting in the country being ranked in sixth position, compared with twentieth in 2011.
- **29.2 percent of network attacks originated in China:** China has the largest population of Internet users[1] in the Asia region, with its Internet population growing to 564 million in 2012.
- **50.0 percent of phishing websites were hosted in the United States:** In 2012, with approximately 275 million Internet users, the United States has the second largest population of Internet users in the world.
- The United States was ranked in first position for the source of all activities except for spam zombies and network attacks, for which India was ranked in first position for spam zombies and China the latter.
- **15.3 percent of bot activity originated in the United States:** The United States was the main source of bot-infected computers, an increase of 2.8 percentage points compared with 2011.
- **34.4 percent of Web-based attacks originated in the United States:** Web-based attacks originating from the United States increased by 0.9 percentage points in 2012.
- **17.1 percent of spam zombies were located in India, a decrease of 0.3 percentage points compared with 2011:** The proportion of spam zombies located in the United States rose by 2.4 percentage points to 4.2 percent, resulting in the United States being ranked in fifth position in 2012, compared with fifteenth position in 2011.
- **17.2 percent of all malicious code activities originated from the United States, an increase of 3.9 percentage points compared with 2011, overtaking India as the main source of malicious code activity in 2012:** With 16.2 percent of malicious activity originating in India, the country was ranked in second position. India has approximately 150 million Internet users, which is 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 if attackers are more or less likely to employ Web-based attacks in the future. To see which vulnerabilities are being exploited by Web-based attacks, see Appendix D: Vulnerability Trends.

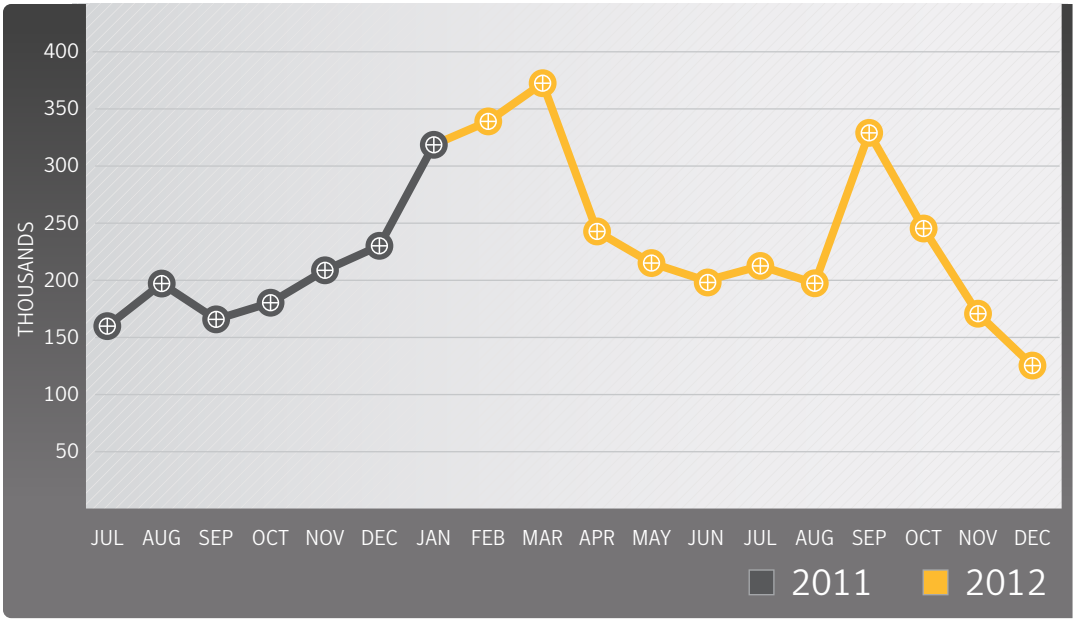
Methodology

This metric assesses changes to the prevalence of Web-based attack activity by comparing the overall volume of activity and the average number of attacks per day in each month during the current and previous reporting periods.

Data

Figure A.8. **Malicious Website Activity, 2011–2012**

Source: Symantec



Commentary

- The average number of malicious websites blocked each day rose by approximately 30 percent for all of 2012 to an average of 247,350, compared with 190,370 in the second half of 2011. A rise in attacks at the beginning of the year contributed in large part to this increase.
- The average number of websites blocked each day in the first half of 2012 compared with the second half of 2011, rose by 48 percent to an average of 281,283.
- The average number of websites blocked each day in the second half of 2012 compared with the second half of 2011 rose by 12 percent to an average of 213,417.
- The peak rate of malicious activity was 339,078 blocks per day in March 2012, when the number of malicious blocks was 37 percent higher than the annual average.
- The lowest rate of malicious activity was 125,384 blocks per day in December 2012, when the number of malicious blocks was 49 percent lower than the annual average.
- Further analysis of malicious code activity may be found in Appendix B: Malicious Code Trends: Overall Top Malicious Code Families, 2012.

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 enterprise 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 Web users in 2012. To determine this, Symantec ranked attack activity by the number of associated incidents associated with each given Web kit.

Data

Figure A.9. **Malicious Website Activity: Attack Toolkit Trends, 2012**

Source: Symantec

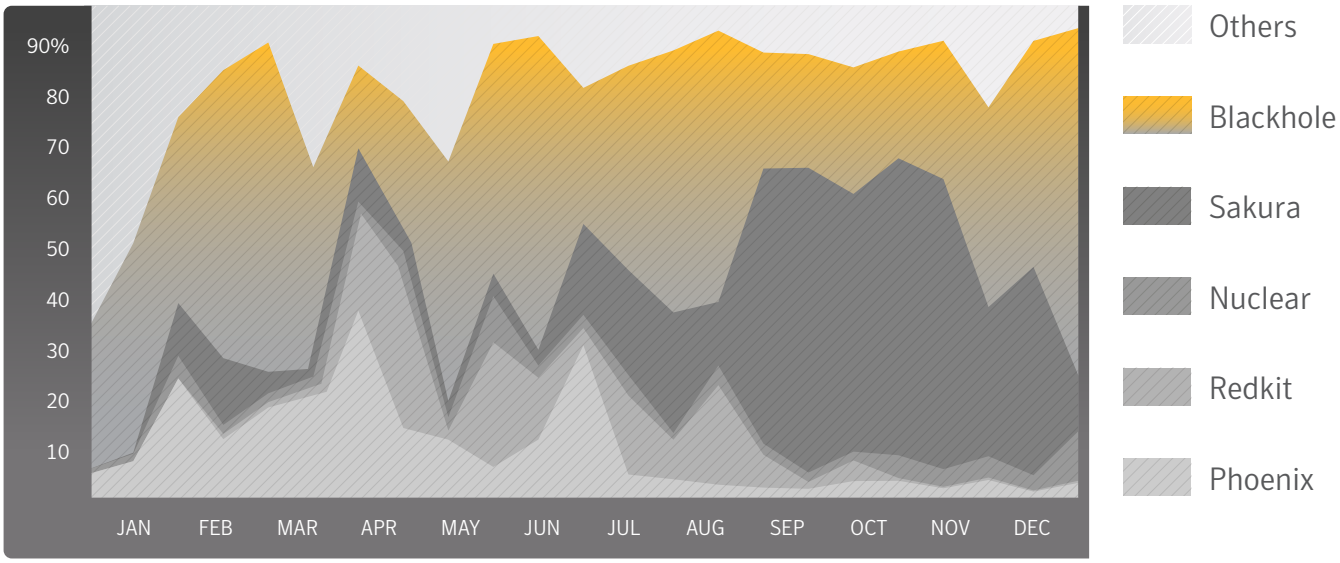
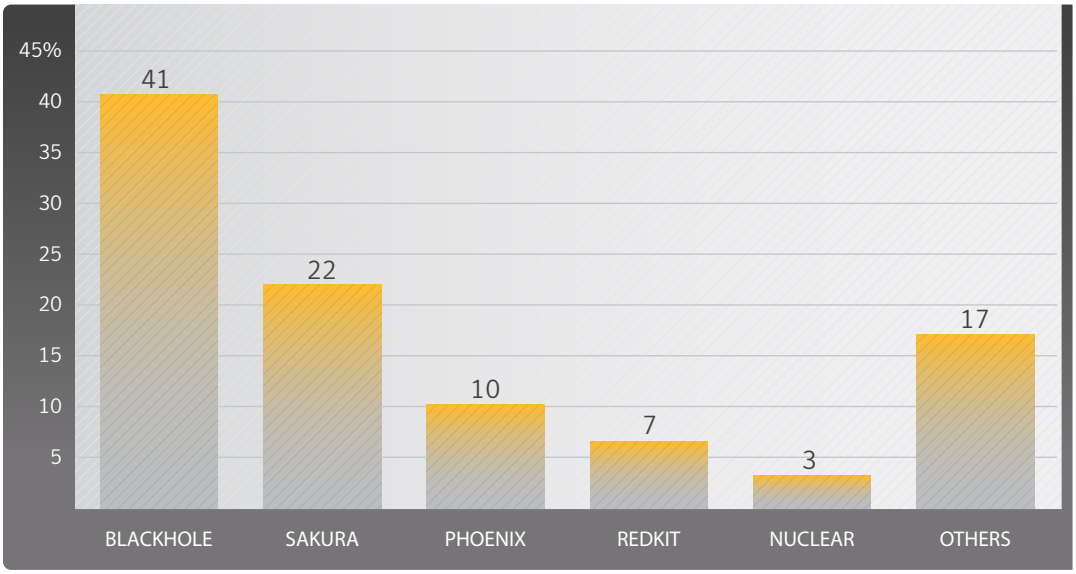


Figure A.10. **Malicious Website Activity: Overall Frequency of Major Attack Toolkits, 2012**

Source: Symantec



Commentary

- Blackhole continues to be the most dominant Web attack kit in 2012, accounting for 40.7 percent of attacks blocked from Web attack toolkits, compared with 44.3 percent in 2011. The Sakura toolkit was ranked second, accounting for 22 percent of attacks blocked and was not ranked in the top 10 in 2011.
- The Sakura Web attack kit was updated to version 1.1 in early 2012. And many of the more common attack toolkits were updated in 2012 to include exploits for the Java Runtime Environment, including CVE-2012-0507, CVE-2012-1723, and CVE-2012-4681.
- The Blackhole kit was updated frequently and the code is highly obfuscated. It is often used to deploy ransomware and fake security software.

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 the 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.

Data

Figure A.11. **Potentially Unwanted Programs: Spyware and Adware Blocked, 2012**

Source: Symantec.cloud

Rank	Top 10 Potentially Unwanted Programs	%
1	Application.DirectDownloader.A	94.2%
2	Spyware.PCAcme	1.5%
3	Adware.JS.Script.C	0.2%
4	Application:Android/Counterclank.A	0.2%
5	Application.InstallCore.E	0.2%
6	Adware:W32/CDN.A	0.2%
7	Adware.Solimba.C	0.2%
8	Spyware.Ardakey	0.2%
9	Adware:Android/AirPush.A	0.2%
10	Spyware.Keylogger	0.1%

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 and 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 2012 was for the DirectDownload software.
- Similarly, Counterclank[2] was ranked fourth in 2012, and was one of two Android-based potentially unwanted programs blocked. Due to the combined behavior of the applications and negative feedback from users who installed the applications, Symantec attempted to have Counterclank[3] removed from the Android Market in 2012, but Google replied quickly, informing us the applications met their Terms of Service and they will not be removed. We expect in the future there may be many similar situations where we will inform users about an application, but the application will remain in the Google Android Market.
- In 2012, three of the top 10 potentially unwanted programs were classified as spyware, compared with two in 2011.
- Figure A.11 accounts for approximately 19 percent of all spyware and adware blocked in 2012. The remainder was blocked using generic detection techniques.

Analysis of Web Policy Risks from Inappropriate Use

Background

Many organizations implement an acceptable usage policy to limit employees' use of Internet resources to a subset of websites that have been approved for business use. This enables an organization to limit the level of risk that may arise from users visiting inappropriate or unacceptable websites, such as those containing sexual images and other potentially illegal or harmful content. Often there will be varying degrees of granularity imposed on such restrictions, with some rules being applied to groups of users or rules that 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 shows the most frequently blocked websites (by category) that breach acceptable use policies defined by clients using the service. In some cases, users will repeatedly try to access unauthorized content; for example, by clicking on different URLs returned in a search results page. Sometimes policies may define that only certain groups within an organization may have access to restricted content (such as social networking), or the access may be limited to certain periods of the day.

Data

Figure A.12. **Web Policies that Triggered Blocks, 2011–2012**

Source: Symantec.cloud

Rank	Top 10 Category	2012	2011	Change
1	Advertisement and Pop-ups	31.8%	46.6%	-14.8%
2	Social Networking	24.1%	22.7%	1.4%
3	Streaming Media	9.0%	18.9%	-9.9%
4	Chat	4.7%	3.2%	1.5%
5	Computing and Internet	4.0%	<0.5%	New
6	Peer-to-Peer	3.3%	<0.5%	New
7	Hosting Sites	2.8%	1.6%	1.2%
8	Games	1.9%	0.6%	1.3%
9	News	1.7%	<0.5%	New
10	Search	1.7%	<0.5%	New

Commentary

- **31.8 percent of Web activity blocked through policy controls was related to advertisement and pop-ups.** 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.
- The second most frequently blocked traffic was categorized as **social networking, accounting for 24.1 percent of policy-based filtering activity blocked**, equivalent to approximately one in every four 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.
- **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 rate is equivalent to one in every 11 websites blocked. The proportion of streaming media blocks made in 2012 was half of the 2011 figure, despite 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 in order to provide better understanding of the types of legitimate websites that may be more susceptible to being compromised and potentially expose users to greater levels of risk.

Web-based malware is increasingly more likely to be found on a legitimate website that has been compromised and used to host malicious content. It is therefore increasingly important that proactive security countermeasures are able to block such malware before it can reach a company's network. This technique has also been employed in some targeted attacks, known as a "watering hole" attack, where the intended recipient is known to frequent a particular website and that website has been compromised.

Methodology

This metric assesses the classification of malicious websites blocked by users of Norton Safe Web technology.[4] Data is collected anonymously from over 50 million computers worldwide, where customers voluntarily contribute to this technology, including Norton Community Watch. Norton Safe Web is processing more than two billion real-time rating requests each day, and monitoring over 12 million daily. Reputation ratings are being tracked for more than 25 million websites.

This metric provides an indication of the levels of infection of legitimate websites that have been compromised or abused for malicious purposes. The malicious URLs identified by the Safe Web technology were classified by category using the Symantec Rulespace[5] technology. RuleSpace proactively categorizes websites into more than 80 categories in 17 languages.

Data

Figure A.13. **Malicious Web Activity: Categories that Delivered Malicious Code, 2012**

Source: Symantec

Rank	Top 10 Most Frequently Exploited Categories of Websites	% of Total Number of Infected Websites
1	Business	7.7%
2	Hacking	7.6%
3	Technology and Telecommunication	5.7%
4	Blogging	4.5%
5	Shopping	3.6%
6	Known Malware Domain	2.6%
7	Hosting	2.3%
8	Automotive	1.9%
9	Health	1.7%
10	Educational	1.7%

Figure A.14. **Malicious Web Activity: Malicious Code by Number of Infections Per Site, 2012**

Source: Symantec

Rank	Top 10 Potentially Most Harmful Categories of Websites	Average Number of Threats Found on Infected Website	Major Threat Type Detected
1	Pornography	4.4	Trojans: 82%
2	Placeholder	3.3	Pay Per Click: 73%
3	Plagiarism	3.2	Malware: 49%
4	Automotive	3.1	Pay Per Click: 66%
5	Gore	3.0	Fake Antivirus: 74%
6	Military	3.0	Malware: 53%
7	Lifestyles	2.8	Fake Antivirus: 53%
8	Automated Web Application	2.8	Malware: 100%
9	Abortion	2.8	Malware: 79%
10	Art and Museums	2.7	Fake Antivirus: 54%

Figure A.15. **Malicious Web Activity: Fake Antivirus by Category, 2012**

Source: Symantec

Rank	Top 10 Potentially Most Harmful Categories of Websites - Fake Antivlrus	% of Threats Found Within Same Category	% of Fake Antivirus Attacks Found Within Top 10 Categories
1	Religion	43%	4%
2	Sports	41%	5%
3	Shopping	39%	18%
4	Health	34%	7%
5	Business	29%	28%
6	Travel	29%	4%
7	Educational	22%	5%
8	Blogging	20%	11%
9	Technology and Telecommunication	15%	10%
10	Hacking	9%	8%

Figure A.16. **Malicious Web Activity: Browser Exploits by Category, 2012**

Source: Symantec

Rank	Top 10 Potentially Most Harmful Categories of Websites - Browser Exploits	% of Threats Found Within Same Category	% of Browser Exploits Found Within Top 10 Categories
1	Anonymizer	32%	8%
2	Blogging	30%	61%
3	Known Malware Domain	6%	7%
4	Dynamic	4%	2%
5	Hosting	4%	4%
6	Hacking	2%	8%
7	Educational	2%	1%
8	Business	1%	5%
9	Technology and Telecommunication	1%	3%
10	Shopping	1%	1%

Figure A.17. **Malicious Web Activity: Social Networking Attacks by Category, 2012**

Source: Symantec

Rank	Top 10 Potentially Most Harmful Categories of Websites - Social Networking	% Used to Deliver Social Networking Attacks
1	Blogging	43%
2	Hacking	14%
3	Dynamic	11%
4	Business	5%
5	Hosting	4%

Commentary

- Approximately 63 percent of websites used to distribute malware were identified as legitimate, compromised websites that could be classified, an increase of two percentage points compared with 2011. This figure excludes URLs that contained just an IP address and did not include general domain parking and pay-per-click websites.
- 7.7 percent of malicious website activity was classified in the Blogging category.
- Websites classified as pornography were found to host the greatest number of threats per site than other categories, with an average of 4.4 threats per website, the majority of which related to Trojans (82 percent).
- Analysis of websites that were used to deliver drive-by fake antivirus attacks revealed that 4 percent of threats found on compromised religion sites were related to fake antivirus software. 43 percent of fake antivirus attacks were found on compromised religion sites. 28 percent of attacks found on compromised business sites were fake antivirus.
- Analysis of websites that were used to deliver attacks using browser exploits revealed that 8 percent of threats found on compromised anonymizer sites were related to browser exploits. 32 percent of browser exploit attacks were found on compromised anonymizer sites. 59 percent of browser exploits were found on compromised blogging sites.
- 43 percent of attacks used on social networking websites 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 hacking accounted for 14 percent of social networking attacks.
- The **Hacking** category is used to classify websites that promote or provide the means to practice illegal or unauthorized acts of computer crime or related programming skills.
- 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 how the user is interacting with it (for example, an Internet search).
- The **Known Malware Domain** category are sites that have no specific broad classification, but where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware or malware. For example, underground websites that may be used to openly discuss and share malcode and related research.
- 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.

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 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 that may be used in identity theft 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; rather, 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 actively attacking bots or bots that send out spam; for example, 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, systems that participated in the high-profile DDoS Operation Payback attacks in 2010 and 2011 used publically available software such as Low Orbit Ion Cannon (LOIC) in a coordinated effort to disrupt many businesses, website operations. Users sympathetic to the Anonymous cause could voluntarily download the free tool from the Web and participate en masse in a coordinated DDoS campaign and required very little technical knowledge.

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

Data

Figure A.18. **Table of Top 10 Bot Locations by Average Lifespan of Bot, 2011–2012**

Source: Symantec

Rank - 2012	Geography	Average Lifespan of Bot (Days) - 2012	% of World Bots - 2012	Average Lifespan of Bot (Days) - 2011	% of World Bots - 2011	Rank - 2011
1	Romania	24	0.16%	29	0.14%	1
2	Bulgaria	17	0.10%	14	0.13%	2
3	United States	13	15.34%	13	12.56%	3
4	Indonesia	12	0.12%	10	0.14%	6
5	Israel	11	1.34%	5	1.64%	29
6	Egypt	10	0.11%	8	0.11%	14
7	Korea, South	10	0.99%	12	0.99%	4
8	Pakistan	10	0.12%	9	0.25%	10
9	Philippines	10	0.16%	10	0.18%	6
10	Ukraine	10	0.15%	10	0.20%	6

Commentary

- Bots located in Romania were active for an average of 24 days in 2012, compared with 29 days in 2011; 1 in 622 of bots were located in Romania, compared with 1 in 737 in 2011.
- It takes almost twice as long to identify and clean up a bot-infected computer in Romania than in the United States, although the number of infections in the United States is on a magnitude of 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 1 in 7 (15 percent) of global bot-infected computers, the average lifespan for a bot was 13 days, unchanged from 2011.
- All other countries outside the top ten had a lifespan of 9 days or less. The overall average lifespan was 6 days.
- Additionally, 68 percent of bots were controlled using HTTP-based command and control channels, compared with 65 percent in 2011.

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 2012, there was a significant number of vulnerabilities reported that affected mobile devices. Symantec documented 415 vulnerabilities in mobile device operating systems in 2012, compared to 315 in 2011 and 163 in 2010; an increase of 32 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 additional code to them. Symantec has classified the types of threats into a variety of categories based on their functionality.

Data

Figure A.19. **Android Mobile Threats: Newly Discovered Malicious Code, 2011–2012**

Source: Symantec

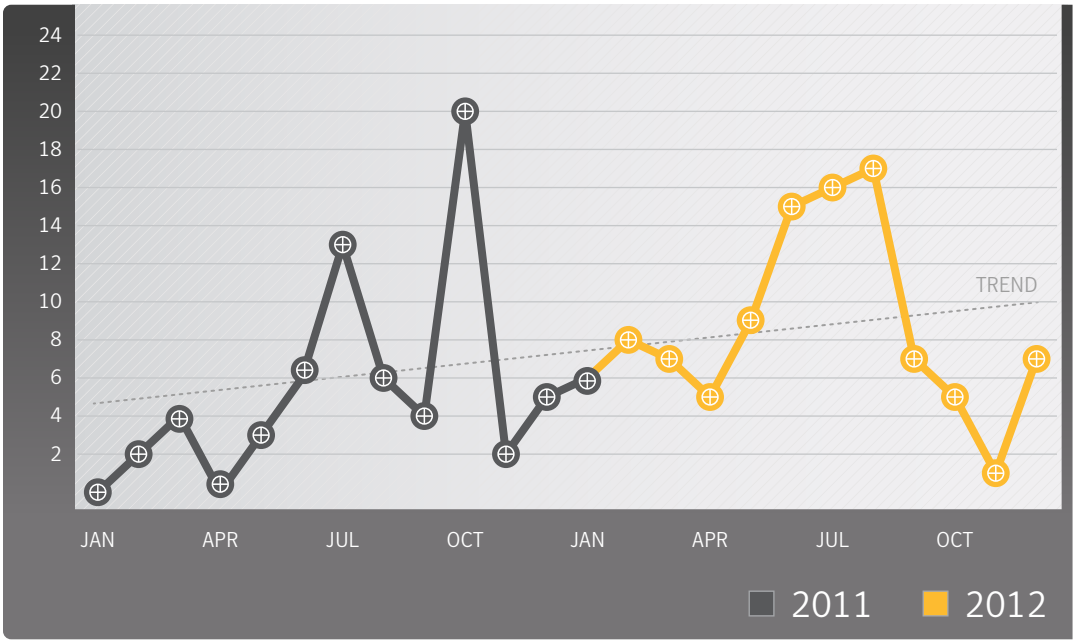


Figure A.20. **Android Mobile Threats: Cumulative Number of Malware Families, 2010–2012**

Source: Symantec

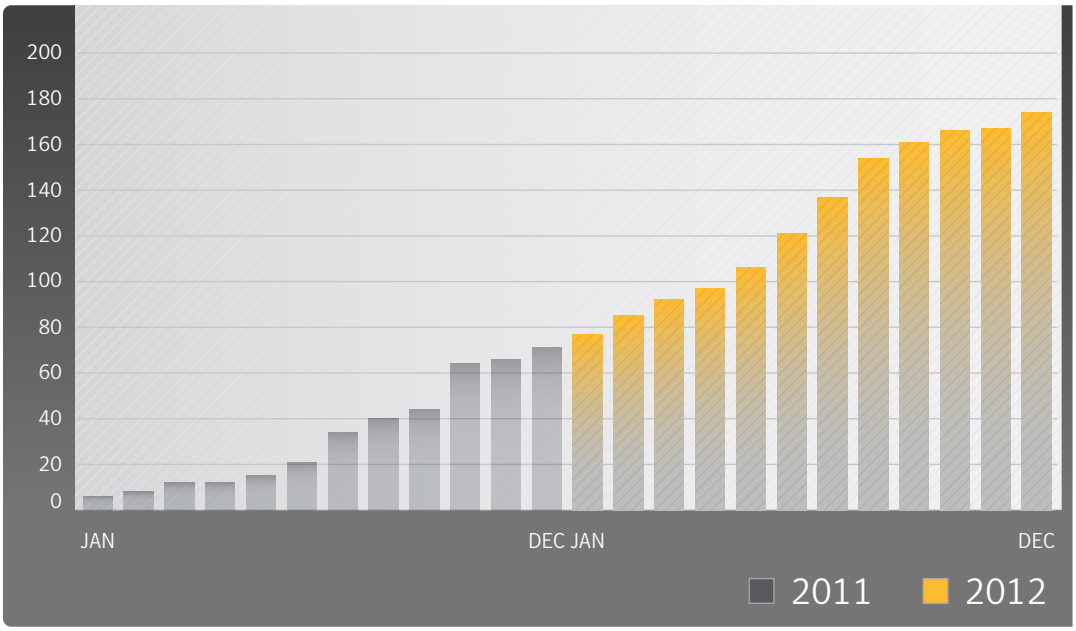


Figure A.21. **Mobile Threats: Malicious Code by Type, 2012**

Source: Symantec

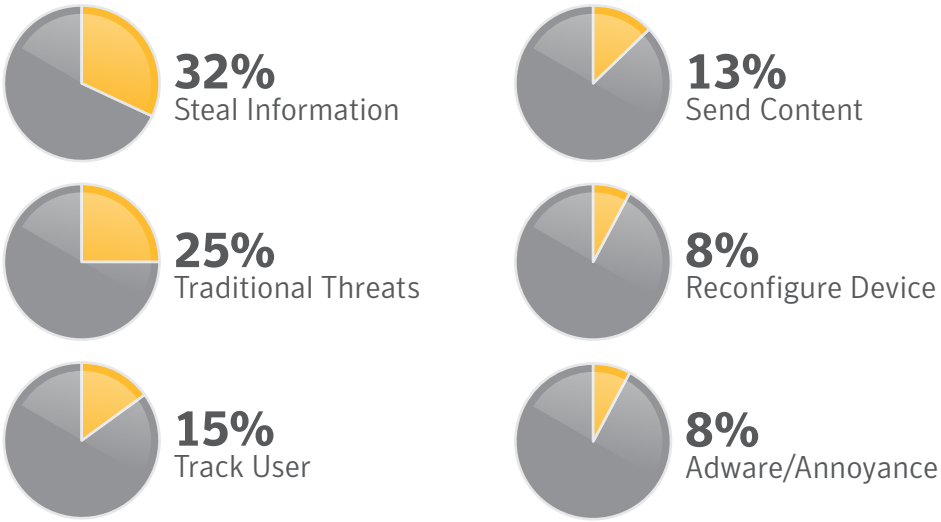


Figure A.22. **Mobile Threats: Malicious Code by Type – Additional Detail, 2012**

Source: Symantec

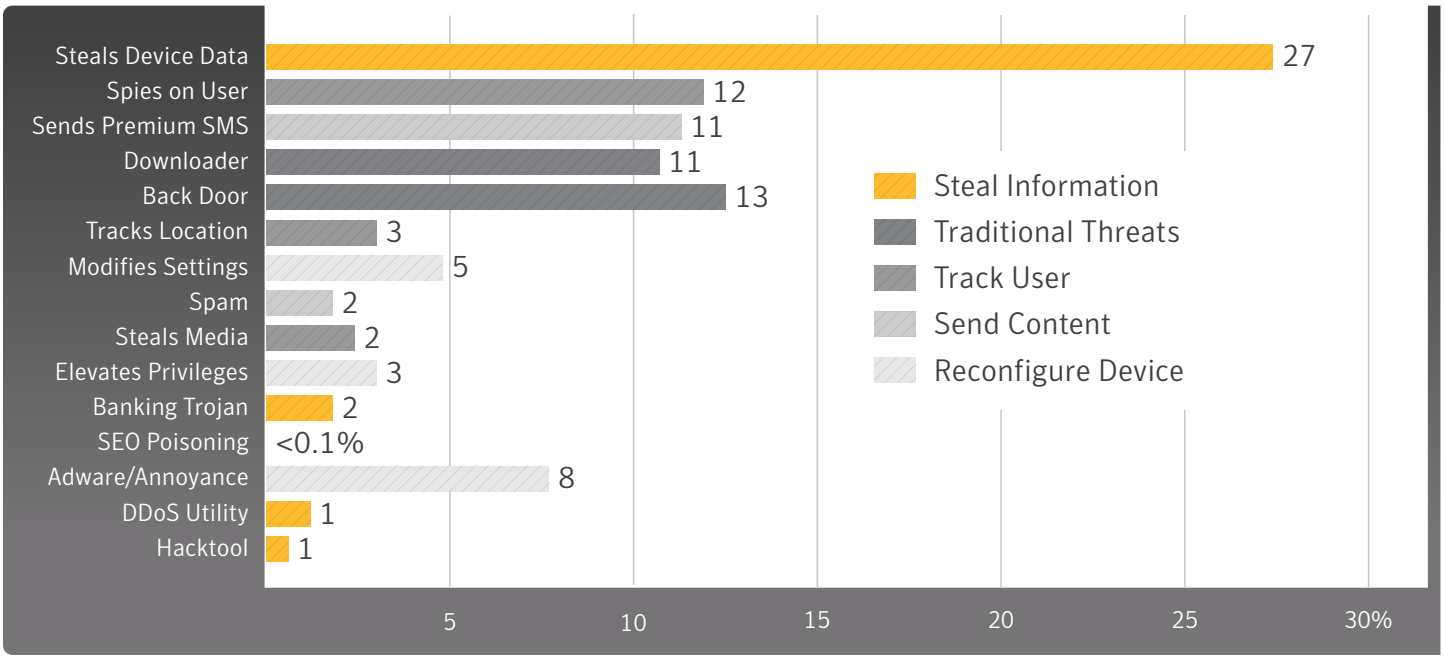
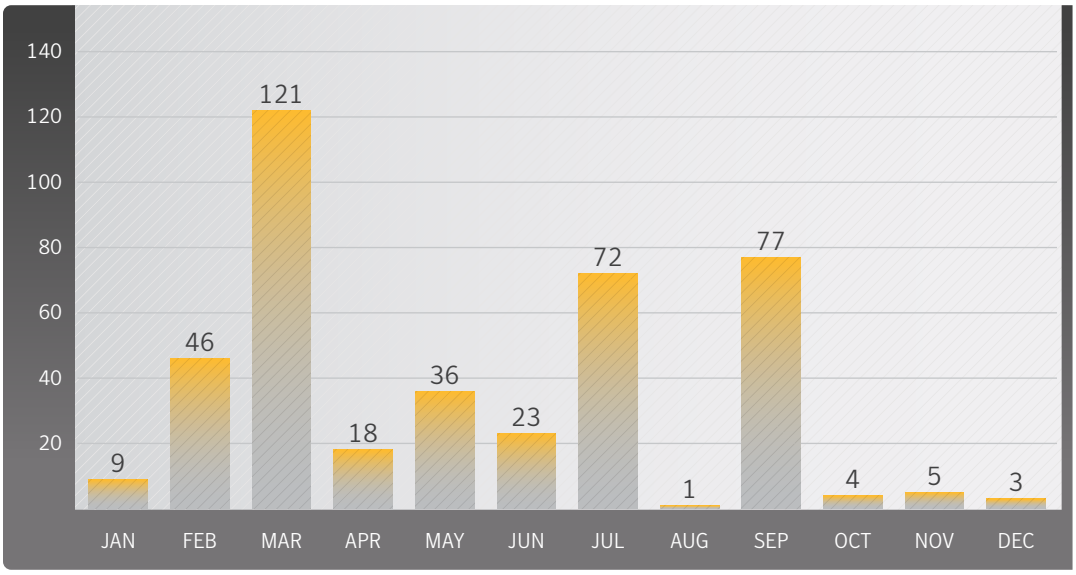


Figure A.23. **Documented Mobile Vulnerabilities, 2012**

Source: Symantec



Platform	Documented Vulnerabilities	%
Apple iOS/iPhone/iPad	387	93.3%
Android	13	3.1%
BlackBerry	13	3.1%
Nokia	0	0%
WebOS	0	0%
Windows Mobile	2	0.5%
TOTAL	**415**	

The following are specific definitions of each subcategory:

- **Collects 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 keep 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.
- **Back door** opens a back door on the compromised device, allowing attackers to perform arbitrary actions.
- **Tracks Location** gathers GPS information from the device specifically to track the user's location.
- **Modifies Settings** changes configuration settings on the compromised device.
- **Spam** sends spam email messages from the compromised device.
- **Steals Media** sends media, such as pictures, to a remote source.
- **Elevates Privileges** attempts to gain privileges beyond those laid out when installing the app bundled with the risk.
- **Banking Trojan** monitors the device for banking transactions, gathering the sensitive details for further malicious actions.
- **SEO Poisoning** periodically sends the phone's browser to predetermined URLs in order to boost search rankings.
- **Adware/Annoyance** contains mobile adware that uses techniques to place advertising in the device's photo albums and calender entries, and may push messages to the notification bar. It may even replace the default ringtone with an ad.

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:

- **Collect Data.** 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[7] and IMSI[8] 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 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 group of risks is bad 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 hopes of bumping certain pages within search rankings.
- **Traditional Threats.** The fourth group contains more traditional threats, such as back doors and downloaders. Attackers often port these types of 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 operating system. The goal for this final group seems to be to perform further actions on the compromised devices.

Commentary

In 2012, Android users especially were potentially vulnerable to a wider variety of threats, predominantly due to the widespread popularity of the Android platform. However, very few of these threats have utilized vulnerabilities in the Android OS in order to spread. Rather, the threats tend to masquerade as legitimate apps and attempt to coerce the user into installing them. Exploits accounted for a minority of the infections, but there are certainly more of them for older platforms (for example, 2.x.x), so a lot of these users were more vulnerable to malicious apps that carry these exploits and use then to obtain "root" super-user privileges (examples of threats that do this include Basebridge, Bmaster, Gonfu.D, Gmaster, and Zeahache).

There are two important distinctions between older and newer Android versions regarding security features:

- In response to feedback from users annoyed by advertising platforms that push notifications to the status bar, Google added a feature in 4.x to identify the app that generates a certain notification and even block that app from pushing notifications.
- Owing to the rise of threats that silently send premium text messages (Opfake, Premiumtext, Positmob, Rufraud, etc.), Google added in 4.2 a feature to prompt the user to confirm sending such premium text messages (they compiled a list of ranges of short-code numbers for many countries). This can be very helpful in protecting most users, however Android 4.2 devices account only for 1.4 percent of users at the time of writing.[9]

We haven't seen a large number of Android vulnerabilities in 2012, and phone manufacturers pushed (over the air) updates for the more serious ones. The Android ecosystem makes it more challenging to keep everyone up to date. Google controls the official reference platform that works out of the box only on Nexus devices. From there each manufacturer modifies and releases its own platform updates, which are picked up by mobile network operators, which in turn also customize for their platforms.

This makes it very difficult for any change coming from Google to be pushed out quickly to in-the-field devices. Any change to the platform requires thorough testing, which is performed by each manufacturer and operator, all adding to the time required to deploy to the end users.

Having so many device models also multiplies the amount of resources all these companies have to allocate for each update, which may partly explain why these updates are infrequently released. Another factor is that the newest platforms are optimized for the latest, more powerful hardware, which could actually degrade the performance on older models if pushed out universally. Of course, some commentators argue that manufacturers and operators are not really motivated to release so many updates in order to encourage people to purchase the newer phones, but we cannot comment on this. For most exploits in the OS, Google quickly releases the fixes, but it still entails a long time for most users to receive the appropriate fix for their device from their network operators.

Some exploits are not in the original OS itself, but in the custom modifications made by manufacturers, such as the recent Samsung exploit for Galaxy S2/S3, Note, etc. Although they were quick to fix it, the fix still had to propagate through network operators to reach users. In the event that a major vulnerability appeared that was being exploited in huge numbers of older versions of Android, we don't think Google (or the phone manufacturers) would have any choice but to release an OTA patch for it. The question is would it reach all Android users and how long would it take?

Tighter control from Google over the platform may resolve some of the "fragmentation" issues, but this could have a knock-on effect and in turn impact the relationship it has with the device manufacturers. And there is an argument about drawing a line and forcing a cut-off point for older Android users, but it is usually the manufacturers that determine this; they are the ones to say whether or not they will continue to upgrade a particular model to support a newer version of Android. As devices pass their end-of-life support period, they may still be usable and adequately functional, but they are unlikely to receive support from the manufacturers in terms of updates and patches. In general, Google would only have to win from having most users using up-to-date versions of Android, but with the current model, they may not have much say in the matter.

Data Breaches that Could Lead to Identity Theft

Background

Hacking continued to be the primary way data breaches occurred in 2012, in much the same way as it was in 2011. However, where politically motivated hacktivism in 2011 resulted in some of the biggest data breaches we've seen, such activity waned somewhat in 2012. This is most apparent when looking at the biggest caches of stolen identities. In 2011, there were five data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 70 million identities. In contrast, 2012 saw only one breach larger than 10 million identities. As a result the overall average size of breaches has dropped significantly, down from 1.1 million to 604,826 identities per breach.

That's not to say that the threat posed by data breaches has dropped in the last year. While the average size has declined, the medium number of identities stolen is up, and significantly at that. Where the median number of identities stolen was 2,400 per breach in 2011, this number is up to 8,350 in 2012. That's an increase of around 3.5 times. Using the median is a useful measure because it ignores the extremes, the rare events that resulted in large numbers of identities being exposed, and is more representative of the underlying trend.

There were many high-profile hacking breaches last year that received lots of media attention for obvious reasons. Hacking can undermine institutional confidence in a company, and loss of personal data can result in damage to an organizations reputation. Despite the media hype around these breaches, hacking came in second to old-fashioned theft as the greatest source of data breaches last year according to the Norton Cybercrime Index data.[10] In the event of a data breach, many countries have existing data breach notification legislation that regulates the responsibilities of organizations conducting business after a data breach has occurred.

Methodology

The data for the data breaches that could lead to identity theft is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model that measures the levels of threats, including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. 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.[11] 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, or 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.

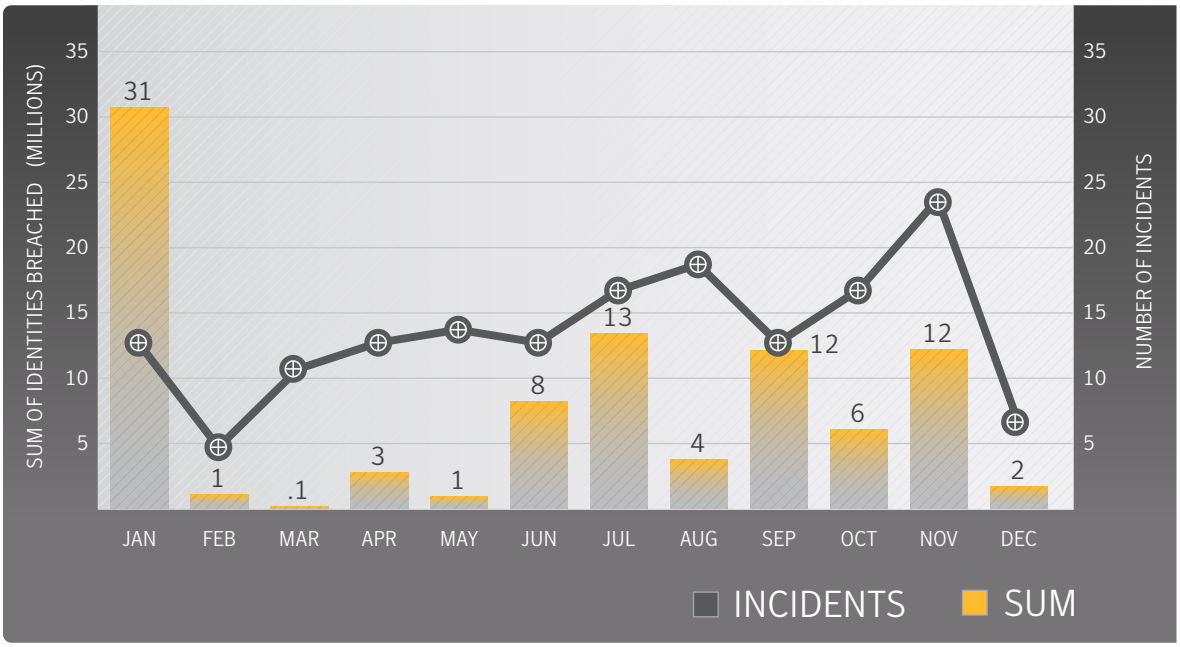
The sector that experienced the loss along with the cause of loss that occurred is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

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. (Hacking is an intentional act with the objective of stealing data that can be used for purposes of identity theft or other fraud.)

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.[12] 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 not required or encouraged to report data breaches may be under-represented in this data set.

Figure A.24. **Timeline of Data Breaches Showing Identities Breached in 2012, Global**

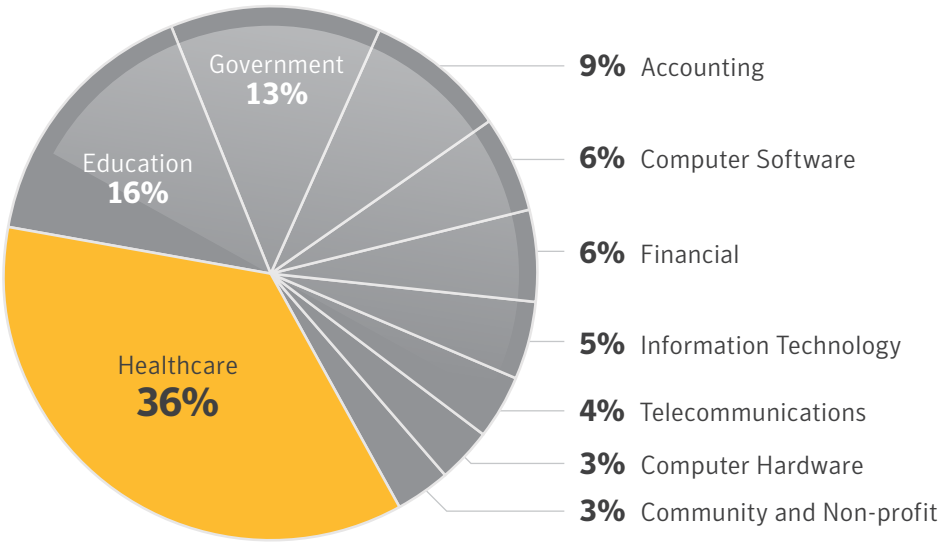
Source: Based on data provided by Norton Cyber Crime Index



Data and Commentary for Data Breaches that Could Lead to Identity Theft by Sector

Figure A.25. **Data Breaches that Could Lead to Identity Theft (Top 10 Sectors by Number of Data Breaches)**

Source: Based on data provided by Norton Cyber Crime Index



- *Healthcare and education sectors ranked top for number of data breaches, making up just over 50 percent of all data breaches. However, retail and the government sectors represent more than half of the identities exposed.*
- *This indicates that the sectors responsible for the most data breaches don't necessarily result in the largest caches of stolen identities.*

Figure A.25. **Data Breaches that Could Lead to Identity Theft (Top 10 Sectors by Number of Identities Exposed)**

Source: Based on data provided by Norton Cyber Crime Index

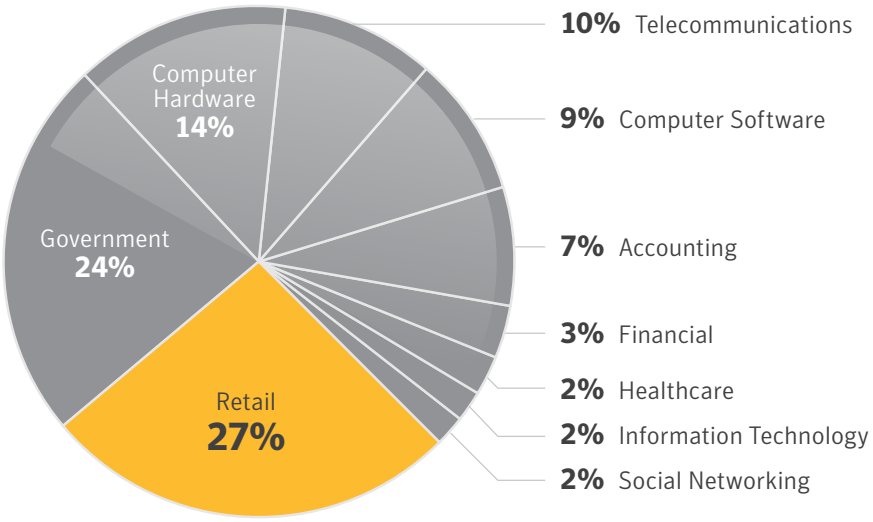
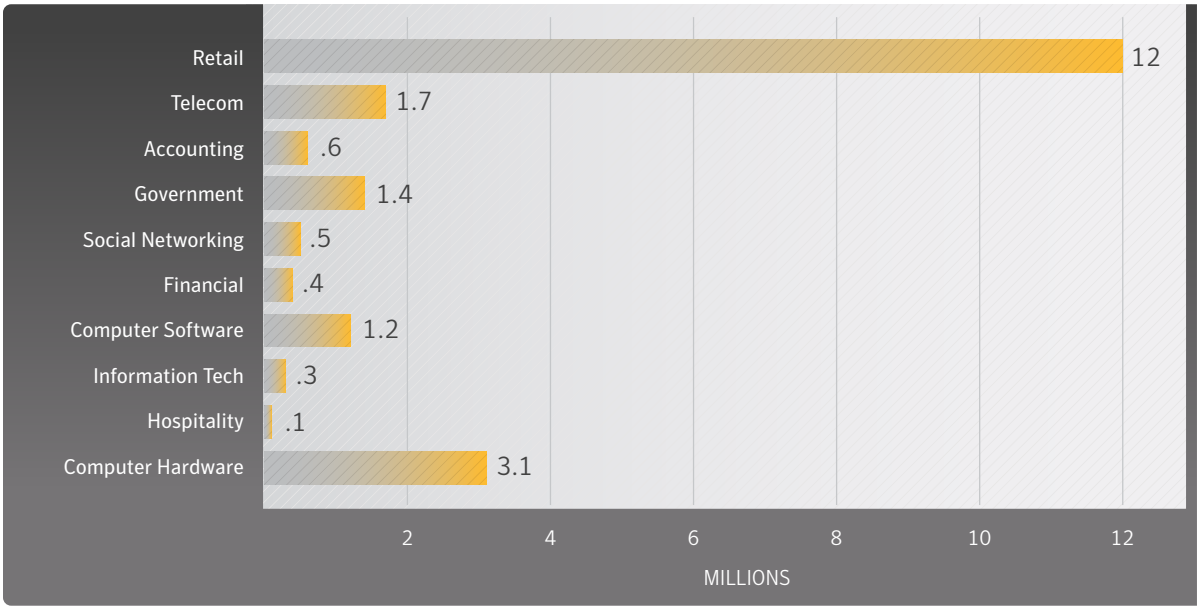


Figure A.26. **Average Number of Identities Exposed Per Data Breach by Notable Sector**

Source: Based on data provided by Norton Cyber Crime Index

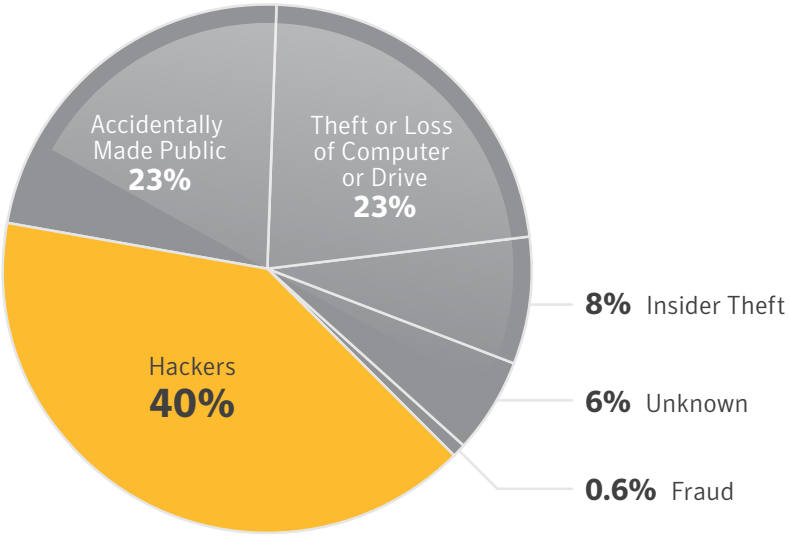


The largest number of identities exposed per breach in 2012 occurred in the retail sector, where one breach topped 10 million identities.

Data and Commentary for Data Breaches that Could Lead to Identity Theft by Cause

Figure A.27. **Data Breaches that Could Lead to Identity Theft by Number of Breaches**

Source: Based on data provided by Norton Cyber Crime Index



Hackers were the top cause for data breaches: The most frequent cause of data breaches (across all sectors) that could facilitate identity theft in 2012 was hacking attempts, which accounted for 40 percent of breaches that could lead to identities being exposed and this equated to approximately 18.5 million identities exposed in total.

Figure A.27. **Data Breaches that Could Lead to Identity Theft by Number of Identitites Exposed**

Source: Based on data provided by Norton Cyber Crime Index

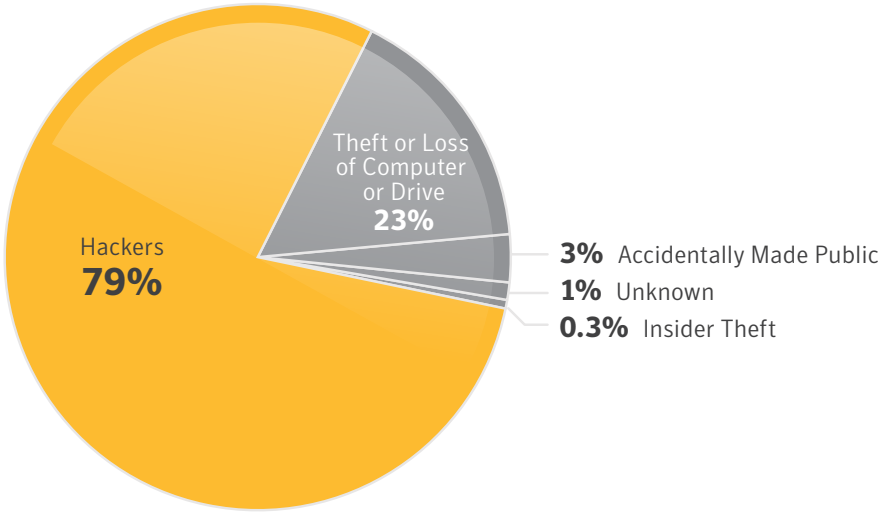
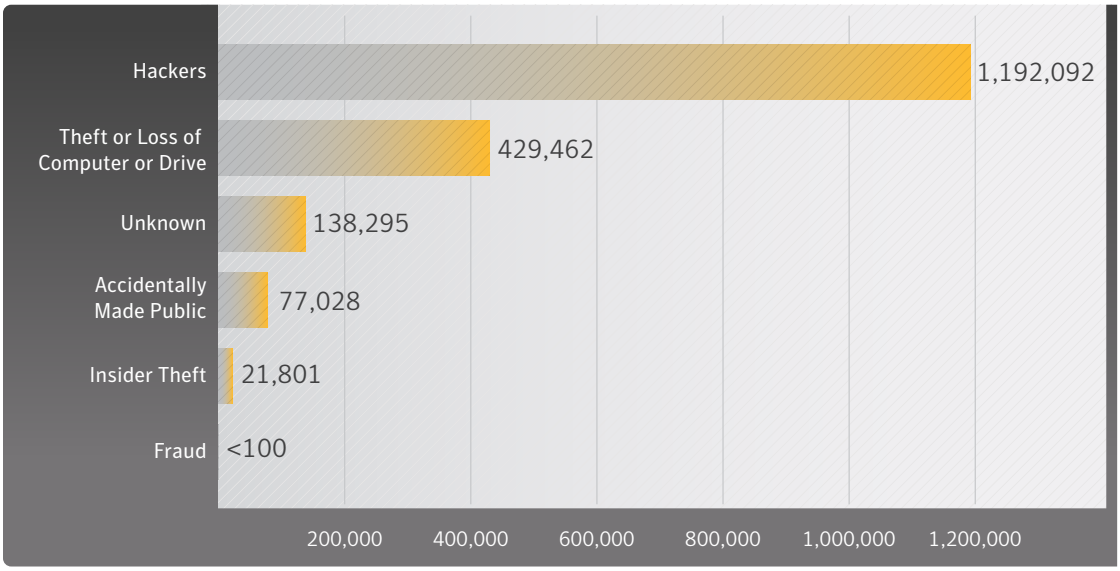


Figure A.28. **Average Number of Identities Exposed Per Data Breach by Cause**

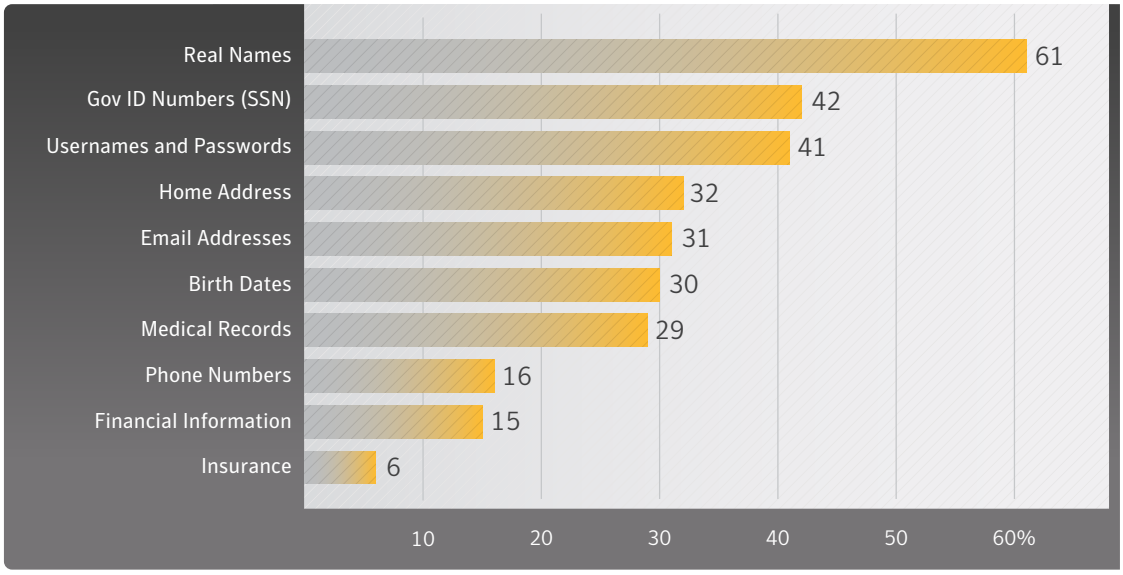
Source: Based on data provided by Norton Cyber Crime Index



- *Hacking was the leading source for reported identities exposed. Hackers were responsible for almost 80 percent of the identities exposed in the largest data breaches that occurred in 2012.*
- *The average number of identities exposed per data breach in hacking incidents was approximately 1.2 million.*

Figure A.29. **Type of Information Exposed in Deliberate Breaches**

Source: Based on data provided by Norton Cyber Crime Index



- *The most common types of identity information leaked in deliberate data breaches were real names, accounting for two-thirds of the identities breached in 2012.*
- *Government ID numbers, such as Social Security numbers, were found in 42 percent of breaches*
- *Usernames and passwords were identified in 41 percent of the identity breaches.*

Threat Activity Trends Endnotes

01 Internet population and penetration rates in 2012 courtesy of Internet Word Stats http://www.internetworldstats.com.

02 See http://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99.

03 See http://www.symantec.com/connect/blogs/update-androidcounterclank.

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 International Mobile Equipment Identity.

08 International Mobile Subscriber Identity.

09 See http://developer.android.com/about/dashboards/index.html.

10 See http://www.nortoncybercrimeindex.com/.

11 See http://www.idanalytics.com/.

12 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/HIP AAGenInfo/.

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. Well over 133 million 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 with which 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.

In this section, the following malicious code trends are analyzed for 2012:

- Top Malicious Code Families
- Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
- Propagation Mechanisms
- Industrial Espionage: Targeted Attacks and advanced Persistent Threats (APTs)

Top Malicious Code Families

Background

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.

Symantec analyzes new and existing malicious code families to determine which threat types and attack vectors 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 them to 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 threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway or cloud-based filtering.

Methodology

A malicious code family is initially compromised up 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 family rankings tend to be weighted towards file-infecting threats due to their nature. These threats tend to infect large numbers of executable files in the hopes that they will spread or be shared out to other computers. This propagation approach increases their overall presence when looking at the total number of malicious files in the threat landscape. In contrast, a threat like a Trojan, which doesn't use automatic propagation techniques, will not rank as highly. As a result, malicious code families that include file-infecting functionality are picked up by antivirus sensors more frequently and will rank higher in overall numbers.

Overall, the top ten list of malicious code families accounted for 41.2 percent of all potential infections blocked in 2012.

Figure B.1. **Overall Top Malicious Code Families, 2012**

Source: Symantec

Rank	Name	Type	Propagation Mechanisms	Impacts/Features	% Overall
1	W32.Ramnit	Virus/Worm	Executable files and removable drives	Infects various file types, including executable files, and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	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.	7.6%
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.	5.4%
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.	3.7%
5	W32.SillyFDC	Worm	Removable drives	Downloads additional threats and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	3.1%
6	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.	2.1%
7	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.	1.5%
8	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.	1.2%
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.	0.6%
10	W32.Xpaj	Virus	Executables/removable, mapped, and network drives	Infects .dll, .exe, .scr, and .sys files on the compromised computer.	0.6%

Figure B.2. **Relative Volume of Reports of Top 10 Malicious Code Families in 2012 by Percentage**

Source: Symantec

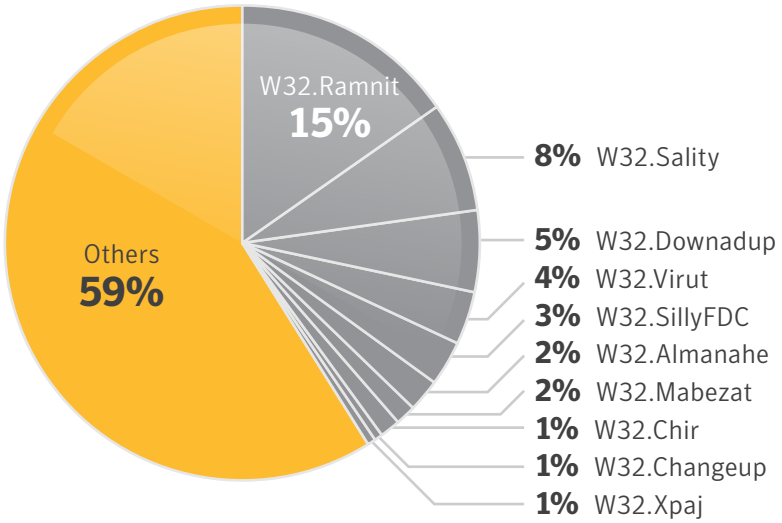


Figure B.3. **Relative Proportion of Top 10 Malicious Code Blocked in Email Traffic by Symantec.cloud in 2012 by Percentage and Ratio**

Source: Symantec

Rank	Malware	% of Email Malware	Equivalent Ratio in Email
1	Exploit/SpoofBBB	1.58%	1 in 63.4
2	Trojan.Bredolab	1.46%	1 in 68.7
3	EML/Worm.XX.dam	0.85%	1 in 117.5
4	Exploit/SuspLink	0.78%	1 in 127.9
5	Exploit/LinkAliasPostcard-4733	0.66%	1 in 151.0
6	W32/Netsky.c-mm	0.58%	1 in 171.1
7	Trojan.Sasfis.dam	0.53%	1 in 187.5
8	Exploit/Link-FakeACHUpdate	0.52%	1 in 190.7
9	Exploit/FakeAttach	0.51%	1 in 194.7
10	W32/Netsky.P-mm	0.51%	1 in 196.7

Figure B.4. **Trend of Malicious Code Blocked in Email Traffic by Symantec.cloud – 2011 vs 2012**

Source: Symantec.cloud

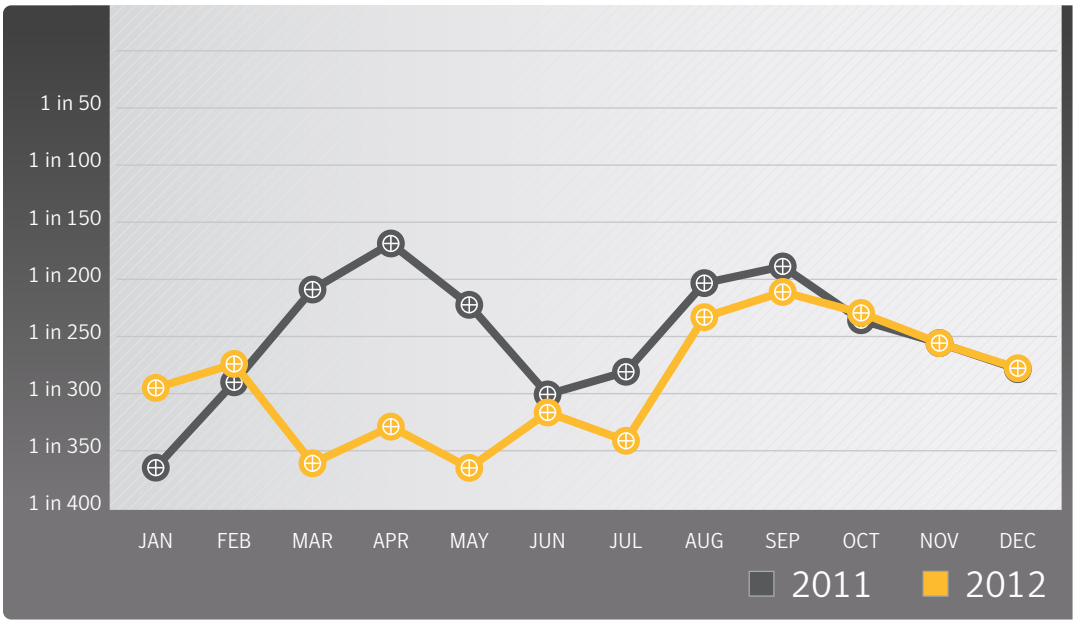


Figure B.5. **Relative Proportion of Top 10 Malicious Code Blocked in Web Traffic by Symantec.cloud In 2012 by Percentage and Ratio**

Source: Symantec.cloud

Rank	Name	% of Email Malware	Equivalent Ratio in Email
1	Trojan.JS.Iframe.AOX	10.6%	1 in 9.5
2	Trojan.Iframe.XI	7.1%	1 in 14.2
3	Infostealer.Gampass	5.2%	1 in 19.3
4	Dropped:Rootkit.49324	4.6%	1 in 21.6
5	Exploit.Link-JavaScript-4cda	4.4%	1 in 22.9
6	Exploit.Link-JavaScript-3f9f	4.0%	1 in 25.1
7	Suspicious.Emit	3.3%	1 in 30.1
8	Trojan.Script.12023	3.2%	1 in 31.5
9	Dropped:Trojan.PWS.OnlineGames.KDVN	3.1%	1 in 32.0
10	W32.Almanahe.B	2.2%	1 in 46.3

Commentary

- **Ramnit again beats Sality to become the most prevalent malicious code family in 2012.** Ranked first again in 2011, the top malicious code family by volume of potential infections in 2012 was Ramnit.

  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 2012, Sality (7.6 percent).

  First discovered in 2010, W32.Ramnit has been a prominent feature of the threat landscape since then, often switching places with Sality throughout the year as the two families jockey for first position.

  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 and others) effective vehicles for installing additional malicious code on computers.

- **The Sality family of malware, ranked second, 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 a bit of momentum:** Downadup (a.k.a. Conficker) was ranked in third position in 2012, compared with 2011 when it was ranked fourth-most malicious code family by volume of potential infections in 2011. Downadup propagates by exploiting vulnerabilities in order to copy itself to network shares. Downadup was estimated to have infected slightly more than 2 million PCs worldwide at the end of 2012,[1] compared with approximately 3 million at the end of 2011.

- **Overall in 2012, 1 in 281.8 emails was identified as malicious**, compared with 1 in 238.8 in 2011; **22.5 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 39.1 percent in 2010, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the Web.

- In 2012, 12.6 percent of malicious code detected 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.

- **Exploit/SpoofBBB** was the most frequently blocked malware in email traffic by Symantec.cloud in 2012, with **Trojan.Bredolab** taking the second position.

- **Trojan.JS.Iframe.AOX** was the most frequently blocked malicious activity in Web traffic filtered by Symantec.cloud in 2012. Detection for a malicious IFRAME is triggered in HTML files that contain hidden 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.

- **Stuxnet in 2012:** Despite being developed for a very specific type of target, the number of reports of potential Stuxnet infections observed by Symantec in 2012 placed the worm at a rank beyond 30 among malicious code families, compared with 18 in 2011. The Stuxnet worm generated a significant amount of attention in 2010 because it was the first malicious code designed specifically to attack Programmable Logic Controller (PLC) industry control systems.[2] Notably, Stuxnet was the first malicious code family that may directly affect the physical world and proves the feasibility for malicious code to cause potentially dramatic physical destruction.

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. Of course, there may also be other factors at work, based on the local economic conditions that may 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 because they are less likely to have the same levels of in-depth defenses as a larger organization, which is more likely to have greater budgetary expenditure applied to their security countermeasures.

Methodology

Analysis of malicious code activity based on geography, industry, and size are based on the telemetry analysis from Symantec.cloud clients for of threats detected and blocked against those organizations in email traffic during 2012.

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

Data

Figure B.6. **Proportion of Email Traffic Identified as Malicious by Industry Sector, 2012**

Source: Symantec.cloud

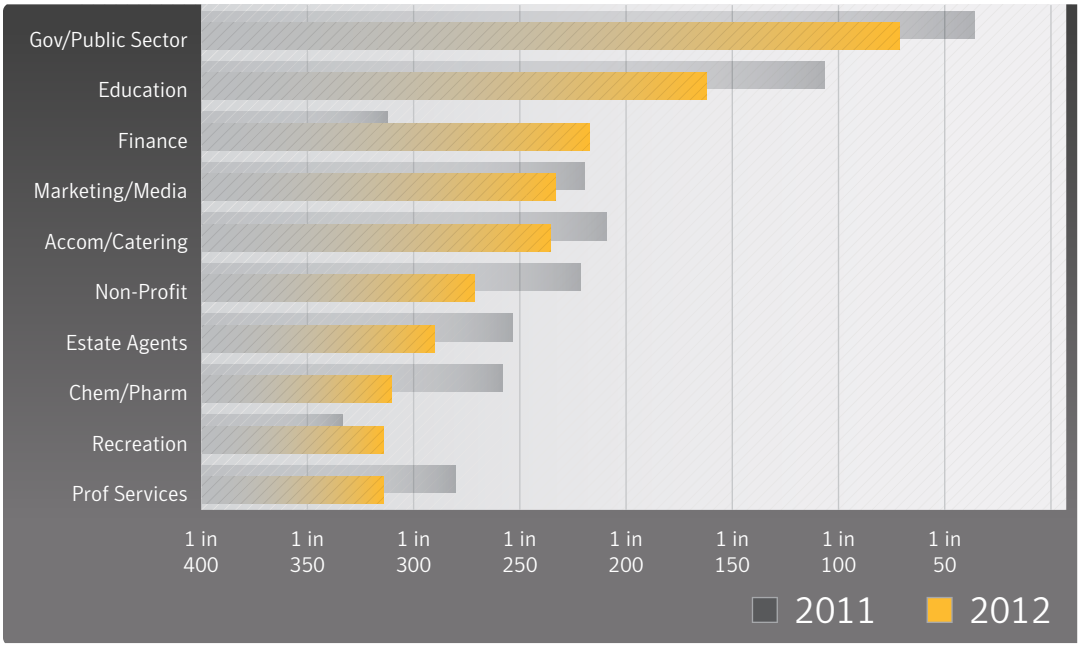


Figure B.7. **Proportion of Email Traffic Identified as Malicious by Organization Size, 2012**

Source: Symantec.cloud

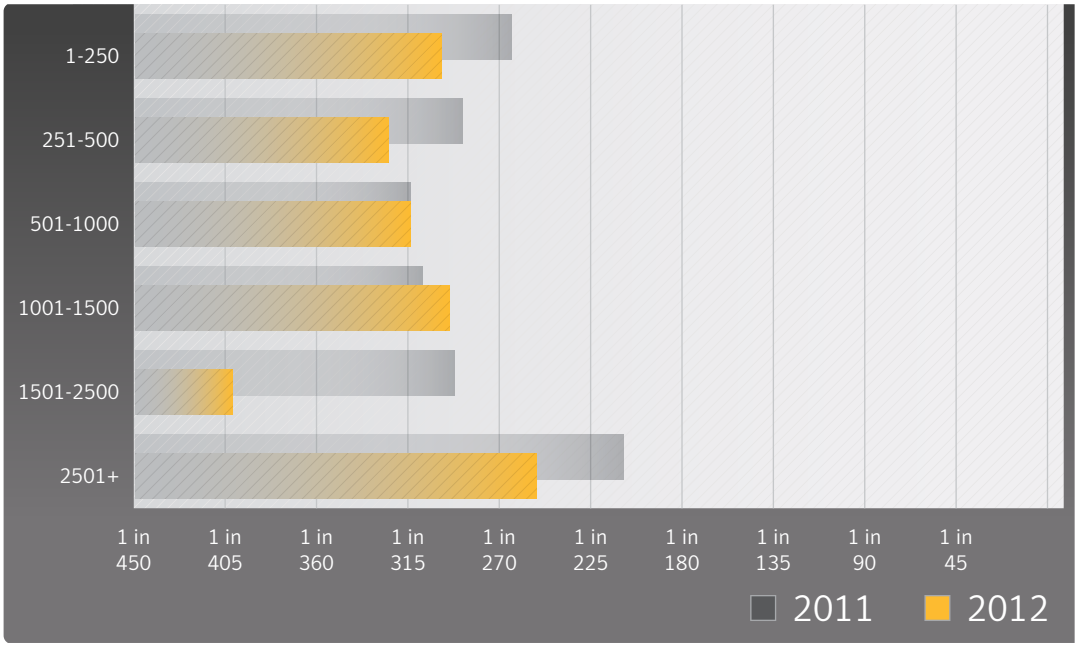
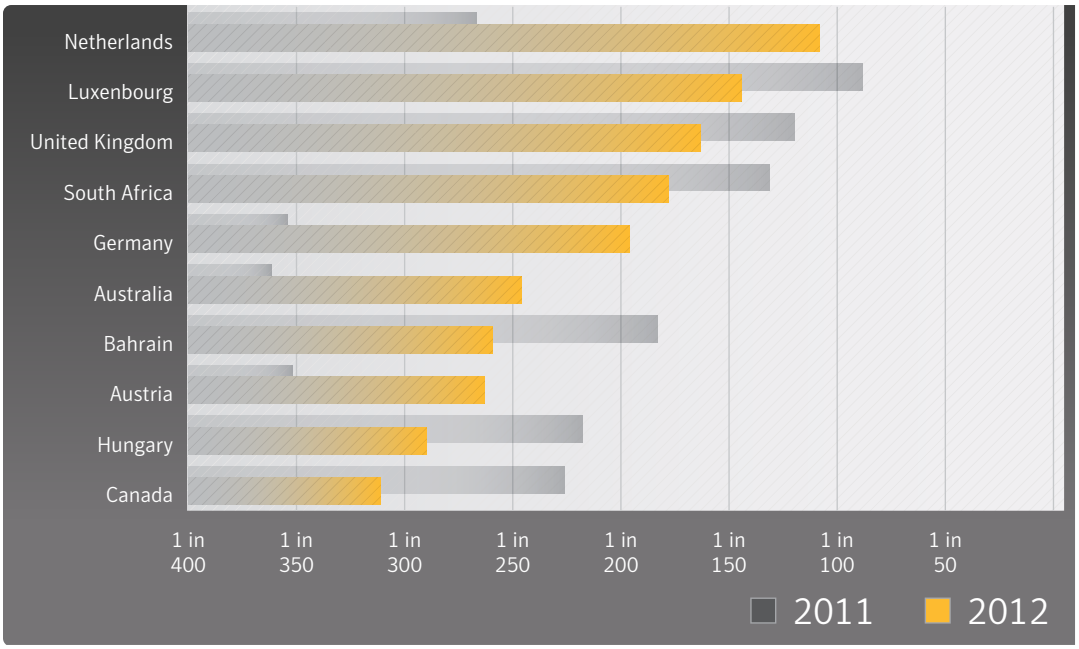


Figure B.8. **Proportion of Email Traffic Identified as Malicious by Geographic Location, 2012**

Source: Symantec.cloud



Commentary

- The rate of malicious attacks carried by email has increased for four of the top 10 geographies being targeted and decreased for the other six; malicious email threats fell in 2011 for organizations in Luxembourg, United Kingdom, South Africa, Bahrain, Hungary, and Canada.
- Businesses in the Netherlands were subjected to the highest average ratio of malicious email-borne email in 2012, with 1 in 108.0 emails blocked as malicious, compared with 1 in 266.8 in 2011.
- Globally, organizations in the Government and Public sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 72.2 emails blocked as malicious in 2012, compared with 1 in 41.1 for 2011.
- Malicious email threats have increased for all sizes of organizations, with 1 in 252.1 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2012, compared with 1 in 205.1 in 2011.
- 1 in 299.2 emails were blocked as malicious for SMBs with between 1-250 employees in 2012, compared with 1 in 267.9 in 2011

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.[3] 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.[4]

Data

Figure B.9. **Propagation Mechanisms**

Source: Symantec

Rank	Propagation Mechanisms	2012 Percentage	Change	2011 Percentage
1	**EXECUTABLE FILE SHARING.** The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	71%	-5%	76%
2	**FILE TRANSFER, CIFS CIFS.** This 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.	33%	-10%	43%
3	**REMOTELY EXPLOITABLE VULNERABILITY.** The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	26%	-2%	28%
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%	-6%	14%
5	**FILE TRANSFER, P2P.** The malicious code copies itself to folders on an infected computer that are associated with P2P file sharing applications. When the application runs, the malicious file will be shared with other users on the same P2P network.	4%	-3%	7%
6	**FILE TRANSFER, NON-EXECUTABLE FILE SHARING.** The malicious code infects non-executable files.	3%	+1%	2%
7	**FILE TRANSFER, HTTP, EMBEDDED URL, 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%	+2%	1%
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%	-0%	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%	-4%	5%
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 2012, 71 percent of malicious code propagated as executables, a decrease from 76 percent in 2011. 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 2012.
- **Remotely exploitable vulnerabilities decrease:** The percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2012 at 26 percent was 2 percentage points lower than in 2011. Examples of attacks employing this mechanism also include Downadup, which gains a bit of momentum and is still a major contributing factor to the threat landscape, ranked third position in 2012.
- **File transfer using CIFS is in decline:** The percentage of malicious code that propagated through CIFS file transfer fell by 10 percentage points between 2011 and 2012, a deeper decline than the one seen in 2011. Fewer attacks exploited CIFS as an infection vector in 2012.
- **File transfer via email attachments continues to decline:** It is worth noting the continued decline in the percentage of malicious code that propagated through email attachments for the fifth year running. Between 2011 and 2012, the proportion of malware using this mechanism fell by six percentage points.
- While this propagation mechanism is still effective, it was expected that this downward trend would contine; however, the shift towards using malicious URLS that was observed in 2011 did not continue as expected into 2012.

Industrial Espionage: Targeted Attacks and Advanced Persistent Threats (APTs)

Background

With targeted attacks and advanced persistent threats being very much in the news in 2012, in this section we review targeted attacks and look more closely at what has been described as "advanced persistent threats" or APTs. Terms such as APT have been overused and sometimes misused, but APTs are a real threat to some companies and industries.

As noted earlier in this section, overall in 2012, 1 in 281.8 emails were identified as malicious, but approximately 0.2 percent of those were highly targeted. This means that highly targeted attacks, which may be the precursor to an APT, account for approximately one in every two million emails, still a rare incident rate. However, targeted malware in general has grown in volume and complexity in recent years, but as it is designed to steal company secrets, it can be very difficult for recipients to recognize, especially when the attacker employs compelling social engineering techniques, as we highlight in this report.

Targeted attacks have been around for a number of years now, and when they first surfaced back in 2005, Symantec.cloud identified and blocked approximately one attack each week. Over the course of the following year, this number rose to one or two per day, and over the following years it rose still further. The global average number of attacks per day in 2012 was 116, compared with 82 in 2011 and 77 in 2010. We witnessed one large attack in April (see Figure B.10). Events like this are extremely rare, and this particular attack resulted in a large jump for that month. Without adjusting for this, the global average would be nearer to 143 per day with this company included.

A highly targeted attack is typically the precursor to an APT, and the typical profile of a highly targeted attack will commonly exploit a maliciously crafted document or executable, which is emailed to a specific individual, or small group of individuals. These emails will be dressed up with a social engineering element to make it more interesting and relevant.

The term "APT" has evolved to describe a unique category of targeted attacks that are specifically designed to target a particular individual or organization. APTs are designed to stay below the radar, and remain undetected for as long as possible, a characteristic that makes them especially effective, moving quietly and slowly in order to evade detection. Unlike the fast-money schemes typical of more common targeted attacks, APTs may have international espionage and/or sabotage objectives.

The objective of an APT may include military, political or economic intelligence gathering, confidential or trade secret threat, disruption of operations, or even the destruction of equipment.

Another characteristic of an APT is that it will be part of a longer-term campaign and not follow the opportunistic "smash-and-grab" approach typical of most malware in circulation today. Its purpose will be to remain undetected for as long as possible, perhaps using a variety of attacks over that period. If one attack fails, then a different approach—one more likely to succeed—will be taken in the weeks to come. If successful, an attacker can use the compromised systems as a beachhead for subsequent attacks.

All of which illustrate how these attacks can be both advanced and persistent threats. They are advanced because of the methods employed to avoid detection, such as the use of zero-day exploits, and the means used to communicate with the command and control network; command and control instructions often involve encrypted traffic, typically sent in small bursts and disguised as normal network traffic. The key to ensuring that any stolen information can be exfiltrated without detection requires the attacker to avoid using easily detectable encryption, and to use common protocol channels that would not look out of place, but while making sure the data remains hidden.

Furthermore, they can be described as persistent because the aim is to maintain a foothold within the compromised company's infrastructure, and in order to achieve this, the attacker will use numerous methods. The attackers have a very clear and specific objective, they are well-funded and well-organized, and without the right protection in place, these threats have both the capability and the intent to achieve their desired goals.

Methodology

Defining what is meant by targeted attacks and APT is important in order to better understand the nature of this mounting threat and to make sure that you have invested in the right kinds of defenses for your organization.

The types of organizations being targeted are often thought to be large, well-known multi-national organizations, often within particular industries, including the public sector, defense, energy, and pharmaceutical. In more recent years the scope has widened to include almost any organization, including SMBs. But what do we really mean by targeted attacks and advanced persistent threats?

An attack can be considered as targeted if it is intended for a specific person or organization, typically created to evade traditional security defenses and frequently using advanced

social engineering techniques. However, not all targeted attacks lead to an APT; for example, the Zeus banking Trojan can be targeted and will use social engineering in order to trick the recipient into activating the malware. But Zeus is not an APT. The attacker doesn't necessarily care about who the individual recipient is; they may have been selected simply because the attacker is able to exploit information gathered about that individual, typically harvested through social networking websites.

Social engineering has always been at the forefront of many of these more sophisticated types of attack. Without strong social engineering, or "head-hacking," even the most technically sophisticated attacks are unlikely to succeed. Many socially engineered attacks are based on information harvested through social networking and social media websites. Once the attackers are able to understand their targets' interests, hobbies, with whom they socialize, and who else may be in their networks, they are often able to construct more believable and convincing attacks.

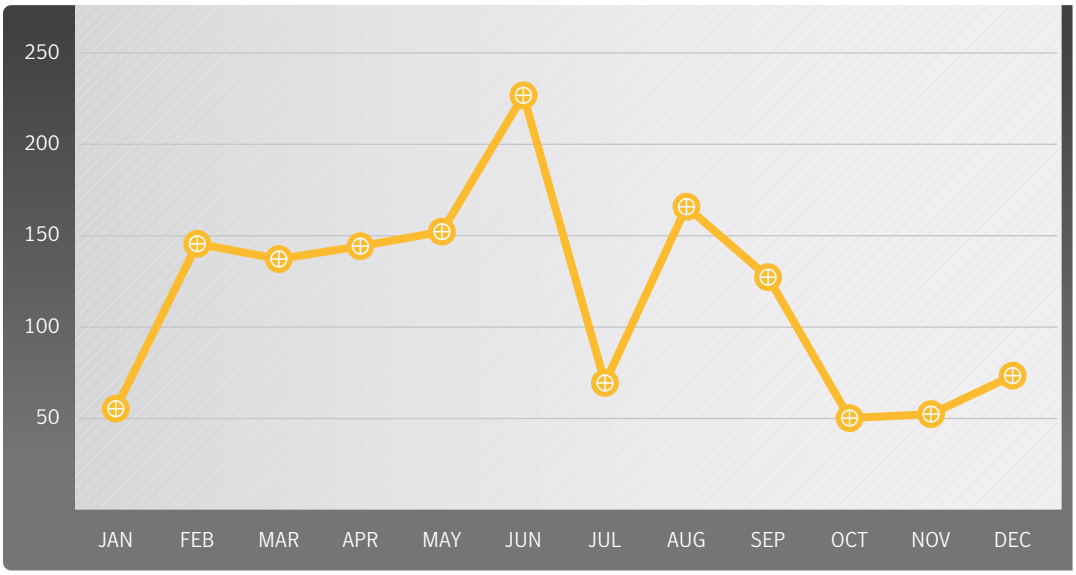
The data in this section is based on analysis of targeted email malware identified and blocked by Symantec.cloud on behalf of its customers in 2012.

Data and Commentary

Malware such as Stuxnet in 2010, Duqu in 2011, and Flamer and Disttrack in 2012 show increasing levels of sophistication and danger. For example, the Disttrack malware used in the Shamoon attacks on a Saudi oil firm had the ability to wipe hard drives.[5]

The same techniques used by cybercriminals for industrial espionage may also be used by states and state proxies for cyber attacks and political espionage. Sophisticated attacks may be reverse-engineered and copied so that the same or similar techniques can be used in less discriminate attacks. A further risk is that malware developed for cybersabotage may spread beyond its intended target and infect other computers in a kind of collateral damage.

Figure B.10. **Average Number of Targeted Email Attacks Per Day, 2012**
Source: Symantec.cloud



Targeted attacks have become an established part of the threat landscape and safeguarding against them has become one of the main concerns of CISOs and IT managers. Targeted attacks are commonly used for the purposes of industrial espionage to gain access to the confidential information on a compromised computer system or network. They are fewer but potentially the most difficult attacks to defend against. It is difficult to attribute an attack to a specific group or a government without sufficient evidence. The motivation and the resources of the attacker sometimes hint to the possibility that the attacker could be state sponsored, but finding clear evidence is difficult. Attacks that could be state sponsored appear to be rare in comparison with regular cybercrime, though they have often gained more notoriety. They can be among the most sophisticated and damaging of these types of threats. Governments are undoubtedly devoting more resources to defensive and offensive cyberwarfare capabilities. In 2012, it was still unlikely that most businesses would encounter such an attack, and the greatest risk comes from the more prevalent targeted attacks that are created for the purposes of industrial espionage. Increasingly, SMBs are finding themselves on the frontline of these attacks as they have fewer resources to combat the threat and a successful attack here may subsequently be used as the springboard to further attacks against a larger organization to which they may be a supplier.

To understand the nature of targeted attacks, Symantec collected data on over 55,000 attacks that could clearly be identified as targeted. These attacks were email-based and contained a malicious payload.

We saw a 41.5 percent increase in targeted attacks with more attacks aimed at companies with fewer than 250 staff members. One possible explanation is that attackers have accelerated their use of small companies as a way to infiltrate larger organizations further up the supply chain. Attackers started using watering hole attacks, a technique where malware on infected third-party websites is used to target employees of companies who might visit those websites.

The total number of attacks aimed at organizations with fewer than 2,500 employees is roughly equal to attacks aimed at organizations with greater than 2,500 employees.

R&D, sales, C-level, and senior employees were the most targeted in the same order.

Attackers want to capture the knowledge workers who have access to intellectual property (IP), but they don't have to attack them directly to get the information they want.

Too often organizations think that if they are not the target of a high profile attack, or if one attack has been blocked, that their troubles are over. However, our research shows that a targeted attack can go on for months. The attack will change over time, with new social engineering, new malware, and often leveraging multiple zero-day vulnerabilities. What our research does not show is attackers giving up after one attempt to breach an organization.

The Characteristics of a Targeted Attack

When comparing the number of targeted attacks directed at companies with 2,500 or more employees and companies with fewer than 2,500, we see an equal split.

Thirty-five percent of all targeted attacks are targeted at companies with fewer than 500 employees, as illustrated in figure B.13. And despite the commonly held belief of small businesses that they would never be the victims of a targeted attack, 30.8 percent of all targeted attacks are directed at companies with up to 250 employees.

Figure B.11. **Targeted Attacks by Company Size, 2012**

Source: Symantec.cloud

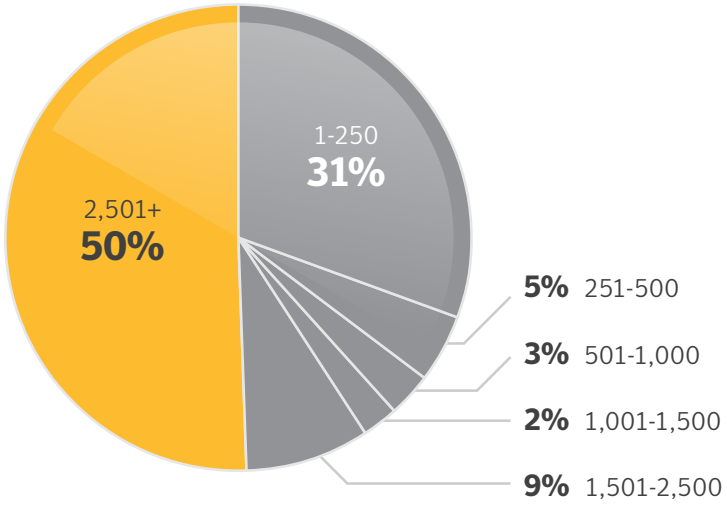
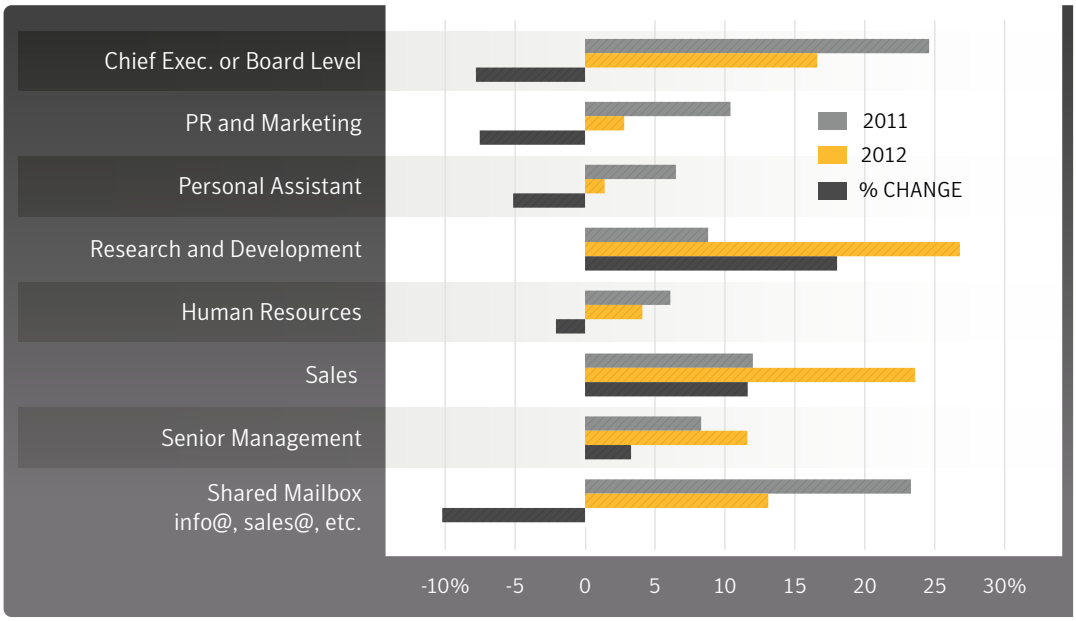


Figure B.12. **Targeted Attacks Against Job Function, 2012**

Source: Symantec.cloud



While 55 percent of the mailboxes targeted for attack are high-level executives, senior managers and people in R&D, the majority of targets are people that are unlikely to have such information. Why then are they targeted?

As we've said, they provide a stepping stone to the ultimate target. And in the case of personal assistants, sales and media (public relations), they work closely with people who are the ultimate target. But just as important, these people are also easy to find and research online: email addresses for public relations people, shared mailboxes, and recruiters are commonly found on a company's website.

Additionally, these people are used to being contacted by people they do not know. And in many cases part of the job requires them to open unsolicited files from strangers. Think of how many resumes a recruiter receives each day in a document or PDF file attachment. Finally, under the illusion that targeted attacks are only aimed at high-level executives or those working with the company's intellectual property (IP), they are less likely to have their guard up against social engineering.

In Figure B.16, we can see that malicious EXEs are largely used in targeted attacks (over one-third of attacks). However, malicious DOCs and PDFs are commonly used by attackers (44.4 percent of the attacks).

Looking at the break out of targeted attacks by industry, Manufacturing was the most-targeted sector in 2012, with 24.3 percent of targeted attacks destined for this sector, compared with 15 percent in 2011. Attacks against government and public sector organizations fell from 25 percent in 2011, when it was the most targeted sector, to 12 percent in 2012. It's likely the frontline attacks are moving down the supply chain, particularly for small to SMBs.

Conclusion

Targeted attacks should be concern for all organization, large and small. While C-level executives and those that work with a company's IP should be careful, everyone in an organization is at risk of being targeted. This is especially true of workers who in the course of their jobs typically receive email from people they don't know. In the end, no matter the size or type of organization you have or your role in that organization, you are at risk and best practices must be followed to protect the organization. Don't become the weakest link in the supply chain.

Figure B.13. **Breakdown of Document Types Being Attached to Targeted Attacks, 2012**

Source: Symantec.cloud

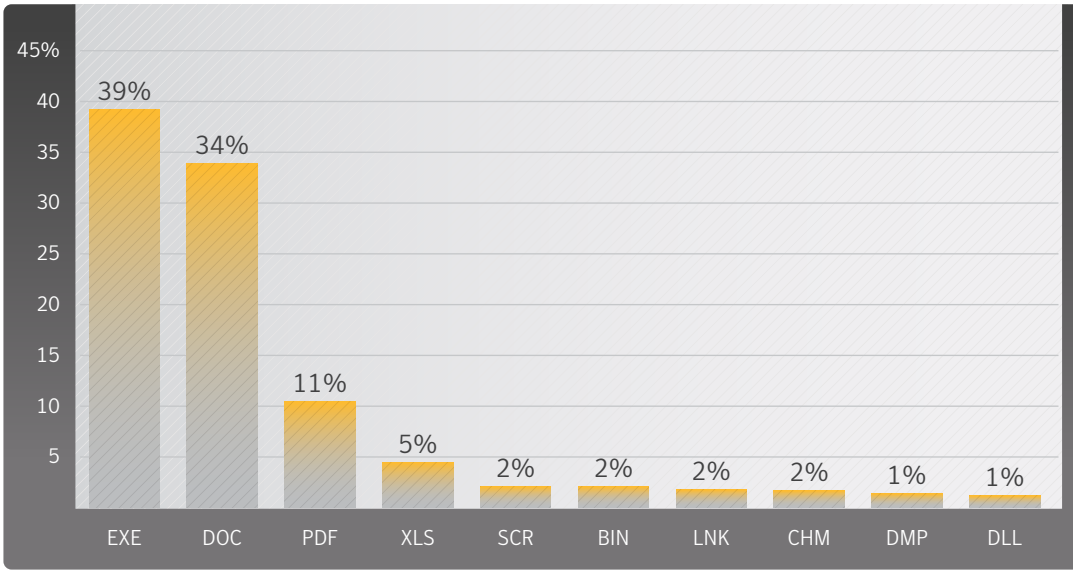
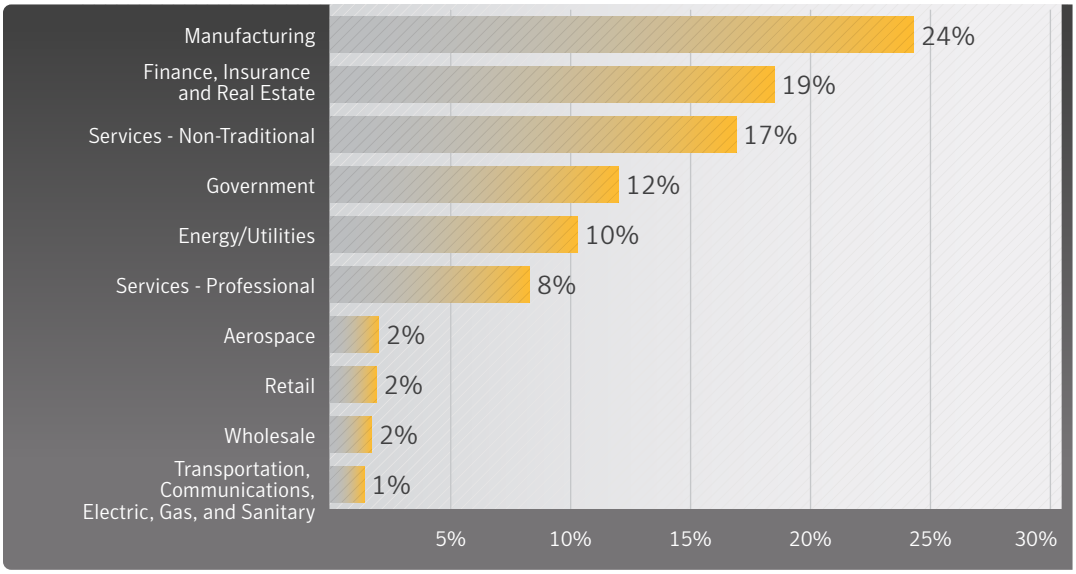


Figure B.14. **Analysis of Targeted Attacks by Top 10 Industry Sectors, 2012**

Source: Symantec.cloud



Malicious Code Trends Endnotes

01 See http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking#toc15.

02 See http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

03 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.

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

05 See http://www.symantec.com/connect/blogs/shamoon-attacks.

APPENDIX :: C SPAM AND FRAUD ACTIVITY TRENDS

Spam and Fraud Activity Trends

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 covers phishing and spam trends. It also discusses activities observed on underground economy servers because that is where much of the profit is made from phishing and spam attacks.

- 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
- Spam by Category
- Phishing Activity Trends
- Analysis of Phishing Activity by Geography, Industry Sector, and Company Size

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 2012

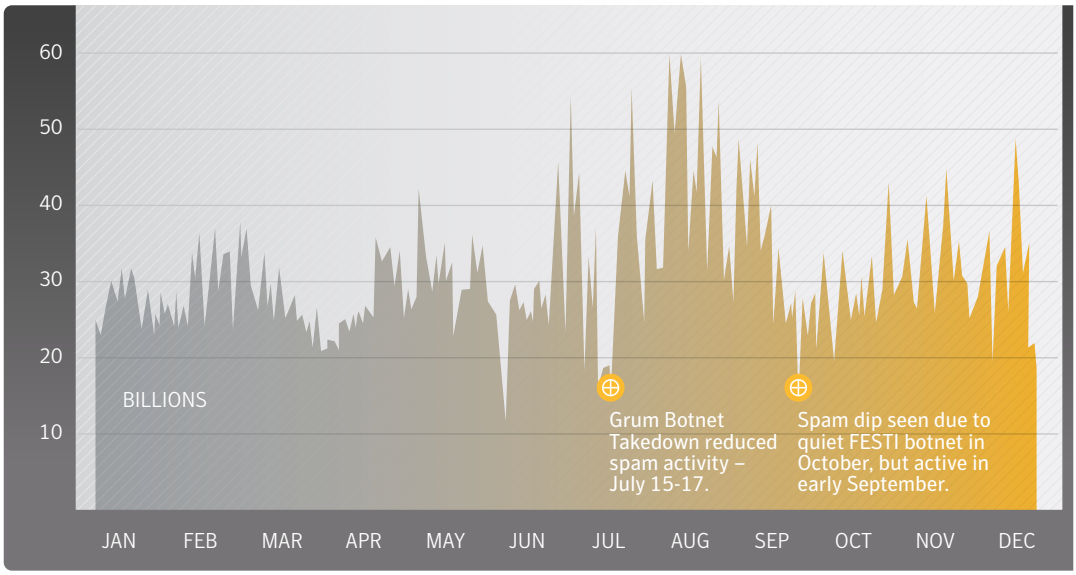
Methodology

The analysis for this section is based on global spam and overall email volumes for 2012. Global values are determined based on the statistically representative sample provided by Symantec's Brightmail[2] operations and spam rates include spam blocked by Symantec.cloud.

Data and Commentary

Figure C.1. **Global Spam Volume in Circulation, 2012**

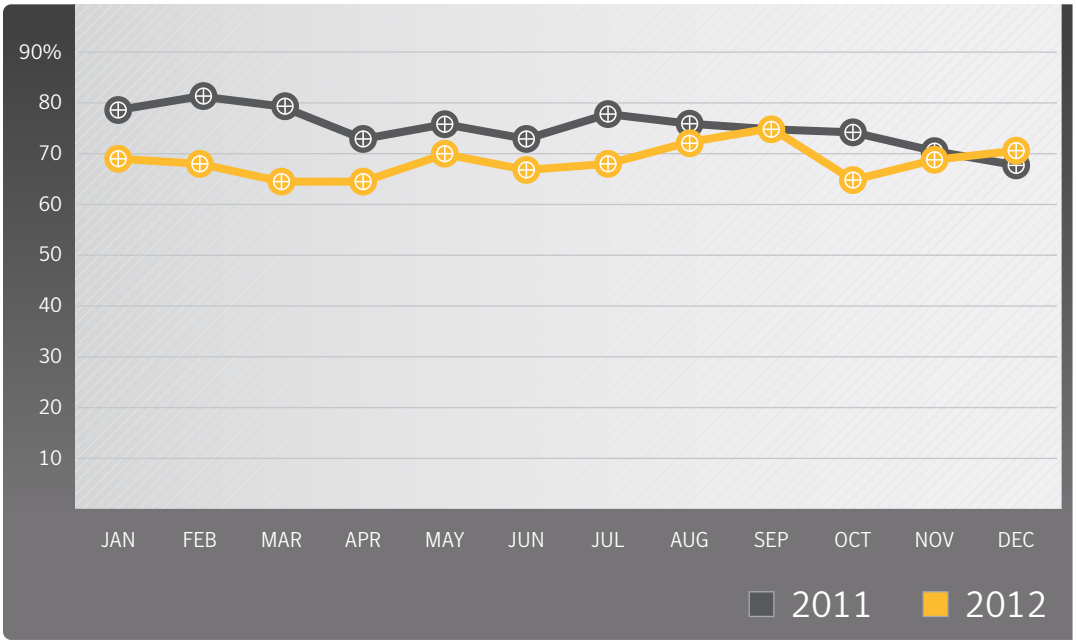
Source: Symantec



There were approximately 30 billion spam emails in circulation worldwide each day overall in 2012, compared with 42.1 billion in 2011; a decrease of 28.6 percent in global spam volume.

Figure C.2. **Proportion of Email Traffic Identified as Spam, 2011–2012**

Source: Symantec.cloud



Overall for 2012, 68.5 percent of email traffic was identified as spam, compared with 75.1 percent in 2011; a decrease of 6.6 percentage points.

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

Background

Spam activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace that can drive down prices, increasing adoption rates. Of course, there may also be other factors at work based on the local economic conditions that may 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 based on the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. SMBs may find themselves the target of a spam attack because SMBs are perceived to be softer targets because they are less likely to have the same levels of security countermeasures as larger organizations, which are more likely to have greater budgetary expenditure applied 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 2012.

Data

Figure C.3. **Proportion of Email Traffic Identified as Spam by Industry Sector, 2012**
Source: Symantec.cloud

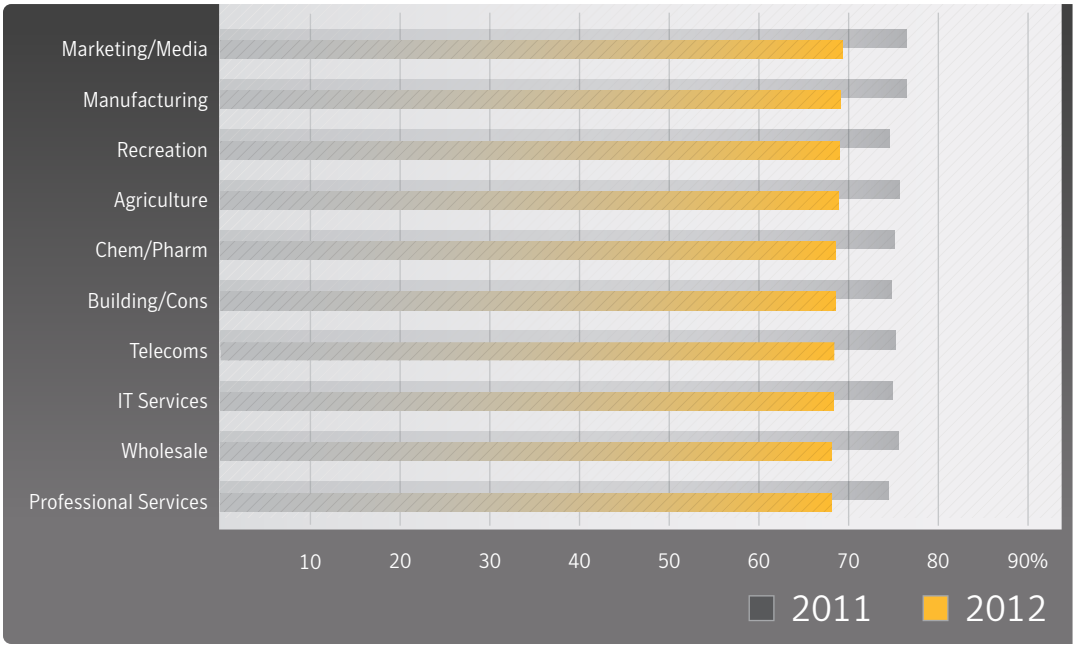


Figure C.4. **Proportion of Email Traffic Identified as Spam by Organization Size, 2012**

Source: Symantec.cloud

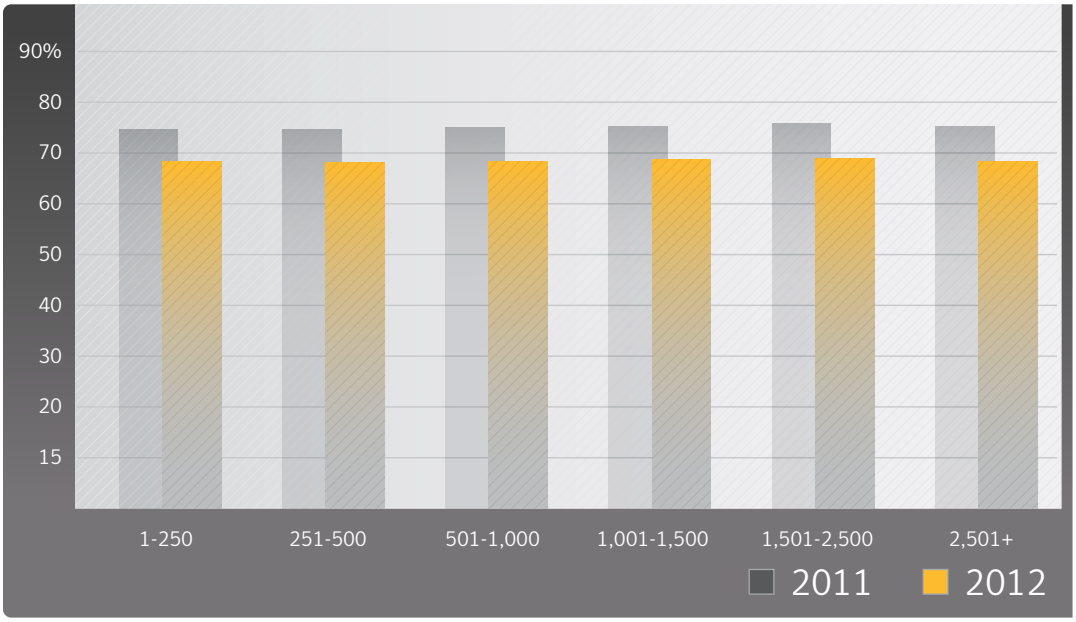
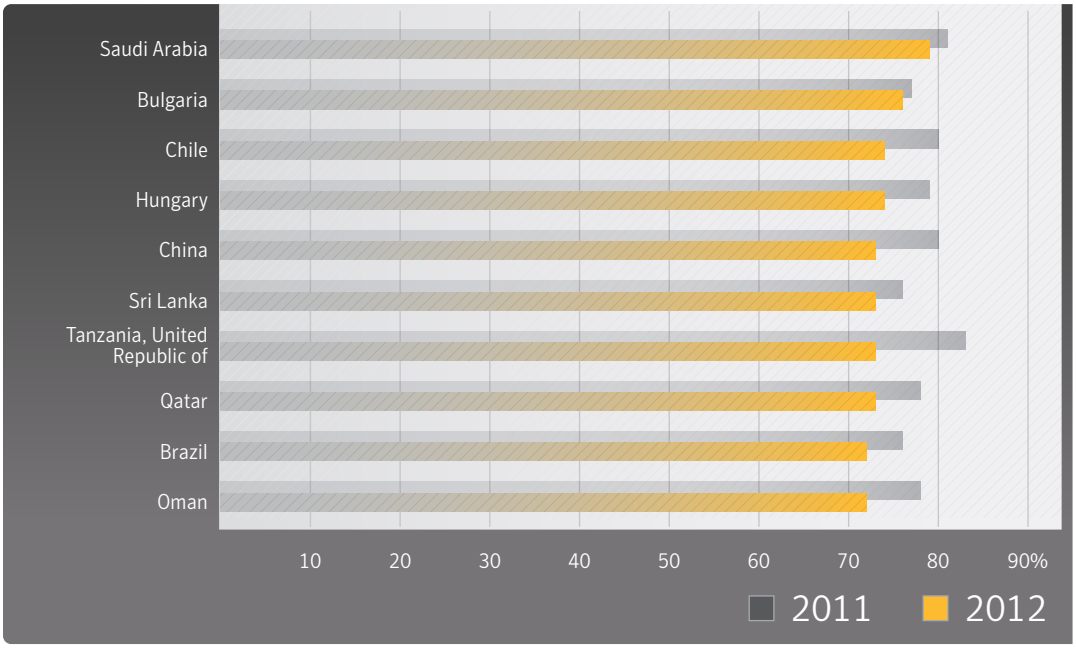


Figure C.5. **Proportion of Email Traffic Identified as Spam by Geographic Location, 2012**

Source: Symantec.cloud



Commentary

- The spam rate has decreased across all top 10 geographies in 2012. The highest rate for spam is for organizations in Saudi Arabia, with an overall average spam rate of 79.1 percent. In 2011, the highest rate was in Saudi Arabia, with an overall average spam rate of 80.9 percent.
- The spam rate has decreased across all top 10 industry sectors in 2012. Organizations in the Marketing/Media sector were subjected to the highest spam rate of 69.3 percent in 2012; in 2011, the automotive sector had the highest spam rate of 77.9 percent.
- The spam rate has decreased for all sizes of organization in 2012. 68.4 percent of emails sent to large enterprises with more than 2,500 employees in 2012 were identified as spam, compared with 75.2 percent in 2011.
- 68.4 percent of emails sent to SMBs with up to 250 employees in 2012 were identified as spam, compared with 74.6 percent in 2011.

Analysis of Spam Delivered by Botnets

Background

This section discusses botnets and their use in the sending of spam. Like ballistics analysis in the real world can reveal the gun used to fire a bullet, botnets can similarly be identified by common features within the structure of email headers and corresponding patterns during the SMTP transactions.[3] 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 for financial fraud or DDoS attacks.

Methodology

Symantec.cloud spam honeypots collected between 5–10 million spam emails each day during 2011. These are 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 are 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 data is up to date and accurate.

Data

Figure C.6. **Percentage of Spam Sent from Botnets in 2012**

Source: Symantec.cloud

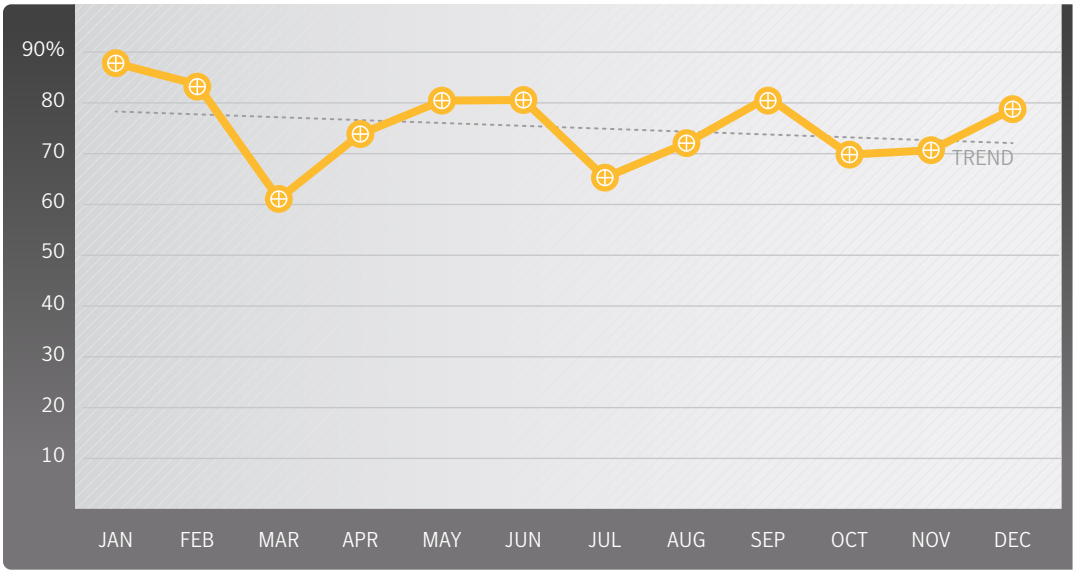


Figure C.7. **Analysis of Spam-sending Botnet Activity, 2012**

Source: Symantec.cloud

Botnet Name	% of Botnet Spam	Est. Spam Per Day	Top Sources of Spam from Botnet		
LETHIC	43.4%	9,632,000,000	India (14%)	Vietnam (6%)	Poland (5%)
CUTWAIL	21.8%	4,838,000,000	India (15%)	Russia (6%)	Brazil (6%)
GRUM	16.2%	3,585,000,000	India (18%)	Vietnam (13%)	Pakistan (10%)
FESTI	15.0%	3,331,000,000	Saudi Arabia (39%)	India (24%)	Turkey (12%)
MAAZBEN	1.3%	277,000,000	Brazil (12%)	India (10%)	United States (8%)
GHEG	0.7%	149,000,000	Indonesia (14%)	India (12%)	Vietnam (9%)
KELIHOS	0.6%	140,000,000	India (20%)	Peru (14%)	Turkey (12%)
XARVESTER	0.4%	90,000,000	UK (13%)	Italy (8%)	India (7%)
WALEDAC	0.2%	52,000,000	India (10%)	Kazakhstan (5%)	Brazil (5%)
BAGLE	0.2%	48,000,000	United States (20%)	China (18%)	Brazil (10%)

Commentary

- In 2011, approximately 78.8 percent of all spam was distributed by spam-sending botnets, compared with 88.2 percent in 2011, a decrease of 9.4 percentage points. This was in large part owing to the disruption of the Rustock botnet on 16 March 2011. By the end of 2011, this number rose to 81.2 percent.
- In the 7 days prior to the disruption of the Rustock botnet, each day approximately 51.2 billion spam emails were in circulation worldwide. In the 7 days following, this number fell to 31.7 billion, a decrease of 38.0 percent in global spam volume.
- The global spam rate during the 7 days prior to when the Rustock botnet ceasing spamming was 78.2 percent, compared with 70.0 percent in the 7 days after.
- During the second half of 2011, the change in frequency of botnet spam being distributed from botnets became much more noticeable, as shown in figure C.6. Large spam runs often lasted for only two or three days and when the spam run ceased, the volume of botnet-spam fell considerably; however, when Rustock was in operation during 2010 and during the first quarter of 2011, it was almost continually sending spam at a fairly regular and steady rate.

Significant Spam Tactics

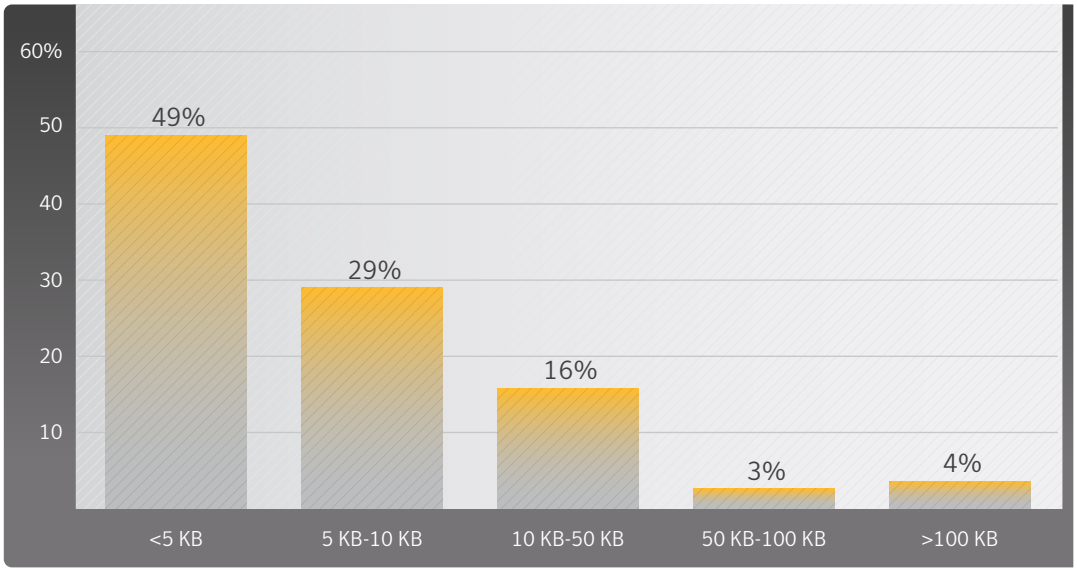
Background

This section discusses significant spam tactics used throughout 2012, including the size of spam messages and the languages used in spam emails.

Size of Spam Messages

Figure C.8. **Frequency of Spam Messages by Size, 2012**

Source: Symantec

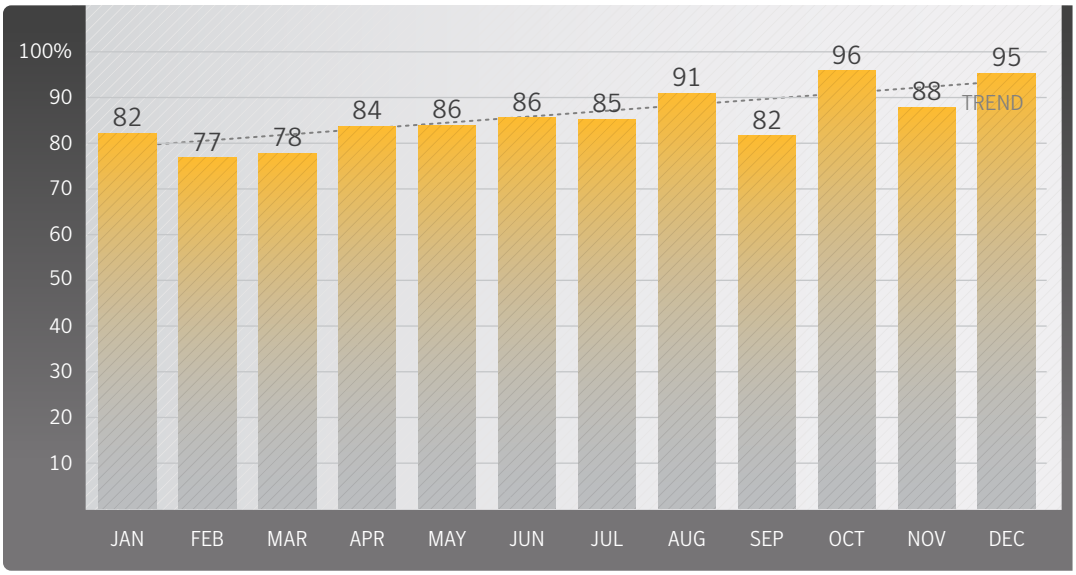


- *In 2012, 49 percent of spam messages were less than 5 KB in size. For spammers, smaller file sizes mean more messages can be sent using the same resources.*
- *Increased sizes are often associated with malicious activity, where email attachments contain malicious executable code.*

Proportion of Spam Messages Containing URLs

Figure C.9. **Proportion of Spam Messages Containing URLs, 2012**

Source: Symantec

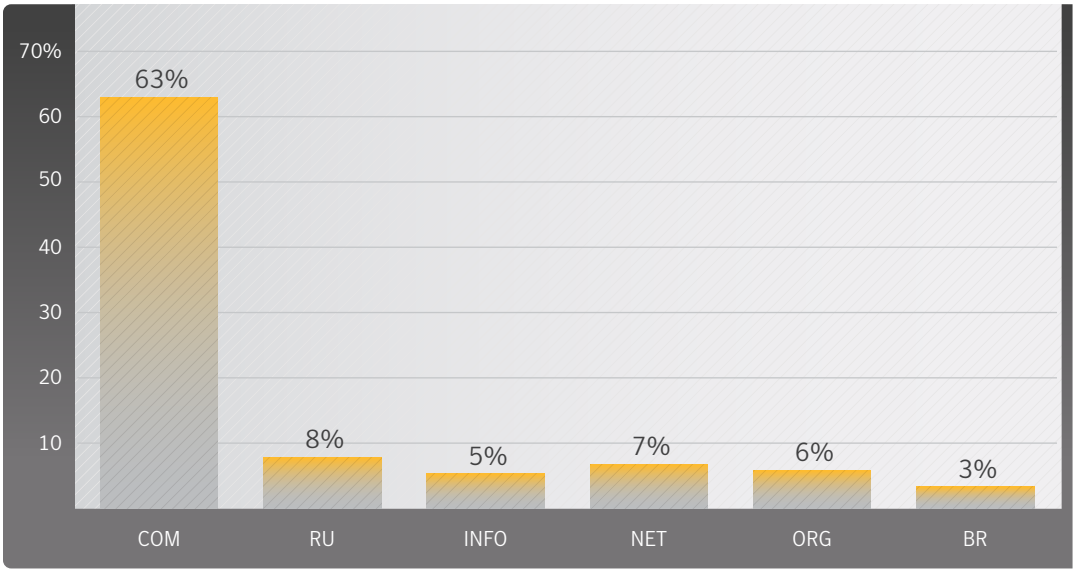


In 2012, 85.3 percent of spam messages contained at least one URL hyperlink, compared with 86.2 percent in 2011, a decrease of 0.9 percentage points.

Top-level Domains (TLD) Identified in Spam URLs

Figure C.10. **Analysis of Top-level Domains Used in Spam URLs, 2012**

Source: Symantec



Spam by Category

Background

Spam is created in a variety of different styles and complexities. Some spam is plain text with a URL; some is cluttered with images and/or attachments. Some comes 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 to "pollute" 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 would need 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 as to classifying the message as pharmaceutical spam or in the watches/jewelry category. Another challenge occurs when a pharmaceutical spam contains no obvious pharmaceutical-related words, but only 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. The most accurate way to overcome the ambiguity faced by using automated techniques to classify spam 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 view 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

Data

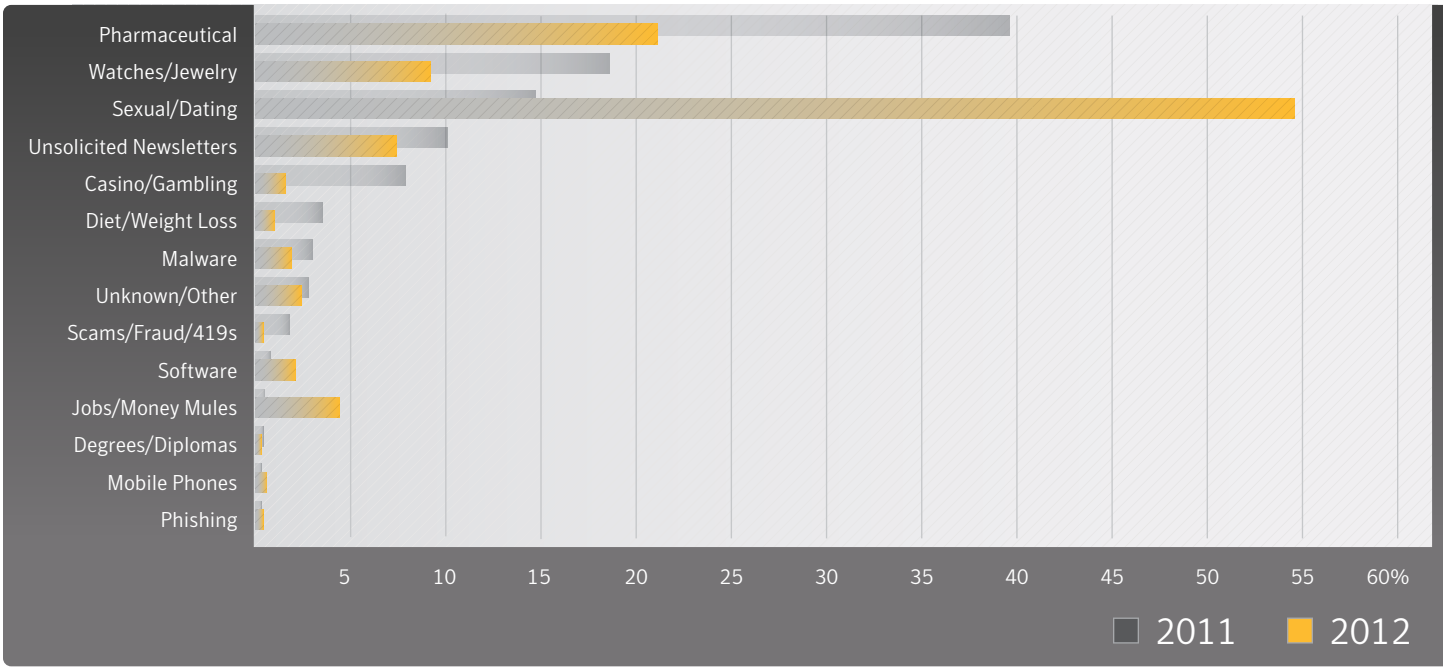
Figure C.11. **Spam by Category, 2012**

Source: Symantec.cloud

Category	2012	2011	Change
Pharmaceutical	21.1%	39.6%	-18.5%
Watches/Jewelry	9.2%	18.6%	-9.4%
Sexual/Dating	54.6%	14.7%	39.9%
Unsolicited Newsletters	7.4%	10.1%	-2.7%
Casino/Gambling	1.6%	7.9%	-6.3%
Diet/Weight Loss	1.0%	3.5%	-2.5%
Malware	1.9%	3.0%	-1.1%
Unknown/Other	2.4%	2.8%	-0.4%
Scams/Fraud/419s	0.4%	1.8%	-1.4%
Software	2.1%	0.8%	1.3%
Jobs/Money Mules	4.4%	0.5%	3.9%
Degrees/Diplomas	0.3%	0.4%	-0.1%
Mobile Phones	0.6%	0.3%	0.4%
Phishing	0.4%	0.3%	0.2%

Figure C.12. **Spam by Category, 2012**

Source: Symantec.cloud



Commentary

- Adult spam dominates this year, with more than half (54.6 percent) of all spam in 2012 related to adult spam, an increase of 39.9 percentage points compared with 2011. 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 Web cam site. Often any IM conversation would be handled by a bot responder, or a person working in a low-pay, offshore call center.
- The disruption of the Grum and Festi botnet in July and October 2012 respectively had a major impact on the decline in pharmaceutical spam products.
- 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 30 billion spam emails were sent globally each day in 2012. 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 in the categories 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™ [4] technology and analysis of phishing emails collected in spam honeypots. Symantec.cloud spam honeypots collected between 2–5 million spam emails each day during 2012.

Data

Figure C.13. **Phishing Rates, 2011–2012**

Source: Symantec.cloud

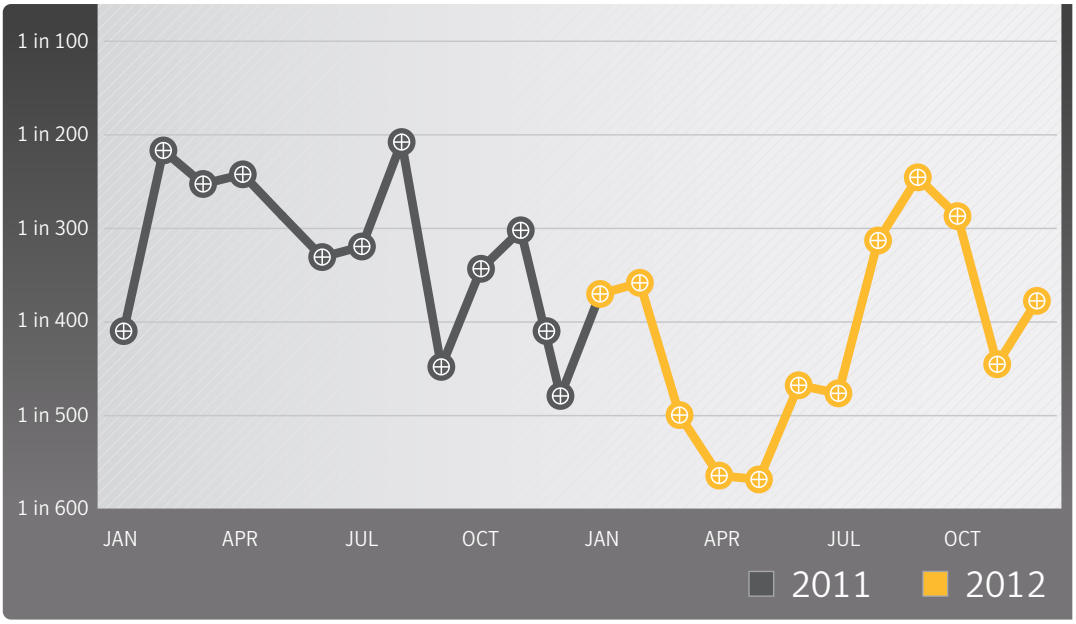


Figure C.14. **Phishing Category Types, Top 200 Organizations, 2012**
Source: Symantec.cloud

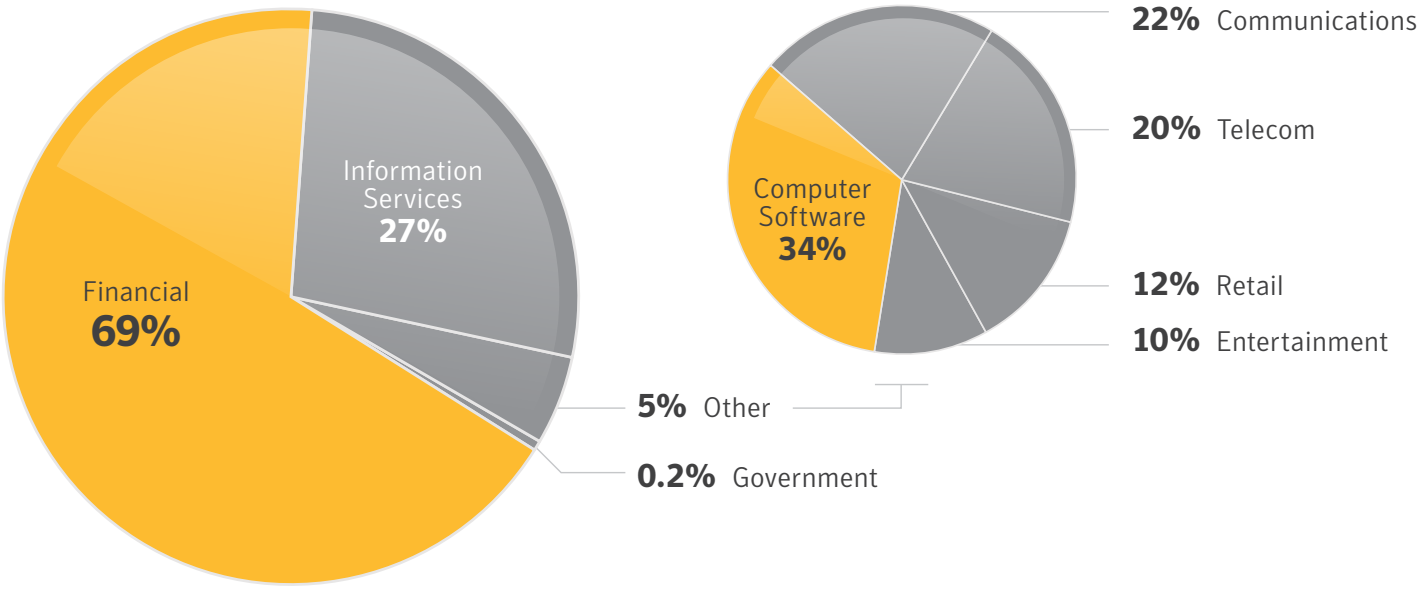
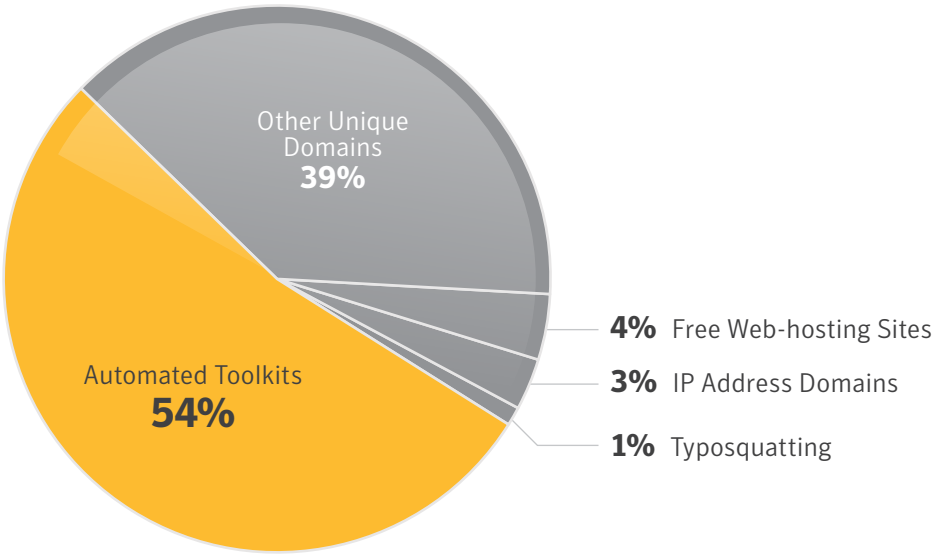


Figure C.15. **Tactics of Phishing Distribution, 2012**
Source: Symantec.cloud



Commentary

- Overall for 2012, 1 in 414.3 emails was identified and blocked as a phishing attack, compared with 1 in 298.9 in 2011; an decrease of 0.09 percentage points.
- 67.3 percent of phishing attacks in 2012 related to spoofed financial organizations, compared with 85.2 percent in 2011.
- Phishing attacks on organizations in the Information Services sector accounted for 27.2 percent of phishing attacks in 2012.
- 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.
- Phishing schemes continued to use major events to entice recipients:

  One scam featured references to increased numbers of Syrian refuges in southern Turkey as a result of the ongoing struggle in Syria, stating, *"But you must assure me that you will use at least 50 percent of my wealth to help the Syrian refugees in Turkey. Turkish Disaster Management Agency (AFAD) said that the Syrian refugees in southern Turkey has risen to 101, 834. You must promise me that you will use 50 percent of my wealth to help the Syria people that are suffering in Turkey."*

  The Syrian conflict again featured in scams such as, "*I am Sgt Douglas Miller Owen, a U.S Army being deployed from Afghanistan to Damascus, Syria on a 6 month mission before i finally return back home [...] Out of the total fund my share was $12,000,000 (Twelve Million US Dollars)*"

  The Libyan revolution and Arab Spring continued to be referenced in scams during 2012, including, "*My name is Aisha daughter of Shukri Ghanem. We fled from Libya last year following the uprising against Col Muammar Gaddafi. [...] My father's death is no longer news but my mother's deteriorating health made me want to do this despite the fact that I barely know you.*"
- 53.7 percent of phishing attacks were conducted through the use of phishing toolkits.

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 because of the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. SMBs may find themselves the target of a spam attack because SMBs are perceived to be softer targets because they are less likely to have the same levels of in-depth defenses, while larger organizations are more likely to have greater budgetary expenditure applied to their antispam 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 2012.

Figure C.16. **Proportion of Email Traffic Identified as Phishing by Industry Sector, 2012**

Source: Symantec.cloud

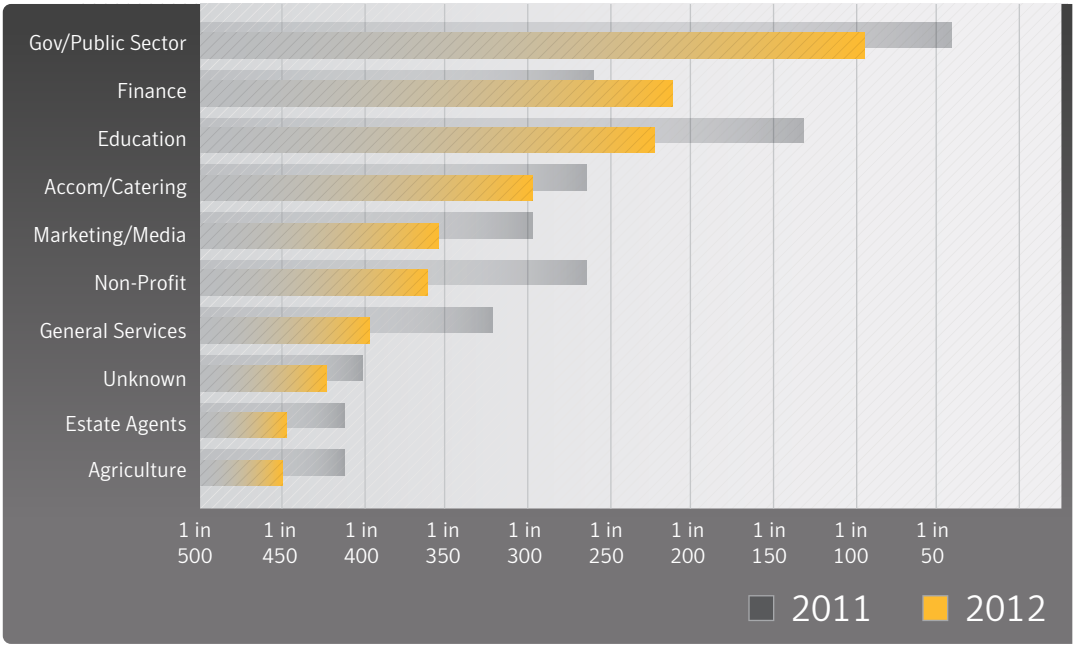


Figure C.17. **Proportion of Email Traffic Identified as Phishing by Organization Size, 2012**

Source: Symantec.cloud

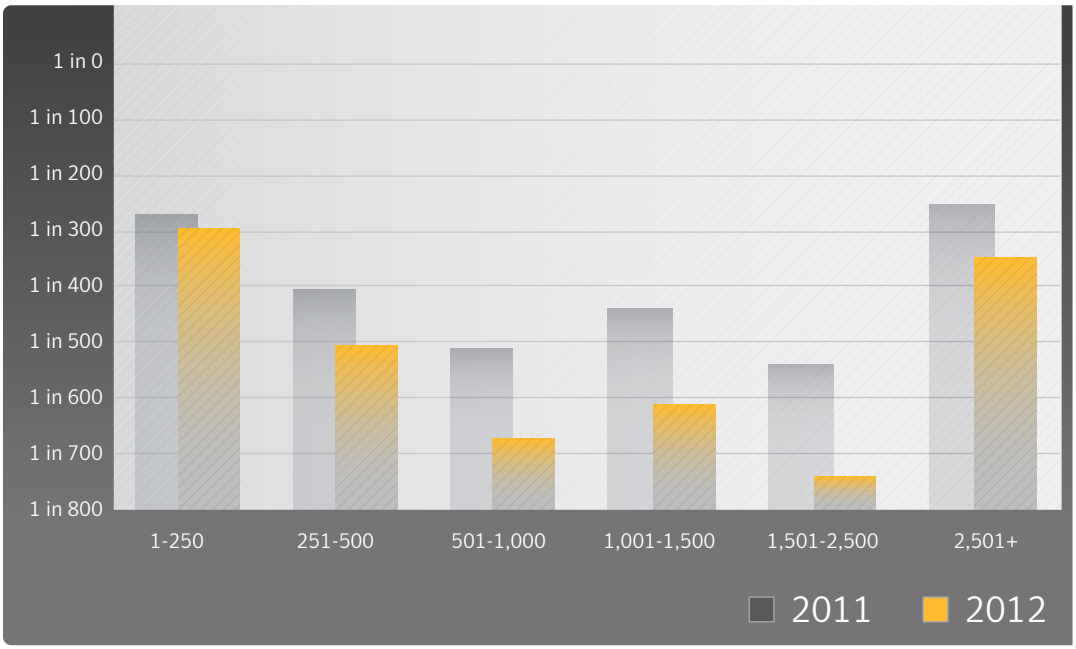
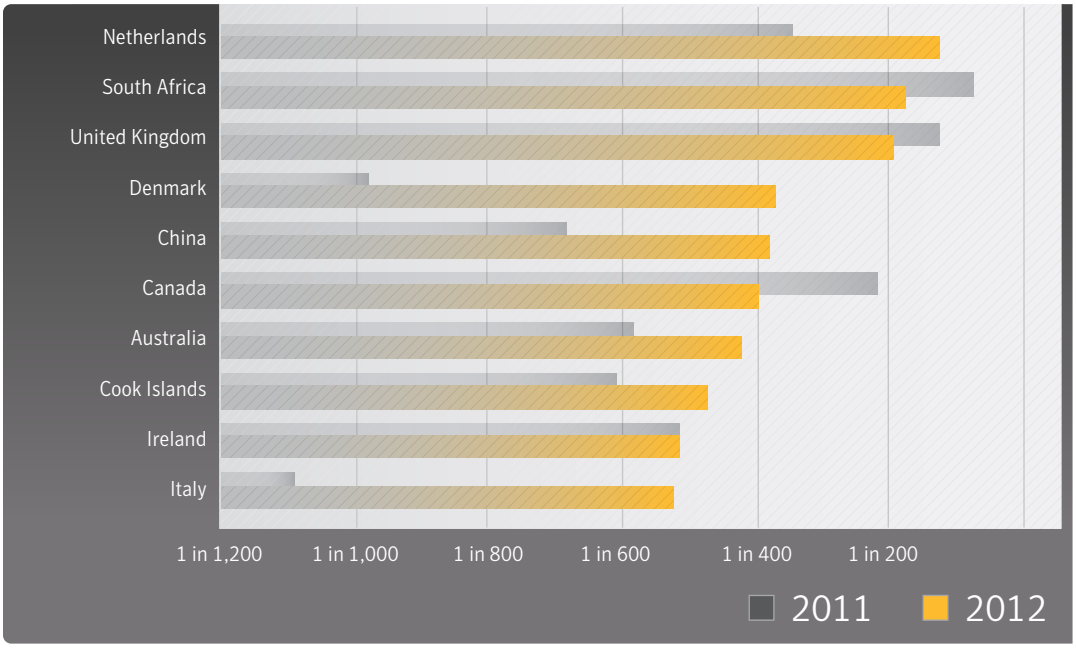


Figure C.18. **Proportion of Email Traffic Identified as Phishing by Geographic Location, 2012**

Source: Symantec.cloud



Commentary

- The phishing rate has significantly increased for six of the top 10 geographies in 2012. The highest average rate for phishing activity in 2012 was for organizations in the Netherlands, with an overall average phishing rate of 1 in 123.1. In 2011, the highest rate was also for South Africa, with an overall average phishing rate of 1 in 96.3.
- The phishing rate has decreased across nine of the top 10 industry sectors in 2012, except for Finance. Organizations in the Government and Public Sector were subjected to the highest level of phishing activity in 2012, with 1 in 95.4 emails identified and blocked as phishing attacks. In 2011 the sector with the highest average phishing rate was also the Government and Public Sector, with a phishing rate of 1 in 49.4.
- The phishing rate has decreased for all sizes of organization in 2012. 1 in 346.0 emails sent to large enterprises with more than 2,500 employees in 2012 were identified and blocked as phishing attacks, compared with 1 in 250.5 in 2011.
- 1 in 293.8 emails sent to businesses with up to 250 employees in 2012 were identified and blocked as phishing attacks, compared with 1 in 266.1 in 2011.

Spam and Fraud Activity Endnotes

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

02 See http://www.symantec.com/security_response/landing/spam/.

03 Simple Mail Transfer Protocol.

04 See http://www.symanteccloud.com/sv/se/globalthreats/learning_center/what_is_skeptic.

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 covers selected vulnerability trends and provides analysis and discussion of the trends indicated by the data. The following metrics are discussed:

- Total Number of Vulnerabilities
- Zero-day Vulnerabilities
- Web Browser Vulnerabilities
- Web Browser Plug-in Vulnerabilities
- Web Attack Toolkits

Total Number of Vulnerabilities

Background

The total number of vulnerabilities for 2012 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. 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. Symantec gathers information on all of these vulnerabilities as part of its DeepSight vulnerability database and alerting services. Examining these trends also provides further insight into other topics discussed in this report.

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 over 52,795 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.

Data

Figure D.1. **Total Vulnerabilities Identified, 2006–2012**

Source: Symantec

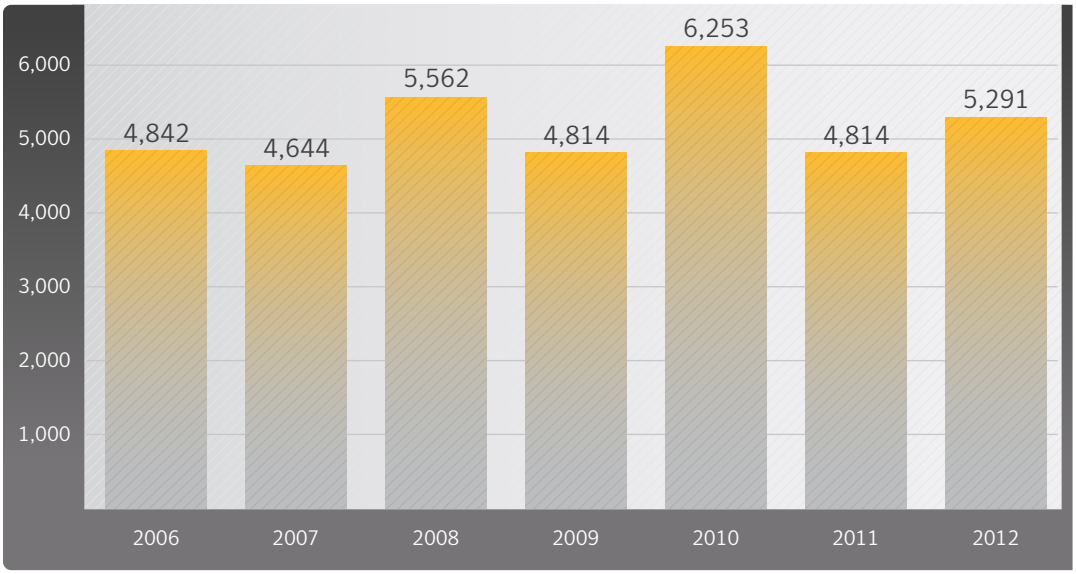


Figure D.2. **New Vulnerabilities Month by Month, 2011 and 2012**

Source: Symantec

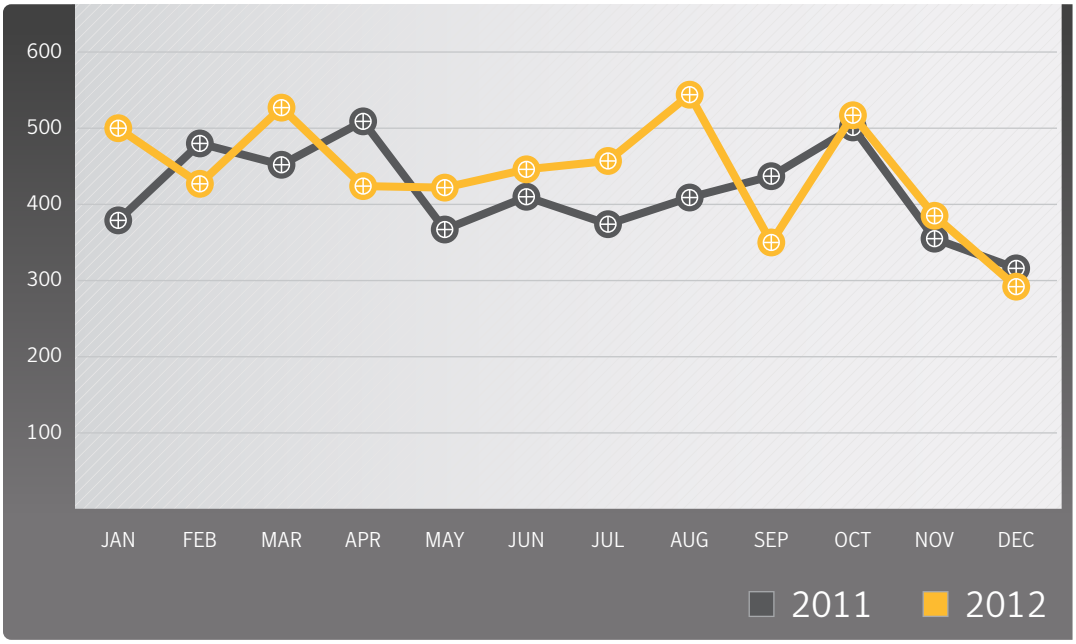
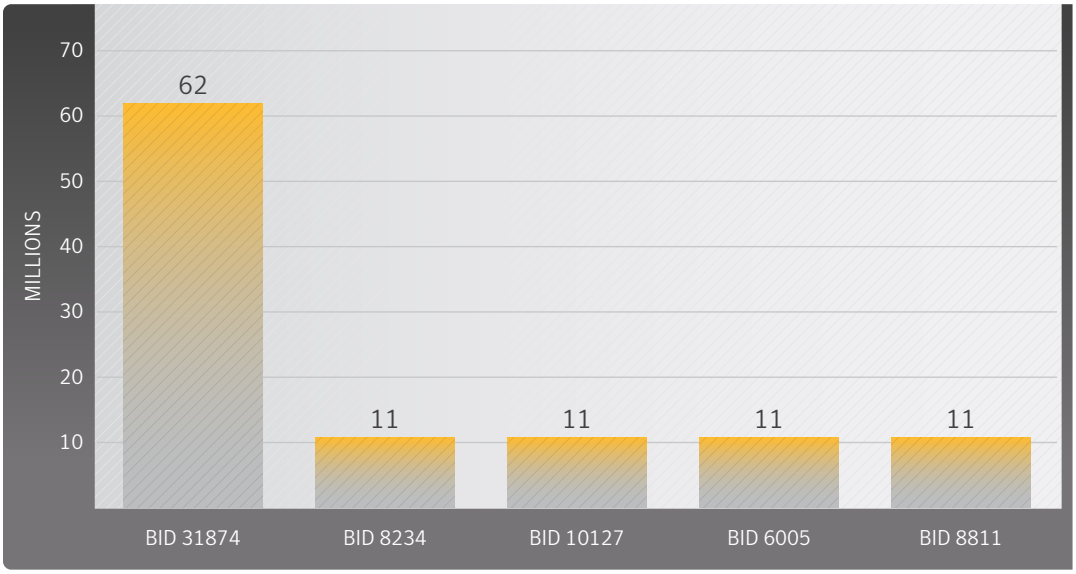


Figure D.3. **Most Frequently Attacked Vulnerabilities in 2012**
Source: Symantec



BID	Detail
BID 31874	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
BID 8234	Microsoft Windows RPC Service Denial of Service Vulnerability
BID 10127	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
BID 6005	Microsoft Windows RPC Service Denial of Service Vulnerability
BID 8811	Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability

Commentary

- **Actual number of new vulnerabilities reported is up, and trend is still upwards:** The total number of new vulnerabilities reported in 2012 stood at 5,291. This figure works out to approximately 101 new vulnerabilities a week. Compared with the number from 2011, which was 4,989, it represents an increase of 6 percent from that of 2011. We can see that the overall pattern is still on an upward trajectory. The number of vulnerabilities reported in January 2013 amounts to 503, which is more than the numbers reported in the same month last year.
- **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 show 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 61.9 million attempts to exploit it in 2012. This figure represents 5.7 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 RPCSS Multi-thread Race Condition Vulnerability (BID 8811[6]), reported in October 2003.
- **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 could be 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, tried-and-tested vulnerabilities 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 applies 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 a window of opportunity for criminals to exploit and they are all too aware of this.
- File-based vulnerabilities: The most commonly exploited data file format is the PDF file format. One of the PDF related vulnerabilities, Adobe Acrobat, Adobe Reader, and Adobe Flash Player Remote Code Execution Vulnerability (BID 35759[9]) registered as the fifth most often used vulnerability in 2011 with just over 1 million attacks reported. PDF files containing vulnerabilities are often associated with Advanced Persistent Threat (APT[10]) style attacks, rather than self-replicating malware. However, in this particular case, the vulnerability in question was most often used in Web toolkit-based attacks. This attack scenario involves creating malicious websites to host exploit code. Users may then be tricked into visiting these malicious toolkit websites either by website redirection (for example, malicious IFRAMEs), SEO poisoning or by sending out spam emails, instant messages or social media updates with links to the malicious website. More information on Web browser vulnerabilities can be found later in this report.
- 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. The fact that there are so many Web-kit-based exploit attempts made using this old vulnerability may suggest that a considerable number of users have not updated their PDF readers to a non-vulnerable version.

Zero-day Vulnerabilities

Background

A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available. 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.

Data

Figure D.4. **Volume of Zero-day Vulnerabilities, 2006–2012**

Source: Symantec

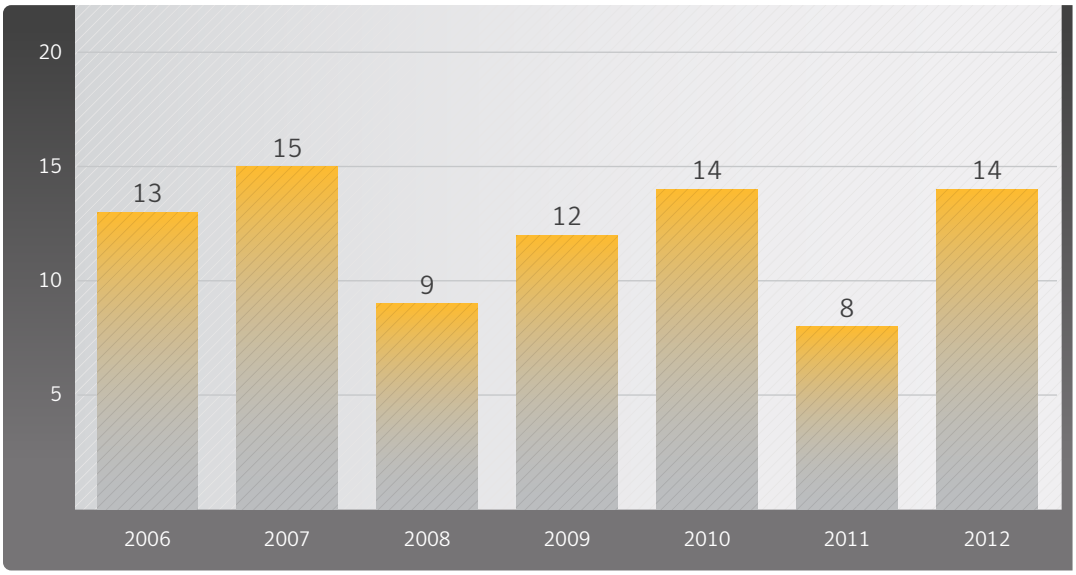


Figure D.5. **Zero-day Vulnerabilities Identified in 2012**

Source: Symantec

CVE	Detail
CVE-2012-0003	Microsoft Windows Media Player “winmm.dll” MIDI File Parsing Remote Buffer Overflow Vulnerability
CVE-2012-0056	Linux Kernel CVE-2012-0056 Local Privilege Escalation Vulnerability
CVE-2012-0507	Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability
CVE-2012-0767	Adobe Flash Player CVE-2012-0767 Cross Site Scripting Vulnerability
CVE-2012-0779	Adobe Flash Player CVE-2012-0779 Object Type Confusion Remote Code Execution Vulnerability
CVE-2012-1535	Adobe Flash Player CVE-2012-1535 Remote Code Execution Vulnerability
CVE-2012-1856	Microsoft Windows Common Controls ActiveX Control CVE-2012-1856 Remote Code Execution Vulnerability
CVE-2012-1875	Microsoft Internet Explorer CVE-2012-1875 Same ID Property Remote Code Execution Vulnerability
CVE-2012-1889	Microsoft XML Core Services CVE-2012-1889 Remote Code Execution Vulnerability
CVE-2012-4792	Microsoft Internet Explorer “CDwnBindInfo” Use-After-Free Remote Code Execution Vulnerability
CVE-2012-4969	Microsoft Internet Explorer Image Arrays Use-After-Free Remote Code Execution Vulnerability
CVE-2012-5076	Oracle Java SE CVE-2012-5076 Remote Java Runtime Environment Vulnerability
CVE-MAP-NOMATCH	Parallels Plesk Panel Unspecified Remote Security Vulnerability
CVE-MAP-NOMATCH	Microsoft Windows Digital Certificates Spoofing Vulnerability

Commentary

- 2012 sees an increase in number of zero-day vulnerabilities compared to 2011. There was a 75 percent increase in vulnerabilities seen in 2012 compared with 2011. However, the number of vulnerabilities seen in 2012 was inflated due to Microsoft file-based vulnerabilities whereas Adobe based-vulnerabilities total up to three compared to four in 2011, when they topped the chart.
- There were three zero-day browser vulnerabilities seen in 2012, an increase of 2 from 2011. This corresponds with the dramatic increase in browser vulnerabilities compared to the total seen in 2011. With the trend moving into Web attacks, more and more browser vulnerabilities are leveraged by the attackers.
- 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 vulnerabilities in Microsoft technologies accounted for almost 50 percent of the zero-day vulnerabilities seen in 2012.
- Most of the attack scenarios are planned in such a way that an attacker crafts a malicious Web page to leverage 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 plug-in components also results in a wider potential attack surface for client-side attacks.

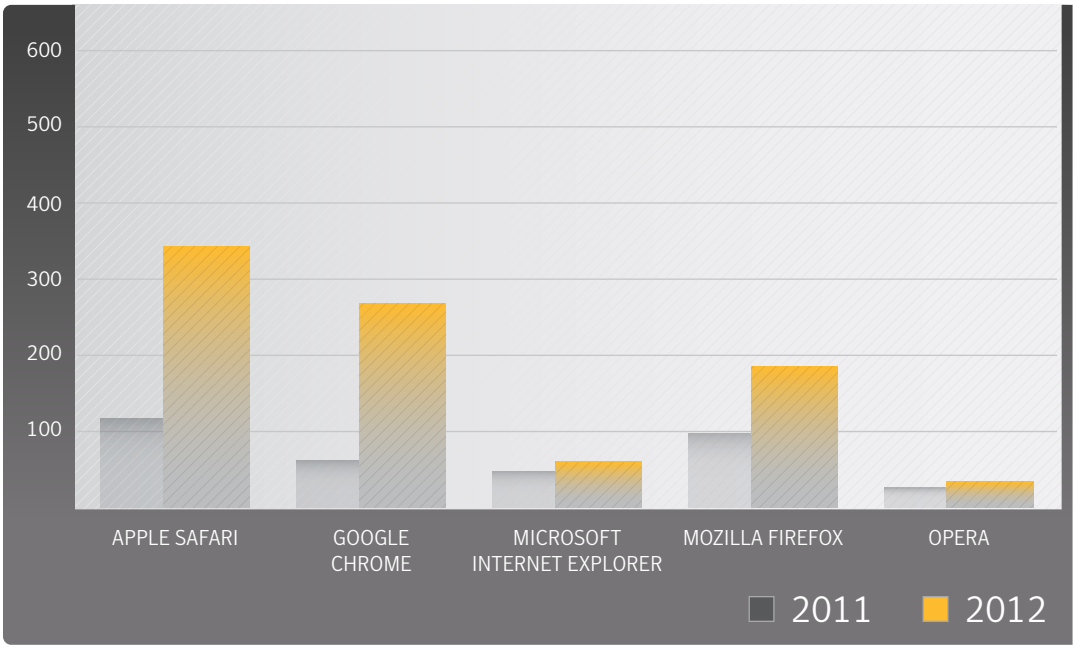
Methodology

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.

Data

Figure D.6. **Browser Vulnerabilities, 2011 and 2012**

Source: Symantec



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

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

Commentary

- All vulnerabilities dramatically increased in 2012, except Opera and Microsoft Internet Explorer, which saw a slight increase.
- Chrome vulnerabilities increased dramatically in 2012 (268). This could be due to the series of exploits developed to prove that Chrome is not unbreakable. After a spike in 2010 (191), the documented vulnerabilities for Chrome browser dropped to 62 for 2011, which is a similar level as in previous years. Several bug bounty programs were organized in 2012, which has contributed to the exposure of a lot of Chrome vulnerabilities.
- These five browsers combined had 891 reported vulnerabilities in total in 2012, which is a strong increase from 351 in 2011. This increase is due to dramatically increased vulnerabilities seen in Safari, Chrome, and Firefox.

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 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 these 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 and then have full access to download any malware to the endpoint system.

Some plug-in technologies include automatic update mechanisms that aid in keeping software up to date, which may aid in limiting exposure to certain vulnerabilities. Enterprises that choose to disable these updating mechanisms, or continue to use vulnerable versions, will continue to put their enterprises at considerable risk to silent infection and exploitation. With the hundreds of millions of drive-by download attacks that Symantec identified in 2011, Web attacks continue to be a favorite 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.

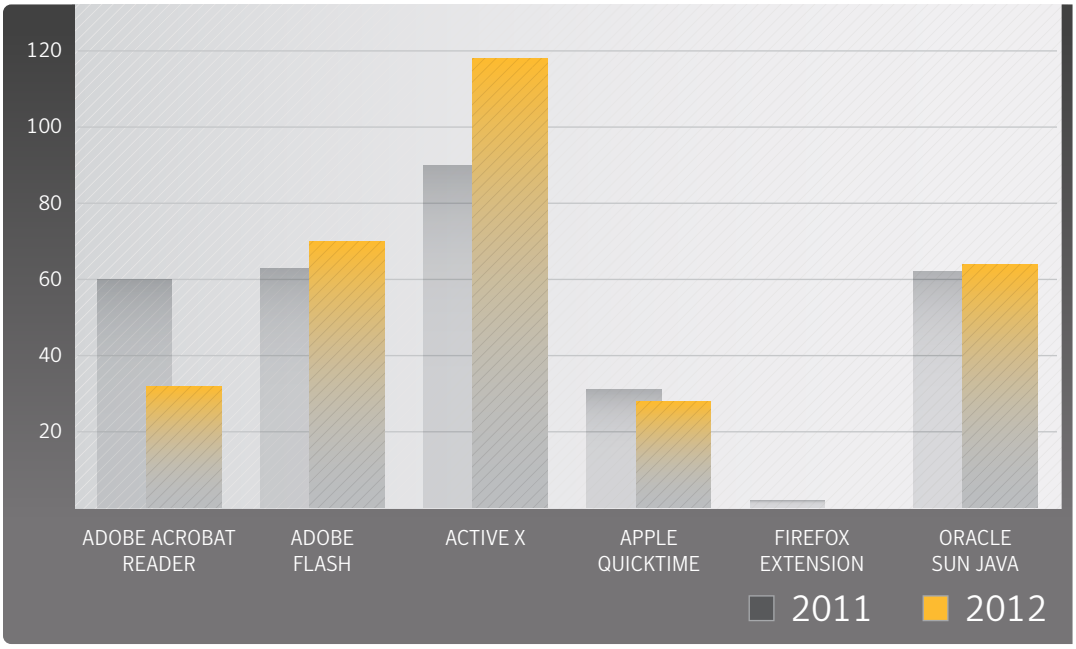
Methodology

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.

Data

Figure D.7. **Browser Plug-in Vulnerabilities in 2011 and 2012**

Source: Symantec



Symantec identified the following plug-in technologies as having the most reported vulnerabilities in 2012:

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

Commentary

- In 2012, 312 vulnerabilities affecting browser plug-ins were documented by Symantec, a very slight increase compared to 308 vulnerabilities affecting browser plug-ins in 2011.
- ActiveX vulnerabilities increased in 2012, which may be due to the increase in Internet Explorer vulnerabilities.
- Adobe Flash Player and Java vulnerabilities increased in 2012. This trend was already visible in 2011 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 2012.

Web Attack Toolkits

Background

Web attack toolkits are a collection of scripts, often PHP files, which are used to create malicious websites that will use Web exploits to infect visitors. There are a few dozen known families used in the wild. Many toolkits are traded or sold on underground forums for US$100-1,000. Some are actively developed and new vulnerabilities are added over time, such as the Blackhole and Eleonore toolkits, which both added exploits for a variety of vulnerabilities during 2012.

Each new toolkit version released during the year was accompanied with increased malicious Web attack activity. As a new version emerges that incorporates new exploit functionality, we see an increased use of it in the wild, making as much use of the new exploits until potential victims have patched their systems.

Since many toolkits often use the same exploits, it is often difficult to identify the specific attack toolkit behind each infection attempt. On average, an attack toolkit contains around 10 different exploits, mostly focusing on browser independent plug-in vulnerabilities found in applications such as Adobe Flash Player, PDF viewers, and Java. In general, older exploits are not removed from the toolkits, since some systems may still be unpatched. 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. Therefore, the security of SCADA technologies and protocols is a concern related to national security because the disruption of related services can result in the failure of infrastructure and potential loss of life, among other consequences.

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 governments and/or enterprises that are 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 there is likely private security research 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.

Data

The number of SCADA vulnerabilities decreased dramatically in 2012. In 2012, there were 85 public SCADA vulnerabilities, a massive decrease when compared to the 129 vulnerabilities in 2011.

Commentary

Since the emergence of Stuxnet in 2010, the security of SCADA systems has been an area of concern. SCADA systems are generally not designed to be connected to the public Internet, but as Stuxnet demonstrated, this is not always a guarantee of security as locally connected networks may become compromised and USB devices may also be used as an infection vehicle. As new vulnerabilities are discovered, the importance of providing a fix quickly is even greater for SCADA systems, but they can sometimes remain unpatched for longer than traditional software vulnerabilities.

Vulnerability Trends Endnotes

01 See http://www.first.org/cvss/cvss-guide.html.

02 See http://www.securityfocus.com/bid/31874.

03 See http://www.securityfocus.com/bid/8234.

04 See http://www.securityfocus.com/bid/10127.

05 See http://www.securityfocus.com/bid/6005.

06 See http://www.securityfocus.com/bid/8811.

07 See http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/231900575/more-exploits-for-sale-means-better-security.html.

08 See http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99.

09 See http://www.securityfocus.com/bid/35759.

10 See http://go.symantec.com/apt.

About Symantec

Symantec protects the world's information and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

More Information

- Symantec.cloud Global T hreats: http://www.symanteccloud.com/en/gb/globalthreats/
- Symantec Security Response: http://www.symantec.com/security_response/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec. Confidence in a connected world.

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

03/13 21284438