SYMANTEC ENTERPRISE SECURITY

Symantec
Confidence in a connected world.

Symantec Global Internet Security Threat Report

Trends for 2009

Volume XV, Published April 2010

Marc Fossi
Executive Editor
Manager, Development
Security Technology and Response

Dean Turner
Director, Global Intelligence Network
Security Technology and Response

Eric Johnson
Editor
Security Technology and Response

Trevor Mack
Associate Editor
Security Technology and Response

Téo Adams
Threat Analyst
Security Technology and Response

Joseph Blackbird
Threat Analyst
Symantec Security Response

Stephen Entwisle
Threat Analyst
Symantec Security Response

Brent Graveland
Threat Analyst
Security Technology and Response

David McKinney
Threat Analyst
Security Technology and Response

Joanne Mulcahy
Senior Analyst
Security Technology and Response

Candid Wueest
Threat Analyst
Security Technology and Response

Volume XV, Published April 2010

Symantec Global Internet Security Threat Report

Contents

Contents for Tables and Figures

Introduction

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries and territories monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 5 million decoy accounts; MessageLabs Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries. Over 8 billion email messages, as well as over 1 billion Web requests, are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

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

Symantec *Global Internet Security Threat Report* now has tweetable stats

- Click the links wherever this symbol **Tweet** appears to tweet stats from this report.
- Follow the #ISTR hashtag to particpate in the ISTR discussion on Twitter.
- Follow us on Twitter @threatintel.

Executive Summary

This summary will discuss current trends, impending threats, and the continuing evolution of the Internet threat landscape in 2009 based on data discussed within the Symantec *Global Internet Security Threat Report*. There are a number of recent and growing trends in the threat activity landscape that were observed by Symantec in 2009. These trends include that malicious activity continues to be pushed to emerging countries, targeted attacks on enterprises are increasing, with Web-based attacks continuing to be a favored attack vector, readily available malicious code kits are making it simple for neophyte attackers to mount attacks, and the online underground economy and malicious activity are benefiting from the downturn in the global economy.

Emerging countries

The previous edition of the Symantec *Global Internet Security Threat Report* noted a shift in malicious activity to emerging countries.[1] In 2009, this trend became more pronounced. For example, for the first time since Symantec began examining malicious activity by country in 2006, a country other than the United States, China, or Germany has ranked in the top three, as Brazil ranked third in malicious activity in 2009, behind the United States and China, respectively (table 1).

Overall Rank		Country	Percentage		2009 Activity Rank				
2009	2008		2009	2008	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Table 1. Malicious activity by country
Source: Symantec Corporation

Tweet

Brazil became more prominent in all of the specific category measurements in 2009 except for spam zombies, where it was already the top-ranked country. Brazil's significant increases across all categories are related to the growing Internet infrastructure and broadband usage there. The growing level of malicious code activity affecting Brazil has also resulted in the proposal of a new cybercrime bill in the country.[2] The initiative may also be a result of a number high-profile cyber attacks there in recent years.[3] One of the attacks resulted in a massive power grid blackout, while another resulted in the exposure of valuable data and a $350,000 ransom request after a government website was compromised.[4] The latter case resulted in over 3,000 employees being unable to access the site for 24 hours.

[1] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 4
[2] http://www.eff.org/deeplinks/2009/07/lula-and-cybercrime
[3] http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/
[4] All currency in U.S. dollars.

Tweet

India also experienced a surge in malicious activity in 2009, moving from 11th for overall malicious activity in 2008 to fifth in this period. In 2009, India also accounted for 15 percent of all malicious activity in the Asia-Pacific/Japan (APJ) region, an increase from 10 percent in 2008. For specific categories of measurement in the APJ region, India increased rank in malicious code, spam zombies and phishing hosts from 2008. Its high ranking in spam zombies also contributed to India being the third highest country of spam origin globally. Malicious activity tends to increase in countries experiencing rapid growth in broadband infrastructure and connectivity, and the level of malicious activity occurring in India has been increasing steadily over several reporting periods as its broadband infrastructure and user base grows.[5]

Targeted attacks focus on enterprises

Targeted attacks using advanced persistent threats (APT) that occurred in 2009 made headlines in early 2010.[6] Most notable of these was the Hydraq Trojan (a.k.a., Aurora).[7] In January 2010, reports emerged that dozens of large companies had been compromised by attackers using this Trojan.[8] While these attacks were not novel in approach, they highlighted the methods by which large enterprises could be compromised.

Typically, this type of attack begins with some reconnaissance on the part of attackers. This can include researching publicly available information about the company and its employees, such as from social networking sites. This information is then used to create specifically crafted phishing email messages, often referred to as spear phishing, that target the company or even specific staff members.[9] These email messages often contain attachments that exploit vulnerabilities in client-side applications, or links to websites that exploit vulnerabilities in Web browsers or browser plug-ins. A successful attack could give the attacker access to the enterprise's network.

In the case of the Hydraq attack, a previously unknown vulnerability in Microsoft® Internet Explorer® and a patched vulnerability in Adobe® Reader® and Adobe Flash® Player are exploited to install the Trojan.[10] Once the Trojan is installed, it lets attackers perform various actions on the compromised computer, including giving them full remote access. Typically, once they have established access within the enterprise, attackers will use the foothold that they have established to attempt to connect to other computers and servers and compromise them as well. They can do this by stealing credentials on the local computer or capturing data by installing a keystroke logger.

Usually, when this type of attack is performed against individuals or by less sophisticated attackers, the attack is used to gather all the information immediately available and move on to the next target. However, APT attacks are designed to remain undetected in order to gather information over prolonged periods. This type of attack has been observed in other large-scale data breaches that caused large numbers of identities to be exposed (figure 1).[11]

[5] http://point-topic.com/dslanalysis.php and/or http://www.indiabroadband.net/india-broadband-telecom-news/11682-india-register-500-growth-broadband-services-within-5-years.html
[6] An advanced persistent threat (APT) is usually a sophisticated threat that hides its presence to remain installed and undetected on a computer.
[7] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99
[8] http://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions
[9] Spear phishing is a targeted form of phishing where the apparent source of the email is likely to be an individual within the recipients' company and generally someone in a position of authority. This is discussed in greater detail in "Phishing activity by sector," further down in the report.
[10] http://www.securityfocus.com/bid/37815
[11] http://news.bbc.co.uk/2/hi/americas/7970471.stm

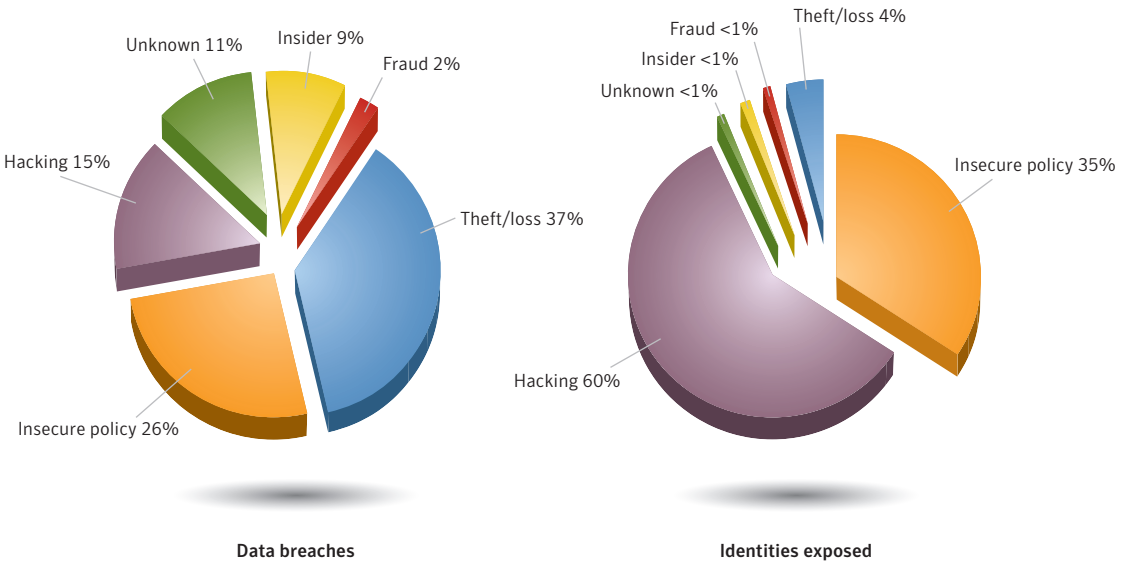

Figure 1. Data breaches that could lead to identity theft by cause and identities exposed[12]
Source: Based on data provided by OSF DataLoss DB

In 2009, 60 percent of identities exposed were compromised by hacking attacks, which are another form of targeted attack. The majority of these were the result of a successful hacking attack on a single credit card payment processor.[13] The hackers gained access to the company's payment processing network using an SQL-injection attack. The attackers then installed malicious code designed to gather sensitive information from the network, which allowed them to easily access the network at their convenience. The attacks resulted in the theft of approximately 130 million credit card numbers. An investigation was undertaken when the company began receiving reports of fraudulent activity on credit cards that the company itself had processed. The attackers were eventually tracked down and charged by federal authorities.

Tweet

This type of targeted hacking attack is further evidence of the significant role that malicious code can play in data breaches. Although data breaches occur due to a number of causes, the covert nature of malicious code is an efficient and enticing means for attackers to remotely acquire sensitive information. Furthermore, as is discussed in the "Threats to confidential information" metric, the frequency of malicious code threats that expose confidential information underscores the significance of identity theft to attackers who author and deploy malicious code.

According to the Symantec State of Enterprise Security Report 2010, 75 percent of enterprises surveyed experienced some form of cyber attack in 2009, showing that this issue is not limited to a few larger enterprises.[14] Protecting the enterprise infrastructure and information, developing and enforcing IT policies, and properly managing systems can help mitigate or prevent targeted attacks. Administrators can limit potential exposure to attack activity by securing endpoints, messaging, and Web environments, as well as by implementing policies to remediate threats. Distributing patches and enforcing patch levels through automated processes can also prevent exploitation of known vulnerabilities.

Tweet

[12] Due to rounding, percentages might not equal 100 percent.
[13] http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html
[14] http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf : p. 8

Web-based attacks take on all comers

While targeted attacks frequently use zero-day vulnerabilities and social engineering to compromise enterprise users on a network, similar techniques are also employed to compromise individual users. In the late 1990s and early 2000s, mass-mailing worms were the most common means of malicious code infection. Over the past few years, Web-based attacks have replaced the mass-mailing worm in this position. Attackers may use social engineering—such as in spam messages, as previously mentioned—to lure a user to a website that exploits browser and plug-in vulnerabilities. These attacks are then used to install malicious code or other applications such as rogue security software on the victim's computer.[15]

Of the top-attacked vulnerabilities that Symantec observed in 2009, four of the top five being exploited were client-side vulnerabilities that were frequently targeted by Web-based attacks (table 2). Two of these vulnerabilities were in Adobe Reader, while one was in Microsoft Internet Explorer and the fourth was in an ActiveX® control. This shows that while vulnerabilities in other network services are being targeted by attackers, vulnerabilities in Web browsers and associated technologies are favored. This may be because attacks against browsers are typically conducted through the HTTP protocol that is used for the majority of Web traffic. Since so much legitimate traffic uses this protocol and its associated ports, it can be difficult to detect or block malicious activity using HTTP.

Rank	BID	Vulnerabilities
1	36299	Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution
2	35759	Adobe Reader and Flash Player Remote Code Execution
3	33627	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution
4	35558	Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution
5	34169	Adobe Reader Collab 'getIcon()' JavaScript Method Remote Code Execution

Table 2. Top attacked vulnerabilities, 2009
Source: Symantec

Tweet

The top Web-based attacks observed in 2009 primarily targeted vulnerabilities in Internet Explorer and applications that process PDF files (table 3). Because these two technologies are widely deployed, it is likely that attackers are targeting them to compromise the largest number of computers possible. As is discussed in the "Web browser vulnerabilities" discussion in this report, Mozilla® Firefox® had the most reported vulnerabilities in 2009, with 169, while Internet Explorer had just 45, yet Internet Explorer was still the most attacked browser. This shows that attacks on software are not necessarily based on the number of vulnerabilities in a piece of software, but on its market share and the availability of exploit code as well.[16]

[15] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf
[16] http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0

Overall Rank 2009	2008	Attack	Percentage 2009	2008
1	2	PDF Suspicious File Download	49%	11%
2	1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	18%	30%
3	N/A	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution	6%	N/A
4	6	Microsoft Internet Explorer MS Snapshot ActiveX File Download	4%	5%
5	4	Adobe SWF Remote Code Executable	3%	7%
6	14	Microsoft Internet Explorer Malformed XML Buffer Overflow	3%	1%
7	5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	3%	6%
8	20	Microsoft Internet Explorer WPAD Spoofing	3%	1%
9	N/A	Microsoft MPEG2TuneRequestControl ActiveX Buffer Overflow	2%	N/A
10	N/A	Microsoft MPEG2TuneRequestControl ActiveX Instantiation	1%	N/A

Table 3. Top Web-based attacks
Source: Symantec

Many of the vulnerabilities observed through Web-based attacks in 2009 have been known and patched for some time. For example, the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness[17] was published on August 23, 2003, and fixes have been available since July 2, 2004, yet it remains the second-ranked Web-based attack. This is likely because of the use of Web attack kits like Fragus,[18] Eleonore,[19] and Neosploit.[20] These kits come bundled with a variety of different exploits, including some exploits for older vulnerabilities. Because an older vulnerability is likely to be included in more kits, it will probably be seen in more attacks than many of the newer vulnerabilities. These exploit and attack kits are often frequently used in conjunction with some of the crimeware kits available in the underground economy, as is discussed in the next section.

Lowering the bar

A crimeware kit is a toolkit that allows people to customize a piece of malicious code designed to steal data and other personal information. The Zeus[21] kit can be purchased for as low as $700, but can also be found for free on some forums.[22] These kits can be bought in the underground economy and various Web forums. Crimeware kits like Zeus make it easier for unskilled attackers to compromise computers and steal information.[23] These kits allow anyone who buys them to customize them to their own needs. In 2009, Symantec observed nearly 90,000 unique variants of the basic Zeus toolkit and it was the second most common new malicious code family observed in the APJ region during this time.

Tweet

Tweet

Variants of the Zeus kit use spam to lure users to a website that uses social engineering or that exploits a Web browser vulnerability to install the bot on a victim's computer. The bot then allows remote access to the computer and can be used to steal information such as the user's online banking credentials. Each bot can then be used to send additional spam runs to compromise new users.

[17] http://www.securityfocus.com/bid/10514/discuss
[18] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23391
[19] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23481
[20] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23588
[21] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99
[22] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf : p. 1
[23] http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits

These kits have gained enough popularity among cybercriminals that competition and new business models have arisen. For example, the SpyEye kit, in addition to stealing information, also has the ability to detect if a computer already has Zeus installed and, if so, to intercept its communications.[24] In another example, the Fragus exploit kit contains mechanisms to prevent buyers from reselling their copies of it.[25]

A side effect of these kits is the creation of tens of thousands of new malicious code variants that may only each be seen by a single user. In 2009, Symantec observed nearly 90,000 unique variants of binary files created by the Zeus toolkit. Approximately 57 percent of threat instances that Symantec protected its customers from via reputation-based techniques corresponded to singletons.[26] This suggests that security technologies that rely on signatures should be complemented with heuristics, behavioral monitoring techniques, and reputation-based security.

The lowering of barriers for neophyte attackers to enter into the cybercrime realm is evident in the increase in malicious code that steals confidential information. For example, the percentage of threats to confidential information that incorporate remote access capabilities increased to 98 percent in 2009, from 83 percent in 2008 (figure 2). One reason for the popularity of this attack vector is that there is an increasing number of people performing online banking. For instance, in the United Kingdom and France, more than 50 percent of Internet users perform online banking, while in Canada the number rises to 60 percent.[27] In the United States, eight out of 10 online households now bank online.[28] In addition, with the availability of online banking continuing to grow, there is no shortage of potential victims. These factors helped to contribute to the over $120 million in reported losses due to online banking fraud reported in the third quarter of 2009.[29]

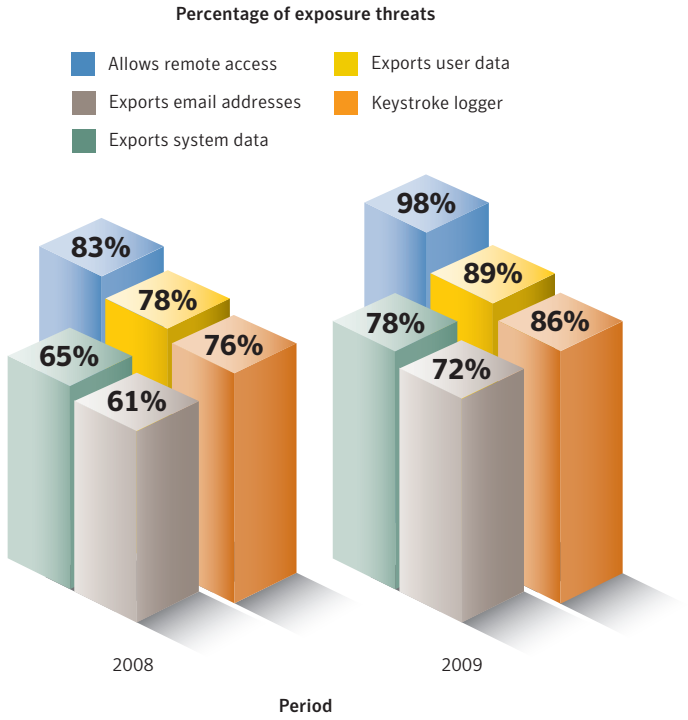

Figure 2. Threats to confidential information, by type
Source: Symantec

[24] http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot
[25] http://www.symantec.com/connect/blogs/fragus-exploit-kit-changes-business-model
[26] Singletons are file instances that are seen on only one computer.
[27] See http://www.ukpayments.org.uk/media_centre/press_releases/-/page/871/ and http://www.comscore.com/press/release.asp?press=2524
[28] https://www.javelinstrategy.com/research/brochures/brochure-150
[29] http://ecommerce-journal.com/news/27287_online-banking-fraud-hovered-120-million-third-quarter-2009-fdci-reports

No financial crisis for cybercriminals

A number of large financial institutions in many countries were severely affected by the latest global financial crisis, resulting in some banks being acquired or merging with others. The downturn, though, does not appear to have hindered the underground economy or cybercrime targeting financial services in any significant way. In 2009, the financial sector remained the sector most heavily targeted by phishing attacks, accounting for 74 percent of the brands used in phishing campaigns (table 4). The next closest sector was Internet service providers, at only 9 percent. This indicates that phishing financial services brands continues to be lucrative for attackers or they would likely have abandoned it in favor of other targets.

Sector	2009 Percentage	2008 Percentage
Financial	74%	79%
ISP	9%	8%
Retail	6%	4%
Insurance	3%	2%
Internet community	2%	2%
Telecom	2%	2%
Computer hardware	1%	1%
Government	1%	1%
Computer software	<1%	<1%
Transportation	<1%	<1%

Table 4. Unique brands phished, by sector
Source: Symantec

The volume of financial services spam also remained relatively unchanged in 2009 (figure 3). While the levels of financially oriented spam and phishing have remained relatively constant despite the recent economic downturn, attackers have made adjustments in their tactics. For example, Symantec observed more messages advertising refinancing of debts and mortgages along with offers of loans or opportunities to earn money while working from home. This shows that attackers are able to rapidly adapt their social engineering techniques to better take advantage of current events and situations.

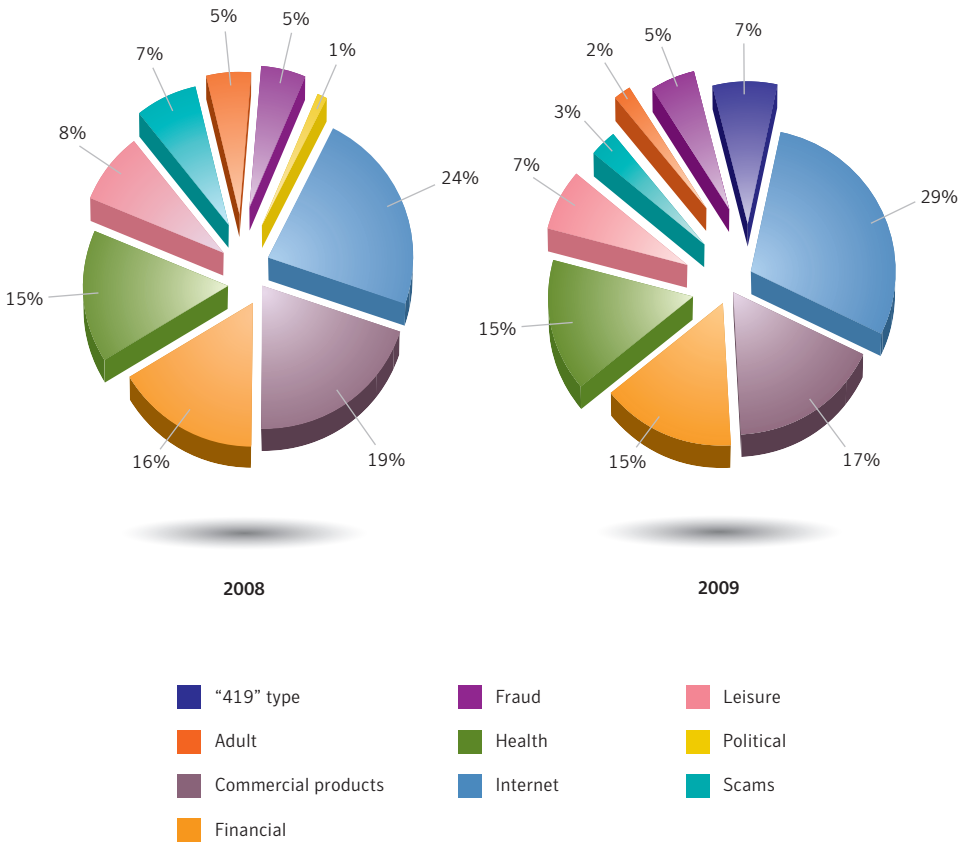

Figure 3. Top spam categories
Source: Symantec

While financial phishing and spam did not experience significant changes in 2009, the percentage of advertisements for credit card information on underground economy servers decreased (table 5). Although the drop from 32 percent in 2008 to 19 percent in 2009 appears to be significant, the percentage observed in 2007 was 21 percent, which may indicate that there was higher availability of credit card numbers on underground economy servers in 2008. The number of data breaches reported in those years is a further indication of this. There were over twice as many data breaches reported in 2008 than in 2007. Similarly, there were almost twice as many data breaches reported in 2008 than there were in 2009.

Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec

While there was a decline in credit card advertisements in 2009, it is likely that they will continue to be a significant factor in the underground economy. With the wide availability of the previously mentioned crimeware kits, it is becoming easier for neophytes to operate in the online underground economy. This will likely increase the availability of credit cards on underground economy servers.

Conclusion

As government agencies and industries in many countries increase their efforts to combat malicious code activity, that activity is increasingly shifting to emerging countries with rapidly growing Internet infrastructures. Meanwhile, some emerging countries may experience an even greater influx of malicious activity due to the aforementioned increased ease of mounting attacks for neophyte cybercriminals. That said, it is critical to note that, just because attackers are relocating malicious activities such as phishing hosts, bot networks, and spam zombies to other countries, these attacks can still be directed at targets anywhere worldwide.

Targeted attacks against enterprises have been occurring for some time now. However, during 2009 a large-scale targeted attack occurred that brought these types of incidents into the spotlight.[30] The wide-scale reporting of this attack impelled many organizations to re-examine their security postures and mitigation strategies against zero-day vulnerabilities.[31] Symantec believes it is likely that targeted attacks of this nature will continue to play a large part in the threat landscape in the near future.

Financially motivated attacks against both enterprises and individuals remain a large part of the threat landscape. The underground economy continues to flourish even while the mainstream economy begins recovering from the financial crisis. Many cybercriminals have shifted their efforts toward creating kits they can sell to new entrants in the underground economy. This enables relatively inexperienced attackers with little technical knowledge to mount attacks without too much difficulty. As these developments make it easier for more attackers to enter into the online underground economy, Symantec expects attacks against Web browsers and malicious code variants installed through these attacks to increase. This increases the importance of reputation-based security techniques and other technologies that act to catch malicious code beyond simple signature-based detection.

[30] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
[31] http://www.informationweek.com/news/services/disaster_recovery/showArticle.jhtml?articleID=222301351

Highlights

Threat Activity Trends Highlights

Tweet
- In 2009, the United States had the most overall malicious activity measured by Symantec, with 19 percent of the total; this is a decrease from 23 percent in 2008, when the United States also ranked first.
- The United States was the top country of attack origin in 2009, accounting for 23 percent of worldwide activity; this is a decrease from 25 percent in 2008.

Tweet
- The top Web-based attack in 2009 was associated with malicious PDF activity, which accounted for 49 percent of the total.

Tweet
- The United States was the top country of origin for Web-based attacks in 2009, accounting for 34 percent of the worldwide total.

Tweet
- The education sector accounted for 20 percent of data breaches that could lead to identity theft during this period, more than any other sector; this is a decrease from 27 percent in 2008, when it was also the highest ranked sector for data breaches.
- The financial sector was the top sector for identities exposed in 2009, accounting for 60 percent of the total; this is a significant increase from 29 percent in 2008.

Tweet
- In 2009 physical theft or loss accounted for 37 percent of data breaches that could lead to identity theft—a decrease from 48 percent in 2008.

Tweet
- Hacking accounted for 60 percent of the identities exposed in 2009, a marked increase from 22 percent in 2008.
- Symantec observed an average of 46,541 active bot-infected computers per day in 2009; this is a 38 percent decrease from the 75,158 per day average observed in 2008.
- Symantec observed 6,798,338 distinct bot-infected computers during this period; this is a 28 percent decrease from 2008.
- The United States was the country of the most bot-infected computers observed by Symantec in 2009, accounting for 11 percent of the global total—a slight decrease from 12 percent in 2008.
- Taipei was the city with the most bot-infected computers in 2009, accounting for 5 percent of the worldwide total.
- In 2009 Symantec identified 17,432 distinct new bot command-and-control servers, an increase from 15,197 in 2008; of these, 31 percent operated through IRC channels and 69 percent used HTTP.
- The United States was the country with the most bot command-and-control servers in 2009, with 34 percent of the total observed by Symantec; this is an increase from 33 percent in 2008, when the United States also ranked first.
- The United States was again the country most frequently targeted by denial-of-service attacks in 2009, accounting for 56 percent of the worldwide total—an increase from 51 percent in 2008.

Vulnerability Trends Highlights

- Symantec documented 4,501 vulnerabilities in 2009. This is a decrease from the 5,491 vulnerabilities documented in 2008.
- Mozilla Firefox was affected by 169 new vulnerabilities in 2009, more than any other browser; there were 94 new vulnerabilities identified in Apple® Safari®, 45 in Microsoft Internet Explorer, 41 in Google® Chrome and 25 in Opera™. Tweet Tweet
- Of the 374 vulnerabilities documented in Web browsers in 2009, 14 percent remain unpatched by the vendors at the time of writing. Of the 232 Web browser vulnerabilities documented in 2008, 18 percent remain unpatched.
- Of all browsers Symantec analyzed in 2009, Safari had the longest window of exposure (the time between the release of exploit code for a vulnerability and a vendor releasing a patch), with a 13-day average; Internet Explorer, Firefox, and Opera had the shortest windows of exposure in 2009, averaging less than one day each. Tweet Tweet
- There were 321 browser plug-in vulnerabilities identified in 2009, fewer than the 410 identified in 2008. ActiveX technologies still constituted the majority of new browser plug-in vulnerabilities, with 134; however, this is a 53 percent decrease from the 287 ActiveX vulnerabilities identified in 2008. Tweet
- The top attacked vulnerability for 2009 was the Microsoft Windows® SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability.
- In 2009, Symantec documented 12 zero-day vulnerabilities, compared to nine in 2008. Tweet

Malicious Code Trends Highlights

- Symantec created 2,895,802 new malicious code signatures in 2009, a 71 percent increase over 2008; the 2009 figure represents 51 percent of all malicious code signatures ever created by Symantec. Tweet
- Of the top 10 new malicious code families detected in 2009, six were Trojans, two were worms with back door components, one was a worm, and one was a virus.
- Trojans made up 51 percent of the volume of the top 50 malicious code samples reported in 2009, a decrease from 68 percent in 2008. Tweet
- Four of the top 10 staged downloaders in 2009 were Trojans, two were worms that incorporated a back door component, three were worms, and one was a worm that incorporated a virus component.
- In 2009, eight of the top 10 threat components downloaded by modular malicious software were Trojans, one was a worm, and one was a back door.
- In 2009, the proportional increase of potential malicious code infections was greatest in the Europe, the Middle East, and Africa region.
- The percentage of threats to confidential information that incorporate remote access capabilities increased to 98 percent in 2009, a significant increase from 83 percent in 2008. Tweet
- In 2009, 89 percent of threats to confidential information exported user data and 86 percent had a keystroke-logging component; these are increases from 78 percent and 76 percent, respectively, in 2008.

- In 2009 propagation through file-sharing executables accounted for 72 percent of malicious code that propagates—up from 66 percent in 2008.
- The percentage of documented malicious code samples that exploit vulnerabilities increased from 3 percent in 2008 to 6 percent in 2009.
- The top potential infections in 2009 were, in order, the Sality.AE virus, the Brisv Trojan, and the SillyFDC worm.

Phishing, Underground Economy Servers, and Spam Trends Highlights

Tweet
- The majority of brands used in phishing attacks in 2009 were in the financial services sector, accounting for 74 percent, down from the 79 percent identified in 2008.
- In 2009, Symantec detected 59,526 phishing hosts, an increase of 7 percent over 2008 when Symantec detected 55,389 phishing hosts.

Tweet
- In 2009, 36 percent of all phishing URLs identified by Symantec were located in the United States, considerably less than 2008 when 43 percent of such sites were based there.
- The most common top-level domain used in phishing lures detected in 2009 was .com, accounting for 68 percent of the total; it was also the highest ranking top-level domain in 2008 when it accounted for 39 percent of the total.
- The five top phishing toolkits observed by Symantec in 2009 were responsible for a combined average of 23 percent of all observed phishing attacks for the year.

Tweet
- Credit card information was the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 19 percent of all goods and services advertised; this is a decrease from 2008 when credit card information accounted for 32 percent of the total.

Tweet
- Credit card information was advertised on underground economy servers known to Symantec for $0.85 to $30 per credit card number, depending on factors such as bulk purchase sizes, rarity of the card type, and the amount of personal information bundled with the card number.
- The United States was the top country for credit cards advertised on underground economy servers, accounting for 67 percent of the total; this is unchanged from 2008.

Tweet
- The most common type of spam detected in 2009 was related to Internet-related goods and services such as online degrees, which made up 29 percent of all detected spam; in 2008, this was also the most common type of spam, accounting for 24 percent of the total.
- In 2009, spam made up 88 percent of all email observed by Symantec.
- In 2009, the United States was again the top-ranked country for originating spam, with 23 percent of the global total. This is a decrease from 29 percent in 2008.

Tweet
- In 2009, bot networks were responsible for the distribution of approximately 85 percent of all spam email.

Threat Activity Trends

This section of the Symantec *Global Internet Security Threat Report* will provide an analysis of threat activity, as well as other malicious activity, data breaches, and Web-based attacks that Symantec observed in 2009. The malicious activity discussed in this section not only includes threat activity, but also phishing hosts, malicious code, spam zombies, bot-infected computers, and bot command-and-control (C&C) server activity. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS), intrusion prevention system (IPS), or firewall. Definitions for the other types of malicious activities can be found in their respective sections within this report.

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

- Malicious activity by country
- Web-based attacks
- Countries of origin for Web-based attacks
- Data breaches that could lead to identity theft, by sector
- Data breaches that could lead to identity theft, by cause
- Bot-infected computers
- Threat activity—protection and mitigation

Malicious activity by country

This metric will assess the countries in which the largest amount of malicious activity takes place or originates. To determine this, Symantec has compiled geographical data on numerous malicious activities, including bot-infected computers, phishing hosts, malicious code reports, spam zombies, and attack origin. The rankings are determined by calculating the average of the proportion of these malicious activities that originated in each country.

In 2009, the United States was again the top country for overall malicious activity observed by Symantec, making up 19 percent of the total (table 6), a decrease from 2008 when the United States had 23 percent of the total. Within specific category measurements, the United States maintained first rank in malicious code, phishing hosts, bot C&C servers, and originating attacks.

Overall Rank		Country	Percentage		2009 Activity Rank				
2009	2008		2009	2008	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Table 6. Malicious activity by country
Source: Symantec

The decreased proportion of overall malicious activity for the United States is attributable to increased activity in other countries and to its lower percentage for spam zombies. This is similar to the decrease in 2008, as discussed in Volume XIV of the Symantec *Global Internet Security Threat Report*.[32] In 2009, the Federal Trade Commission shut down an Internet service provider (ISP) that was known to host or actively distribute malicious code, bot C&C servers, and illegal pornography, among other content.[33]

One of the botnets linked to this ISP was Pandex (a.k.a., Cutwail).[34] This botnet was responsible for as much as 35 percent of spam observed globally before dropping to 8 percent after the ISP was shut down.[35] Spam zombies that lack a critical command system are unable to send out spam. Additionally, a security researcher allegedly attacked and disabled 250,000 computers associated with the Ozdok (a.k.a., Mega-D) botnet.[36] The volume of spam sent by both botnets recovered several days afterwards because unaffected zombies were instructed to significantly increase their spam output, indicating that these events may have been a large factor in the decrease of spam zombies in the United States.

China had the second highest amount of overall worldwide malicious activity in 2009, accounting for 8 percent of the total; this is a decrease from 9 percent in 2008. China's rankings within most specific category measurements remained consistent with those of 2008, except for spam zombies. For example, its rank for phishing hosts and attack origin remained unchanged, while its rank for malicious code and bot-infected computers dropped by one place for each. For spam zombies, China dropped from fourth in 2008 to eighth in 2009.

China's rank may decline further in 2010 because of an enhanced domain registration procedure introduced by China's Internet Network Information Center (CNNIC) on December 11, 2009.[37] The changes require domain applications to include paper copies of the application form, the official business seal, and the registrant's personal identification. Prior to this change, registrants could register a .cn domain in the guise of a legitimate company and send spam from that domain, which could be interpreted by the spam recipient as coming from a legitimate source. Early observations indicate that the daily volume of spam originating from .cn domains fluctuated around 20 percent after the changes were implemented, down from an average of around 40 percent prior to the changes.

Brazil ranked third for malicious activity in 2009 with 6 percent of the total. This is an increase from 4 percent in 2008 and is the first time since Symantec introduced this metric in 2006 that a country other than the United States, China, or Germany has ranked in the top three. Brazil became more prominent in all of the specific category measurements except for spam zombies, where it was already the top-ranked country. Brazil's significant increases across all categories are related to the growing Internet infrastructure and broadband usage there, as has been discussed in previous versions of the Symantec *Global Internet Security Threat Report*.[38]

[32] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 18
[33] http://www.ftc.gov/opa/2009/06/3fn.shtm
[34] http://www.symantec.com/security_response/writeup.jsp?docid=2007-042001-1448-99
[35] http://searchsecurity.techtarget.com.au/articles/32685-Rogue-ISP-shutdown-slows-spam-torrent
[36] See http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99, http://www.networkworld.com/news/2009/111009-fireeye-moves-quickly-to-quash.html, and http://blog.fireeye.com/research/2009/11/smashing-the-ozdok.html
[37] http://www.symantec.com/connect/blogs/drop-cn-spam
[38] http://www.point-topic.com

Brazil's rise as a source of malicious activity to third place in 2009 was mainly due to a significant increase in its ranking for malicious code, for which it rose up to fifth in 2009 from 16th in 2008. One possible reason for the large increase in malicious code ranking for Brazil was the Downadup (a.k.a., Conficker) worm.[39] This worm drew a lot of attention in late 2008 and early 2009 by infecting a large number of computers worldwide. Brazil was one of the most affected countries, ranking fourth for countries by number of Downadup infections. One explanation for the success of Downadup in Brazil is that it is able to specifically target certain regions based on the identification of the language setting of the computer, one of which is was "Portuguese (Brazilian)."[40]

In addition, Brazil ranked third globally for potential infections by viruses and fourth for potential infections by worms. These rankings represent large increases from previous reporting periods. Brazil has been a major source of successful malicious code that steals banking information, and some very successful malicious code that has originated from Brazil remains active.[41] For example, the Bancos Trojan was first discovered there in 2003 and was still one of the top 50 malicious code samples for potential infections in 2009, mainly due to the continuous release of new variants.[42]

The growing level of malicious code activity affecting Brazil has resulted in the proposal of a new cybercrime bill in the country.[43] The initiative may also be a result of a number high-profile cyber attacks there in recent years.[44] One of the attacks resulted in a massive power grid blackout, while another resulted in the exposure of valuable data and a $350,000 ransom request after a government website was compromised, which also resulted in over 3,000 employees being unable to access the site for 24 hours.

In previous reports, Symantec has observed and discussed indications that countries such as Brazil, Turkey, Poland, India, and Russia would continue to increase their overall share of malicious activity because of their rapidly growing broadband populations and expanding Internet infrastructures.[45] This trend has continued and, with the exception of Turkey ranking 12th, these countries now all rank in the top 10 for malicious activity. Even though it dropped in ranking, and despite increases in the malicious code and phishing hosts categories, Turkey's decrease is attributed mostly to larger increases in overall malicious activity in Russia, India, and Poland. These countries may continue to account for larger percentages within specific categories because their relatively new and growing Internet infrastructures could be exposed to increasing levels of malicious activity until security protocols and measures mature enough to counter these activities. The United States and China account for large enough percentages within specific category measurements that they will likely continue to outrank other countries for overall malicious activity unless there are fundamental changes to Internet usage governance and infrastructure.

There needs to be continued coordinated efforts among law enforcement to address malicious activity occurring globally. This is especially critical in the absence of an agreed-upon international framework for combating cybercrime.

Finally, it is worth noting that malicious activity in countries where the overall percentage dropped, such as the United Kingdom and Germany, was relatively consistent with previous years. The reduced percentages for these countries in 2009 are primarily the result of the increased activity in emergent countries such as Brazil and India.

[39] See http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed1.pdf and http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
[40] http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1_0.pdf : p. 16
[41] http://www.symantec.com/connect/blogs/brazilian-msn-worm-looks-familiar
[42] http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99
[43] http://www.eff.org/deeplinks/2009/07/lula-and-cybercrime
[44] http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/
[45] http://www.point-topic.com

Web-based Attacks

This metric will assess the top distinct Web-based attacks originating from compromised legitimate sites and intentionally malicious sites set up to target Web users. The increasing pervasiveness of Web browser applications along with increasingly common, easily exploited Web browser application security vulnerabilities (as noted in the "Vulnerabilities Trends" section) 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. Instead, they can focus on attacking and compromising websites to mount additional, client-side attacks.

These attack types can be found globally and Symantec identifies each by an associated distinct detection signature. Most attack types target specific vulnerabilities or weaknesses in Web browsers or other client-side applications that process content originating from the Web.

The most common Web-based attack observed in 2009 was related to malicious PDF activity,[46] which accounted for 49 percent of Web-based attacks (table 7). This is a sizeable increase from 11 percent in 2008. Specifically, this attack consists of attempts by attackers to distribute malicious PDF content to victims through the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious PDF file would be designed to exploit arbitrary vulnerabilities in applications that are able to process PDFs. Successful attacks could ultimately result in the compromise of the integrity and security of the affected computers.

This attack is assumed to be popular due to the common use and distribution of PDF documents on the Web. In addition, browsers can be set up to automatically render a PDF document. Specific exploit activity related to malicious PDF files was observed in 2009, including an attack that preyed on public concerns about the H1N1 virus,[47] an attack against the Adobe Reader Collab.getIcon vulnerability,[48] and an attack that exploits a vulnerability in Foxit Reader.[49]

Overall Rank 2009	2008	Attack	Percentage 2009	2008
1	2	PDF Suspicious File Download	49%	11%
2	1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	18%	30%
3	N/A	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution	6%	N/A
4	6	Microsoft Internet Explorer MS Snapshot ActiveX File Download	4%	5%
5	4	Adobe SWF Remote Code Executable	3%	7%
6	14	Microsoft Internet Explorer Malformed XML Buffer Overflow	3%	1%
7	5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	3%	6%
8	20	Microsoft Internet Explorer WPAD Spoofing	3%	1%
9	N/A	Microsoft MPEG2TuneRequestControl ActiveX Buffer Overflow	2%	N/A
10	N/A	Microsoft MPEG2TuneRequestControl ActiveX Instantiation	1%	N/A

Table 7. Top Web-based attacks
Source: Symantec

[46] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153
[47] See http://www.symantec.com/connect/blogs/malicious-code-authors-jump-swine-flu-bandwagon and http://www.securityfocus.com/bid/33751/info
[48] See http://www.symantec.com/connect/blogs/yet-another-pdf-vulnerability-exploited-collabgeticon and http://www.securityfocus.com/bid/34169
[49] See http://www.symantec.com/connect/blogs/foxit-pdf-reader-being-exploited-wild-so-now-where-do-we-go#M192 and http://www.securityfocus.com/bid/34035

The "Vulnerability Trends" section of this report notes that the percentage of plug-in vulnerabilities affecting Adobe Reader in comparison to the total number of browser plug-in vulnerabilities increased to 15 percent in 2009, from 4 percent in 2008 (figure 9). In the previous volume of this report, Symantec noted that attackers are increasingly targeting Adobe Reader. The large growth of Web-based attacks using malicious PDF files and plug-in vulnerabilities affecting Adobe Reader—as observed in 2009 and noted above—indicates that this is a continuing trend. Considering that some users may be unaware of the danger or are slow to install patches for the issue, it is reasonable to assume that attacks against existing PDF-related vulnerabilities will continue in the near future.

In 2009, the second most common Web-based attack was associated with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness,[50] which accounted for 18 percent of the global total—a decrease from 2008 when this vulnerability accounted for 30 percent of the total during that reporting period. This vulnerability allows attackers to install malicious files on a vulnerable computer when a user visits a website hosting an exploit. To carry out this attack, an attacker must exploit an arbitrary vulnerability that bypasses Internet Explorer security settings. The attacker can then execute malicious files installed by the initial security weakness. This vulnerability was disclosed on August 23, 2003, and fixes have been available since July 2, 2004. This indicates that a large percentage of computers are not being adequately patched in a timely manner.

In their efforts to exploit vulnerabilities, attackers not only employ manual methods, but they also use automated tools, such as Neosploit to exploit client-side vulnerabilities on a massive scale.[51] Such toolkits have become widely available and are easy enough to implement that even people with minimal technical knowledge can use them effectively. The market for these toolkits is now sophisticated enough that updated versions are released on a development schedule, advertising the inclusion of exploits for the latest vulnerabilities while retaining previous exploits. This may well contribute to the continued prevalence of the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness. Despite a patch being released in 2004, there are still a significant number of toolkit-based attacks occurring that attempt to exploit this issue. This underlines the importance of security measures and patches that address old issues as well as new ones.

The Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness was the most common Web-based attack in 2008, and the reduced activity observed in 2009 may indicate that fewer computers are running older, susceptible versions of Internet Explorer (as is discussed in the "Web browser vulnerabilities" metric). It is reasonable to assume that the prominence of this attack will continue to decline as more users make the switch to browser versions that are not affected by the weakness.

The third most common Web-based attack in 2009 exploited the Internet Explorer 7 Uninitialized Memory Code Execution Vulnerability,[52] accounting for 6 percent of the total. This vulnerability was published on February 10, 2009, and fixes have been available since that time. Seven days after that date, the issue was being actively exploited in the wild and exploit code was publicly available on February 18, 2009.

[50] See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or http://www.securityfocus.com/bid/10514
[51] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=1
[52] See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23291 or http://www.securityfocus.com/bid/33627

An attacker can exploit this vulnerability by enticing a victim to open a malicious Web page. A successful attack will allow an attacker to execute remote code on a victim's computer. This vulnerability may be appealing to attackers because, rather than relying on a plug-in that may or may not be installed on a target computer, it relies only on the use of a version of a popular browser, thereby increasing the number of potential victims.[53]

Vulnerabilities such as those in the top 10 for 2009 continue to generate a large amount of observed attack activity because they can be reliably exploited on systems that are not routinely kept up to date. This makes these vulnerabilities prime candidates for automation. Despite the fact that fixes are available, as mentioned, it is likely that there are still enough unpatched systems in existence that these attacks continue to enjoy success. When attacks prove successful, they are often adopted by attack toolkits. This can cumulatively create a large amount of observed attack activity. It is also likely that older malicious code variants continue to attempt to automatically exploit these vulnerabilities as a means of propagation.

Countries of origin for Web-based attacks

This metric will assess the top countries of origin for Web-based attacks against users in 2009 by determining the location of computers from which the attacks occurred. Note that an attacker in one country can compromise a Web server in another country that is visited by a user from another country. Therefore, the location of attacks does not dictate the location of the actual attacker, who could be located elsewhere.

Once an attacker has compromised a legitimate website, users who visit the website can be attacked by several additional means. One method is a drive-by download, which results in the installation of malicious code without the user's knowledge or consent.[54] Another way is to redirect the user to another website that is hosting malicious code. Sites and servers hosting a variety of malicious exploits can be found worldwide, and multiple domains can be associated with a single compromised site that is being used to exploit one or more security vulnerabilities in affected client browsers.

Computers located in the United States were the leading source of Web-based attacks against users globally in 2009, accounting for 34 percent of the total (table 8). This is a slight decrease from 38 percent in 2008. Computers in the United States continue to account for a large percentage of Web-based attacks compared to other high-ranking countries. This is not surprising considering the extent of the Internet infrastructure in the country, as well as the amount of malicious activity occurring on computers there, as previously discussed in "Malicious activity by country." Furthermore, the United States accounts for a significant percentage of worldwide broadband usage, meaning that there are a greater number of computers that could potentially be used to launch attacks.[55] All of these factors combined to create a convenient and established launching point for some attackers.

[53] See http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2 and http://www.w3schools.com/browsers/browsers_stats.asp
[54] A drive-by download is any download that occurs without a user's prior knowledge or authorization and does not require user interaction. Typically, this is an executable file.
[55] http://www.point-topic.com

Rank	Country	Percentage
1	United States	34%
2	China	7%
3	Brazil	4%
4	United Kingdom	4%
5	Russia	4%
6	Germany	4%
7	India	3%
8	Italy	2%
9	Netherlands	2%
10	France	2%

Table 8. Top countries of origin for Web-based attacks
Source: Symantec

In 2009, 7 percent of Web attacks originated from computers in China, which is a decrease from 13 percent in 2008. As was discussed in the previous version of this report, the higher percentage in 2008 was likely due to compromised websites relating to the 2008 Beijing Olympic Games.[56] It is reasonable to assume that the number of attacks from these websites has tapered off since the conclusion of the games and may be a significant factor in the decrease of Web attacks originating from computers in China in 2009.

Brazil was the third-ranked country of origin for Web-based attacks in 2009, accounting for 4 percent of the total. While there were no noteworthy high-profile Web-based attacks in Brazil in 2009, the amount of overall malicious activity increased significantly, particularly in regards to malicious code. Web-based attacks are an effective means of installing malicious code on the computers of unsuspecting users, indicating that the increase in malicious activity in Brazil may be closely related to increases in Web-based attacks originating there. Furthermore, the growth in bot-infected computers in Brazil may also have been a contributing factor because bots are commonly used to launch Web-based attacks.

Web-based attacks are a major threat to computer networks for both enterprises and consumers. The covert nature of these types of attacks (such as drive-by downloads) makes them very difficult to protect against because most users are unaware that they are being attacked. Organizations are thus confronted with the complicated task of having to detect and filter attack traffic from legitimate traffic. Since many organizations now rely on Web-based tools and applications to conduct business, it is likely that the Web will continue to be the primary conduit for attack activity favored by malicious code developers. To avoid the likelihood of threats, organizations can implement strong security policies and the latest software patches as well as educate staff about potential security issues and how to prevent becoming a victim.

[56] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 18

Data breaches that could lead to identity theft, by sector

Identity theft continues to be a high-profile security issue. In a recent survey, 65 percent of U.S.-based poll respondents said that they were either "very concerned" or "extremely concerned" about identity theft.[57] Furthermore, 100 percent of enterprise-level respondents surveyed for the Symantec *State of Enterprise Security Report 2010* experienced loss or theft of data.[58]

The danger of data breaches is of particular importance for organizations that store and manage large amounts of personal information. Not only can compromises that result in the loss of personal data undermine customer and institutional confidence, result in costly damage to an organization's reputation, and result in identity theft that may be costly for individuals to recover from, they can also be financially debilitating to organizations.[59] In 2009, the average cost per incident of a data breach in the United States was $6.75 million, which is slightly higher than the average for 2008. Considering that the average cost per incident has also been rising in recent years (having risen from $4.5 million in 2005, for example), it is reasonable to assume that average costs will continue to rise in coming years. Reported costs of lost business ranged from $750,000 to $31 million.[60]

Using publicly available data, Symantec has determined the sectors that were most often affected by these breaches and the most common causes of data loss.[61] Using the same publicly available data, this discussion will also explore the severity of the breach in question by measuring the total number of identities exposed to attackers.[62]

It should be noted that some sectors might need to comply with more stringent reporting requirements for data breaches than others. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[63] 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.

The education sector accounted for the highest number of known data breaches that could lead to identity theft, accounting for 20 percent of the total (figure 4). This was a decrease from 27 percent in 2008 when the education sector also ranked first.

[57] http://arstechnica.com/security/news/2009/10/americans-fear-online-robberies-more-than-meatspace-muggings.ars
[58] http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf
[59] http://www.wired.com/threatlevel/2009/11/pos?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29
[60] http://www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf
[61] Open Security Foundation (OSF) Dataloss DB, see http://datalossdb.org
[62] An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.
[63] Please see http://www.privacyrights.org/fs/fs6a-facta.htm and http://www.cms.hhs.gov/HealthPlansGenInfo/12_HIPAA.asp

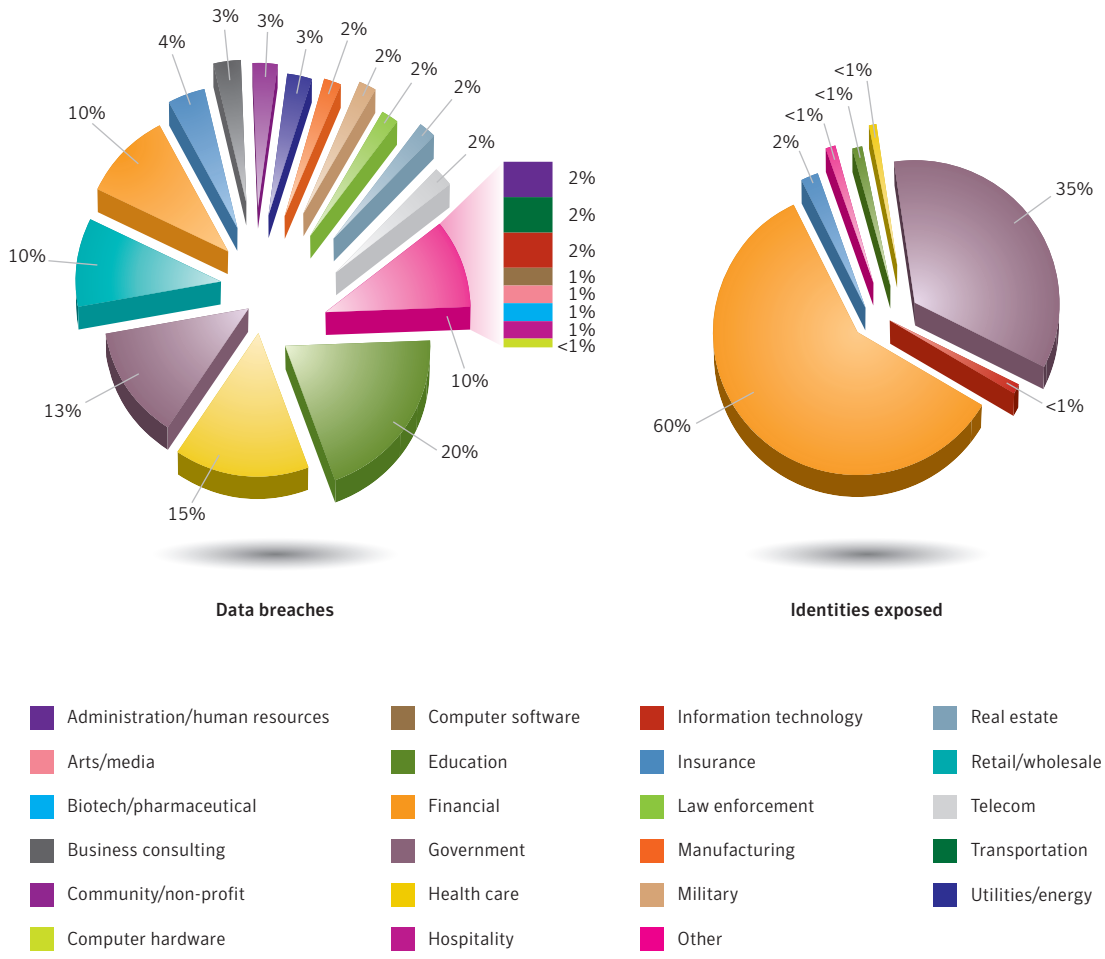

Figure 4. Data breaches that could lead to identity theft by sector and identities exposed by sector[64]
Source: Based on data provided by OSF DataLoss DB

Institutions in the education sector often store a wide range of personal information belonging to students, faculty, and staff. This information may include government-issued identification numbers, names, or addresses that could be used for the purposes of identity theft. Finance departments in these institutions also store bank account information for payroll purposes and may hold credit card information for people who use this method to pay for tuition and fees. These institutions—particularly larger universities—often consist of many autonomous departments. Sensitive personal identification information held by these individual departments may be stored in separate locations and be accessible to many people using separate and distinct control systems. Educational institutions are faced with the difficult task of standardizing and enforcing security across dispersed locations, as well as educating everyone with access to the data on the security policies. This may increase the opportunities for an attacker to gain unauthorized access to data because there are multiple points of potential security weakness or failure.

[64] Due to rounding, percentages might not equal 100 percent.

Although the education sector accounted for the largest percentage of data breaches in 2009, those breaches accounted for less than 1 percent of all identities exposed during the reporting period and ranked fourth (figure 4). This is similar to 2008, when a significant percentage of breaches affected the education sector but only accounted for 4 percent of all identities exposed that year. This is mainly attributed to the relatively small size of databases at educational institutions compared to those in the financial or government sectors. Each year, even the largest universities in the United States only account for students and faculty numbering in the tens of thousands, whereas financial and government institutions store information on millions of people.[65] As such, data breaches in those sectors can result in much larger numbers of exposed identities.

In 2009, the health care sector ranked second, accounting for 15 percent of data breaches that could lead to identity theft. In 2008, this sector also accounted for 15 percent, but ranked third. This rise in rank is most likely due to the decreased percentage of breaches that could lead to identity theft in the government sector. The health care sector accounted for less than 1 percent of exposed identities in 2009—a decrease from 5 percent in 2008. Like the education sector, health care institutions store data for a relatively small number of patients and staff compared to some organizations in the financial and government sectors.

Additionally, health care organizations often store information that may be more sensitive than that stored by organizations in other sectors and this may be a factor in the implementation of certain regulatory measures. For instance, as of 2010, greater responsibility for data breaches will be enforced for health care organizations in United States because of regulations introduced by the Health Information Technology for Economic and Clinical Health Act (HITECH).[66]

The government sector accounted for 13 percent of breaches that could lead to identity theft in 2009 and ranked third. This is a decrease from 20 percent in 2008 when the government sector ranked second. Although the percentage of these breaches has decreased in recent years, they account for a larger percentage of exposed identities. In 2009, data breaches in the government sector exposed 35 percent of reported identities exposures, an increase from 17 percent in 2008.

The increase in percentage of identity exposures in the government sector is primarily due to a breach attributed to insecure policy from the National Archives and Records Administration in the United States.[67] A faulty hard drive containing unencrypted personal information on 76 million military veterans was sent to a third-party electronics recycler without first removing the data. This was the largest ever exposure of personal information by the United States government. Earlier in 2009, another hard drive belonging to the National Archives and Records Administration was either lost or stolen; it is believed to have contained highly sensitive information about White House and Secret Service operating procedures, as well as data on more than 100,000 officials from the Clinton administration.[68]

The financial sector was subject to one of the most notable data breaches reported in 2009. This sector ranked fifth for breaches with 10 percent of the total, but accounted for the largest number of identities exposed with 60 percent. The majority of this percentage was the result of a successful hacking attack on a single credit card payment processor.[69] The attackers gained access to the company's payment processing network using an SQL-injection attack. They then installed malicious code designed to gather sensitive information from the network on the compromised computers, which also allowed them to easily access the network at their convenience. The attack resulted in the theft of approximately 130 million credit card

[65] http://www.osu.edu/osutoday/stuinfo.php
[66] http://findarticles.com/p/articles/mi_hb4365/is_21_42/ai_n47569144/
[67] http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/
[68] http://fcw.com/Articles/2009/05/20/Web-NARA-missing-hard-drive.aspx
[69] http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html

numbers. An investigation began when the company began receiving reports of fraudulent activity on credit cards that the company itself had processed. The attackers were eventually tracked down and charged by federal authorities.

Notably, one of the hackers was Albert "Segvec" Gonzalez, who had been previously convicted of other attacks. He plead guilty to 19 counts of conspiracy, wire fraud and aggravated identity theft charges in March 2010 and was sentenced to serve up to 25 years in prison. He had also worked as an FBI informant at one point, providing information about the underground economy.[70] These attacks and the events surrounding them were discussed previously in the Symantec *Report on the Underground Economy*.[71]

This attack is evidence of the significant role that malicious code can play in data breaches. Although data breaches occur due to a number of causes, the covert nature of malicious code is an efficient and enticing means for attackers to remotely acquire sensitive information. Furthermore, the frequency of malicious code threats that expose confidential information, which is discussed in the **"Threats to confidential information"** metric, underscores the significance of identity theft to attackers who author and deploy malicious code.

Data breaches that could lead to identity theft, by cause

The primary cause of data breaches, across all sectors, that could facilitate identity theft in 2009 was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium.[72] Theft or loss made up 37 percent of all data breaches in 2009, a decrease from the previous reporting period when it accounted for 48 percent of all reported breaches (figure 5).

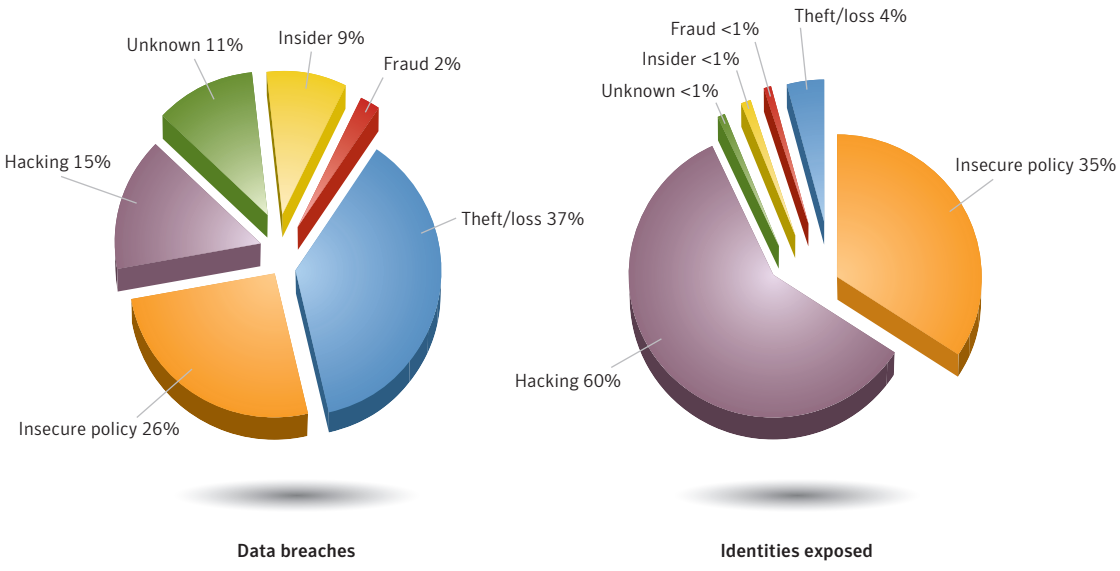

Figure 5. Data breaches that could lead to identity theft by cause and identities exposed[73]
Source: Based on data provided by OSF DataLoss DB

[70] See http://www.wired.com/threatlevel/2009/12/gonzalez-heartland-plea/ and http://yro.slashdot.org/article.pl?sid=10/03/26/124256
[71] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
[72] This cause will be referred to as "theft or loss" for the remainder of the report.
[73] Due to rounding, percentages might not equal 100 percent.

Despite the significant percentage of reported breaches, theft or loss accounted for only 4 percent of all identities exposed in 2009 (figure 5). This was a large decrease from 2008, when the number of identities exposed from theft or loss accounted for 66 percent of the total. This is a dramatic decrease in identities exposed; however, as was discussed in the previous version of this report, the three largest data breaches reported in 2008 resulted from lost or missing disks and exposed personal information relating to an estimated 41 million people. Therefore, this decrease is primarily due to the lack of large-scale identity exposures by theft or loss as well as the large-scale increases to exposed identities due to insecure policy.

Insecure policy was the second most common cause of data breaches across all sectors that could lead to identity theft in 2009, accounting for 26 percent of all incidents. A data breach is considered to be caused by insecure policy if it can be attributed to a failure to develop, implement, and/or comply with adequate security policy. This is an increase from 21 percent in 2008, when insecure policy also ranked second.

The increase in exposed identities was much more significant. Insecure policy accounted for the second largest number of exposed identities in 2009, with 35 percent of the total. This is a significant increase from 2008, when insecure policy accounted for only 8 percent of exposed identities. This is primarily attributed to the breach of National Archives and Records Administration data that was discussed above. That incident alone exposed 76 million identities, which is much greater than the combined exposures due to insecure policy that were reported in 2008, totaling only 6.5 million.[74]

The third most common cause of data breaches that could lead to identity theft in 2009 was hacking, which accounted for 15 percent of the total. 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 also ranked third in 2008 for breaches that could facilitate identity theft, when it accounted for 17 percent of the total.

Hacking was the leading source for reported identities exposed in 2009, increasing substantially to 60 percent of the total, from 22 percent in 2008. For this discussion, Symantec considers hacking to be an intentional act with to the objective of stealing data that can be used for purposes of identity theft or other fraud. Attackers can take advantage of site-specific and Web-application vulnerabilities to gain access to networks and steal personal information. This is exemplified by the attack on the credit card payment processor, discussed above, that used malicious code to steal approximately 130 million credit card numbers. This breach is also the primary reason that hacking as a cause for reported identities exposed surged as much as it did in 2009.

Bot-infected computers

Bots are programs that are covertly installed on a user's computer to allow an attacker to remotely control the targeted computer through a communication channel, such as Internet relay chat (IRC), peer-to-peer (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.

[74] http://datalossdb.org

Bots allow for a wide range of functionality and most can be updated to assume increased 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 model because they are difficult to disable and allow the attackers to hide in plain site 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.

In 2009, Symantec observed underground economy advertisements for as little as $0.03 per bot. This is similar to 2008, when $0.04 was the cheapest price advertised for bots. It should be noted that botnets generally consist of large numbers of bot-infected computers and despite the low cost per bot, they are typically sold in bulk lots ranging from hundreds to tens-of-thousands of bots per lot, meaning that the actual cost of a botnet is significantly higher than the per-bot price.

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. In 2009, Symantec observed an average of 46,541 active bot-infected computers per day (figure 6), which is a 38 percent decrease from 2008. Symantec also observed 6,798,338 distinct bot-infected computers during this period, which is a 28 percent decrease from 2008. This decrease is primarily considered the result of bots sending larger volumes of spam instead of propagating, as is discussed below. Another possible reason for this decrease is that some bots may be performing non-typical activity that is not being monitored.

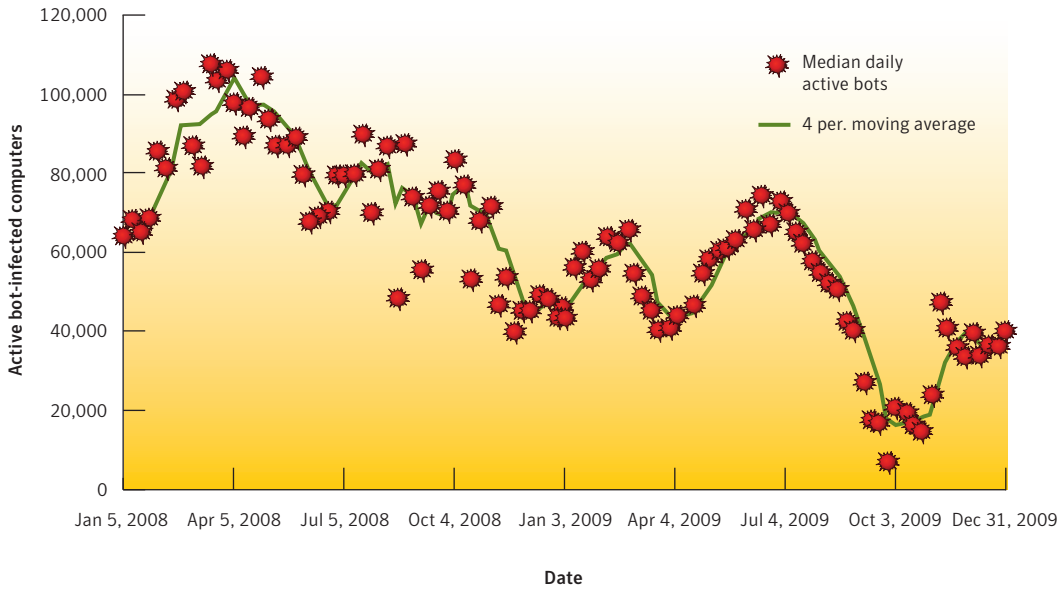

Figure 6. Active bot-infected computers, by day
Source: Symantec

The Downadup worm, which first appeared late in 2008, attracted a lot of attention in the first half of 2009 because it was used to rapidly create a large botnet. This contributed significantly to daily activity levels observed during this reporting period, particularly at the beginning of the year. The increase in active bots per day is also indicative of the predicted growth and recovery of several prominent botnets—Srizbi,[75] Rustock,[76] Ozdok, and Pandex—following the shutdown of two U.S.-based Web hosting companies late in 2008.[77] The Web hosts were allegedly hosting large numbers of C&C servers and there was a noticeable decline in botnet activity following the shutdowns. As these botnets recovered and grew, so did their levels of technical sophistication. This was apparent when, following the shutdown of two other botnet hosts in 2009 and a subsequent decrease in spam levels, the volume of spam returned to normal soon afterward, indicating that the botnet controllers had implemented contingency plans in case of shutdown.

The dip in activity between March and July 2009 coincides in part with the release of two Downadup variants as well as with increased spam output from the Pandex botnet. The first of the Downadup variants, Downadup.B,[78] was released in March and lacked a propagation routine, which may have contributed to the downward slope toward April, until the release of the second variant, Downadup.C,[79] which did include a propagation routine. The increased spam output by Pandex, one of the most prominent botnets following the previously mentioned ISP shutdowns in 2008, was likely achieved at the expense of further propagation. The increased output of spam was observed from April to June and the lack of propagation activity may have contributed to the drop in overall botnet activity.

There are several possible contributing factors to the large decline in botnet activity that began in late June and continued through to November. Between July and November, four notable botnets—Grum,[80] Maazben,[81] Festi,[82] and Rustock—increased their spam output volumes significantly during overlapping one- to three-month periods.[83] Additionally, Symantec observed increased spam output from the Donbot[84] botnet from April to December. As mentioned, increased spam output may come at the cost of propagation activity and may have contributed to the reduced activity observed during 2009.

There were also two ISP shutdowns in 2009 that could be related to the decline. The first shutdown in late June was the previously discussed shutdown ordered by the United States Federal Trade Commission and the second was an ISP in Latvia.[85] Both of these ISP shutdowns resulted in an immediately noticeable reduction in spam volume, particularly from Pandex; however, spam volumes returned to normal levels within a matter of days. This may have been the result of continued increases to spam output at the cost of propagation as well as redundancies built into the botnet.

Another contributing factor to the decline in botnet activity during the second half of 2009 may have been that there was a notable increase in spam containing malicious code in both September and October.[86] This may have resulted from botnet administrators wanting to maintain the increased spam output per bot while offsetting the reduction in propagation through IRC, P2P, and HTTP channels.

[75] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
[76] http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99
[77] See http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf and http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf
[78] http://www.symantec.com/security_response/writeup.jsp?docid=2008-123015-3826-99
[79] http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-010717-4209-99
[80] http://www.symantec.com/security_response/writeup.jsp?docid=2007-033016-1857-99&tabid=1
[81] http://www.symantec.com/connect/blogs/evaluating-botnet-capacity
[82] http://www.symantec.com/connect/blogs/festi-botnet-spins-become-one-main-spamming-botnets
[83] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 8–10
[84] http://www.symantec.com/security_response/writeup.jsp?docid=2009-012112-4859-99
[85] http://www.symantec.com/connect/blogs/latvian-isp-closure-dents-cutwail-botnet
[86] See http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_10-2009.en-us.pdf and http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_11-2009.en-us.pdf

As mentioned previously, the technical sophistication of bots increased during this reporting period. As such, the authors of these threats may be shifting toward different channels of propagation, such as P2P. This may also explain the decline in activity observed from July through September. Consumer reaction to Downadup may also have contributed to this decline. As public attention to Downadup grew, users may have become more active in patching and protecting their computers from infection by the worm. Similarly, the attention may have alerted users already infected with Downadup who would not have otherwise been aware of the problem. As the number of computers secured against the worm increases, the activity levels of the worm should decline. Furthermore, no other Downadup variants have been released that could exploit other vulnerabilities and counteract the actions taken by users.

In 2009, the day-to-day bot activity levels were less sporadic than they were in 2008. Significant increases and decreases in activity occurred gradually over the course of several days or months. One possible explanation is that, following the shutdown of the two U.S.-based Web hosting companies discussed above, botnets may have been managed with more consistent commands in an effort to bolster against future shutdown attempts or to make up for decreased resources following shutdowns.

The levels of bot activity are always in flux as new techniques are deployed for existing bots or new families of malicious code are launched, and in the last quarter of 2009, bot activity began to rise again. As mentioned in the **"Malicious activity by country"** metric, CNNIC made substantial changes to the .cn domain registration procedure, which appeared to have an immediate effect on spam levels. This change may continue to have a noticeable effect on the activity levels of botnets that send spam in 2010.

Threat activity—protection and mitigation

There are a number of measures that enterprises, administrators, and end users can employ to protect against malicious activity. Organizations should monitor all network-connected computers for signs of malicious activity including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organizations should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[87] Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

Symantec recommends that organizations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place. Organizations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users. In addition, egress filtering is one of the best ways to mitigate a DoS attack. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

[87] Defense-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defense-in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. By creating and enforcing policies that identify and restrict applications that can access the network, organizations can minimize the effect of malicious activity, and hence, minimize the effect on day-to-day operations. In addition, administrators should limit privileges on systems for users that do not require such access and they should restrict unauthorized devices such as external portable hard-drives and other removable media.

To reduce the likelihood of identity theft, organizations that store personal information should take the necessary steps to protect data transmitted over the Internet or stored on their computers. This should include the development, implementation, and enforcement of a secure policy requiring that all sensitive data be encrypted. Organizations should implement a data loss protection (DLP) solution that not only serves to prevent data breaches but that can also mitigate potential data leaks from within an organization. Access to sensitive information should be restricted and organizations should enforce compliance to information storage and transmission standards such as the Payment Card Industry (PCI) standard.[88] Policies that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorized individuals should be put in place and enforced. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access. This would ensure that even if the computer or medium on which the data were stored, lost, or stolen, the data would not be accessible. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access.

[88] https://www.pcisecuritystandards.org/

Vulnerability Trends

This section will discuss selected vulnerability trends in greater depth, providing analysis and discussion of the trends indicated by the data. The following metrics will be discussed:

- Web browser vulnerabilities
- Window of exposure for Web browsers
- Web browser plug-in vulnerabilities
- Top attacked vulnerabilities
- Zero-day vulnerabilities
- Vulnerabilities—protection and mitigation

Web browser vulnerabilities

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. Web browsers are particular security concerns because they are exposed to a greater amount of potentially untrusted or hostile content than most other applications. This is a concern because every year there is an increased reliance on browsers and their plug-ins as the Internet becomes more integral to business and leisure activities. Attacks can originate from malicious websites as well as legitimate websites that have been compromised to serve malicious content. Browsers can also facilitate client-side attacks because of their use of plug-ins and other applications in handling potentially malicious content served from the Web, such as compromised documents and media files.

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

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox[89]
- Opera

During 2009, 169 vulnerabilities affected Firefox (figure 7). This is more than the 99 vulnerabilities that were documented in 2008 for Mozilla browsers.

[89] As of this report, Symantec has limited the Mozilla browsers studied to include only Firefox because the Mozilla suite is no longer supported by the Mozilla Foundation.

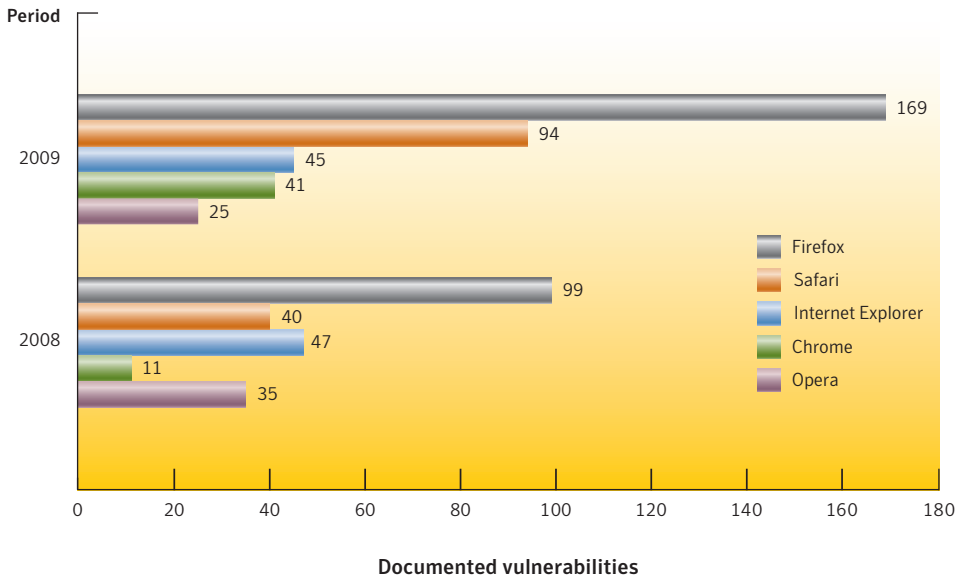

Figure 7. Web browser vulnerabilities
Source: Symantec

Internet Explorer was subject to 45 new vulnerabilities in 2009. This is fewer than the 47 new vulnerabilities documented in Internet Explorer in 2008. One particular vulnerability in Internet Explorer was the third most attacked of all of the vulnerabilities discovered in 2009.[90] Interestingly, reports of attacks in the wild began to surface seven days after the vulnerability was announced by Microsoft. Patches were available when Microsoft first published the vulnerability. Numerous publicly and commercially available exploits were subsequently made available. The potential for reliable exploitation and the market share of Internet Explorer were factors in the large number of attacks targeting this vulnerability. This demonstrates that Internet Explorer is still a popular target of Internet attackers despite the trend toward attacks on browser plug-ins and other client-side vulnerabilities that do not target the browser directly.

The results for the remaining three browsers analyzed in 2009 were as follows: Safari was affected by 94 new vulnerabilities, which is more than double the 40 vulnerabilities identified in Safari in 2008; Symantec documented 25 new vulnerabilities in Opera, which is down from 35 in 2008; finally, Chrome was affected by 41 vulnerabilities, which is significantly more than the 11 documented for 2008—although it should be noted that Chrome was only officially released in September 2008.

[90] http://www.securityfocus.com/bid/33627

According to recent statistics from late 2009, there was an increase in the market share of Chrome, Firefox, and Safari at the expense of Internet Explorer over the course of the year.[91] Symantec speculates that security concerns may have been a factor in the shifting browser demographics. While it is certain that the increase in the percentage of Internet Explorer 8 users is due to installations of Windows 7, which includes the browser by default, enhanced security is also believed to be a factor in its increased use even as Internet Explorer loses market share overall. That said, the shifting market share should not significantly endanger browsers other than Internet Explorer in terms of attacks in the wild as it is unlikely that a tipping point has yet been reached that will make the development of concerted attacks on other browsers sufficiently profitable to be viable.

In order to reduce the threat of successful exploitation of Web browsers, administrators should maintain a restrictive policy regarding which applications are allowed within the organization. The security of applications should be evaluated on a platform-by-platform basis to ensure that platform-specific security issues do not arise when the application is installed. This will ensure that desktops within the organization are not running unauthorized software. Browser security features and add-ons should be employed wherever possible to disable JavaScript™, Adobe Flash Player, and other content that may present a risk to the user when visiting untrusted sites. Organizations should consider adopting a policy of identifying a list of whitelisted, trusted, or authorized websites and block access to all other sites. Whitelists must be actively maintained due to the risk presented when trusted sites are compromised and used to host attacks or malicious software.

Window of exposure for Web browsers

The window of exposure for Web browsers is the difference in days between the time when exploit code affecting a vulnerability is made public and the time when the affected vendor makes a patch publicly available for that vulnerability. During this time, the computer or system on which the affected application is deployed may be susceptible to attack. The metric is derived from the average amount of time it takes to release a patch in comparison to the average amount of time it takes for exploit code to be made publicly available. This metric also includes maximum patch times, which is the maximum amount of time required to release a patch for all of the patched vulnerabilities in the data set.

Measuring the time that it takes for vendors to release patches for vulnerabilities may provide insight into overall vendor security responsiveness. Some vulnerabilities examined were patched by the vendor at the time they were announced. This may be due to an internal security audit by the vendor, which may have revealed the vulnerability, or it may have been because security researchers discovered the vulnerability and responsibly disclosed it to the vendor. Other vulnerabilities are independently reported by security researchers prior to the release of a patch, indicating that security researchers may not have coordinated with the vendor to disclose the vulnerability. This may be because the researcher did not responsibly disclose the vulnerability, or else it is possible that the researcher attempted to responsibly report the vulnerability but the vendor was unresponsive. The patch release time is compared against the average time for vulnerability exploits to become publicly available in order to determine the window of exposure.

[91] http://www.w3schools.com/browsers/browsers_stats.asp

This metric will examine the window of exposure for the following Web browsers:[92]

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

In 2009, the average window of exposure for Safari was 13 days, based on a sample set of 78 patched vulnerabilities (figure 8). It should be noted that there are now full versions of Safari for both Macintosh® and Windows. The window of exposure for Safari in 2008 was nine days, based on a sample set of 31 patched vulnerabilities. The maximum time for Apple to patch a Safari vulnerability in 2009 was 145 days. The maximum time to release a patch in 2008 was 156 days.

In 2009, there were a number of vulnerabilities targeting cross-browser JavaScript, HTML, and graphics rendering engines. This accounts for the increase in the window of exposure because, in some cases, Apple released patches for these vulnerabilities later than other patches. This could reflect the difficulty of testing and patching these vulnerabilities. Other browser vendors were similarly affected because many browsers are now using third-party and/or open-source engines and components. While browsers have been prone to similar attacks in the past because they have had to implement the same features as competitors, the use of shared components puts multiple vendors at risk when a vulnerability is discovered in an affected component.

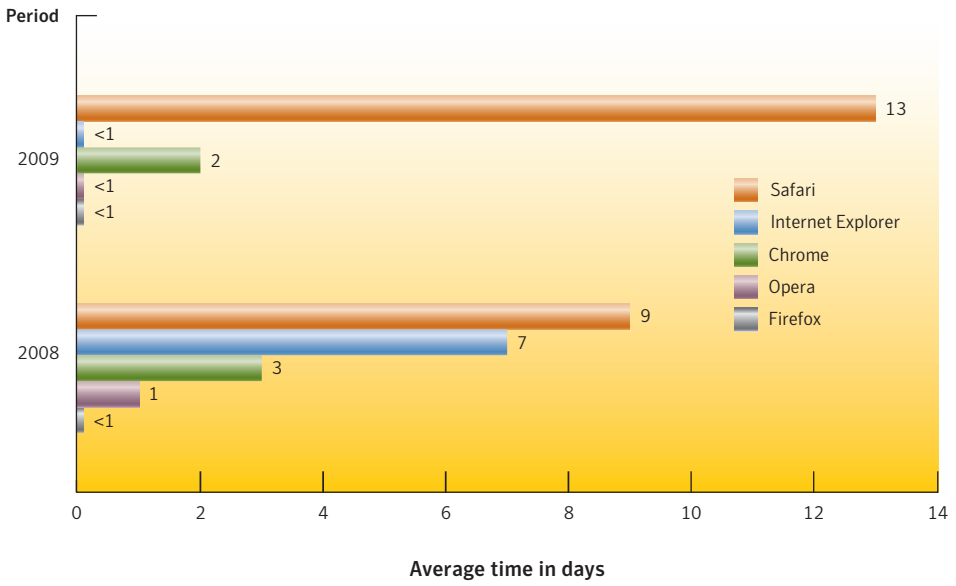

Figure 8. Window of exposure for Web browsers
Source: Symantec

[92] It should be noted that this metric examines all versions of each browser; vulnerabilities affecting multiple versions of a browser are counted as a single vulnerability.

The average window of exposure for Internet Explorer in 2009 was less than one day, based on a sample set of 28 patched vulnerabilities. Eighteen days was the maximum amount of time to release a patch for Internet Explorer in 2009. Internet Explorer had an average window of exposure of seven days in 2008, based on a sample set of 31 patched vulnerabilities. The maximum amount of time to release a patch in 2008 was 147 days.

It took an average of one day for Microsoft to release a patch for Internet Explorer, while on average public exploits emerged two days after vulnerability publication. Usually, Microsoft has kept the window of exposure to a minimum; however, its monthly patch cycles can potentially introduce important exceptions in cases where vulnerabilities are disclosed publicly. In November 2009, exploit code was released for a new vulnerability in Internet Explorer.[93] A patch was released for the vulnerability (18 days after the release of the exploit code) as part of the monthly Microsoft patch release for December. While, in general, Microsoft was able to release patches before exploit code was publicly available, the longest patch turnaround time for the year was in relation to a vulnerability with working public exploit code.

Chrome had a window of exposure of two days in 2009, from a sample set of 29 patched vulnerabilities. In 2009, the maximum of amount time for a patch to become available for Chrome was 16 days. In 2008, Symantec documented an average window of exposure of three days for Chrome, based on a sample set of six patched vulnerabilities.[94] The maximum patch time for a vulnerability was 11 days.

In 2009, the window of exposure for Opera was less than one day, based on a sample set of 16 patched vulnerabilities—the maximum patch time was three days. The window of exposure for Opera in 2008 was one day, based on a sample set of 33 patched vulnerabilities. In 2008, the maximum time to patch a vulnerability was 29 days.

In 2009, Firefox had a window of exposure of less than one day for a sample set of 151 vulnerabilities and the maximum patch time was 75 days. Firefox had a window of exposure of less than one day in 2008, based on a sample set of 83 patched vulnerabilities, and the maximum patch time was 30 days.

Mozilla continues to maintain a narrow window of exposure despite the challenges of patching the largest number of vulnerabilities of any browser vendor. This is due to factors such as aggressive auditing from the security and development community in addition to Mozilla's security bug bounty program that compensates security researchers for responsibly disclosing vulnerabilities in Mozilla products.[95]

The browsers analyzed in 2009 all had an average window of exposure of less than one day except for Chrome and Safari. Additionally, all browsers except Safari either remained *status quo* or showed an improvement in the window of exposure. This demonstrates an increased effort by vendors to minimize the amount of time that users are exposed to exploits. While Internet Explorer remains the most targeted of the browsers and the most likely to be associated with zero-day and malicious code attacks, other browser vendors enjoying an increase in market share seem to be anticipating the risks posed by such attacks.

[93] http://www.securityfocus.com/bid/37085
[94] It should be noted for comparison that Google Chrome data for the previous year begins in September 2008 because that is when Chrome was officially released to the public.
[95] http://www.mozilla.org/security/bug-bounty.html

During the window of exposure, administrators and end users need to mitigate the possibility of exploitation by employing current best practices and the best available mitigation technologies. To reduce the risk posed by unpatched browsers during the windows of exposure, organizations should subscribe to security intelligence alerting services to track vulnerabilities, mitigations, best practices, and patch information. Intrusion prevention and detection systems, in combination with antivirus solutions, can help repel attacks on the browser. Organizations should actively maintain a whitelist of trusted websites and implement policies to limit access to all other sites. It is important to keep whitelists up to date because of the risk that trusted websites might be compromised to host attacks and malicious software. Organizations can temporarily remove such sites from the whitelist at their discretion to limit the risk to users. Browser security features and add-ons can allow users to block access to certain content such as JavaScript and Flash. This security measure should be implemented when visiting sites that are untrusted or unfamiliar.

Web browser plug-in vulnerabilities

This metric will examine 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. Often, these plug-ins allow additional multimedia content from Web pages to be rendered in the browser. They can also enable execution environments that allow applications to be run inside the browser. Browser plug-in vulnerabilities are also used in a range of client-side attacks. Many browsers 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 some may even be required to effectively use the internal sites of enterprises.

The following plug-in technologies will be examined:

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

In 2009, Symantec documented 321 vulnerabilities affecting plug-ins for Web browsers (figure 9). ActiveX technologies were affected by 134 vulnerabilities, which was the highest among the plug-in technologies examined. Of the remaining technologies, Java SE had 84 vulnerabilities, Adobe Reader had 49 vulnerabilities, QuickTime had 27 vulnerabilities, and Adobe Flash Player was subject to 23 vulnerabilities. The remaining four vulnerabilities affected extensions for Firefox.

It should be noted that, in 2009, some vulnerabilities fell into multiple categories. For example, the Java SE ActiveX vulnerability[96] counts in two categories, ActiveX and Java SE. This is because there is a version of Java SE that is implemented as an ActiveX control. Similarly, the Firefox plug-in for the Adobe Reader vulnerability[97] counts in both the Adobe Reader and Firefox extensions categories; this is because Adobe has released a version of Adobe Reader that is implemented as a plug-in for Firefox.

[96] http://www.securityfocus.com/bid/34931/
[97] http://www.securityfocus.com/bid/36669

The 321 total vulnerabilities in plug-in technologies for Web browsers for 2009 is less than the 424 in 2008. Of the total for 2008, 287 vulnerabilities affected ActiveX, which is significantly more than any other plug-in technology. Of the remaining plug-ins for which vulnerabilities were documented, there were 54 vulnerabilities identified in Java SE, 40 in QuickTime, 17 in Adobe Reader, 16 in Adobe Flash Player, and 5 vulnerabilities in Firefox extensions.

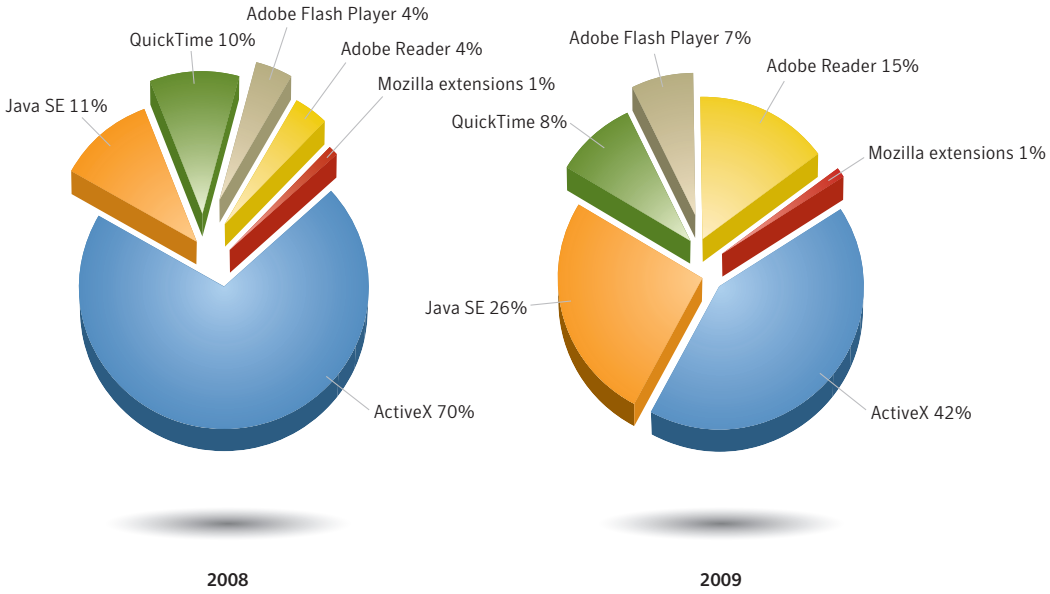

Figure 9. Web browser plug-in vulnerabilities
Source: Symantec

The decrease of ActiveX plug-in vulnerabilities to 42 percent of the total in 2009 from 70 percent of the total in 2008 is influenced by a number of factors. Symantec has observed that automated vulnerability discovery tools such as fuzzers were a large factor in the number of ActiveX vulnerabilities published in previous years. As of 2009, hundreds or possibly thousands of ActiveX components have been audited by the security research community. Since much of the vulnerability research can be attributed to a few popular tools, it is likely that these tools are beginning to reach their limitations. New approaches or more in-depth security research techniques may change this trend and result in the discovery of increasingly more ActiveX vulnerabilities per year. However, for the moment it appears that this trend is on the decline. Interestingly, a number of vulnerabilities were discovered in one of the tools used for conducting ActiveX vulnerability research. In March 2009, a vulnerability was discovered in the iDefense COMRaider ActiveX fuzzing software.[98] Later, in July 2009, two vulnerabilities were discovered in the same software.[99]

[98] http://www.securityfocus.com/bid/33942
[99] http://www.securityfocus.com/bid/35725

Volume XIV of the Symantec *Global Internet Security Threat Report* questioned whether the security enhancements in Internet Explorer 8 would further limit the viability of ActiveX vulnerabilities.[100] In 2009, Internet Explorer 8 went from 0.6 percent market share at the beginning of the year to 13.5 percent market share at the end of the year.[101] As a result, Internet Explorer 8 is now the most widely used version of the Internet Explorer browser. This may correlate to the decline of ActiveX vulnerabilities because ActiveX security has been further enhanced in this version, potentially limiting the viability of many ActiveX vulnerabilities.

While ActiveX vulnerabilities are currently on the decline, vulnerabilities in other plug-in technologies such as Java SE and Adobe Reader are on the rise. The prior focus on ActiveX vulnerabilities among security researchers and attackers was due to the ubiquity of ActiveX technologies as a whole—mostly because of the high market share of Internet Explorer. However, the vulnerabilities themselves were scattered among hundreds of disparate vendors. In contrast, Java SE and Adobe Reader are not only ubiquitous, but they are cross-browser and cross-platform technologies.

Among the vulnerabilities discovered in 2009, a vulnerability affecting both Adobe Reader and Flash Player was the second most attacked vulnerability.[102] This was also one of four zero-day vulnerabilities affecting Adobe plug-ins during 2009. Two of the vulnerabilities were in the top five attacked vulnerabilities for 2009. Additionally, Adobe vulnerabilities have been associated with malicious code attacks such as the Pidief.E Trojan.[103] Symantec observed the use of targeted PDFs for Trojan attacks earlier in the year.[104] Among the vulnerabilities discovered in 2008, a vulnerability in Java SE was the second most attacked vulnerability.[105] Ultimately, both security researchers and attackers have diverted their efforts to these platforms.

Organizations should employ vulnerability assessment and policy compliance software to ensure that unauthorized software is not installed on desktops. This may help remove the risk presented by software that was intentionally or unintentionally installed by users within the organization. Users should use browser security features and add-ons to prevent their browser from invoking plug-in functionality to render or display potentially harmful content.

Top attacked vulnerabilities

This metric will examine the top attacked vulnerabilities. This data is based on events collected from Symantec IPS and Symantec's Global Intelligence Network. The events are triggered by IPS signatures that are specifically designed to detect unique vulnerabilities. When an event is triggered, it does not necessarily indicate that the exploit was successful, but merely that the activity identified by the signature has been detected. This normally indicates an attempted attack.

For the purposes of this discussion, the attacked vulnerabilities are divided by their year of publication. This provides insight into which vulnerabilities published in 2008 and 2009 are being attacked in the wild. The discussion will cover the top five attacked vulnerabilities from each year, according to the amount of activity associated with each vulnerability. This will help to pinpoint trends, such as the types of vulnerabilities that are associated with most attack activity, and the degree to which exploitation for

[100] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 41
[101] http://www.w3schools.com/browsers/browsers_explorer.asp
[102] http://www.securityfocus.com/bid/35759
[103] http://www.symantec.com/security_response/writeup.jsp?docid=2009-021212-5523-99
[104] http://www.symantec.com/connect/blogs/targeted-pdfs-used-exploits
[105] http://www.securityfocus.com/bid/32608

these vulnerabilities has been automated by attackers. Enterprises may benefit from this information because it provides an indication of the types of vulnerabilities that attackers are most likely to employ in attacks and how to best protect against these vulnerabilities.

The top attacked vulnerability in 2009 was the Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability (table 9).[106] Publicly announced in September 2009, this vulnerability was initially believed to be a DoS vulnerability that would let attackers crash Windows.[107] However, within a week it was discovered that the vulnerability could let attackers execute arbitrary code and completely compromise affected computers.[108] A number of publicly and commercially available exploits for the vulnerability were subsequently released. In October 2009, Microsoft released patches to address the vulnerability. Considering that exploits for this vulnerability can be easily automated, it is interesting that the vulnerability has not been associated with any worm activity. Symantec believes that the cause of the attack activity is due to the availability of reliable exploits that are either standalone or bundled with a number of freely and commercially available penetration testing tools.

The vulnerability is limited to Windows Vista®, Windows Server® 2008, and pre-release versions of Windows 7. The security features in these newer versions have been an obstacle for attackers, who have thus far relied on vulnerabilities in third-party software such as Web browsers and browser plug-ins to gain a foothold on these new versions. However, a successful exploit of this vulnerability will compromise the affected computer at the kernel level, which could let attackers install rootkits once the computer has been compromised. These factors could indicate that attackers are increasingly targeting newer versions of the Windows operating system. Additionally, since the attacker does not need to entice the victim to perform actions such as visiting a malicious Web page, it is possible for attackers to scan the Internet for potential targets and initiate attacks at random. Since the attack can be automated at little cost to the attacker, they can reach a large number of publicly facing targets that are affected by the vulnerability. This is in contrast to the other vulnerabilities on the top five, which are client-side in nature. Client-side vulnerabilities can be used to attack harder to reach targets on the internal network of an organization. The top attacked vulnerability from 2008 could also be exploited in the same automated fashion (table 10). When vulnerabilities possess the characteristics necessary to facilitate automated scanning and exploitation, attackers will continue to capitalize on them.

Rank	BID	Vulnerabilities
1	36299	Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution
2	35759	Adobe Reader and Flash Player Remote Code Execution
3	33627	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution
4	35558	Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution
5	34169	Adobe Reader Collab 'getIcon()' JavaScript Method Remote Code Execution

Table 9. Top attacked vulnerabilities, 2009
Source: Symantec

[106] It should be noted that Symantec uses the same signature to detect BID 36594 Microsoft Windows SMB2 Command Value Remote Code Execution Vulnerability; however, Symantec believes that the majority of attack activity was associated with the Smb2ValidateProviderCallBack vulnerability due to the number of public exploits associated with that vulnerability.
[107] http://www.securityfocus.com/bid/36299
[108] http://www.symantec.com/connect/blogs/bsod-and-possibly-more

The remainder of the top attacked vulnerabilities in 2009 comprised several client-side vulnerabilities. In July 2009, Symantec observed widespread attacks on the MPEG2TuneRequest vulnerability in relation to the Fostrem Downloader.[109] In this report, the Fostrem Downloader was the eighth-highest ranked new malicious code sample for 2009. The Adobe Reader Collab getIcon vulnerability was found to be associated with the NeoSploit attack toolkit.[110]

Attacks continue to evolve for the purpose of evading detection by intrusion detection and prevention systems and improving the reliability of exploitation. In February 2009, Symantec noted new attempts to obfuscate attacks on vulnerabilities, including the second-top attacked vulnerability for 2008.[111] These attacks were also associated with various Trojans and rogue security applications. In September 2009, Symantec published a blog analyzing various techniques employed in the wild to obfuscate malicious PDFs to evade detection by security software.[112] Additionally, a Symantec blog discussed various techniques (presented at the Black Hat® Technical Security Conference in 2009) that were being used in drive-by attacks to better guide exploits against browsers, plug-ins, and client software.[113] These techniques are already deployed in attack toolkits such as MPack,[114] Firepack, Neosploit, and Luckysploit.[115] Lastly, Symantec observed a malicious PDF attack that attempted to exploit three separate vulnerabilities with the same malicious file.[116] The goal of the attack was to install malicious code to steal sensitive information.

Rank	BID	Vulnerabilities
1	31874	Microsoft Windows Server Service RPC Handling Remote Code Execution
2	32608	Java SE Runtime Environment and Java SE Development Kit Multiple Security Vulnerability
3	30114	Snapshot Viewer for Microsoft Access® ActiveX Control Arbitrary File Download
4	32721	Microsoft Internet Explorer XML Handling Remote Code Execution
5	28157	RealNetworks RealPlayer® 'rmoc3260.dll' ActiveX Control Memory Corruption

Table 10. Top attacked vulnerabilities, 2008
Source: Symantec

To limit exposure to attacks, organizations should deploy IDS and IPS systems along with antivirus on desktops within the enterprise. This may aid in detecting and preventing client-side, malicious code, and other attacks on users within the organization. Heuristic detections within these products may block malformed content and prevent unknown attacks. Behavioral detection may detect and prevent attacks that result in anomalous behavior. Organizations should consider running operating systems that include address space layout randomization (ASLR) [117] and other memory protection technologies that can complicate the exploitation of many vulnerabilities. Third-party intrusion prevention products often offer ASLR and memory protection capabilities.

[109] http://www.symantec.com/connect/blogs/another-unpatched-vulnerability-being-massively-exploited-internet-explorer
[110] http://www.symantec.com/connect/blogs/yet-another-pdf-vulnerability-exploited-collabgeticon
[111] http://www.symantec.com/connect/blogs/new-obfuscated-scripts-wild-lgpl
[112] http://www.symantec.com/connect/blogs/fight-against-malicious-pdfs-using-ascii85decode-filter
[113] http://www.symantec.com/connect/blogs/black-hat-2009-drive-improvements
[114] http://www.symantec.com/connect/blogs/mpack-packed-full-badness#M93
[115] http://www.symantec.com/connect/blogs/black-hat-2009-drive-improvements
[116] http://www.symantec.com/connect/blogs/has-elvis-left-building
[117] ASLR is a security mechanism that randomizes data in memory to prevent the success of attacks that leverage memory corruption vulnerabilities, such as buffer overflows.

Zero-day vulnerabilities

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 that at the time of the exploit activity the vendor had not released a patch. In the absence of available patches, zero-day vulnerabilities represent a serious threat since, in many cases, they likely will be able to evade purely signature-based detection. It is the unexpected nature of zero-day threats that causes concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

In 2009, Symantec documented 12 zero-day vulnerabilities, which is more than the nine zero-day vulnerabilities documented in 2008. In 2009, there was some diversification in the types of zero-day vulnerability documented. In previous years, Symantec observed a trend toward targeting Microsoft Office® suite and Internet Explorer. In 2009, four zero-day vulnerabilities were related to Adobe Reader, while six were related to various Microsoft components including DirectX®, IIS, and Office. Additionally, there were no "region-specific" applications targeted in 2009, as was seen in previous years. It may be that attackers no longer view attacks on region-specific applications as profitable.

Zero-day vulnerabilities continue to be employed in malicious code attacks. In June 2009, a zero-day vulnerability affecting Microsoft DirectShow® was exploited to install Trojan.Cipevas on vulnerable computers.[118] In early attacks for this vulnerability, malicious web pages that exploited the vulnerability were linked to phishing sites. In addition to attempting to steal credentials in phishing attacks, these attacks also directed to malicious pages that were attempting to exploit the vulnerability.

In February of 2009, attackers were exploiting a zero-day vulnerability in Microsoft Excel® to install the Mdropper.AC Trojan horse.[119] Attacks exploiting this vulnerability used various techniques to try to evade detection. Firstly, to avoid arousing suspicion when the victim of the attack opened a malicious document, the exploit presented a legitimate spreadsheet. Secondly, binary code embedded in the malicious spreadsheet was obfuscated to make it more difficult to detect the payload of the attack. These types of techniques are becoming standard practice in client-side attacks because of heuristic detections that have been able to identify suspicious and malformed files in a generic manner. Thus, attacks employing malformed documents and files must implement sufficient obfuscation or appear normal enough to not trigger heuristic detections.

Another zero-day vulnerability was exploited in February of 2009 in Pidief.E Trojan attacks targeting Adobe Reader. Symantec believes that the motive for these attacks was to compromise high-ranking individuals within different organizations.[120] The exploit attempts also used the ability to embed JavaScript within PDF documents as means to improve the reliability of exploitation. Adobe Reader was the target of other zero-day attacks during the year, such as the Pidief.H attack that occurred in December of 2009.[121]

Vulnerabilities—protection and mitigation

In addition to the specific steps required to protect against the vulnerabilities discussed in this section, there are general steps that should be taken to protect against the exploitation of vulnerabilities. Administrators should employ a good asset management system to track the assets that are deployed on the network and to determine which ones may be affected by the discovery of new vulnerabilities.

[118] http://www.symantec.com/connect/blogs/directshow-exploit-wild
[119] http://www.symantec.com/security_response/writeup.jsp?docid=2009-022310-4202-99
[120] http://www.symantec.com/connect/blogs/targeted-pdfs-used-exploits
[121] http://www.symantec.com/connect/blogs/zero-day-xmas-present

Administrators should monitor vulnerability mailing lists and security websites to keep abreast of new vulnerabilities affecting their assets. Where possible, patch deployments should be automated to ensure that vulnerabilities are addressed across the organization in a timely manner.

Symantec recommends that administrators employ vulnerability assessment services, a vulnerability management solution, and vulnerability assessment tools to evaluate the security posture of the enterprise. These measures should be incorporated into infrastructure change management processes. Organizations should employ third-party consulting and penetration testing services to identify security exposures. For any products or applications developed by the organization, code auditing software and services may help to identify and address vulnerabilities at various stages of development.

Unpatched vulnerabilities should be identified by administrators, and assessed and mitigated according to the risk they present. Where possible, problematic applications with many unpatched vulnerabilities should be removed or isolated. IPS systems can aid in detecting known attacks against such applications and provide generic protection against vulnerabilities. Security information and event management should be deployed to assist in data management within the enterprise infrastructure and aid in policy compliance.

In order to protect against successful exploitation of Web browser vulnerabilities, Symantec advises users and administrators to upgrade all browsers to the latest, patched versions. Symantec recommends that organizations educate users to be extremely cautious about visiting unknown or untrusted websites and viewing or following links in unsolicited emails. Administrators should also deploy Web proxies in order to block potentially malicious script code. Administrators and end users should actively maintain a whitelist of trusted sites and disable individual plug-ins and scripting capabilities for all other sites. This will not prevent exploitation attempts from whitelisted sites, but may aid in preventing exploits from all other sites. Organizations can also implement an egress filtering policy at the network perimeter to regulate outgoing access by end users. Antivirus and host-based IDS and IPS solutions at the desktop level also provide a layer of protection against attacks that originate from the Web.

Enterprises should subscribe to a vulnerability alerting service in order to be notified of new vulnerabilities. They should also manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development practices, such as the Security Development Lifecycle and threat modeling.[122] If possible, all Web applications should be audited for security prior to deployment and only those applications that have been certified should be deployed. Web application security solutions and a number of products and services are available to detect and prevent attacks against these applications.

When deploying applications, administrators should ensure that secure, up-to-date versions are used, and that applications are properly configured to avoid the exploitation of latent vulnerabilities. Symantec recommends the use of secure shared components that have been audited for common Web application vulnerabilities. As much as possible, enterprises are advised to avoid deploying products that are not regularly maintained or that are not supported by the vendor.

[122] The Security Development Lifecycle is a development paradigm that incorporates security at every stage from the initial architecture to programming, and in the quality assurance/testing phases; threat modeling is a security auditing methodology to identify and map out all possible attack vectors for an application.

Malicious Code Trends

Symantec gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Underpinning these products are the Symantec Digital Immune System and Symantec Scan and Deliver technologies, as well as Norton Community Watch, which allow customers to automate the process of reporting viruses and other malicious code threats.

This discussion is based on malicious code samples reported in 2009, with the following trends being analyzed:

- Malicious code signatures
- New malicious code families
- Prevalence of malicious code types
- Staged downloaders—multiple infections by type
- Downloaded components
- Geolocation by type of malicious code
- Threats to confidential information
- Propagation mechanisms
- Malicious code that exploits vulnerabilities
- Malicious code—protection and mitigation

Malicious code signatures

Symantec monitors the proliferation of malicious code by examining the number of new malicious code signatures created to detect threats from each reporting period. Monitoring trends in the number of new malicious threats can help improve awareness of their danger and underscores the importance of maintaining robust security, including up-to-date antivirus signatures and software patches.

In 2009, Symantec created 2,895,802 new malicious code signatures (figure 10). This is a 71 percent increase over 2008, when 1,691,323 new malicious code signatures were added. Although the percentage increase in signatures added is less than the 139 percent increase from 2007 to 2008, the overall number of malicious code signatures by the end of 2009 grew to 5,724,106. This means that of all the malicious code signatures created by Symantec, 51 percent of that total was created in 2009. This is slightly less than 2008, when approximately 60 percent of all signatures at the time were created.

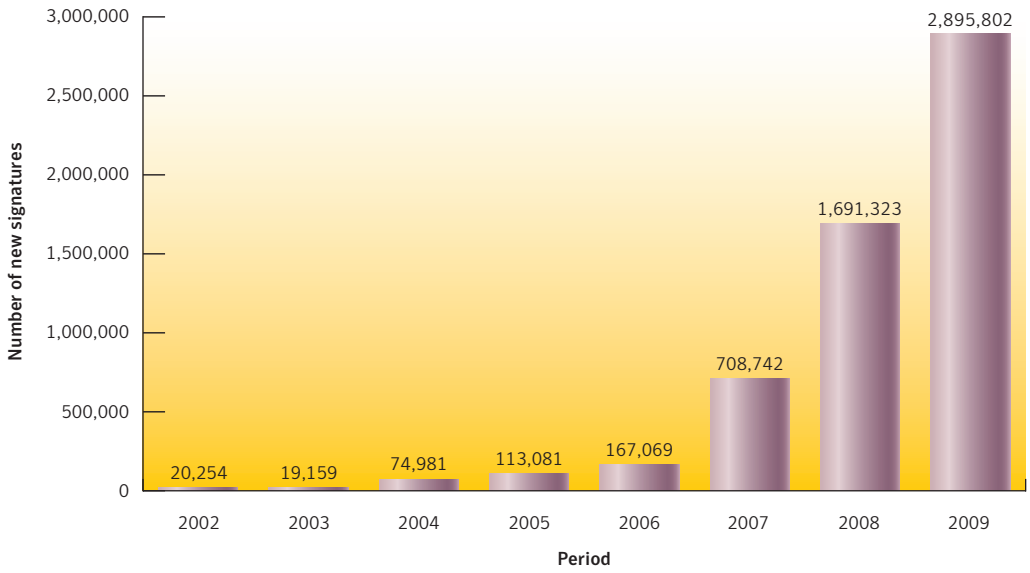

Figure 10. New malicious code signatures
Source: Symantec.

The number of new malicious code signatures has shown significant growth by more than doubling on a year-to-year basis between 2006 and 2008. New signature creation in 2009 continued the upward trend and resulted in a near doubling of the total number of signatures. The previous Symantec *Global Internet Security Threat Report* noted that malicious code being developed for the underground economy is increasingly well organized and professional.[123] This trend is likely continuing to drive the creation of malicious software because of the lucrative nature of online fraud.

The slight decline in the rate of growth should not discount the significant number of new signatures created in 2009. Signature-based detection is lagging behind the creation of malicious threats—something which makes newer antivirus technologies and techniques, such as behavioral-based detection, increasingly important. For example, of the threat instances that Symantec's reputation-based techniques protected users from in 2009, approximately 57 percent corresponded to singletons. This finding is consistent with the overall observation that malicious code authors are creating unique threats using techniques such as packing, obfuscation, and server-side polymorphism. This trend suggests that security technologies that rely on signatures should be complemented with additional heuristics, behavioral monitoring techniques, and reputation-based security. Moreover, with the advent of malicious software toolkits (such as Zeus), relatively inexperienced users can quickly create targeted threats.[124] For example, in 2009 an unnamed but targeted Trojan successfully stole bank account credentials and was directly responsible for the theft of thousands of dollars.[125]

[123] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 10
[124] http://securitywatch.eweek.com/botnets/playing_god_zeus_diy_botnet_kit_evolves.html
[125] http://www.krebsonsecurity.com/2010/01/money-mules-helped-to-rob-w-va-bank/

New malicious code families

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

In 2009, there were six Trojans, three worms, and one virus in the top 10 new malicious code families detected (table 11). Two of the three worms include a back door component.[126] Volume XIII of the Symantec *Global Internet Security Threat Report* noted that the growing prevalence of Trojans is indicative of multistage attacks.[127] A multistage attack typically involves an initial compromise followed by the installation of an additional piece of malicious code, such as a Trojan that downloads and installs adware. As with 2008, in 2009 four of the top 10 new malicious code families downloaded additional threats (these multistage attacks are examined in detail in **"Staged downloaders—multiple infections by type"**). It should also be noted that, although Downadup was a major threat and received significant media attention, it was discovered in 2008 and is, therefore, not considered a new malicious code family for this reporting period.

Rank	Sample	Type	Vectors	Impact
1	Induc	Virus	Delphi® files	Infects the Delphi compilation process to spread to all compiled Delphi files
2	Changeup	Worm	Mapped and removable drives	Downloads additional threats
3	Bredolab	Trojan	N/A	Downloads additional threats, including Trojan.Fakeavalert
4	Ergrun	Trojan	N/A	Downloads additional threats
5	Pilleuz	Worm, back door	File-sharing, instant messages, removable drives	Allows remote access
6	Mibling	Worm, back door	Instant messages	Allows remote access and lowers security settings
7	Kuaiput	Trojan	N/A	Downloads additional threats
8	Fostrem	Trojan	N/A	Downloads additional threats
9	Interrupdate	Trojan	N/A	Blocks security-related updates and sniffs network traffic
10	Swifi	Trojan	N/A	Exploits a vulnerability in Adobe Flash Player and may lower security settings

Table 11. Top new malicious code families
Source: Symantec

[126] Back door components allow attackers to remotely connect to a compromised computer, typically using a specialized application. Once connected, the attacker can perform numerous actions such as taking screenshots, changing configuration settings, and uploading, downloading, or deleting files.
[127] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 46

During this reporting period the Induc virus[128] was the most widely observed new malicious code family. This virus is notable because it does not perform any known malicious actions other than proliferating. Induc propagates by embedding itself into installations of the Delphi[129] application development environment.[130] When the virus first runs, it attempts to locate an installation of Delphi, specifically targeting versions 4.0 through to 7.0. If it fails to find an appropriate Delphi installation, nothing else happens. This means that the virus is benign for users who do not have Delphi installed.[131]

The primary reason for the prevalence of Induc in 2009 is that developers using an infected Delphi installation were unknowingly including Induc in their released products. Induc would be included with every new build, resulting in legitimate, official installation packages that included the virus. This resulted in the virus spreading directly through multiple vendors' software distribution channels, such as automatic software updates and trusted download locations. There were multiple reported cases of legitimate applications inadvertently including the Induc virus.[132]

It is possible that Induc was created as a proof-of-concept method of spreading malicious software. Other development environments are equally susceptible to this form of subversion, leading to potentially widespread infection. The successful spreading of the Induc virus may mean that there will be more viruses exploiting this technique in the future.

The second most observed new malicious code family in 2009 was the Changeup[133] worm. This worm propagates by copying itself to removable and mapped drives, using an autorun instruction file to trigger the worm's automatic execution whenever a local or shared drive is accessed.[134] Changeup also connects to TCP port 8000 on a remote website and downloads additional threats, possibly including Trojans or back doors.

The Bredolab[135] Trojan was the third most observed new malicious code family in 2009. Along with using a range of obfuscation techniques to avoid detection, Bredolab uses several different advanced tactics to propagate, including social engineering, server-side polymorphism, and encrypted communications. It is primarily distributed through spam and drive-by-download attacks. When Bredolab is executed, it copies itself to a computer and creates a registry entry to ensure that it is run every time the computer starts.

Bredolab has been observed downloading numerous other disparate malicious threats, including password stealers, rootkits, back doors, and misleading applications, and its C&C server operators can determine what additional components are downloaded at any time.[136] Servers have been observed hosting Bredolab in China, Germany, and Ukraine. It has been used to target social networking sites and to advertise fraudulent money-making scams.[137] The popularity of Bredolab in the underground economy potentially stems from its flexibility and robustness, making it a threat that Symantec expects will likely remain popular with attackers into the near future.

[128] http://www.symantec.com/security_response/writeup.jsp?docid=2009-081816-3934-99
[129] http://www.embarcadero.com/products/delphi
[130] http://edn.embarcadero.com/article/39851
[131] http://www.symantec.com/connect/blogs/delphi-falls-prey
[132] http://channel.hexus.net/content/item.php?item=19853
[133] http://www.symantec.com/security_response/writeup.jsp?docid=2009-081806-2906-99
[134] Autorun is a function of the Windows operating system that launches newly detected processes or applications (e.g., the insertion of a CD-ROM or USB drive). Windows searches the root directory of the drive for an autorun information file that contains instructions for what process or application to launch.
[135] http://www.symantec.com/security_response/writeup.jsp?docid=2009-052907-2436-99
[136] http://www.symantec.com/connect/blogs/taking-closer-look-trojanbredolab
[137] See http://www.symantec.com/connect/blogs/bredolab-trojan-now-using-popular-social-networking-brand-spread and http://www.symantec.com/connect/blogs/bredolab-delivers-more-parcels-and-cash

Prevalence of malicious code types

Analyzing the prevalence of malicious code types provides insight into the general diversity of the threat landscape. Combined with the data from other metrics, this helps Symantec more accurately determine emerging trends in malicious code. During this reporting period, the overall volume of the top 50 potential malicious code infections doubled from 2008 to 2009; therefore, decreases in percentages do not likely indicate a year-over-year decline in potential infections. As in previous reporting periods, Trojans composed the highest percentage of the volume of the top 50 potential malicious code infections (figure 11), although the percentage dropped from 68 percent in 2008 to 56 percent in 2009.[138]

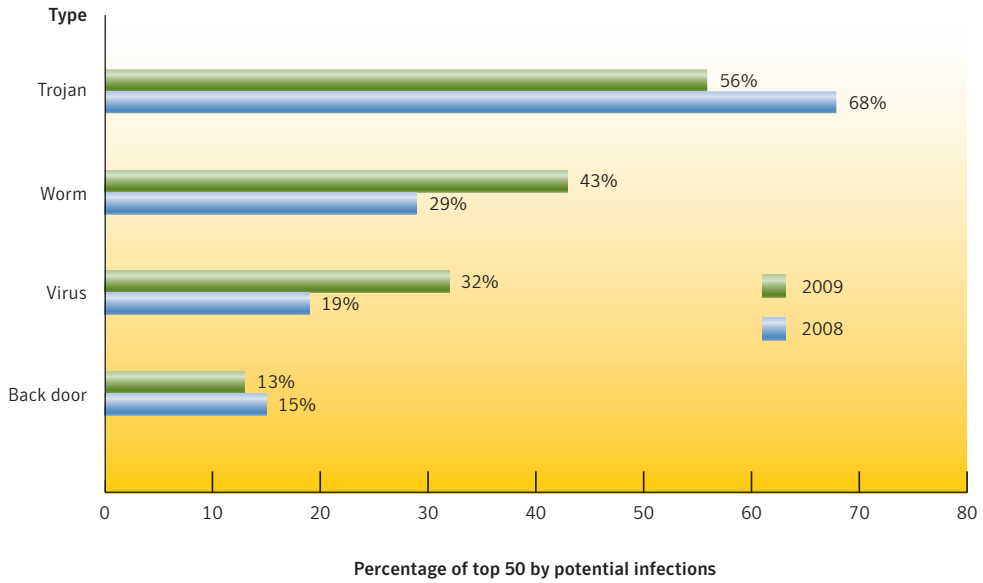

Figure 11. Prevalence of malicious code types by potential infections
Source: Symantec

The previous two volumes of the Symantec *Global Internet Security Threat Report* discussed the possibility that attackers are gravitating toward the extensive use of a smaller number of more successful Trojans.[139] The Bredolab Trojan is a good example of this: its flexibility, style of downloading new threats, obfuscation, and polymorphism mechanisms together enable it to be easily customized for specific targets. Its success corroborates the hypothesis of attackers using smaller numbers of more successful Trojans more often.

The proportionate decline in Trojan activity observed in 2009 is also likely due to the rise in worm and virus activity. For example, the top malicious code sample causing potential infections in 2009 was the Sality.AE[140] virus. The main goal of Sality.AE is to download and install additional malicious software on a victim's computer. The virus also prevents access to various security-related domains, stops security-related services, and deletes security-related files. The virus also infects .exe and .scr files on a victim's local drive as well as on any writable network resource. It also spreads by copying itself to attached removable drives.

[138] Because malicious code samples may be comprised of multiple components that are each classified as different types, cumulative percentages discussed in this metric may exceed 100 percent.
[139] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf and http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf
[140] http://www.symantec.com/security_response/writeup.jsp?docid=2008-042106-1847-99

In 2008, the Brisv[141] Trojan was the most widely reported new malicious code family. Its prevalence rose in 2009 to the point that it was the second ranked sample causing potential infection. Brisv scans computers for a range of multimedia files.[142] The Trojan then modifies a data marker in the files with a malicious URL. The marker is a part of the Windows Media® Audio (WMA) format. Although other applications appear to be unaffected, when the files are opened using Windows Media Player the marker is automatically processed, causing the application to open a Web browser window and access the malicious URL. Accessing the malicious URL may expose the user to additional threats.

The effectiveness of Brisv is heightened by the possibility that unknowing victims may share the compromised multimedia files with others, through P2P networks, or email, etc. As a result, the compromised files can potentially affect users whose computers were not exposed to the Trojan itself. Moreover, when Brisv scans for multimedia files, it converts all MP2 and MP3 files it encounters into the WMA format prior to injecting the malicious code, even while preserving the original file extensions of the (now) converted files. The reason for converting files into the WMA format is so that Windows media player will process the injected marker data properly. This is an example of increased sophistication in malicious code development.

The second highest percentage of the top 50 potential malicious code infections for 2009 belonged to worms, which increased to 43 percent from 29 percent in 2008. Six of the top 10 threats in 2009 had worm components, compared with only four in 2008. The Downadup worm is likely responsible for a significant amount of the increase in worm activity. Nonetheless, although Downadup maintained a high profile in 2009, SillyFDC[143] and Sality.AE were both more prolific.

Viruses made up the third highest percentage of the top 50 potential malicious code infections in 2009 increasing to 32 percent in 2009 from 19 percent previously. In total, five of the top 10 malicious code samples in 2009 were classified as viruses. Along with Sality.AE, the others were Brisv, Mabezat,[144] Gammima,[145] and Almanahe.[146] In 2008, only three of the top 10 samples were classified as viruses.

Back doors continued to decline in 2009, dropping from 15 percent in 2008 to 13 percent in 2009. In 2008, there were two threats with back door components in the top 10. In 2009, Downadup was the only sample in the top 10 with a back door component to it.

Staged downloaders—multiple infections by type

Staged downloaders are threats that download and install other malicious code onto a compromised computer. These threats allow attackers to alter the downloadable component to any type of threat to suit their changing objectives over time. For example, attackers can install a Trojan that relays spam, rather than one that steals confidential information. As the attackers' objectives change, they can change any later components that will be downloaded to perform the requisite tasks.

Of the top 50 potential malicious code infections, 75 percent downloaded additional threats, down from 79 percent in 2008. In 2009, the Brisv Trojan was the most prevalent downloader component (table 12). As noted previously, the Brisv Trojan was also the second-ranked overall malicious code threat in 2009, moving up from 10th overall in 2008, when it was the top-ranked new malicious code family detected.

[141] http://www.symantec.com/security_response/writeup.jsp?docid=2008-071823-1655-99
[142] Primarily .asf, .mp2, .mp3, .wma, and .wmv
[143] http://www.symantec.com/security_response/writeup.jsp?docid=2009-081106-1401-99
[144] http://www.symantec.com/security_response/writeup.jsp?docid=2007-111202-0601-99
[145] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032206-2043-99
[146] http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99

Rank	Sample	Type	Impact
1	Brisv	Trojan	Infects media files and downloads files from remote addresses
2	Sality.AE	Virus, worm	Downloads files from remote addresses
3	Wimad	Trojan	Uses Microsoft Windows Media Digital Rights Manager to trick user into downloading files
4	Vundo	Trojan	Redirects browser to malicious Web page
5	SillyFDC	Worm	Downloads files from remote addresses
6	Downadup.B	Worm, back door	Downloads files from remote addresses
7	Imaut	Worm	Downloads files from remote addresses
8	Spybot	Worm, back door	Downloads files from remote addresses
9	Zlob	Trojan	Downloads files from remote addresses
10	Imaut.AA	Worm	Downloads files from remote addresses

Table 12. Top staged downloaders
Source: Symantec.

The second most prevalent downloader component observed by Symantec in 2009 was the Sality.AE virus. Once it is installed on a computer, Sality.AE attempts to contact certain IP addresses to download and install its secondary components. One of the files it attempts to install is an adware program that will periodically display pop-up advertisements. If clicked, these ads will generate income for the malicious code author (and possibly the adware developer, if they happen to be separate people).

The Wimad Trojan[147] was the third most common staged downloader component in 2008. This Trojan arrives on computers as a license-protected multimedia file. When the file is opened, Wimad exploits the intended functionality of digital rights management (DRM) technology in order to open a window and access an attacker-controlled URL. When an attacker's Web page is processed, a deceptive message is displayed that asks the user to click a button. If clicked, the Trojan will download other threats, including adware and spyware.

Downloaded components

The most prevalent downloaded component in 2009 was the Gampass[148] Trojan (table 13). Gampass uses keystroke-logging functionality to steal authentication credentials for online gaming accounts. Popular targets include Lineage,[149] Rexue, Jianghu, and Rohan, which are all popular games in the APJ region. Gampass is commonly downloaded by worms such as Mummawow,[150] Wowinzi,[151] and Fubalca.[152]

[147] http://www.symantec.com/security_response/writeup.jsp?docid=2005-011213-2709-99
[148] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[149] http://www.symantec.com/security_response/writeup.jsp?docid=2005-011211-3355-99
[150] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032015-4300-99
[151] http://www.symantec.com/security_response/writeup.jsp?docid=2008-050714-5642-99
[152] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062214-3636-99

Rank	Sample	Type	Impact
1	Gampass	Trojan	Steals online gaming account information
2	FakeAV	Trojan	Displays false antivirus alerts and lowers security settings
3	Graybird	Back door	Allows remote access, logs keystrokes, and steals passwords
4	Gammima	Worm	Steals online gaming account information
5	Adclicker	Trojan	Generates traffic to websites and banner ads
6	Onlinegame	Trojan	Steals online gaming account information
7	Bancos	Trojan	Steals online banking account information
8	Banker.C	Trojan	Steals online banking account information
9	Lineage	Trojan	Steals online gaming account information
10	KillAV	Trojan	Disables security applications

Table 13. Top downloaded components
Source: Symantec

The second most downloaded component observed by Symantec in 2009 was the FakeAV[153] Trojan. This Trojan displays false antivirus alerts and lowers security settings on compromised computers. The fake security alert attempts to trick users into visiting a website in order to download a fake antivirus application or spyware removal application. These types of rogue security software applications and components flourished in 2009. It is common for these applications to attempt to scare users into purchasing the software in order to resolve fake or overblown issues.[154] If malicious software authors cannot directly coerce users to install the misleading applications, installing them as a component to a staged downloader is an attractive alternative.

Graybird[155] was the third most frequently downloaded component in 2009. This back door gives an attacker full remote access to a compromised computer. It also captures cached passwords, logs keystrokes, and then sends all of this information to the remote attacker. Graybird also allows the attacker to download and install additional threats on the computer.

Many of the top downloaded components in 2009 were similarly ranked in 2008, indicating that these families continue to be prevalent and effective threats. In 2008, six of the 10 most downloaded components involved password stealing, keystroke logging, or advertisement promotion. In 2009, this has increased to nine of the top 10 most downloaded components, strongly indicating that profit continues to be the driving motivation for malicious code authors.

Exemplifying this trend in 2009 was the Banker.C[156] Trojan. It was used in two notable attacks on a bank in 2009.[157] Bank employee computers were compromised with the Trojan, allowing attackers to gain access to bank account credentials. One company lost $179,000 in a transfer to a Russian bank account, and another company lost $81,000 to an unspecified offshore location.

[153] http://www.symantec.com/security_response/writeup.jsp?docid=2007-101013-3606-99
[154] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf
[155] http://www.symantec.com/security_response/writeup.jsp?docid=2003-040217-2506-99
[156] http://www.symantec.com/security_response/writeup.jsp?docid=2007-040208-5335-99
[157] http://www.krebsonsecurity.com/2010/02/a-tale-of-two-victims/

Banker.C is part of the Zeus crimeware kit (a.k.a., Zbot[158]), which is designed to steal sensitive information relating to online banking, social networking sites, Web-based email sites, and saved passwords. It also downloads further threats based on a configuration file that allows malicious software authors to easily modify Zeus's behavior. Zeus is readily available for sale in underground forums and is relatively simple to use, allowing novice attackers to create customized Trojans and C&C servers for attacks—typically spread through spam and drive-by downloads.[159] This may explain why Zeus has become a prevalent threat that is responsible for widespread bot networks.

Geolocation by type of malicious code

Symantec examines the types of malicious code causing potential infections in each region. The increasing regionalization of threats can cause differences between the types of malicious code being observed from one area to the next, such as when threats employ certain languages or localized events as part of their social engineering techniques. Threats that steal confidential information can also be tailored to steal information that is more commonly available in some countries than in others. Because of the varying propagation mechanisms used by different malicious code types, and the diverse effects that each malicious code type may have, information about the geographic distribution of malicious code can help network administrators improve their security efforts. It should be noted that the numbers below represent proportional geographic percentages, and that proportional percentage fluctuations over time may not indicate an actual change to the raw number of reports from a specific region.

In 2009, the regional proportion of potential infections from malicious code remained largely unchanged; however, in all cases, the actual number of reports for each malicious code type from each region increased.[160] While there were small variances in some regions, the changes were not representative of significant shifts in the threat landscape. The numbers of reports from Europe, the Middle East, and Africa (EMEA) increased proportionally more than the other regions, which may indicate that the concentration of threats targeting countries in EMEA is growing faster than the concentration in other regions. This may also signal that there is a greater concentration of malicious code authors, or organizations employing those authors, in EMEA than elsewhere.

Regionally, the overall infection counts changed proportionally according to the global prevalence of malicious code types. As an example, Trojans had slightly less activity compared to worms in infection counts, but proportionately in each region, they did not change substantially. This is due to users being targeted in an increasingly equal fashion worldwide even though attack origins changed over time.

[158] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99
[159] http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits
[160] Due to rounding, cumulative totals might not equal 100 percent.

Trojans

In 2009, 34 percent of Trojans were reported from North America (NAM) region, 30 percent from EMEA, 28 percent from APJ, and 8 percent from Latin America (LAM) (table 14). Although the number of Trojans reported from NAM and EMEA appears to have dropped slightly, this is mainly attributable to the proportional increase in Trojans reported from APJ and LAM, indicating that a similar amount of Trojan activity was reported in both NAM and EMEA in 2009. Although the 2009 percentages are similar to 2008 percentages, it should be noted that the volume of infection counts for all regions approximately doubled in 2009.

Region	2009 Percentage	2008 Percentage
NAM	34%	35%
EMEA	30%	34%
APJ	28%	24%
LAM	8%	6%

Table 14. Geolocation of Trojans
Source: Symantec

Trojan infection counts in the APJ region continued to gain on EMEA in 2009 and were close enough that APJ could potentially overtake EMEA in 2010. Even though both the proportionate increase and absolute counts for LAM were comparatively small, infection counts in that region increased the most, more than doubling in 2009.

Worms

The EMEA region reported 39 percent of the potential worm infections 2009, followed by APJ with 37 percent, LAM with 14 percent, and NAM with 10 percent (table 15). EMEA overtook APJ as the leader in worm infections in 2009, although the numbers are close enough that it may not suggest a significant shift in the threat landscape. The drop in APJ and NAM is only due to the larger proportionate increases in EMEA and LAM. All regions have approximately doubled in infection counts, but the infection count in LAM increased the most, increasing by 187 percent, followed by EMEA increasing by 150 percent.

Region	2009 Percentage	2008 Percentage
EMEA	39%	36%
APJ	37%	40%
LAM	14%	11%
NAM	10%	13%

Table 15. Geolocation of worms
Source: Symantec

Of particular note for infections in 2009 is the Downadup worm. It appeared in late November 2008, but was most prevalent in 2009. China was by far the most infected country by the height of the spread of Downadup into 2009.[161] The prevalence of Downadup points out the need to keep computers updated as much as possible. For example, although Microsoft patched the specific vulnerability that the worm exploits to propagate on October 23, 2008, Symantec recorded an infection count for Downadup of more than 1.5 million in December 2009 alone, more than a year after the vulnerability had been patched.[162]

Back door infections

EMEA again accounted for the largest proportion of potential back door infections reported worldwide in 2009, with 37 percent of the total—a slight decrease from 39 percent in 2008. APJ accounted for the second largest percentage, with 31 percent, followed by NAM again at 23 percent, and LAM at 10 percent (table 16). All regions worldwide approximately doubled in potential infection counts for back doors.

Region	2009 Percentage	2008 Percentage
EMEA	37%	39%
APJ	31%	29%
NAM	23%	23%
LAM	10%	9%

Table 16. Geolocation of back doors
Source: Symantec

While the regional percentages of potential back door infections can show wide variances, it is important to note that the worldwide volume of back door threats was significantly lower than Trojans and worms. Therefore, the percentage variance between regions actually represents a much smaller difference in raw numbers than the percentage differences between worms and Trojans. With the worldwide volume of potential back door infections being a much smaller number compared to other infection types, the proportionate rise in infections can likely be attributed to the spread of the Downadup worm with its back door functionality.

Viruses

The EMEA region overtook the APJ region for the highest concentration of reported potential infections caused by viruses in 2009. EMEA rose to 45 percent, with APJ dropping to 40 percent (table 17). LAM and NAM also exchanged proportionate positions in 2009. LAM increased its proportionate share from 6 percent of the total in 2008 to 9 percent in 2009. Meanwhile, virus proportions in NAM dropped from 15 percent in 2008 to 6 percent in 2009. It should be noted that, although APJ and NAM decreased in proportional percentage total, there was a rise in potential virus counts in all of the regions in 2009. In fact, potential infection counts for viruses rose significantly more than any other infection type in 2009. Proportions in LAM increased by 389 percent, followed by EMEA at 314 percent, APJ at 238 percent, and NAM by only 27 percent. Thus, although it appears as though there was a large drop in NAM, the decrease is attributed to the significant proportional rise in other regions with much larger infection counts.

[161] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf : p. 12
[162] http://technet.microsoft.com/en-us/security/dd452420.aspx

Region	2009 Percentage	2008 Percentage
EMEA	45%	38%
APJ	40%	41%
LAM	9%	6%
NAM	6%	15%

Table 17. Geolocation of viruses
Source: Symantec

The Sality.AE virus was the top overall malicious threat in both APJ and EMEA, and the Mabezat.B virus was the second overall malicious threat in EMEA. These two threats are the primary cause for the disparity in infection counts between the top two and bottom two regions for virus activity in 2009.

The largest contributing countries for virus threats in 2009 were India, Egypt, and Brazil, with top-ranked India having approximately twice the infection count of second-ranked Egypt. As noted in the "Executive Summary," India and Brazil are two countries specifically cited as countries expected to increase in their share of malicious activity.[163] The growth of viruses in 2009 in these countries bears this out.

Although the 2009 increase in LAM is quite large, the actual infection counts are only approximately 20 percent as high as second-ranked APJ. Meanwhile, the EMEA and APJ regions are within a few percentage points of each other in infection counts, which likely makes their swapped positions are merely due to typical variances in potential infection counts.

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats may expose sensitive data such as system information, confidential files and documents, or logon credentials. Some malicious code threats, such as back doors, can give a remote attacker complete control over a compromised computer. Threats to confidential information are a particular concern because of their potential for use in criminal activities. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

In 2009, four of the top 10 most prevalent malicious threats observed expose confidential information or provide remote access. Three of the top 10 new threats directly expose information, while four are staged downloaders that might also expose information, depending on the downloaded components. Operators in the underground economy use these malicious threats to gain access to banking and credit card information, online credentials, and to target specific enterprises.

Within the enterprise, the exposure of confidential information can lead to significant data loss. If it involves customer-related data such as credit card information, customer confidence in the enterprise can be severely undermined. Moreover, it can also violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies could also be leaked from compromised computers.

[163] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 19

In 2009, 98 percent of confidential information threats had a remote access component (figure 12). This was an increase from 83 percent in 2008. The continued increase is likely because the addition of remote access features (as well as other confidential information threats) to malicious software has become fairly simple for authors to do; thus, almost all new threats include them. The sophistication and effectiveness of malicious software creation toolkits has also likely contributed to the increase.

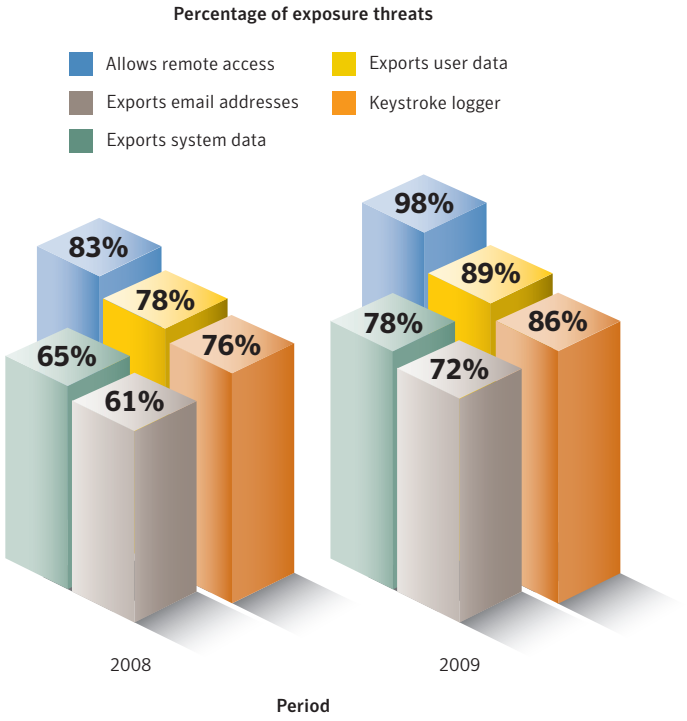

Figure 12. Threats to confidential information, by type
Source: Symantec

Malicious code that exports user data accounted for 89 percent of threats to confidential information in 2009, up from 78 percent in 2008. This is unsurprising since threats that attempt to steal bank account information, authentication credentials, and other confidential information could lead to monetary gain.

Confidential information threats with a keystroke logging capability made up 86 percent of threats to confidential information, up from 76 percent in 2008. Malicious code incorporating keystroke loggers that target online gaming account credentials continues to be popular. Four of the top 10 threats downloaded by modular malicious software specifically target online game account information. These are Gampass, Gammima, Onlinegame,[164] and Lineage, and they continue to account for a significant number of potential infections, with three of the four (excepting Gammima) also ranking in the top 10 downloaded components in 2008.

[164] http://www.symantec.com/security_response/writeup.jsp?docid=2008-011012-0102-99

Overall, every category of threats to confidential information increased in 2009. This is considered to be due to the continuing increased professionalization of the threat landscape. The creation of toolkits designed specifically to create malicious packages is making it relatively easy for even neophyte attackers to create threats with increasing complexity and sophistication over time.

Organizations can take several steps to limit the exposure of confidential information by successful intrusions. Data loss prevention solutions can block sensitive data from being stored on endpoint computers. Encrypting sensitive data that is stored in databases will limit an attacker's ability to view and/or use the data. However, this step may require sufficient resources to be made available since adequately managing encryption keys and ensuring that archived data is actually encrypted can be costly. Furthermore, encrypting stored data will not protect against man-in-the-middle attacks that intercept data before it is encrypted.[165] As a result, data should always be transmitted through secure channels such as SSH, SSL, and IPSec.[166]

Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, 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), P2P, and remotely exploitable vulnerabilities.[167] Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a back door server and using it to upload and install itself. The samples discussed here are assessed according to the percentage of potential infections.

In 2009, 72 percent of potential malicious code infections propagated as file-sharing executables, up from 66 percent in 2008 (table 18).[168] File-sharing executables are the propagation mechanisms employed by viruses and some worms to copy themselves onto removable media. The continuing resurgence in this vector over the past few years coincides with the increased use of removable drives and other portable devices. It is also an easy vector to exploit because old malicious code developed for floppy disks can be easily modified for current removable media devices. Downadup.B was the most prolific threat globally in 2009 that employed this propagation method, potentially accounting for this increase.

To limit the propagation of threats through removable drives, administrators should ensure that all such devices are scanned for viruses when they are connected to a computer. If removable drives are not needed within the enterprise, endpoint security and policies can prevent computers from recognizing these drives when they are attached. Additionally, best practices policies should be implemented to mitigate the dangers of attaching unauthorized devices to computers within the enterprise.

[165] A "man-in-the-middle attack" is an attack in which a third party intercepts communications between two computers. The "man in the middle" captures the data, but still relays it to the intended destination to avoid detection.
[166] Secure shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices; Secure Sockets Layer (SSL) is a cryptographic protocol that provides security for communications over networks such as the Internet; Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.
[167] 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.
[168] Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

Rank	Propagation Mechanisms	2009 Percentage	2008 Percentage
1	File-sharing executables	72%	66%
2	File transfer, CIFS	42%	30%
3	File transfer, email attachment	25%	31%
4	Remotely exploitable vulnerability	24%	12%
5	File sharing , P2P	5%	10%
6	File transfer, HTTP, embedded URI, instant messenger	4%	4%
7	SQL	2%	3%
8	Back door, Kuang2	2%	3%
9	Back door, SubSeven	2%	3%
10	File sharing, data files	1%	1%

Table 18. Propagation mechanisms
Source: Symantec

In 2009, 42 percent of malicious code that propagated did so through the CIFS protocol, up from 30 percent in 2008. Propagation through the CIFS protocol overtook propagation through email in 2009. The increase may be linked to the diversification of mechanisms discussed above. Three of the top 10 malicious code threats for 2009 employed the CIFS propagation mechanism, up from two in 2008. This includes the Downadup, Mabezat and Almanahe worms.

The CIFS propagation mechanism can be a threat to organizations because file servers use CIFS to give users access to their shared files. If a computer with access to a file server becomes infected by a threat that propagates through CIFS, the infection could spread to the file server. Since multiple computers within an organization likely access the same file server, this could facilitate the rapid propagation of the threat within the enterprise. If malicious software can infect a single computer through any other propagation method such as email or malicious websites, the CIFS propagation method can rapidly spread infection throughout an entire organization. This is increasingly becoming a threat to home environments as well, because home networks with multiple devices are becoming more commonplace.

To protect against threats that use the CIFS protocol to propagate, all shares should be protected with strong passwords, and only users who require the resources should be given access to them. If other users do not need to write to a share, they should only be given “read” permissions. This will prevent malicious code from copying itself to the shared directory or modifying shared files. Finally, CIFS shares should not be exposed to the Internet. Blocking TCP port 445 at the network boundary will help to protect against threats that propagate using CIFS.[169]

Propagation occurring through email attachments dropped from 31 percent in 2008 to 25 percent in 2009, continuing its decline from 32 percent in 2007. Email attachments have now been surpassed by both executable file sharing and CIFS propagation methods.

[169] TCP port 445 is the default port used to run CIFS on TCP.

The previous volume of the Symantec *Global Internet Security Threat Report* surmised that the growing gap in email propagation was because malicious code authors may not have been experiencing as much success with attacks using email attachments as in past years.[170] Increased user awareness and greater vigilance and accuracy for email protection mechanisms may be a factor in this decrease. Another factor in the decrease in email attachment propagation is that there was a 23 percent increase in malicious code variants propagating through email in 2009, but only half the email per variant, resulting in an overall decrease in malicious email.[171]

One specific example of the propagation of malicious code through email was through the Pandex botnet in 2009.[172] This botnet sent approximately 3.6 billion spam messages containing the Bredolab Trojan per day in October 2009 alone. Bredolab was the third-ranked top new malicious software threat in 2009.

With over 87 percent of all email reported as spam, the prevalence of distributing malicious threats through email remains a viable propagation method. To limit the propagation of email-borne threats, administrators should ensure that all email attachments are scanned at the gateway. Additionally, all executable files originating from external sources such as email attachments or those downloaded from websites should be treated as suspicious. All executable files should be checked by antivirus scanners using the most current definitions.

The propagation of malicious code by remotely exploiting vulnerabilities doubled between 2008 and 2009. This potentially can be explained by the success of the Downadup worm. In 2009, Downadup and Downadup.B were both highly ranked malicious code threats and accounted for a significant increase in the propagation by remote vulnerabilities.

Malicious code that exploits vulnerabilities

Assessing the proportion of malicious code that exploits vulnerabilities helps to show how popular this technique is for distributing new variants of malicious code. The popularity of exploiting vulnerabilities (and especially vulnerabilities that have available fixes) as a means of malicious code propagation illustrates the need for administrators to apply patches in a timely manner. Applying all available patches in a timely manner can greatly reduce propagation through vulnerabilities.

In 2009, 6 percent of the 1,560 documented malicious code instances exploited vulnerabilities.[173] This is an increase from the 3 percent proportion of the malicious code instances documented for 2008. In 2009, four of the top 50 global malicious threats exploited vulnerabilities, up from three in 2008. The effectiveness of this method of propagation is borne out by the fact it was the fourth-ranked propagation mechanism in both 2008 and 2009.

Malicious threats that do not themselves exploit vulnerabilities to propagate may still be installed on computers through threats that do. The primary example of this is with modular threats. One example is worms that exploit vulnerabilities to gain initial access to a computer and then download and install further threats. Another example is drive-by downloads, in which the exploitation of a vulnerability in a Web browser allows a modular threat to also download and install further threats.

[170] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 69
[171] http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf : p. 30
[172] http://www.symantec.com/connect/blogs/2009-year-worth-learning
[173] The number of documented malicious code instances differs from the number of malicious code submissions; documented malicious code instances are those that have been analyzed and documented within the Symantec malicious code database.

Of significant note regarding this propagation method is Downadup. Since November 2008 it has risen to be the sixth-ranked staged downloader component and, overall, the fifth-ranked potential infection for 2009. As noted earlier, there were more than 1.5 million infection counts of the Downadup worm observed by Symantec in December 2009 alone, and it was estimated that Downadup was on more than 6 million PCs worldwide at the end of 2009, even though Microsoft issued a patch for it on October 23. 2008.[174]

Downadup exploits a vulnerability in Microsoft Windows that allows attackers to remotely gain administrative privileges on computers. Microsoft states that there were limited and targeted attacks up to two weeks prior to patching the issue.[175] Proof-of-concept exploit code was released October 24, 2008, and the first worm exploiting the vulnerability was Wecorl,[176] which was discovered on November 2, 2008. Downadup was discovered on November 21. Approximately four weeks elapsed between the availability of the patch addressing the vulnerability that Downadup exploits and Downadup's discovery.

The A and B variants of Downadup account for the vast majority of infections worldwide, with Downadup.C infecting less than half a million computers by the end of 2009. Successive variants after C affect even fewer computers.

The success of Downadup illustrates that, even though there are small numbers of samples that exploit vulnerabilities, they have great success in compromising unpatched computers. End users and enterprises should ensure that vulnerabilities in affected software are patched as soon as fixes are available. The continuing prevalence of the older A and B variants of Downadup, in particular, illustrate the importance of software updates. Intrusion prevention systems and antivirus software can help protect against malicious code that exploits vulnerabilities for which no patch is available.

Malicious code—protection and mitigation

It is critical that end users and enterprises maintain the most current antivirus definitions to protect against the high quantity of new malicious code threats. IDS, IPS, and other behavior-blocking technologies should also be employed to prevent compromise by new threats. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications—such as HTTP, FTP, SMTP, and DNS servers—and that are accessible through a firewall or placed in a DMZ. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

[174] See http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker and http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[175] http://blogs.technet.com/msrc/archive/2008/10/23/ms08-067-released.aspx
[176] http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-110306-2212-99

To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of IPS technologies can prevent exploitation of browser and plug-in vulnerabilities through signatures and behavior-based detection in addition to ASLR. End users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

Phishing, Underground Economy Servers, and Spam 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 brand, usually one that is well known, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Phishing generally requires end users to enter their credentials into an online data entry field. This is one of the characteristics that distinguishes phishing from spam-based scams (such as the widely disseminated "419 scam" and other social engineering scams).[177] The data that end users enter can then be used for fraudulent purposes.

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 attempts.[178] Spam can also be used to deliver drive-by downloaders, which require no end user interaction other than navigation to the URLs contained in the spam messages. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email gateways.

This section will assess phishing and spam trends that Symantec observed in 2009. It will also discuss items that were offered for sale on underground economy servers during this time, since this is where much of the profit is made from phishing and spam attacks. Underground economy servers are black market forums for advertising and trading stolen information and services. This discussion will assess underground economy servers according to the different types of goods and services advertised. It should be noted that this discussion might not necessarily be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec monitored during this period.

The results used in this analysis are based on data returned from the Symantec Probe Network, as well as the Symantec Brightmail AntiSpam™ customer base and MessageLabs Intelligence. Specifically, statistics are only gathered from enterprise customers' Symantec Brightmail AntiSpam servers that each receive more than 1,000 email messages per day. This ensures that smaller data samples (that is, smaller customers and test servers) are excluded, thereby allowing for a more accurate representation of data. Statistics obtained on underground economy servers are gathered by proprietary Symantec technologies that monitor communications on those servers.

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attacks. An attack can consist of one or more messages. The goal of the Symantec Probe Network is to simulate a wide variety of Internet email users, thereby attracting a stream of traffic that is representative of spam activity across the Internet as a whole. For this reason, this network is continuously optimized in order to attract new varieties of spam attacks.

[177] The scam is referred to as such because 419 is the section of Nigerian criminal code that deals with fraud; Nigeria has become notorious as the source for this sort of scam. http://nortontoday.symantec.com/features/security_at_30.php
[178] http://news.bbc.co.uk/2/hi/technology/6676819.stm

This section will address the following metrics:

- Phishing activity by sector
- Countries hosting phishing URLs and top targeted sectors
- Automated phishing toolkits
- Underground economy servers—goods and services available for sale
- Spam by category
- Countries of spam origin
- Spam delivered by botnets
- Phishing, underground economy servers, and spam—protection and mitigation

Phishing activity by sector

This section will explore phishing activity in two ways. First, it will analyze the unique brands being spoofed in phishing attacks according to the sector to which they belong. Second, it will explore the sectors whose brands were most frequently spoofed by phishing URLs. These considerations are important for an enterprise because the use of its brand(s) in phishing activity can significantly undermine consumer confidence in its reputation.

Phishing URLs are usually delivered by spam email (in which case it is known as phishing email) and multiple URLs can lead to the same phishing website. A phishing website is a site that is designed to mimic the legitimate website of the organization whose brand is being spoofed. In many cases, it is set up by the attacker to capture authentication information or other personal identification information from victims; any information gathered is then typically used in identity theft or other fraudulent activity.

The motive behind most—if not all—phishing is for financial gain. Phishers typically exploit brands associated with the financial sector because data garnered from phished financial websites is likely to yield online banking account and login details. One element that greatly facilitates the success of phishing attempts is the increased use of the Internet for financial transactions. For instance, in the United Kingdom and France, more than 50 percent of Internet users perform online banking, while in Canada the number rises to 60 percent. In the United States, eight out of 10 online households now bank online. It is not surprising then that, given its gainful capability, the majority of phishing activity targets brands in the financial sector. The prosperous nature of these phished credentials is borne out by the fact that credit card details and banking credentials remained the most frequently advertised items on underground economy servers observed by Symantec in 2009.

The majority of brands used in phishing attacks in 2009 were from the financial services sector, accounting for 74 percent of the total (table 19). This was a decrease of 5 percentage points from the 79 percent reported in 2008, but is still 65 percentage points above the second-ranked sector during this reporting period. The number of uniquely phished brands also decreased by 13 percent in 2009. This may be a reflection of the turbulence in the global banking sector in 2009 that saw a number of changes in the ownership and solvency of a number of significant institutions.[179] The decline in the number of banks resulted in there being fewer appealing brands to phish. Another possibility could be that phishers are refocusing their efforts more on larger, more profitable banks, which is indicated by the most phished brands (discussed in "Countries hosting phishing websites and top targeted sectors").

[179] http://www.financialexpress.com/news/us-bank-collapse-toll-touches-94-so-far-this-year/520225/

Sector	2009 Percentage	2008 Percentage
Financial	74%	79%
ISP	9%	8%
Retail	6%	4%
Insurance	3%	2%
Internet community	2%	2%
Telecom	2%	2%
Computer hardware	1%	1%
Government	1%	1%
Computer software	<1%	<1%
Transportation	<1%	<1%

Table 19. Unique brands phished, by sector
Source: Symantec

Analysis of the data for phishing websites in 2009 indicates that the financial services sector also accounted for 78 percent of that total, which was slightly higher than 2008, when the volume of phishing websites for financial services was 76 percent (figure 13). Although this may not seem to be a significant percentage change, the number of phishing URLs targeting the financial services sector in 2009 increased by 35 percent. As previously mentioned, the number of brands targeted by phishing attacks in 2009 decreased by 13 percent when compared to 2008. An increase in the number of phishing URLs targeting fewer brands may indicate that phishers narrowed the focus of their phishing attacks during 2009. This becomes evident when the top phished brands in 2009 are compared with the same brands phished in 2008. In 2009, the top two brands phished belonged to the largest U.S.-based multinational banks. In 2008, these brands ranked 17th and seventh in 2008, respectively. There was nearly a sevenfold increase in phishing URLs that targeted the top-phished brand in 2009 over the previous reporting period, while the second-ranked brand had almost a threefold increase. This indicates that phishers are narrowing their focus. Rather than targeting a wider range of smaller financial institutions, they are specifically targeting the largest banks that are more likely to have a higher number of customers banking online.

One development that Symantec has observed from the increased sophistication of targeting phishing attacks is an increase in spear-phishing campaigns. Spear phishing is a targeted form of phishing in which the apparent source of the email is likely to be an individual within the recipients' company and generally someone in a position of authority. Victims are much more likely to fall for a spearphishing attempt because of the level of familiarity with the sender and the contents of the message, given that the contents would have been specifically crafted for the recipients. Spear phishing is a growing concern as attackers turn their attention toward targeted attacks aimed at stealing an organization's intellectual property. These attacks are likely to target senior officials of organizations who have access to significant amounts of their organization's intellectual property because successful attacks are likely to garner greater financial yield for attackers. Symantec anticipates that this trend will increase through 2010.[180]

[180] http://www.symantec.com/business/resources/articles/article.jsp?aid=20091110_multi_channel_security

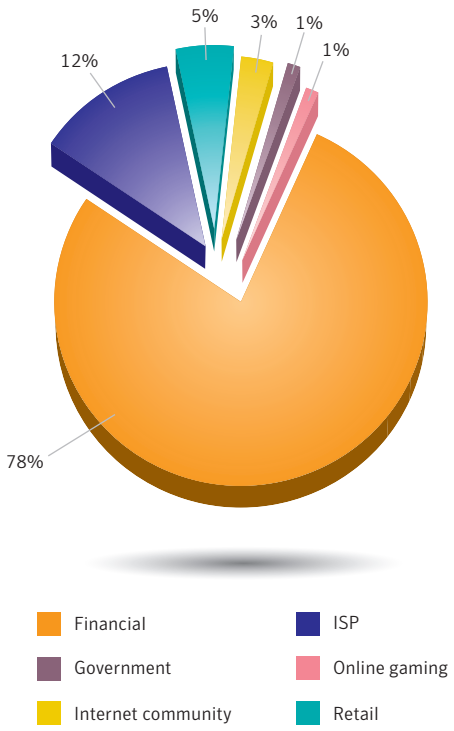

Figure 13. Phished sectors by volume of phishing URLs
Source: Symantec

In 2009, the ISP sector ranked second for spoofed brands, accounting for 9 percent of the total. The ISP sector also ranked second for volume of phishing lures in 2009, accounting for 12 percent of the total—a slight increase from the 10 percent recorded in 2008. Although there was little change in the number of unique brands phished in this sector, the volume of lures targeting these brands increased by 50 percent.

The increase in the volume of lures targeting this sector was likely due the financially advantageous nature of these accounts. Once phishers gain access to Webmail accounts they could sell them in the underground economy. While credentials stolen during ISP-targeted attacks do not offer much direct financial gain for the phishers, they do offer a wealth of user information that can be used in other phishing, spear phishing, or social engineering attacks.[181] At the very least, phishers can harvest the user's address list for further spamming opportunities. It has also been observed by Symantec that phishers sometimes use the free Web-hosting space often included with these ISP accounts to set up fraudulent websites, from which they launch new attacks.

The third most phished sector for 2009 was the retail services sector. This accounted for 6 percent of organizations whose brands were spoofed by phishing attacks in 2009, an increase of 2 percentage points from the 4 percent recorded in 2008; this also accounted for a 36 percent increase in the number of unique phished brands in the retail sector. The retail sector is an attractive target for phishers for numerous reasons.

[181] In spear phishing attempts, the email appears to be from organizations or individuals the potential victims would normally get emails from; for more information see: http://www.symantec.com/norton/products/library/article.jsp?aid=spear_phishing_scam_not_sport

The growth of the online retail sector has been considerable over the last several years and this is one sector seemingly unaffected by the global recession; for example, one survey found that, in 2009, shoppers were spending 94 percent more per order online and that, in the United States, online retail sales increased over 14 percent from 2008.[182] Phishers are capitalizing on the fact that online retailers regularly require the input of financial information that, if obtained by the phishers, can be sold or used for fraudulent financial gain. If phishing attempts to acquire usernames, passwords, and credit card information prove successful, then the resultant information can be used on legitimate websites to purchase goods using the stolen credit card information.

Despite the fact that it offers promise for potential gain, it would appear that phishers did not target the retail sector in 2009 as much as in previous years. Even though the number of unique phished brands increased by 36 percent, the number of phishing URLs targeting those brands decreased by almost 20 percent when compared to 2008 data. This suggests that it is probably easier and more lucrative for an attacker to buy a credit card number on the underground economy or obtain credit card details via an online banking scam, rather than taking the time to phish a retail account. For example, stolen credit can be easily laundered online, such as through online gambling sites where a number of "players" could populate an entire poker game and arrange to lose money to one another, which is easier than having to fence products procured from phished retail accounts that could be easily traced. This is another possible explanation for the significant increase in the number of URLs targeting the financial sector and the reduction in the number of URLs targeting the retail sector in 2009. Symantec predicts that this trend will continue through 2010.

Countries hosting phishing URLs and top targeted sectors

This metric will assess the countries in which the most phishing URLs were hosted in 2009. This data is a snapshot in time and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also be noted that the fact that a phishing URL is hosted in a certain country does not necessarily mean that the attacker is located in that country.

In 2009, 36 percent of all phishing URLs detected by Symantec were located in the United States (table 20). This is considerably less than 2008 and 2007, when 43 percent and 69 percent of phishing URLs originated there, respectively. This declining trend was discussed in the previous version of the Symantec *Global Internet Security Threat Report*, which suggested that the threat landscape was shifting from the United States to emerging countries with rapidly expanding broadband infrastructures.[183]

Of the phishing URLs situated in the United States, 70 percent of phished brands were associated with financial services. This is in keeping with the global trend, in which 74 percent of phishing URLs detected across the Internet as a whole were associated with the financial services sector. This is in keeping with the global trend, since 74 percent of phishing URLs detected across the Internet as a whole were associated with financial service organizations. This trend of targeting the financial sector is reflected in the top 10 countries hosting phishing URLs in 2009. As previously discussed in **"Phishing activity by sector,"** the financial sector offers the best chance of lucrative financial reward for phishers.

[182] http://www.coremetrics.com/company/2009/pr12-21-09-online_retail_sales.php
[183] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 8

Rank	Country	Percentage 2009	Percentage 2008	2009 Top Sector Targeted in Country	2009 Percentage of URLs Targeting Top Sector
1	United States	36%	43%	Financial services	70%
2	South Korea	5%	4%	Financial services	91%
3	Spain	4%	2%	Financial services	88%
4	Poland	4%	6%	Financial services	89%
5	Romania	4%	<1%	Financial services	89%
6	Russia	4%	3%	Financial services	73%
7	United Kingdom	3%	3%	Financial services	70%
8	Germany	3%	3%	Financial services	76%
9	Canada	3%	3%	Financial services	61%
10	France	2%	4%	Financial services	74%

Table 20. Top countries hosting phishing URLs and top-targeted sectors
Source: Symantec

In 2009, South Korea had 5 percent of the total of phishing URLs observed globally, up from 4 percent in 2008 when it ranked fourth in this measurement. The reason for South Korea's high ranking here may be its extensive broadband infrastructure, which makes an appealing target for attackers looking to host phishing and spam sites. According to a recent survey, South Korea ranked second globally for online connectivity.[184] Internet users in South Korea spend an average of 11.5 hours a week on the Web; in 2008, household broadband penetration was at 97 percent.[185] Moreover, the previous volume of the Symantec *Global Internet Security Threat Report* noted the increasing levels of fiber-to-the-home/building (FTTH/B) deployment in South Korea.[186] FTTH/B connections currently provide the highest bandwidth capacities, compared to traditional DSL or cable lines, and South Korea has the highest penetration of FTTH/B worldwide. With a strong culture of Internet usage with high-speed available broadband and a thriving personal computer market, it is easy to see why attackers might favor South Korea as a location for sending spam and hosting phishing attacks.

Spain moved into third place in 2009, accounting for four percent of the total for countries hosting phishing URLs. This was an increase of two percentage points over 2008 when it ranked 13th. Symantec also recorded that this two percent change accounted for a fourfold increase in the numbers of lures seen emanating from Spain in 2009. This is not unusual when considering recent trends in Spain. The most recent report on global broadband subscriptions shows Spain as having the fifth highest rate of broadband subscription globally.[187] Spain is also ranked 14th for countries sending the most spam in 2009. Given these factors, it is probable that a higher percentage of broadband-connected computers in Spain are susceptible to compromise and are likely serving as hosts for phishing URLs and spam servers, both of which could be used to generate and distribute phishing lures.

[184] http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user_p2&tdim=true&dl=en&hl=en&q=global+internet+usage#met=it_net_user_p2&idim=country:USA:KOR:FRA:DEU:ESP:ITA:CAN:GBR&tdim=true
[185] http://news.zdnet.com/2100-3513_22-137772.html
[186] http://www.ftthcouncil.org/en/newsroom/2010/02/26/g-20-need-to-speed-up-on-fiber-to-the-home
[187] http://point-topic.com/contentDownload/operatorsource/dslreports/world%20broadband%20statistics%20q1%202009.pdf : p. 25

Romania moved into fifth place and accounted for four percent of the total for countries hosting phishing URLs in 2009. This was a dramatic change compared to 2008, when Romania ranked 28th, and accounted for less than one percent of the total for countries hosting phishing URLs. The four percent increase noted by Symantec, accounted for approximately an eighteen-fold increase in the number of phishing URLs originating from Romania during 2009. Romania's broadband sector has also developed rapidly in recent years.[188] In addition to hosting phishing URLs, it was noted by Symantec that Romania moved from 20th position in 2008 to 12th position in 2009 for countries sending the most spam. Given these facts, it is clear that attackers are looking at Romania as a favorable target for hosting malicious activity. Symantec anticipates this trend will continue through 2010.

Another significant change in the rankings in 2009 was China's move from third-ranked position in 2008 for countries responsible for hosting phishing URLs to 18th in 2009. One reason for this drop may be that Chinese companies and government organizations last year formed an antiphishing group that may have helped reduce phishing incidents.[189]

Automated phishing toolkits

A phishing toolkit is a set of scripts that allows an attacker to automatically create websites that spoof the legitimate websites of different brands, including the images and logos associated with those brands. The scripts also help to generate corresponding phishing email messages. Because each script generates pseudo-random phishing URLs with a distinctive pattern, the particular script used to generate a particular phishing URL can be identified from that pattern. All phishing URLs reported to Symantec can be sorted and grouped according to those specific patterns.

Phishing toolkits are developed by groups or individuals who, along with using the kits themselves, sell the kits in the underground economy. Therefore, independent groups can use the same toolkit. Note that toolkits sold in the underground economy often go unnamed. Unlike legitimate software, for which naming plays an important marketing role, phishing toolkits often become popular based on who has produced them. Moreover, their names are usually not integral given the limited lifespan of a great many of them. Consequently, phishing toolkits discussed here cannot be named specifically and will instead be referred to by numbers.

Phishing Kit 1 relies on a strong social engineering component and is typically active only around holiday seasons. This explains why it was responsible for more than 29 percent of all phishing campaigns, in January 2009, but then its activity dropped to an average of 6.35 percent for the year overall (figure 14). Kit 1 only targets one popular Webmail service and uses domain names that are often related to images or pictures, such as "ellie.cool-xmas-pics.com" or "kyleman.cool-xmas-pics.com." They are often sent using the same targeted Webmail service to other users, with text such as "Hey is this you on [*sic*] this picture?"

Phishing Kit 1 is a domain-based phishing toolkit. Domain-based phishing toolkits require the phisher to own or register a unique domain such as "aphishingsite.com" and host it on a bot network or on an ISP. The phisher can then create phishing links with random subdomains, such as "mybank.aphishingsite.com," "anotherbank.aphishingsite.com," and so on.

[188] http://www.mindbranch.com/Romania-Telecommunications-Q1-R302-9378/
[189] http://news.techworld.com/security/3208909/chinese-virus-makers-end-up-in-jail/

On the other hand, defacement-based phishing toolkits do not require the registration of domains or DNS servers, so they are easier to set up. Defacement-based phishing toolkits require a phisher to compromise existing Web pages, after which the phisher can simply upload the page of the spoofed brand. Defacement-based toolkits are often favored by phishers because of their ease of use and the fact that they can piggyback on the reputation of the original domain. For example, in 2009 Symantec detected many image-hosting sites that were compromised and used for phishing attacks.

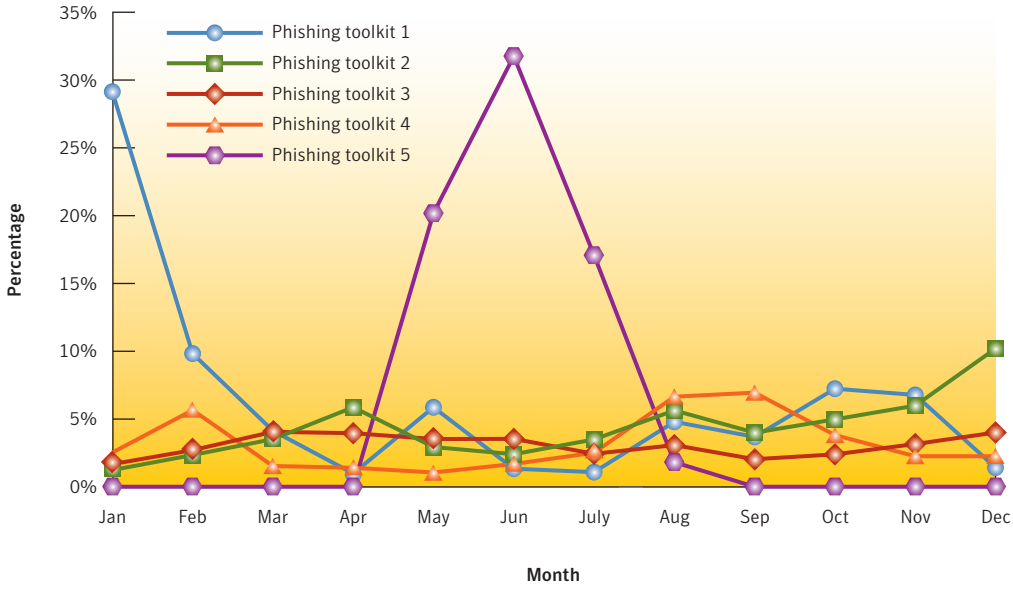

Figure 14. Automated phishing toolkits
Source: Symantec

Phishing Kit 5 appeared in May 2009. It was responsible for 20 percent of that month's phishing attacks, followed by 32 percent in June and 17 percent in July. After this spike, its usage dropped to less than two percent and then it vanished completely. Volume XIII of the Symantec *Global Internet Security Threat Report* discussed this tendency and noted that the rapid change in preferred toolkits is likely driven by a need for phishers to adapt and constantly change the toolkits they use to avoid detection by antiphishing software.[190] This is likely the driving factor behind the dramatic upward spike and subsequent decline of many toolkits. Moreover, this specific attack used one single domain, which made it easier for security companies to block once it was detected.

On average, each of the top five phishing kits was responsible for nearly 5 percent of all the attacks observed in 2009, with small fluctuations over time. Overall, there was an increase in the total number of different phishing kits used. Most kits are becoming more sophisticated in an attempt to make it harder for security researchers and users to detect them.

[190] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 73

Underground economy servers—goods and services available for sale

This discussion focuses on the most frequently advertised items for sale on underground economy servers observed by Symantec. The underground economy is an evolving and self-sustaining black market where underground economy servers, or black market forums, are used for the promotion and trade of stolen information and services. This information can include government-issued identification numbers such as Social Security numbers (SSNs), credit card numbers, debit card information, user accounts, email address lists, and bank accounts. Services include cashiers, scam page hosting, and job advertisements such as for scam developers or phishing partners. Much of this commerce is built within channels on IRC servers. For an in-depth analysis of how the underground Internet economy functions, please see the Symantec *Report on the Underground Economy*, published November 2008.[191]

The measure of goods and services available for sale is by distinct messages, which are considered as single advertisements for a good or service, though the same advertisement may appear thousands of times. To qualify as a new message there must be variations such as price changes or other alterations in the message.

In 2009, credit card information was the good most frequently advertised for sale on underground economy servers observed by Symantec, accounting for 19 percent of all advertised items (table 21). This was a decrease from 32 percent in 2008. Although this appears to be a significant drop, the percentage observed in 2007 was 21 percent, which may indicate that there was higher availability of credit card numbers on underground economy servers in 2008. The number of data breaches reported in those years is a further indication of this. There were more than twice as many data breaches reported in 2008 than in 2007. Similarly, there were almost twice as many data breaches reported in 2008 than there were in 2009. Credit card information advertised on the underground economy consists of the credit card number and expiry date, and may include the name on the card (or business name for corporate cards), billing address, phone number, CVV2 number, and PIN.[192]

Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 21. Goods and services advertised for sale on underground economy servers
Source: Symantec

[191] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
[192] Card Verification Value 2 (CVV2) is a three- or four-digit number on the credit card and used for card-not-present transactions, such as Internet or phone purchases. This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card.

Another contributing factor for the drop in the percentage of advertisements for credit card information may have been the increase in advertisements for credit card dumps; these increased in rank from 13th in 2008 to seventh in 2009. While credit card information includes things such as the credit card number, expiry date, and account holder name, a credit card dump is an exact copy of the encoded data contained in the magnetic stripe on a credit card.[193] The dump data can be written to the magnetic stripes of counterfeit credit cards and then the duplicates can be used as though they were the original card.

The drop in percentage may also be related to credit card companies, credit card issuers, and banks taking more secure precautions to verify and authenticate users. Multi-level security systems for card-present transactions (such as EMV chip-based cards) can make it more difficult for criminals to obtain and use financial information.[194] These technologies are being increasingly implemented as more companies opt for compliance with new security standards. As the usage of this technology grows, criminals may resort to other means of making fraudulent transactions.

Stolen credit card information can be quickly and easily used to purchase goods online because, often, only minimal credit card information is required for online purchases. In addition to physical goods purchased online for subsequent delivery, criminals can purchase digital goods such as domain registrations, music, software, and gift certificates for online stores, which they receive immediately. Someone with sufficient knowledge could make many transactions with a stolen card before the suspicious activity is detected and the card is suspended. However, there is a chance that the activity will be detected and if this happens before physical goods are shipped, the fraudulent transaction will have failed. Additionally, a shipping address must be provided for physical goods, which may help law enforcement agents in locating the criminal. However, criminals often obfuscate their connections to fraudulent online transactions by having the purchased goods delivered to the address of an intermediary (referred to as a mule or a drop) who then ships the goods to the criminal.[195]

Aside from the shipping address, these mules may have no obvious ties to the initial transaction and are often unaware that they are facilitating illegal transactions and money laundering. The service of mules is even advertised on underground economy servers by scammers who have deceived unsuspecting people into carrying out a seemingly legitimate job.

Scammers acquire mules by attracting unsuspecting victims with work-from-home job opportunities advertised in the guise of legitimate employment. The job requires the mule to receive packages at a personal address or a post box that they set up on the scammer's behalf. The mule then resends the packages to addresses specified by the scammer. The mule is typically required to pay for any set-up costs and shipping fees out of their own pocket, with promises of reimbursement and an enticing paycheck later. Many victims of mule scams are never paid or reimbursed and end up losing thousands of dollars before realizing that they have been victimized.

[193] Information contained within the magnetic stripe on a credit card, which is made up of two tracks. Both tracks contain the primary account number and expiration date; the first track will contain the cardholder name and CVV. Each credit card issuer will have their own standards for encoding the information in the tracks.
[194] EMV is a standard for authenticating credit and debit card payments (http://www.emvco.com/about.asp); see also http://www.wired.com/threatlevel/2009/10/card-fraud/
[195] http://information-security-resources.com/2009/11/20/online-money-mules-aide-theft-and-fraud/

Counterfeit credit cards made using data dumps can add a sense of legitimacy to fraudulent transactions by allowing criminals to make purchases in person. By immediately acquiring purchased goods during the transaction instead of waiting for delivery, the scammer does not have to worry about the credit card company noticing the purchase and freezing the account because the goods are already in the scammer's possession. However, it is reasonable to assume that even when using counterfeit cards, some scammers will employ a third party to make in-person transactions, thereby reducing personal exposure to surveillance systems that could be monitoring the fraudulent purchase.

Credit card information can be obtained through a variety of means such as monitoring merchant card authorizations or breaking into databases. Data breaches can be very lucrative in the underground economy. For example, the previously mentioned security breach of the credit card payment processor in January 2009 resulted in the exposure of more than 130 million credit card numbers. Even using the lowest advertised price-per-card number in 2009, this breach represents over $110 million in potential profit.

Credit card dumps are harder for underground economy sellers to acquire because they can only be obtained by using skimming machines that physically scan the magnetic stripe of the legitimate card.[196] Because of this, and the pseudo-legitimacy that dumps can provide through counterfeit cards, dumps are rarer and are often advertised at higher rates than credit card information.

The prices of credit card information advertised in 2009 ranged from $0.85 to $30 per card number, a slight change from 2008 when prices ranged from $0.06 to $30. The difference in prices may be a further indication of higher availability in 2008; the low-end price observed in 2007 was $0.40. This is a reflection of simple supply and demand, where higher bulk availability results in lower prices. There were three main factors that influenced the prices: the amount of information included with the card, rarity of the card type, and bulk purchase sizes. Credit cards that bundled in personal information—such as government-issued identification numbers, addresses, phone numbers, and email addresses—were offered at higher prices. Cards that included security features such as CVV2 numbers, PINs, and online verification service passwords were also offered at higher prices.

The value of credit card information is also influenced by the location of the issuing bank as well as the type and rarity of the credit card. Credit cards issued in regions such as Asia, the Middle East, and some European countries are often advertised at higher prices than those in other regions because the availability of information in these regions is lower. In 2009, for example, credit card information from countries such as Italy and France was commonly listed for $6 to $10 each, while cards issued from the United Kingdom, Canada, and the United States were commonly listed at $5 or less per card.

While the maximum advertised price per card number remained the same in 2009 as the previous year, the minimum price of $0.06 was higher than the 2008 minimum price per card number. The primary reason for the rise in minimum price per card number is that there was a notable lack of bulk pricing in advertisements observed in 2009. The bulk rates that were advertised applied to smaller lots of card numbers than has been previously observed. For example, the largest advertised bulk quantity observed by Symantec in 2009 was for 100 credit cards, as opposed to 5,000 credit cards in 2008.

[196] Magnetic stripe skimming devices are small machines designed to scan and retain data contained in the magnetic stripes on credit and debit cards.

Some advertisements mentioned the availability of bulk purchasing but did not mention card number volumes or pricing. This may suggest that some advertisers prefer to negotiate bulk rates on a per-customer basis rather than being locked into offering a set rate. Sellers often make a sample allotment of their credit card numbers available to potential buyers who can use a number checking service to verify that the numbers are valid. The amount of valid numbers would obviously influence negotiated rates. Considering the wide range of prices advertised, this would also allow the seller to increase his or her competitiveness and profit margins by being able to adjust the prices at any time based on rates advertised by other sellers.

As new security technologies evolve and become more commonly integrated, they may make it more difficult for criminals to obtain credit card information, which will likely reduce the utility of the information. For example, cards with a built-in code generator were pilot tested in 2009 and may provide a means of securing card-not-present purchases such as those made online.[197] These cards have an integrated keypad on the back that will generate a one-time verification code whenever the correct PIN is entered. Even if the card is stolen or lost, a criminal would need the PIN to use the card.

Bank account credentials were the second most commonly advertised item on underground economy servers observed by Symantec in 2009, accounting for 19 percent of all advertised goods. This was the same percentage as was observed in 2008. Bank account credentials may consist of account numbers, bank transit numbers, account holder names and/or company names, and may include online banking passwords. Advertisements often include the account type and balance as well as name and location of the financial institution.

The ability to directly withdraw currency from a bank account is advantageous and attractive to criminals, who can realize a more immediate payout than with online purchases, which need to be sold to realize a purely financial reward. Bank account credentials also allow access to full balances in the bank accounts, whereas credit cards may have daily or other transaction limitations on accessing the maximum available credit. Criminals can also use bank accounts as intermediary channels for money laundering or to fund other online currency accounts that only accept bank transfers for payments.

Bank account credentials have been some of the most commonly advertised goods on underground economy servers for the past several years. As noted in the previous Symantec *Global Internet Security Threat Report*, the shift toward online banking provides the potentially increased availability of sensitive information through methods such as phishing or malicious code attacks, which can expose the credentials of both personal and business accounts alike.[198] The availability of sensitive information will likely continue to increase as online financial transactions continue to grow, notwithstanding the recent setbacks in the availability of credit due to the recent global financial crisis.[199]

The advertised prices for bank account credentials depend on the account type, location, and the funds advertised as available. In 2009, prices for these credentials observed on underground economy servers ranged from $15 to $850, a slightly smaller range than in 2008 when prices ranged from $10 to $1,000. The advertised account balances ranged from $1,000 to $177,000; however, the most common advertisements were for bank accounts with balances between $10,000 and $50,000. As in previous years, corporate accounts were typically advertised for a higher price than personal accounts. These bank

[197] http://news.bbc.co.uk/2/hi/8046492.stm
[198] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 76
[199] http://www.comscore.com/Press_Events/Press_Releases/2009/4/2009_State_of_Online_Banking_Report

accounts often have larger balances than those of personal accounts, resulting in significant losses when corporate account credentials are stolen. In 2009, for example, criminals used the valid online banking credentials of a business to steal over $800,000.[200]

Although the country in which the bank is located was sometimes included in advertisements, it did not noticeably affect the prices for this reporting period. Some advertisements for bank account credentials listed minimal details, such as the banking organization only. As with bulk credit card information, this may suggest that some advertisers prefer to negotiate rates on a per-customer basis rather than locking themselves into a set price.

The third most common item advertised for sale on underground economy servers observed by Symantec in 2009 was email accounts, making up 7 percent of the total. This was an increase from 5 percent in 2008. Having access to stolen email accounts has many benefits for criminals. The accounts can be used for sending out spam and/or harvesting additional email addresses from contact lists. Recipients of spam email coming from a known email address may be more likely to trust the validity of the message.

Compromised email accounts can also often provide access to additional sensitive personal information such as bank account data, student identification numbers, mailing addresses and phone numbers, or access to other online accounts (social networking pages, online stock accounts, etc.) that people often store in saved personal emails. Such information can often be used for the password recovery option offered on many online registration sites that send the account holder a new password via email, potentially giving the fraudster complete access to these accounts. This danger is further compounded by the habit many people have of using the same password for multiple accounts. For example, in a major recent data breach it was discovered that simple passwords remain alarmingly popular, despite the risks of hacking.[201] The fraudulently gained personal information can then be used to conduct additional identity theft and fraud.

The advertised prices of email accounts in 2009 ranged between $1 and $20 for each account. Most advertisements listed a flat rate, although some sellers also listed bulk purchase prices such as “30 for $150,” or “$1 each on bulk purchase.” Very few details regarding the email accounts were provided, indicating that the buyers may not be concerned with whether the accounts are for personal or business use. In addition, some of the advertisements stated that Web space was included with the email account and were listed at higher prices. ISPs often include free Web space along with email accounts as a part of the service, which many people never use. Criminals who compromise these accounts can use the space to host phishing sites or malicious code without the knowledge of the account owner.

As in previous reporting periods, the observed distribution of goods and services advertised on underground economy servers continues to be focused on financial information, such as credit card information and bank account credentials. This suggests a trend in which criminals are more focused on purchasing goods that allow them to make a quick profit rather than on exploits that require more time and resources, such as scam pages and email lists for spamming. As steps are taken to make it more difficult to obtain and use this financial information, this trend will likely change, albeit gradually as new security technologies take time to be refined and implemented.

[200] http://www.krebsonsecurity.com/2010/01/texas-bank-sues-customer-hit-by-800000-cyber-heist/
[201] http://www.nytimes.com/2010/01/21/technology/21password.html?partner=rss&emc=rss

Spam by category

Spam categories are assigned based on spam activity that is detected by the Symantec Probe Network. While some of the categories may overlap, this data provides a general overview of the types of spam that are most commonly seen on the Internet today. It is important to note that this data is restricted to spam attacks that are detected and processed by the Symantec Probe Network. Internal upstream processing may filter out particular spam attacks, such as those that are determined to be potential fraud attacks.

The most common type of spam detected by Symantec in 2009 was related to Internet-related goods and services, which contributed 29 percent of all spam observed—an increase from 24 percent in 2008 (figure 15). This category of spam typically contains spam relating to online commodities such as online educational diplomas and degrees. Although "degree spam" is not a new trend, 2009 saw spammers capitalize on the economic recession by advertising online degree courses to all sectors of the workforce. Some of these online educational scams requested financial-related information in the initial application stage, thus providing spammers with an additional way to procure credit card information under the pretense of a legitimate educational facility.

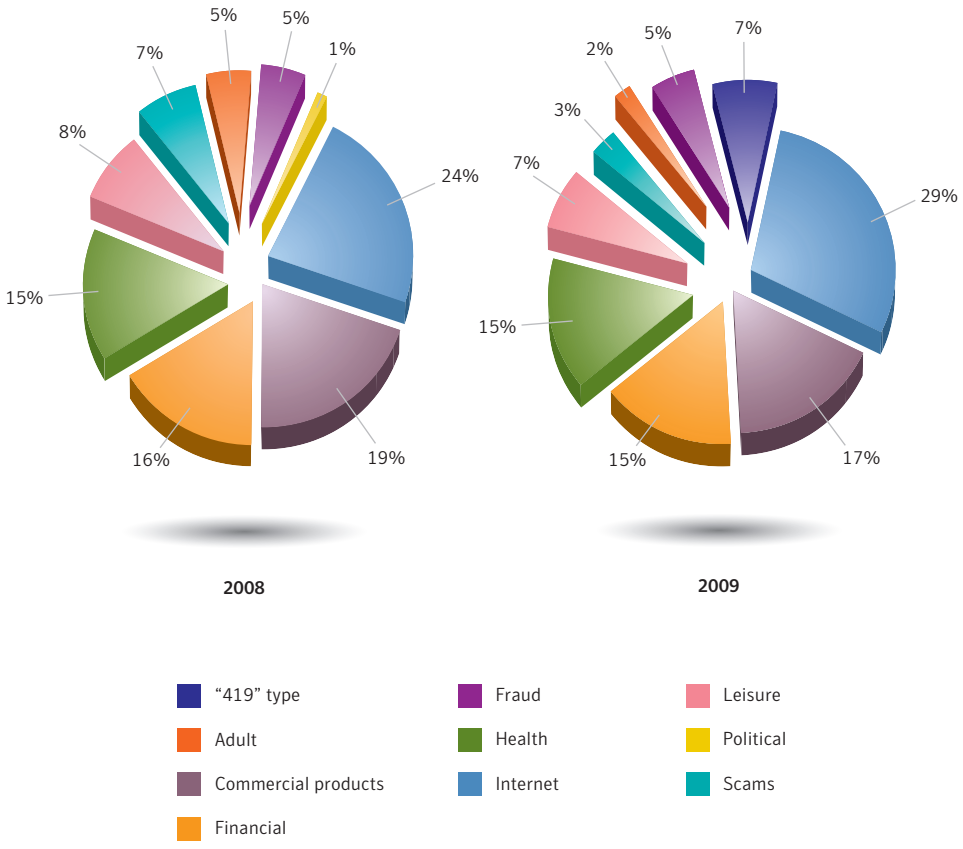

Figure 15. Spam by category
Source: Symantec

The second most common type of spam detected was related to commercial products, which accounted for 17 percent of the spam observed by Symantec in 2009. While some categories had spikes at certain times of the year, the levels of product spam remained constant from January to December. From early January, Symantec noted product spam promoting roses and chocolates for Valentine's Day, to designer watches and footwear in the summer months, to household trinkets for Thanksgiving and Christmas in November and December. This category has also remained relatively constant year after year, while selling commercial paraphernalia remains a fruitful source of revenue for spammers.

Financial services spam remained the third most popular spam category in 2009, accounting for 15 percent of all spam observed. Financial spam contains references to money, the stock market, or other financial opportunities. Even though the percentage of financial spam remains relatively unchanged as far back as 2007, what has changed is the subject lines used to convey the spam in this category. In the early days of the global boom, penny stock was the most common type of financial spam observed by Symantec; these scams attempted to entice recipients to purchase penny stocks and shares, often as part of a pump-and-dump ploy to over-promote certain stocks.

As discussed previously, spammers frequently exploit current events to garner attention for their merchandise. This reporting period was no exception, with spam subject lines preying on the financially vulnerable by offering a risk-free way out of the financial crisis. This includes a barrage of "fear of foreclosure" spam upon the collapse of the real estate bubble, as well as "make $$$ working from home" messages. It has also been noted by Symantec that these work from home scams can often be vehicles for receiving stolen goods or transferring money stolen from online banking.

Countries of spam origin

This section will discuss the top 10 countries of spam origin. This discussion is based on data gathered by customer installations of Symantec Brightmail AntiSpam. The data includes the originating server's IP address, against which frequency statistics are compared. Each IP address is mapped to a specific country and charted over time. The nature of spam and its distribution on the Internet presents challenges in identifying the location of people who are sending it because many spammers try to redirect attention away from their actual geographic location. In an attempt to bypass IP block lists, the spammers use Trojans that relay email, which allow them to send spam from sites distinct from their physical location. To send large volumes of spam, spammers tend to take advantage of geographic areas with large networks of available broadband connections. As a result, the origin of spam tends to increase in countries that have more insecure broadband connections. These high-speed connections are often constantly connected to the Internet. This allows spammers to send out high volumes of spam by zombie connections at any time of the day.

In 2009 the United States remained the top-ranked country for spam origin, accounting for 23 percent of all spam observed by Symantec (table 22). This is down six percentage points from 29 percent in 2008 and down considerably from 45 percent in 2007. The ranking of the United States is not surprising given that it has the second highest number of broadband users globally.[202]

[202] http://point-topic.com

Overall Rank 2009	2008	Country	Percentage 2009	2008
1	1	United States	23%	25%
2	5	Brazil	11%	4%
3	13	India	4%	2%
4	12	South Korea	4%	2%
5	9	Poland	4%	3%
6	4	China	3%	4%
7	3	Turkey	3%	5%
8	2	Russia	3%	6%
9	32	Vietnam	3%	1%
10	19	Colombia	2%	1%

Table 22. Top countries of spam origin
Source: Symantec

Brazil ranked second for originating spam in 2009 with 11 percent of the total observed by Symantec. This is a significant increase from 2008, when Brazil accounted for 4 percent of the total and was ranked fifth. The spam increase noted in Brazil can be attributed to the increased availability of broadband connections there. There has been an enormous increase in investment in IT infrastructure, making Brazil one of the fastest growing global IT markets.[203] This has enabled huge growth in broadband services in Brazil—a recent report showed that broadband adoption in Brazil had 16 percent growth in 2009.[204] In addition, as previously discussed in the "Threat Activity" section of this report, Brazil ranked first for the country hosting the most spam zombies, a rank which it also held in 2008. The substantial growth in broadband availability, along with a thriving market in computer sales,[205] provides a prime environment for spammers looking for a platform to launch their spam attacks.

India ranked third for originating spam observed by Symantec in 2009, accounting for 4 percent of the total. In 2008, India ranked 15th with 2 percent of the total. Similar to Brazil, India has recently seen unprecedented levels of growth in both IT infrastructure and broadband development.[206] Although India's broadband penetration is still expanding to meet its burgeoning economy and large population, it is estimated that India will continue to rise in the rankings for broadband connectivity in the coming future.[207]

Spam delivered by botnets

In 2009, botnets became the dominant force in terms of distributing not only spam, but also malicious code and phishing scams. The processing power of large botnets allows them to generate high volumes of spam. The distributed processing power of botnets makes them an ideal platform for launching large-scale spam campaigns. Because of their distributed nature, even taking down a large number of individual bots has little effect on the percentage of spam delivered by bots.

[203] http://www.officialwire.com/main.php?action=posted_news&rid=50513&catid=1042
[204] http://newsroom.cisco.com/dlls/2009/prod_100209b.html
[205] http://www.reuters.com/article/idUSN0332584720080403
[206] http://point-topic.com/dslanalysis.php
[207] http://www.indiabroadband.net/india-broadband-telecom-news/11682-india-register-500-growth-broadband-services-within-5-years.html

In 2009, botnets were responsible for approximately 85 percent of all spam observed by MessageLabs Intelligence. In 2008, Srizbi, one of the largest botnets observed, had been responsible for almost 26 percent of spam that same year, but after the November 2008 shutdown of an ISP that was believed to be responsible for a considerable amount of spam activity, it virtually disappeared and, by 2009, accounted for less than 1 percent of all spam observed.[208] This resulted in a dramatic fall-off in global spam levels. This void was soon filled by the Pandex and Rustock botnets. Pandex increased from less than 1 percent of botnet-related spam in 2008 to approximately 18 percent in 2009 (table 23). Rustock experienced similar growth, from less than 2 percent of botnet-related spam in 2008 to 18 percent in 2009.

Overall Rank 2009	2008	Botnet	Percentage 2009	2008
1	14	Pandex	18%	<1%
2	7	Rustock	15%	2%
3	3	Mega_d	10%	13%
4	10	Grum	8%	1%
5	19	Donbot	6%	<1%
6	19	Xarvester	5%	<1%
7	13	Bagle	5%	<1%
8	6	Other botnets	5%	2%
9	9	Bobax	2%	2%
10	2	Gheg	2%	1%

Table 23. Percentage of spam from botnets[209]
Source: Symantec

By June 2009, spam levels were at approximately 90 percent of all email. In the same month, there was another shutdown of a rogue ISP, Pricewert LLC.[210] Despite the shutdown, Symantec noted that there was minimal impact to overall spam volumes.

Of all the botnet statistics tracked by Symantec, the Pandex botnet appeared to be the only botnet affected by this ISP closure, with the spam volumes from Pandex dropping by 78 percent before recovering a few days later. A similar pattern was detected by Symantec in August, when Real Host, an ISP based in Latvia, was taken offline by its upstream providers. Again, Pandex appeared to be the only botnet significantly affected by this ISP closure; Symantec noted an 87 percent reduction in spam originating from Pandex after the shutdown. However, unlike the Srizbi botnet that was nearly eliminated by the shutdown of McColo (the ISP that was shut down in November 2008, noted above), Symantec noted that within 24 hours Pandex was again reporting similar volumes of spam messages prior to the Realhost ISP closure.

It appears that the Pandex controllers had learned from the McColo shutdown to incorporate redundancy into their business continuity plans for 2009, as evidenced by how quickly they got back online after the closure of the aforementioned ISPs. This can be attributed to the fact that attackers are using fast-flux domain-named services into the botnet structure,[211] making it less susceptible to a single point of failure such as a single rogue ISP.[212]

[208] See http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 89 and http://www.messagelabs.com/intelligence.aspx MessageLabs Intelligence: 2009 Annual Security Report
[209] Due to rounding, totals may not equal 100 percent
[210] http://www.ftc.gov/opa/2009/06/3fn.shtm
[211] Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious websites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of P2P networking, distributed C&C, Web-based load balancing and proxy redirection makes it difficult to trace the botnets' original geolocation. As industry countermeasures continue to reduce the effectiveness of traditional botnets, Symantec expects to see more attacks using this technique.
[212] http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf : p. 12

Other notable botnets that decreased considerably in 2009 were Gheg,[213] Cimbot, and Warezov_stration.[214] Gheg, which had been responsible for 15 percent of all spam in 2008, was responsible for less than 2 percent of spam in 2009. Cimbot and Warezov_stration were each responsible for 10 percent of observed spam in 2008, but only responsible for less than 1 percent each of observed spam in 2009. As discussed above, it is likely that attackers moved away from these botnets in favor of newer botnets that are more difficult to detect and less susceptible to being taken offline. Symantec believes that the newer P2P botnets will continue to be dominant in 2010 and that older, less sophisticated botnets will be rebuilt or discontinued.

In 2009, two new botnets were observed: Maazben and Festi. Maazben began low-volume spamming in March and continued spamming erratically until it reached a peak during August and September. In total, Maazben was responsible for just under 1 percent of all spam in 2009. Festi was first detected by Symantec in August 2009 and has steadily continued broadcasting, albeit with low volumes, up to the end of 2009. Festi accounted for less than 1 percent of all spam in 2009.

Phishing, underground economy servers, and spam—protection and mitigation

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA). Although this will likely remain the primary point of filtering for phishing, organizations can also use IP-based filtering upstream, as well as HTTP filtering.

DNS block lists also offer protection against potential phishing emails.[215] Organizations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.[216]

To protect against potential phishing activity, administrators should always follow Symantec best practices as outlined in "Appendix A" of this report. Symantec also recommends that organizations educate their end users about phishing.[217] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, as well as provide a means to report suspected phishing sites.[218]

Organizations can also employ Web-server log monitoring to track if and when complete downloads of their websites, logos, and images are occurring. Such activity may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing.

Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[219] So-called typo domains and homographic domains should also be monitored.[220] This can be done with the help of companies that specialize in domain monitoring; some registrars also provide this service.

[213] http://www.messagelabs.com/mlireport/MLIReport_2009.06_June_FINAL.pdf
[214] http://www.symantec.com/security_response/writeup.jsp?docid=2006-091012-5303-99
[215] A DNS block list (sometimes referred to as a black list) is simply a list of IP addresses that are known to send unwanted email traffic. It is used by email software to either allow or reject email coming from IP addresses on the list.
[216] Spoofing refers to instances where phishers forge the "From:" line of an email message using the domain of the entity they are targeting with the phishing attempt.
[217] See basic guidelines on how to avoid phishing at the United States Federal Trade Commission: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
[218] See http://www.antiphishing.org for information on the latest phishing threats.
[219] "Cousin domains" refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com", cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.
[220] Typo domains are domain names that use common misspellings of a legitimate domain name; for example, the domain "symatnec.com" would be a typo domain for "symantec.com". A homographic domain name uses numbers that look similar to letters in the domain name; for example, the character for the number "1" can look like the letter "l".

The use of antiphishing toolbars and components in Web browsers can also help protect users from phishing attacks. These measures notify the user if a Web page being visited does not appear to be legitimate. This way, even if a phishing email reaches a user's inbox, the user can still be alerted to the potential threat.

End users should follow best security practices, as outlined in "Appendix A" of this report. They should use an antiphishing solution. As some phishing attacks may use spyware and/or keystroke-logging applications, Symantec advises end users to use antivirus software, antispam software, firewalls, toolbar blockers, and other software-detection methods. Symantec also advises end users to never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.

Users should review bank, credit card, and credit information frequently. This can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[221] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

Consumers could also take more security precautions to ensure that their information will not be compromised. When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not public ones. Further, they should not store passwords or bank card numbers. They should also avoid following links from within messages (whether in email, instant messages, online forums, etc.) as these may be links to spoofed websites; instead, they should manually type in the URL of the website. In addition, consumers should be aware of the amount of personal information that they post on the Internet, as criminals may take advantage of this public information in malicious activities such as phishing scams.

[221] http://www.fbi.gov/majcases/fraud/internetschemes.htm

Appendix A—Symantec Best Practices

Symantec encourages all users and administrators to adhere to the following basic security best practices:

Enterprise best practices

- Employ defense-in-depth strategies, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated antivirus, firewalls, intrusion detection, and intrusion protection systems on client systems. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.
- Administrators should limit privileges on systems for users that do not require such access and they should restrict unauthorized devices, such as external portable hard-drives and other removable media.
- Turn off and remove services that are not needed for normal company network operations.
- Test security regularly to ensure that adequate controls are in place.
- Educate management on security budgeting needs.
- If malicious code or some other threat exploits one or more network services, disable or block access to those services until a patch is applied.
- Administrators should update antivirus definitions regularly to protect against the high quantity of new malicious code threats and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. IDS, IPS, and other behavior-blocking technologies should also be employed to prevent compromise by new threats.
- Always keep patch levels up to date, especially on computers that host public services and applications—such as HTTP, FTP, SMTP, and DNS servers—and that are accessible through a firewall or placed in a DMZ.
- As compromised computers can be a threat to other systems, Symantec recommends that affected enterprises notify their ISPs of any potentially malicious activity.
- Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
- Enforce an effective password policy. Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place.
- Mail servers should be configured to block email that appears to come from within the company, but that actually originates from external sources.
- Consider using domain-level or email authentication in order to verify the actual origin of an email message to protect against phishers who are spoofing email domains.
- Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.

- Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organization are deployed on desktop computers.
- Isolate infected computers quickly to prevent the risk of further infection within the organization.
- Train employees to not open attachments unless they are expected and come from a known and trusted source, and to not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- Perform a forensic analysis and restore the computers using trusted media.
- Ensure that emergency response procedures are in place. This includes having a backup-and-restore solution in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Employ Web-server log monitoring to track if and when complete downloads of company websites, logos, and images are occurring, as this may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing.
- Network administrators should review Web proxy logs to determine if any users have visited known blacklisted sites.

Consumer best practices

- Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Keep virus definitions updated regularly. By deploying the latest virus definitions, you can protect your computer against the latest viruses known to be spreading in the wild.
- Routinely check to see if your operating system is vulnerable to threats. A free security scan is available through the Symantec Security Check at www.symantec.com/securitycheck.
- Get involved by tracking and reporting attack attempts. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's ISP or local police.
- Deploy an antiphishing solution, such as an antiphishing toolbar for Web browsers. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

- When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not public ones. Further, they should not store passwords or bankcard numbers.
- Review bank, credit card, and credit information frequently to monitor any irregular activities. For further information, the Internet Crime Complaint Center (IC3) has also released a set of guidelines on how to avoid Internet-related scams. See http://www.ic3.gov/default.aspx for more information.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Avoid clicking on links and/or attachments in email or IM messages, as these may also expose computers to unnecessary risks.
- Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.
- Be aware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. These ads may be spyware.

Appendix B—Threat Activities Trends Methodologies

Threat activity trends in this report are based on the analysis of data derived from the Symantec Global Intelligence network, which includes the Symantec DeepSight Threat Management System, Symantec Managed Security Services, the Symantec Honeypot Network, and proprietary Symantec technologies. Symantec combines data derived from these sources for analysis.

Malicious activity by country

To determine the top countries for the "Malicious activity by country" metric, Symantec compiles geographical data on each type of malicious activity to be considered, namely: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The proportion of each activity originating in each country is then determined. The mean of the percentages of each malicious activity that originates in each country is calculated. This average determines the proportion of overall malicious activity that originates from the country in question and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Web-based attacks

To evaluate this metric, Symantec identifies each distinct attack delivered through the Web, hereafter referred to as Web-based attack, hosted on malicious websites that are detected by intrusion prevention technology. A Web-based attack is any attack that is carried out against a client-side application originating from the Web. Symantec determines the top Web-based attacks by determining the most common attacks carried out against users. Due to the nature of Web-based attacks, the total number of attacks carried out is a good measure of the success and popularity of the attack.

Each attack discussed targets a specific vulnerability or weakness in Web browsers or other client-side applications that process content originating from the Web. These attacks can vary in their delivery methods; some rely on misleading a user into downloading a malicious file, while others occur without any knowledge or interaction by the user.

Countries of origin for Web-based attacks

Symantec identifies the Web-based attacks by country by determining the geographic origin that conducts the attack on computers upon visiting a website. Note that the server hosting the exploit may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects their Web browser to a malicious server in another country.

Data breaches that could lead to identity theft

Symantec identifies the proportional distribution of cause and sector for data breaches that may facilitate identity theft based on data provided by the Open Security Foundation (OSF) Dataloss DB.[222] OSF reports data breaches that have been reported by legitimate media sources and have exposed personal information including name, address, Social Security number, credit card number, or medical history. 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.

Bot-infected computers

Symantec identifies bot-infected computers based on coordinated scanning and attack behavior that is observed in global network traffic. An active bot-infected computer is one that carries out at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days. Attacks are defined as any malicious activity carried out over a network that has been detected by an IDS or firewall.

For an attacking computer to be considered to be participating in coordinated scanning and attacking, it must fit into that pattern to the exclusion of any other activity. This behavioral matching will not catch every bot-infected computer and may identify other malicious code or individual attackers behaving in a coordinated way as a botnet. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers. It will also give insight into the population trends of bot-infected computers, including those that are considered to be actively working in a coordinated and aggressive fashion at some point in time during the reporting period.

[222] http://datalossdb.org

Appendix C—Vulnerability Trends Methodologies

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the Bugtraq™ mailing list,[223] which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis. Symantec also maintains one of the most comprehensive vulnerability databases, currently consisting of over 35,000 vulnerabilities (spanning more than two decades) affecting more than 80,000 technologies from over 11,000 vendors.

Vulnerability classifications

Following the discovery and/or disclosure of a new vulnerability, Symantec analysts gather all relevant characteristics of the new vulnerability and create an alert. This alert describes important traits of the vulnerability, such as the severity, ease of exploitation, and a list of affected products. These traits are subsequently used both directly and indirectly for this analysis.

Vulnerability types

After discovering a new vulnerability, Symantec threat analysts classify the vulnerability into one of 12 possible categories based on the available information. These categories focus on defining the core cause of the vulnerability, as opposed to classifying the vulnerability merely by its effect.

The classification system is derived from the academic taxonomy presented by Taimur Aslam, et al (1996),[224] which provides a full description of the possible values below:

- Boundary condition error
- Access validation error
- Origin validation error
- Input validation error
- Failure to handle exceptional conditions
- Race condition error
- Serialization error
- Atomicity error
- Environment error
- Configuration error
- Design error

Web browser vulnerabilities

This metric compares vulnerability data for major Web browsers, namely: Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, Opera, and Apple Safari. However, in assessing the comparative data, it should be noted that for this report the total number of vulnerabilities in these Web browsers is computed, including both vendor confirmed and non-vendor confirmed vulnerabilities.

[223] The Bugtraq mailing list is hosted by SecurityFocus (http://www.securityfocus.com). Archives are available at http://www.securityfocus.com/archive/1
[224] "Use of a taxonomy of Security Faults": http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf

Previous versions of the Symantec *Global Internet Security Threat Report* have discussed vulnerabilities according to whether they were vendor confirmed or non-vendor confirmed, because vulnerabilities that were not confirmed were also included in the data. This differentiation was important, especially given the disparity in patch times between vendors. However, starting with Volume X of the Symantec *Internet Security Threat Report*, this convention is no longer followed and no differentiation is made between vendor-confirmed vulnerabilities and non-vendor-confirmed vulnerabilities when calculating the total number of vulnerabilities.

Individual browser vulnerabilities are difficult to precisely identify. A reported attack may be a combination of several conditions, each of which could be considered a vulnerability in its own right, which may distort the total vulnerability count. Some browser issues have also been improperly identified as operating system vulnerabilities or vice versa. This is partly due to increased operating system integration that makes it difficult to correctly identify the affected component in many cases. Additionally, some browsers are available for mobile and desktop platforms. Therefore, the following caveats exist for this metric:

- Many vulnerabilities in shared operating system components can be exposed to attacks through the browser. This report enumerates only those vulnerabilities that are known to affect the browser itself where sufficient information is available to make the distinction.
- Vulnerabilities in mobile versions of a browser are only counted if they also affect the desktop version of the browser application. This metric is mainly concerned with evaluating vulnerabilities in desktop Web browsers and not their mobile equivalents.

Window of exposure for Web browsers

The window of exposure is calculated for vulnerabilities associated with the following Web browsers:

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

Symantec records the window of time between the publication of an initial vulnerability report and the appearance of third-party exploit code; this is known as the exploit code development time. The time between the disclosure date of a vulnerability and the release date of an associated patch is known as the patch development time. The time lapse between the public release of exploit code and the time that the affected vendor releases a patch for the affected vulnerability is known as the window of exposure. The average window of exposure is calculated as the difference in days between the average patch development time and the average exploit code development time. During this time, the computer or system on which the affected application is deployed may be susceptible to attack, as administrators may have no official recourse against a vulnerability and must resort to best practices and workarounds to reduce the risk of attacks.

Web browser plug-in vulnerabilities

Browser plug-ins are technologies that extend the functionality of the Web browser. They may be developed by the vendor or by a third party. Some plug-ins provide support for additional application programming languages or environments, such as Java SE or Adobe Flash Player. Others are applications in their own right that run in the browser. Examples of these include ActiveX objects for Internet Explorer, and Mozilla extensions and add-ons.

This metric enumerates publicly documented vulnerabilities that affect browser plug-ins. These vulnerabilities are further classified, when applicable, into general groups of browser plug-in technologies. Symantec makes an effort to identify all vulnerabilities affecting the various classes of browser plug-in.

Vulnerabilities that affect the browser itself are not included in the data for this metric when it is possible to make this distinction. In cases where a Web browser ships with a particular plug-in, vulnerabilities affecting that plug-in will be counted. Although in this case, the plug-in may be included in the default browser installation, it is still considered a separate technology and not a native feature of the browser. Native features are considered to be features intrinsic to the primary function of the browser such as support for HTTP/HTTPS, HTML rendering, JavaScript, and other standards that are commonly implemented in most Web browsers. Technologies such as Java SE and Flash may be common to many Web browsers but they are intended to extend their functionality to support additional types of content and are typically optional components.

The definition of browser plug-ins for this report is limited to technologies that are hosted on the same computer as the browser, and whose installation and configuration is managed through the browser or operating system. This distinguishes them from content that is intended to run inside the browser but is typically external to the browser such as Java SE applets or Flash movies. This content is rendered or executed by a browser plug-in but is not considered to be a plug-in in its own right.

Zero-day vulnerabilities

For the purpose of this metric, a zero-day vulnerability is one for which there is sufficient public evidence to indicate that the vulnerability has been exploited in the wild prior to being publicly known. It may not have been known to the vendor prior to exploitation, and the vendor had not released a patch at the time of the exploit activity. This metric is derived from public sources and the Symantec vulnerability database. This metric is meant to calculate the number of high-profile, publicly documented zero-day vulnerability instances during the relevant reporting periods.

Appendix D—Malicious Code Trends Methodologies

Malicious code trends are based on statistics from malicious code samples reported to Symantec for analysis. The data is gathered from over 130 million client, server, and gateway systems that have deployed Symantec's antivirus products in both consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. Observations in this section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from the two databases described below.

Infection database

The Symantec AntiVirus Research Automation (SARA) technology is a technology that helps detect and eradicate computer viruses. It is used to analyze, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec Antivirus customers.

On average, SARA receives hundreds of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. Symantec then analyzes these suspect files, matching them with virus definitions. An analysis of this aggregate data set provides statistics on infection rates for different types of malicious code.

Malicious code database

In addition to infection data, Symantec Security Response analyzes and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, a historical trend analysis was performed on this database to identify, assess, and discuss any possible trends, such as the use of different infection vectors and the frequency of various types of payloads. In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the Symantec *Global Internet Security Threat Report* to the next.

Geographic location of malicious code instances

Several third-party subscription-based databases that link the geographic locations of systems to IP addresses are used along with proprietary Symantec technology to determine the location of computers reporting malicious code instances. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of malicious code instances.

Malicious code that exploits vulnerabilities

Symantec maintains a malicious code database to analyze and document individual instances of malicious code dating back to 1998. The database includes metadata for classifying malicious code by type, discovery date, and by threat profile, in addition to providing mitigating factors and manual removal steps. Where applicable, this database includes correlations between malicious code instances and vulnerabilities from the Symantec vulnerability database. This capability was used as a basis for the data in this metric. Symantec examined the means by which the malicious code propagated, and counted those that propagate by exploiting vulnerabilities.

Appendix E—Phishing, Underground Economy Servers, and Spam Trends Methodologies

Phishing and spam attack trends in this report are based on the analysis of data captured through the Symantec Probe Network, a system of more than 2.5 million decoy accounts, MessageLabs Intelligence, and other Symantec technologies in more than 86 countries from around the globe. Five billion email connections, as well as over one billion Web requests are scanned per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

The Symantec Probe Network data is used to track the growth in new phishing activity. It should be noted that different monitoring organizations use different methods to track phishing attempts. Some groups may identify and count unique phishing messages based solely on specific content items such as subject headers or URLs. These varied methods can often lead to differences in the number of phishing attempts reported by different organizations.

Symantec Brightmail AntiSpam data is also used to gauge the growth in phishing attempts as well as the percentage of Internet mail determined to be phishing attempts. Data returned includes messages processed, messages filtered, and filter-specific data.

Symantec has classified different filters so that spam statistics and phishing statistics can be determined separately. Symantec Brightmail AntiSpam field data includes data reported back from customer installations providing feedback from antispam filters as well as overall mail volume being processed.

Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not the network layer, where DNS block lists typically operate because SMTP -layer spam filtering is more accurate than network-layer filtering and is able to block spam missed at the network layer. Network layer-filtering takes place before email reaches the enterprise mail server. As a result, data from the SMTP layer is a more accurate reflection of the impact of spam on the mail server itself.

Due to the numerous variables influencing a company's spam activity, Symantec focuses on identifying spam activity and growth projections with Symantec Brightmail AntiSpam field data from enterprise customer installations having more than 1,000 total messages per day. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

This section will provide more detail on specific methodologies used to produce the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warrant additional detail.

Phishing activity by sector

The phishing data in this report are aggregated from a combination of sources including Symantec's sensors, strategic partners, customers and security solutions. Phishing sites are categorized according to the brand being phished and its sector. After phishing data are received, Symantec spoof detection technology is used to verify that the website is a spoof site.

Countries hosting phishing URLs and top targeted sectors

The data for this section is determined by gathering links in phishing email messages and cross-referencing the addresses with several third-party subscription-based databases that link the geographic locations of systems to IP addresses. In this case, Symantec counts phishing URLs as the number of unique IP addresses hosting Web pages used for phishing. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of phishing URLs.

Phishing site top-level domains

The data for this section is determined by deriving the top-level domains of each distinct phishing website URL. The resulting top-level domains are tabulated and compared proportionately.

Automated phishing toolkits

The data in this section is derived from URLs gathered by the Symantec PRN. The URLs are sorted and grouped according to specific patterns indicating they were generated by an automated script or phishing kit. Each phishing kit generates URLs with a distinct signature and can be grouped according to these distinguishing characteristics. The monthly total of each group of URLs indicates the level of use of each automated phishing kit.

Underground economy servers—goods and services available for sale

This metric is based on data that is gathered by proprietary Symantec technologies that observe activity on underground economy servers and collect data. Underground economy servers are typically chat servers on which stolen data, such as identities, credit card numbers, access to compromised computers, and email accounts are bought and sold. Each server is monitored by recording communications that take place on them, which typically includes advertisements for stolen data. This data is used to derive the data presented in this metric. It should be noted that this discussion might not necessarily be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec observed during this period.

Description of goods and services advertised on underground economy servers may vary from vendor to vendor. The following list shows typical goods and services that are found on these servers and general descriptions of each:

- **Bank account credentials**—may consist of name, bank account number (including transit and branch number), address, and phone number. Online banking logins and passwords are often sold as a separate item.
- **Cash out**—a withdrawal service where purchases are converted into true currency. This could be in the form of online currency accounts or through money transfer systems and typically, the requester is charged a percentage of the cashout value as a fee.

- **Credit card information**—includes credit card number and expiry date. It may also contain the cardholder name, Credit Verification Value 2 (CVV2) number, PIN, billing address, phone number, and company name (for a corporate card). CVV2 is a three or four-digit number on the credit card and used for card-not-present transactions such as Internet or phone purchases. This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card.
- **Email accounts**—includes user ID, email address, password. In addition, the account may contain personal information such as addresses, other account information, and email addresses in the contact list.
- **Email addresses**—consists of lists of email addresses used for spam or phishing activities. The email addresses can be harvested from hacking databases, public sites on the Internet, or from stolen email accounts. The sizes of lists sold can range from 1 MB to 150 MB.
- **Full identities**—may consist of name, address, date of birth, phone number, and government-issued number. It may also include extras such as driver's license number, mother's maiden name, email address, or "secret" questions/answers for password recovery.
- **Mailers**—an application that is used to send out mass emails (spam) for phishing attacks. Examples of this are worms and viruses.
- **Proxies**—Proxy services provide access to a software agent, often a firewall mechanism, which performs a function or operation on behalf of another application or system while hiding the details involved, allowing attackers to obscure their path and make tracing back to the source difficult or impossible. This can involve sending email from the proxy, or connecting to the proxy and then out to an underground IRC server to sell credit cards or other stolen goods.
- **Shell scripts**—used to perform operations such as file manipulation and program execution. They can also be used as a command line interface for various operating systems.

Countries of spam origin

The data for this section is determined by calculating the frequency of originating server IP addresses in email messages that trigger antispam filters in the field. The IP addresses are mapped to their host country of origin and the data is summarized by country based on monthly totals. The percentage of spam per country is calculated from the total spam detected in the field.

It should be noted that the location of the computer from which spam is detected being sent is not necessarily the location of the spammer. Spammers can build networks of compromised computers globally and thereby use computers that are geographically separate from their location

Spam delivered by botnets

The data for this section is determined by an analysis of emails that trigger antispam filters and the proportion that is detected as originating from a known botnet. The identity and location of spam-sending botnets that is tracked by Symantec MessageLabs Intelligence knowledge base, and is based on the profile of the spam and its headers as it is being transmitted. Each botnet exhibits a unique profile and the information is tracked accordingly, including its location.

About Symantec

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

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

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

04/10 20959302