Symantec.

Confidence in a connected world.

Symantec Internet Security Threat Report
Trends for 2009

Volume XV, Published April 2010

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).

[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

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

| 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

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.

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.

[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.
[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

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]
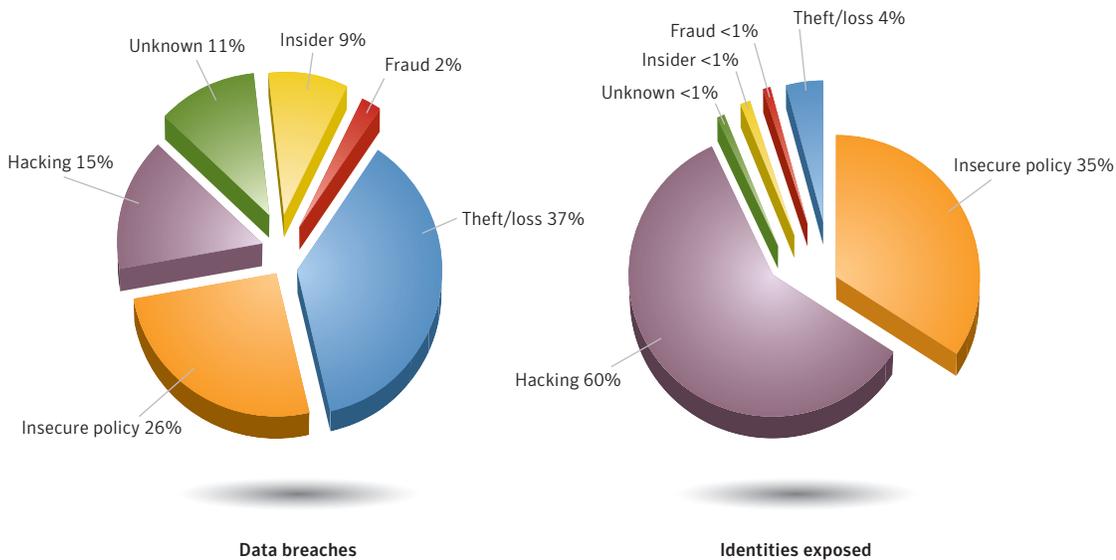

Data breaches   **Identities exposed**

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

[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.
[10] http://www.securityfocus.com/bid/37815
[11] http://news.bbc.co.uk/2/hi/americas/7970471.stm
[12] Due to rounding, percentages might not equal 100 percent.

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.

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, 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.

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.

[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
[15] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf

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

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. Of the Web browsers analyzed by Symantec in 2009, Mozilla® Firefox® had the most reported vulnerabilities, 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]

Overall Rank		Attack	Percentage	
2009	2008		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.

[16] http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0
[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

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 in 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.

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.

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]

[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
[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

Percentage of exposure threats

- Allows remote access
- Exports email addresses
- Exports system data
- Exports user data
- Keystroke logger

2008: Allows remote access 83%, Exports system data 65%, Exports email addresses 61%, Exports user data 78%, Keystroke logger 76%

2009: Allows remote access 98%, Exports user data 89%, Keystroke logger 86%, Exports system data 78%, Exports email addresses 72%

Period

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

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.

2008

2009

Legend:
- "419" type
- Adult
- Commercial products
- Financial
- Fraud
- Health
- Internet
- Leisure
- Political
- Scams
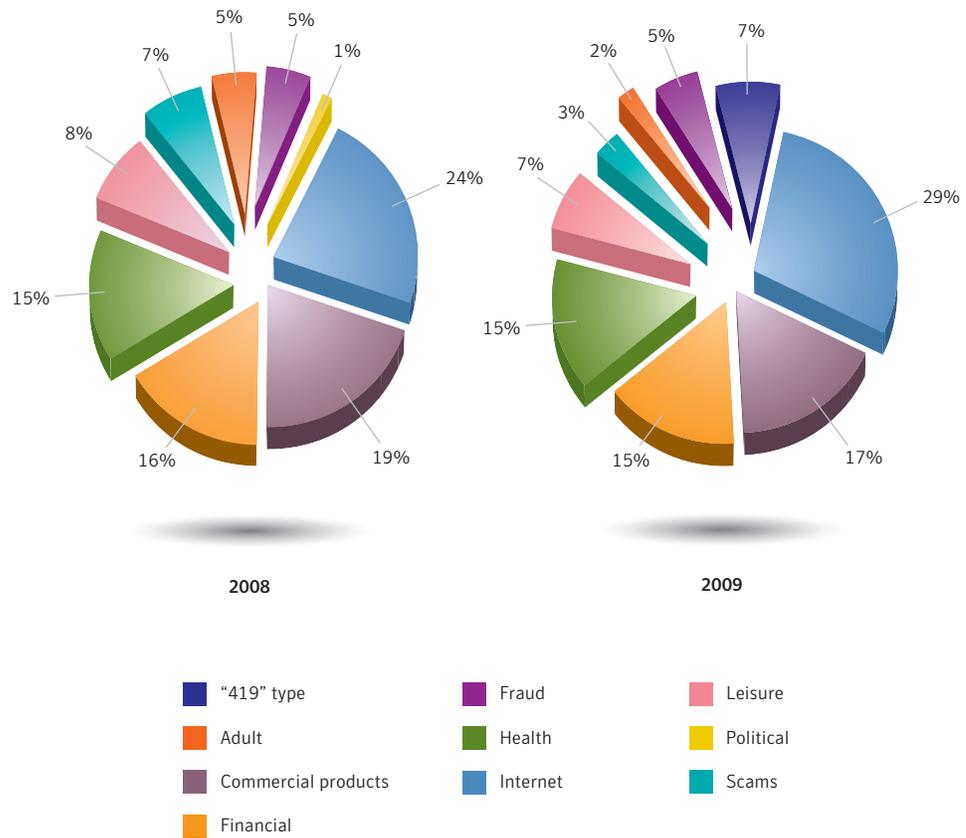
Figure 3. Top spam categories
Source: Symantec

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			Percentage		
2009	2008	Item	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

- 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.

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

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

- 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.

- 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.

- 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™.

- 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.

- 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.

- 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.

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.

- 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.

- 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.

- 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

- 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.

- 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.

- 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.

- 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.

- 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.

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

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