SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Government 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

Gary Kevelson
Global Manager
Symantec Cyber Threat Analysis Program

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

John Stoner
Lead Principal
Symantec Cyber Threat Analysis Program

Scott Thomas
Lead Principal
Symantec Cyber Threat Analysis Program

Volume XV, Published April 2010

Symantec Government Internet Security Threat Report

Contents

Introduction

The Symantec *Government Internet Security Threat Report* provides an annual summary and analysis of trends in attacks, vulnerabilities, malicious code, phishing, and spam as they pertain to organizations in government and critical infrastructure sectors. Where possible, it will also include an overview of legislative efforts to combat these attack patterns and activities. For the purposes of this discussion, government organizations include national, state/provincial, and municipal governments. This report also incorporates data and discussions relevant to threat activity that affects critical infrastructure industries that support or are involved with government and military institutions.

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 Internet Security Threat Report, which gives enterprises and consumers essential information to effectively secure their systems now and into the future. This volume of the Symantec *Government Internet Security Threat Report* will alert readers to current trends and impending threats that Symantec has observed for 2009.

Executive Summary

As has been the case since its inception, the Internet continues to expand and enable new ways of doing business and communicating. While trends such as social networking, cloud computing and virtualization continue to gain traction and are rapidly becoming integral to how business and leisure pursuits are conducted online, these technological advances bring with them additional challenges for the security industry. Notable challenges include the continued growth of persistent threats, the continued evolution of social networking sites as attack and infection vectors, the difficulty of effectively securing emerging technologies, increases in the sophistication of social engineering, and the continued expansion of the underground economy.

Persistent threats are threats that often operate within the shadows, outside of the attention focused on notorious threats such as the Downadup (a.k.a., Conficker) worm.[1] Persistent threats, however, are highly targeted and often use a combination of social engineering and software vulnerabilities to establish footholds within the targeted enterprise. A successfully mounted attack can yield large amounts of intellectual property or other sensitive information. Notable examples of this in 2009 include the attack on the Joint Strike Fighter project,[2] and an attack on a number of non-governmental organizations (NGOs) working in Tibet.[3]

The attacks on the NGOs were dubbed Ghostnet and used a Trojan called gh0st rat that enabled the attackers to infiltrate multiple systems in over 100 countries.[4] Moreover, the source code for gh0st rat is easy to get on underground economy forums and has been proven to be an effective tool for stealing information from compromised computers.[5] Most importantly, though, is that by creating multiple back doors into an organization of interest, attackers could gain access to the agendas of key principals in these NGOs, including their travel plans, negotiating positions, and so on—details that could potentially pose an information and physical security risk.

One of the latest threats identified by Symantec is the Hydraq Trojan (a.k.a., Aurora).[6] This threat uses a zero-day vulnerability in Microsoft® Internet Explorer® to load itself onto a computer. Another method it uses is a social engineering ploy that relies on a maliciously coded PDF sent as an email attachment. Although a number of the command-and-control servers that the Trojan relied on for its propagation are no longer active, additional instances of Hydraq could still exist within an organization's network.[7] While government entities were not specifically targeted in this attack, some critical infrastructure sectors were targeted and such attacks will continue to negatively affect private sector and government organizations until they can be identified and eliminated.

Network protection is not enough to mitigate this type of threat. A comprehensive monitoring program is required to scan all internal and external network traffic. Analysts with an in-depth understanding of persistent threats should be employed and, where necessary, third-party data collectors should be retained to aid in identifying such attacks. In addition to ongoing monitoring and analysis, identifying and securing sensitive and proprietary data within the enterprise is key to protecting the assets of the organization.

[1] 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
[2] http://online.wsj.com/article/SB124027491029837401.html
[3] http://www.forbes.com/2009/03/29/ghostnet-computer-security-internet-technology-ghostnet.html
[4] http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
[5] http://www.symantec.com/connect/blogs/ghostnet-toolset-back-door-click-button
[6] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99
[7] Ibid

Social networking sites should be of particular concern to government organizations. Not only does social networking provide potential attack vectors for threats, such as Koobface,[8] but if network policies and security barriers are not implemented within networks incorporating this collaborative environment, it can create security issues for the organization and its employees. This includes the potential loss of confidential information, bandwidth issues to support operations, and the possible exposure of the organization to liabilities from compliance concerns. One recent example of this occurred in July 2009, when the new head of the British foreign intelligence service was identified publicly by his wife's posts on her profile on a social networking site.[9] Another example is common-interest social networking sites for security personnel. These sites often require members to articulate their security clearance in order to join and group membership is often viewable by anyone.[10]

These problems can be compounded by government organizations having differing responses to social networking. For example, the U.S. Army has issued guidance to its soldiers as well as to civilian employees regarding social networking and what should and should not be disclosed,[11] while the U.S. Marine Corps has banned all access to social networking sites from its network.[12] To effectively manage social networking within government networks, clear policies on access to these sites is required, along with appropriate countermeasures to prevent unauthorized information from being posted. Because these sites are also often accessible from outside of the network environment, stakeholders should establish clear guidelines to users about what should or should not be posted to these sites. They should also develop partnerships to limit sensitive data—such as security clearance data and deployment dates and positions—to ensure the security of data, systems and personnel.

Another issue facing many government organizations is emerging technologies. While new technologies can often drive innovation, reduce costs and increase efficiency across the enterprise, they are equally as often not fully understood from a security perspective and could negatively affect enterprises. For example, organizations moving toward a cloud-computing model should have clear policies on what information is allowed to be uploaded by employees and to monitor it. Clear policies on usage, permissions, and ownership between the organization and the ISP hosting the data should also to be determined.

Virtualization is another ongoing concern for government organizations. Virtualization can be a tremendous benefit for many initiatives, including reducing the physical footprint of the enterprise and, thus, reducing both capital expenditures and energy costs. Virtualization, though, is not a security technology.[13] Many administrators make the mistake of thinking that virtualization has additional security built into it to prevent malicious code from spreading between virtual hosts, or that malicious code cannot transcend a virtual system—which is often not the case. Securing the physical layer of the device is not sufficient; robust security practices also need to be applied to virtual systems as much as to physical systems. This includes employing endpoint security solutions to protect each virtual host.

[8] http://www.symantec.com/connect/blogs/busy-days-koobface-gang
[9] http://www.timesonline.co.uk/tol/news/uk/article6639521.ece
[10] http://www.linkedin.com/groups?gid=95059&trk=anetsrch_name&goback=.gdr_1266009117506_1
[11] http://www.army.mil/-news/2009/07/16/24478-when-using-social-networking-be-mindful-of-personal-opsec/index.html
[12] http://www.wired.com/dangerroom/2009/08/marines-ban-twitter-myspace-facebook/
[13] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-strategic_guide_to_virtualization_20005015-1.en-us.pdf

Another concern is social engineering, which is essentially an attempt to gain access to computers by exploiting human psychology, rather than the attacker having to hack into or physically access the computer.[14] This differs from social networking in that social networking connects individuals by some common interdependency, while social engineering is a threat vector that is used to take advantage of a victim's susceptibility. While social engineering is not a new threat vector, it continues to be an area that gives attackers an avenue into enterprises and is a primary mechanism for getting malicious code such as Trojans onto computers. By making a piece of malicious code seem like an indispensable program—whether that be a codec required to view a video or a fake antivirus program—attackers are able to engineer users to give them access to systems they could not otherwise access.[15] Another example of social engineering is drive-by downloads, where users are lured into visiting websites containing malicious code that is then downloaded onto the users' computer via the browser. Mitigating drive-by attacks includes restricting software to a master software image, restricting users to rights that are below administrative rights, and educating employees about the dangers of visiting unknown or suspect websites.

A final area that continues to be a concern is the flourishing underground economy. While there have been some successful prosecutions of underground economy operators—including the capture and guilty plea of Albert Gonzalez for a number of significant data breaches[16]—highly motivated groups and individuals continue to thrive on underground economy forums. Governments need to ensure that critical and sensitive information is adequately protected, and continued efforts among law enforcement needs to be coordinated to address malicious activity occurring globally. This is especially critical in the absence of an agreed-upon international framework for combating cybercrime.

While it is often difficult to predict the shifting threat landscape, Symantec expects a number of trends to remain prevalent and to grow in the near future. This includes:

- **Social network attacks**—Attackers are expected to target new evolutions of social communities as well as media sharing sites. The goal of these attacks will be to steal personally identifiable information and confidential information by exploiting seemingly normal social networking activities, such as the introduction of new friends looking to connect.
- **Continuing evolution of botnets**—Botnet owners are expected to increase the sophistication and survivability of their botnets to prevent eradication and to secure them against being hijacked by other attackers.
- **Software and platform attacks**—The increase in attacks employing PDF documents will continue to be exploited by attackers. The growing segment of popular development platforms that support open source application program interfaces such as widgets is also a worthy target. For example, Facebook alone supports almost 50,000 widget-type applications.[17] In addition, Microsoft Windows® 7 will likely be an appealing target due to the default security configuration that increases accessibility, but decreases security in order to do so.[18] Finally, the rapid growth of mobile applications will result in increased attacks on mobile consumer devices that target the harvesting of personally identifiable information and confidential account information.

[14] http://www.csoonline.com/article/514063/Social_Engineering_The_Basics
[15] http://www.symantec.com/connect/blogs/misleading-applications-show-me-money
[16] http://news.cnet.com/8301-27080_3-10423008-245.html
[17] http://www.facetime.com/solutions/socialnetworks.aspx
[18] The problem exists with the ability of malicious code to interact and escalate the User Account Control (UAC) settings. The UAC feature debuted with Vista as a security safeguard that would ask users for permissions before application execution.

- **Network Expansion**—Exploits with the potential to initially mask communication channels for attackers will target security gaps within networks, most notably affecting countries with rapidly expanding Internet infrastructures. These countries are emerging as epicenters of attack origin and will need to be monitored more closely for malicious code attacks.

Conclusion

Symantec expects the sophistication of malicious code attacks to continue to evolve using advanced techniques such as code obfuscation and armoring, as well as through the growing complexity of how distinct malicious code samples are increasingly being used to support multistage attacks. Examples include those seen with the introduction of Downadup, as well as the evolution of Hydraq.[19] These trends are placing significant strain on vendors to dedicate the appropriate resources to combat these threats within current product offerings.

Software applications that continue to incorporate additional functionality without establishing technical controls will continue to be leading targets for malicious code writers. Attackers will continue to incorporate these evolving technologies to expand their reach, and government agencies and critical infrastructure organizations need to evolve their threat mitigation strategies to recognize these challenges.

While securing the network is a worthy goal, critical data needs to be identified, controlled, and protected. If an attacker has already established a foothold in the network, data controls might be the only thing left between that data being exposed or remaining secured.

[19] http://www.symantec.com/outbreak/index.jsp?id=trojan-hydraq&inid=us_ghp_link2_ie0day

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 country of origin for attacks targeting the government sector in 2009 was China, which accounted for 14 percent of the total; this was a decrease from 22 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 most common type of attack targeting government and critical infrastructure organizations in 2009 was Web server attacks, accounting for 46 percent of the top 10 attacks.
- In 2009, Symantec documented 14 public SCADA vulnerabilities. This was an increase from 2008 when there were six documented SCADA vulnerabilities.
- 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; this is 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.

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 a back door component, 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, three were worms, of which two were worms that incorporated a back door component, 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; this is an 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 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 website hosts, an increase of 7 percent over 2008 when Symantec detected 55,389 phishing hosts.
- In 2009, 36 percent of all phishing websites 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 URLs 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 government top-level domain that was most spoofed by phishing URLs in 2009 was .go.ro, the top-level domain for websites associated with the government of Romania.
- 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.

Threat Activity Trends

This section of the Symantec *Government 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
- Countries of origin for government-targeted attacks
- Web-based attacks
- Countries of origin for Web-based attacks
- Attacks by type—notable critical infrastructure sectors
- SCADA vulnerabilities
- 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 1), 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 2009	Overall Rank 2008	Country	Percentage 2009	Percentage 2008	2009 Activity Rank: 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

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*.[20] 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.[21]

One of the botnets linked to this ISP was Pandex (a.k.a., Cutwail).[22] 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.[23] 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.[24] 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.

[20] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 18
[21] http://www.ftc.gov/opa/2009/06/3fn.shtm
[22] http://www.symantec.com/security_response/writeup.jsp?docid=2007-042001-1448-99
[23] http://searchsecurity.techtarget.com.au/articles/32685-Rogue-ISP-shutdown-slows-spam-torrent
[24] 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

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. 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.[25]

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.[26] 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*.[27]

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 worm. 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)."[28]

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.[29] 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.[30]

The growing level of malicious code activity affecting Brazil has resulted in the proposal of a new cybercrime bill in the country.[31] The initiative may also be a result of a number high-profile cyber attacks there in recent years.[32] 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.[33]

[25] http://www.symantec.com/connect/blogs/drop-cn-spam
[26] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf
[27] http://www.point-topic.com
[28] http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1_0.pdf : p. 16
[29] http://www.symantec.com/connect/blogs/brazilian-msn-worm-looks-familiar
[30] http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99
[31] http://www.eff.org/deeplinks/2009/07/lula-and-cybercrime
[32] http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/
[33] All figures are in U.S. dollars.

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.[34] 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.

Countries of origin for government-targeted attacks

Malicious code attacks targeting governments on the Web can be motivated by a number of things. Profit is often a motive because governments store considerable amounts of personal identification data that could be used for fraudulent purposes, such as identity theft. Personal data can include names, addresses, government-issued identification numbers, and bank account credentials, all of which can be effectively exploited for fraud by attackers. Government databases also store information that could attract politically motivated attacks, including critical infrastructure information and other sensitive intelligence. It should be noted that attackers often attempt to obscure their tracks by redirecting attacks through one or more servers that may be located anywhere in the world; this means that the attacker may be located somewhere other than the country from where the attacks appear to originate.

China was the top country of origin for attacks that targeted the government sector in 2009, with 14 percent of the total, a decrease from 22 percent in 2008 (table 2). The percentage of government-targeted attacks launched from China was less than a quarter of its percentage for Internet-wide attacks, which accounted for 12 percent of that total in 2009. This indicates that attacks originating from China were not specifically targeting government organizations, but were instead part of more general, widespread attacks.

[34] http://www.point-topic.com

Overall Rank 2009	2008	Location	Percentage 2009	2008
1	1	China	14%	22%
2	2	United States	11%	12%
3	8	Brazil	8%	3%
4	10	Russia	7%	2%
5	12	India	4%	2%
6	6	Italy	3%	4%
7	14	Taiwan	3%	2%
8	7	Germany	3%	4%
9	3	Spain	2%	6%
10	26	Vietnam	2%	1%

Table 2. Top countries of origin for government-targeted attacks
Source: Symantec

In 2009, the United States ranked second for attacks targeting government, with 11 percent of the total, a slight decrease from 12 percent in 2008. This represents less than 10 percent of Internet-wide attacks that originated in the United States, which accounted for 23 percent of the world total. As was the case for China, this indicates that the attacks originating in the United States were not targeting government organizations.

Brazil ranked third in this metric for 2009 and accounted for 8 percent of attacks targeting government organizations, an increase from 3 percent in 2008. Attacks against government organizations accounted for 42 percent of all attacks originating in Brazil. This may suggest that some attackers are specifically targeting government organizations. However, overall malicious activity in Brazil increased significantly in 2009, so it is reasonable to assume that attacks against all infrastructure sectors in Brazil increased as well.

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 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,[35] which accounted for 49 percent of Web-based attacks (table 3). 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,[36] an attack against the Adobe® Reader Collab.getIcon vulnerability,[37] and an attack that exploits a vulnerability in Foxit Reader.[38]

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

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.[39] The previous volume of the Symantec *Global Internet Security Threat Report* noted that attackers are increasingly targeting Adobe Reader.[40] 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.

[35] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153
[36] See http://www.symantec.com/connect/blogs/malicious-code-authors-jump-swine-flu-bandwagon and http://www.securityfocus.com/bid/33751/info
[37] See http://www.symantec.com/connect/blogs/yet-another-pdf-vulnerability-exploited-collabgeticon and http://www.securityfocus.com/bid/34169
[38] 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
[39] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 39
[40] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 30

In 2009, the second most common Web-based attack was associated with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness,[41] which accounted for 18 percent of the global total—a decrease from 30 percent in 2008. 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,[42] to exploit client-side vulnerabilities on a massive scale. 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. 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,[43] 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.

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.[44]

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.

[41] See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or http://www.securityfocus.com/bid/10514
[42] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=1
[43] See. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23291 or http://www.securityfocus.com/bid/33627
[44] See http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2 and http://www.w3schools.com/browsers/browsers_stats.asp

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.[45] 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 4). 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 is 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.[46] All of these factors combined to create a convenient and established launching point for some attackers.

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

[45] 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.
[46] http://www.point-topic.com

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.[47] 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 educating employees about potential security issues and how to prevent becoming a victim.

Attacks by type—notable critical infrastructure sectors

This section of the Symantec *Government Internet Security Threat Report* will focus on the types of attacks detected by sensors deployed in notable critical infrastructure sectors. The ability to identify attacks by type assists security administrators in evaluating which assets may be targeted. In doing so, this may assist them in securing those assets receiving a disproportionate number of attacks. The following sectors will be discussed in detail:

- Government and critical infrastructure organizations
- Government
- Biotech/pharmaceutical
- Health care
- Financial services
- Transportation

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

Government and critical infrastructure organizations

Government and critical infrastructure organizations are the targets of a wide variety of attack types. The most common attack type seen by all sensors in the government and critical infrastructure sectors in 2009 was attacks against Web servers, which accounted for 46 percent of the top 10 attacks (figure 1). SMTP attacks were the second most common, accounting for 24 percent of the top 10 attacks.

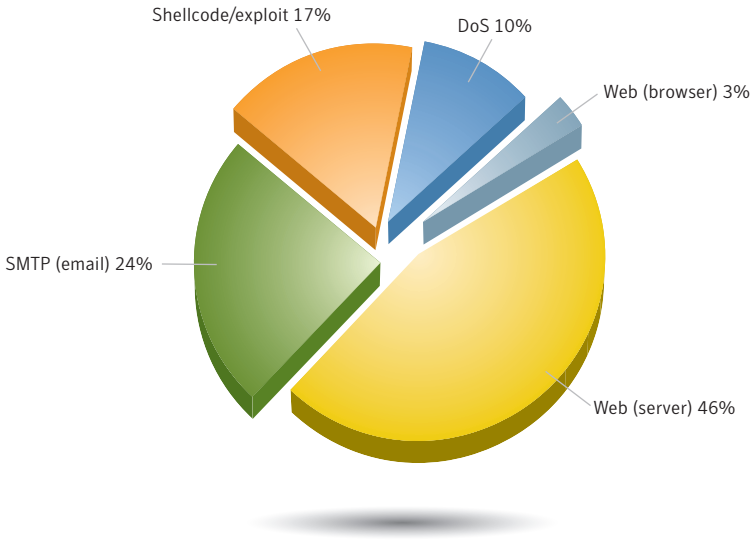

Figure 1. Top attack types, government and critical infrastructure[48]
Source: Symantec

Web servers facilitate a variety of services for government and critical infrastructure sectors, such as hosting publicly available information, customer support portals, and online stores. Some Web servers also host remotely accessible interfaces that employees use to perform routine, job-related tasks from remote locations. Furthermore, a Web server may be a portal to an organization's internal network and database systems.

The wide range of purposes to which Web servers can be deployed provides an enticing target for attackers. Attackers who compromise Web servers may be able to access critical information that could expose customer and employee identities and financial details that may be sold in the underground economy. Attackers can also use the server to host malicious code and launch attacks against legitimate visitors of the website, exploiting the brand loyalty that visitors to the website may have. Compromised Web servers may also have their publicly accessible content defaced to contain lewd material or misleading and false information about the organization.

[48] Due to rounding, percentages may not add up to 100 percent.

The exposure of critical information can be very costly government institutions in terms of public trust and may potentially be a threat to a country's national security. In addition, large legal costs may accrue from locating and prosecuting the perpetrators or in handling lawsuits initiated by people whose information was exposed. Furthermore, attacks that disrupt customer or employee access to services hosted on the server can result in losses to revenue generated by online sales or productivity loss from employees being unable to perform their job-related duties.

SMTP, or simple mail transfer protocol, is designed to facilitate the delivery of email messages across the Internet. Email servers using SMTP as a service are likely targeted by attackers because external access is required to deliver email. While most services can be blocked by a firewall to protect against external attacks and allow access only to trusted users and entities, for email to function effectively for organizations, it has to be available both internally and externally to other email servers. The necessity of allowing both internal and external access increases the probability that a successful attack will improve the attackers' chances of gaining access to the network.

In addition to illegally accessing networks, attackers who compromise email servers may also be attempting to use the email servers to send spam or harvest email addresses for targeted phishing attacks. Because spam can often consume high quantities of unauthorized network bandwidth, these emails can disrupt or overwhelm email services, which could result in DoS conditions. Successful SMTP attacks against government and critical infrastructure organizations could also allow attackers to spoof official government communications and obtain credentials to launch further attacks. These organizations rely heavily on email as a communication tool and, as such, it is essential that email traffic be secured. Symantec recommends that administrators use secure email protocols, deploy antispam and antifraud solutions, and ensure that operating and email solutions are fully patched against all known vulnerabilities.

Top attacks by types, by sectors

In 2009, attacks on email servers were the most common types of attack observed by sensors deployed in the government and financial services sectors (figure 2). These attacks made up 72 percent of the top 10 attacks observed by government sensors and 70 percent in the financial services sector. These attacks also made up a significant percentage of overall attacks on the health care and transportation sectors in 2009, accounting for 29 percent and 30 percent respectively.

As discussed above, successful attacks against email servers may aid attackers in gaining access to internal networks. Attackers can also harvest email addresses for targeted phishing attacks or send spam email in the guise of reputable and legitimate senders. By preying on the trust that spam recipients may have for these organizations, attackers may increase the chances that their emails are accepted as valid. This could, in turn, negatively effect the reputation of the targeted organization.

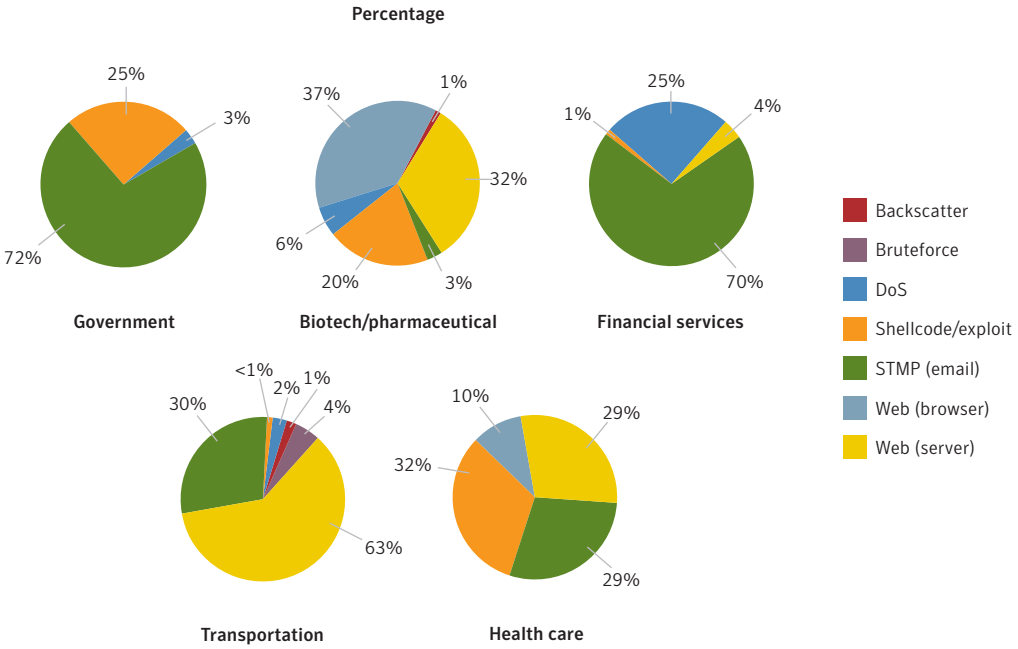

Figure 2. Top attack types, by sector[49]
Source: Symantec

Attacks on Web servers were the most common type of attack observed by sensors deployed in the transportation sector in 2009, and accounted for the second largest percentage of attacks in the biotech/pharmaceutical and health care sectors. As discussed above, attackers who successfully compromise Web servers can gain access to valuable or sensitive information, use the servers as platforms to launch additional attacks, deny access to resources that may be integral to productivity or sales, and perform other malicious actions that can tarnish an organizations reputation.

There was a large decrease in the number of DoS attacks observed during 2009. In 2008, DoS attacks accounted for the largest percentage of attacks in the government, biotech/pharmaceutical, financial services, and transportation sectors by a significant margin. This may indicate that attackers targeting these sectors in 2009 were more interested in discretely leveraging legitimate resources for malicious purposes instead of temporarily disrupting services.

[49] Due to rounding, percentages may not add up to 100 percent.

SCADA vulnerabilities

This metric will examine the SCADA (Supervisory Control and Data Acquisition) security threat landscape. SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes—but is not limited to—power generation, manufacturing, oil and gas, water treatment, and waste management. Therefore, the security of SCADA technologies and protocols is a concern related to national security because the disruption of related services can result in failure of infrastructure and potential loss of life, among other consequences.

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

In 2009, Symantec documented 14 public SCADA vulnerabilities. This is significantly more than the six public SCADA vulnerabilities documented by Symantec in 2008. It should be noted, though, that there were 15 public SCADA vulnerabilities reported in 2007, so the number of public SCADA vulnerabilities reported for this period may just indicate a return to average numbers.

There continues to be a relatively small number of vulnerabilities reported in SCADA technologies in 2009. SCADA is still a very niche area of security research with only a small proportion of the community involved in researching SCADA security vulnerabilities. Symantec believes that there is also a continuing trend towards private or limited disclosure of these vulnerabilities, which means that the number of public vulnerabilities is not representative of the number of vulnerabilities known by SCADA vendors and specialists within the community.

Interestingly, a number of Web application vulnerabilities were discovered in SCADA logic control devices. Multiple cross-site scripting vulnerabilities were discovered in the Rockwell Automation ControlLogix 1756-ENBT/A Ethernet/IP Bridge.[50] The vulnerabilities are present in the Web-based administration interface of the product. Web application vulnerabilities (such as cross-site scripting) are often easy for attackers to discover and exploit. Buffer overflows are also common among the SCADA vulnerabilities reported in 2008 and 2009. Additionally, many SCADA implementations run on Microsoft Windows or other widely deployed operating systems and employ Web applications and browser plug-ins for their functionality. As a result, it is easier for attackers to generalize their existing skills to target these technologies.

The resources and access to technologies remain a challenge for lab testing by security researchers to preemptively discover potential vulnerabilities. However, attackers with malicious intent are able to target live systems and apply their existing knowledge of security vulnerabilities and exploits to these systems. To further illustrate this point, guidelines were published in 2009 on using the Web application testing facilities of Nessus to do vulnerability assessments on control systems.[51]

[50] http://www.securityfocus.com/bid/33683
[51] http://www.digitalbond.com/index.php/2009/07/29/hacking-control-system-web-applications-with-nessus/

In 2009, the Repository of Industrial Security Incidents (RISI) was created to track incidents affecting process control, industrial automation, and SCADA systems.[52] This project is a continuation of the Industrial Security Incidents Database (ISID). This database should provide a valuable resource for the SCADA community to track and verify incidents. As of November 2009, there were 164 incidents in the database. There have been 35 incidents identified in 2009 alone, which contributes to more than 20 percent of all of the incidents to date. These incidents were given a credibility rating of either "Confirmed" or "Likely, but unconfirmed" according to the third-quarter report of the RISI.[53] This trend may be due to increased awareness of SCADA security in the industry and the recent availability of a database for incidents. However, the possibility that incidents are on the rise due to interest shown by malicious parties should not be ruled out.

In September 2009, a former IT consultant was found guilty of tampering with the SCADA systems of an oil and gas exploration company.[54] He was a former consultant who tampered with the systems after being refused a full-time position at the company. This underlines the risk of insider attacks pose to organizations that operate SCADA systems.

Earlier in the year, an attack involving the heating, ventilation, and air conditioning (HVAC) control system at a health clinic was reported.[55] The incident involved a security guard who allegedly compromised computer systems at the clinic and gained access to confidential information and HVAC control systems.[56] It is speculated that disruption of the systems could have posed a safety risk to patients at the clinic. The attacker posted pictures and videos of compromised systems on the Internet, which eventually tipped off authorities and led to the arrest.

SCADA-related incidents can have many different causes. These can include inadvertent incidents due to administrative mistakes or errors during system updates. The incidents described in this section also highlight the threat from insider attacks and hackers seeking attention. There is also the risk of industrial sabotage or state-sponsored attacks aimed at disrupting critical infrastructure. However, in recent years, the SCADA security community has been actively growing and there are a number of security products now available that are aimed at auditing and securing network-accessible devices.

Network-accessible devices may use either common or specialized networking protocols that are prone to attacks that compromise the availability and integrity of affected devices. Therefore, malicious or otherwise malformed network traffic may affect these devices in a manner similar to other network-accessible services within the enterprise. While security researchers have pinpointed vulnerabilities specific to SCADA technologies, there is also a potential threat from vulnerabilities in components connected to SCADA systems. This can include operating systems hosting the SCADA technologies or other components such as database software. Additionally, many SCADA environments employ legacy technologies that are not equipped with mechanisms for authentication or measures to ensure the availability, integrity, and confidentiality of data. These systems may be particularly at risk, especially if they are not fault-tolerant or designed to handle exceptional conditions such as malformed input.

[52] http://www.securityincidents.org/
[53] http://www.securityincidents.org/docs/RISI%20Q1%202009%20Sample%20Analysis%20Report%20Sec.pdf
[54] http://www.networkworld.com/news/2009/092309-contractor-pleads-guilty-to-scada.html
[55] http://www.digitalbond.com/index.php/2009/07/01/control-system-hvac-incident-at-carrel-clinic/
[56] http://dallas.fbi.gov/dojpressrel/pressrel09/dl063009.htm

To limit exposure to attacks, networks running SCADA protocols and devices should be isolated from other networks. These assets should not be connected to the Internet or other networks unless strictly required. If it is not possible to completely limit access by external networks, network access should be strictly regulated by limiting incoming/outgoing traffic to required protocols only. IPSec and VPNs can also be deployed to limit access to authorized networks and individuals. A defense-in-depth strategy should be deployed so that security risks elsewhere in the organization cannot affect the control network. Additional layers of defense should be deployed to protect key assets. Endpoint security products may provide an additional level of protection for hosts within the SCADA environment that run commonly available commercial operating systems.

Securing a SCADA environment may present different challenges than those faced when securing an enterprise. In many cases, it may not be possible to create a test environment for auditing purposes. Furthermore, any disruption of services may be costly or damaging. Therefore, both passive asset discovery as well as vulnerability scanning technologies are best applied to limit the potential for side effects. Antivirus and patch management measures should be undertaken with care and organizations should consult security and control system vendors for support in applying these solutions in a manner that minimizes risk and downtime. Policy compliance and auditing should ensure that configuration benchmarks and security baselines are enforced through the organization and especially on critical control systems. Intrusion detection and prevention systems should be deployed to monitor and prevent attacks on critical systems and networks.

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]

[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.

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 3). This was a decrease from 27 percent in 2008 when the education sector also ranked first.

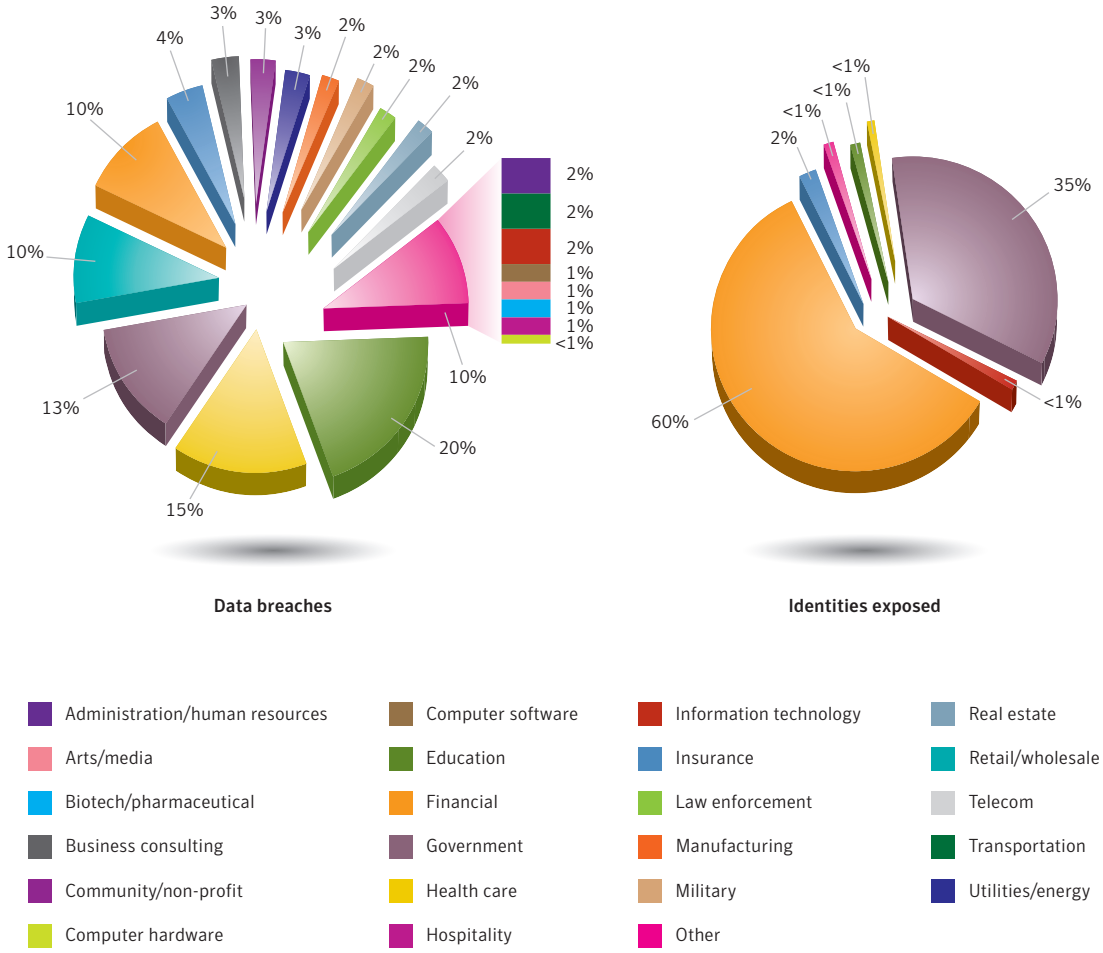

Figure 3. Data breaches that could lead to identity theft by sector and identities exposed by sector[64]
Source: Based on data provided by OSF DataLoss DB

[63] See http://www.privacyrights.org/fs/fs6a-facta.htm and http://www.cms.hhs.gov/HealthPlansGenInfo/12_HIPAA.asp
[64] Due to rounding, percentages might not equal 100 percent.

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.

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.

[65] http://www.osu.edu/osutoday/stuinfo.php
[66] http://findarticles.com/p/articles/mi_hb4365/is_21_42/ai_n47569144/

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 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 attacks on other companies and plead guilty to 19 counts of conspiracy, wire fraud and aggravated identity theft charges in March 2010 and 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.

[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
[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

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 4).

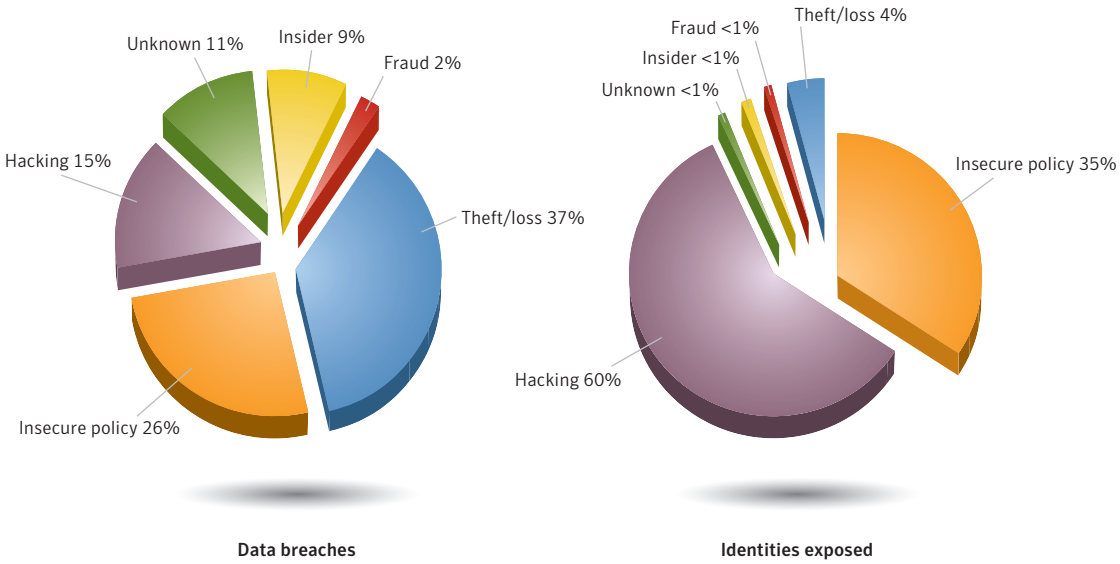

Figure 4. Data breaches that could lead to identity theft by cause and identities exposed[73]
Source: Based on data provided by OSF DataLoss DB

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, discussed below.

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.

[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.

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.

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.

[74] http://datalossdb.org

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 5), 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.

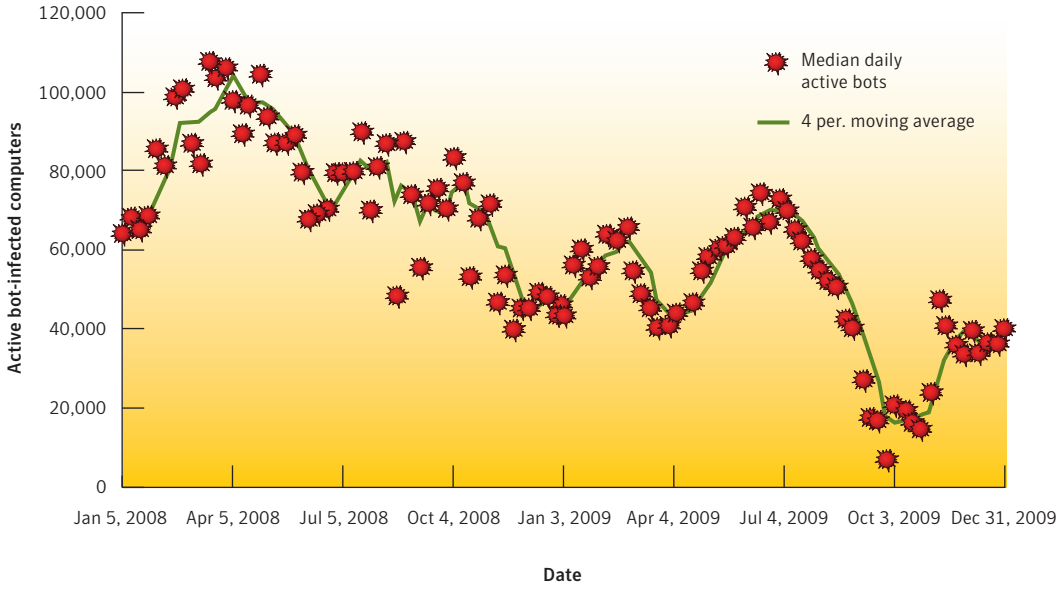

Figure 5. Active bot-infected computers, by day
Source: Symantec

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.[75] 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,[76] Rustock,[77] Ozdok, and Pandex—following the shutdown of two U.S.-based Web hosting companies late in 2008.[78] 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.

[75] See http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf and http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
[76] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
[77] http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99
[78] 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

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,[79] 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,[80] 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,[81] Maazben,[82] Festi, [83] and Rustock—increased their spam output volumes significantly during overlapping one- to three-month periods.[84] Additionally, Symantec observed increased spam output from the Donbot[85] 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 U.S. Federal Trade Commission and the second was an ISP in Latvia.[86] 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.[87] 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.

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, there have not been any further Downadup variants 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.

[79] http://www.symantec.com/security_response/writeup.jsp?docid=2008-123015-3826-99
[80] http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-010717-4209-99
[81] http://www.symantec.com/security_response/writeup.jsp?docid=2007-033016-1857-99&tabid=1
[82] http://www.symantec.com/connect/blogs/evaluating-botnet-capacity
[83] http://www.symantec.com/connect/blogs/festi-botnet-spins-become-one-main-spamming-botnets
[84] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 8–10
[85] http://www.symantec.com/security_response/writeup.jsp?docid=2009-012112-4859-99
[86] http://www.symantec.com/connect/blogs/latvian-isp-closure-dents-cutwail-botnet
[87] 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

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 previously 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.[88] 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.

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 also restrict unauthorized devices such as external portable hard-drives and other removable media.

[88] 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.

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 is encrypted. Organizations should implement a data loss protection (DLP) solution that not only serves to prevent data breaches but they can also mitigate potential data leaks from within an organization. Access to sensitive information should be restricted and organizations should also enforce compliance to information storage and transmission standards such as the PCI standard.[89] 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 was stored were 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.

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

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
- Geolocation by type of malicious code
- Threats to confidential information
- Propagation mechanisms
- 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 6). 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.

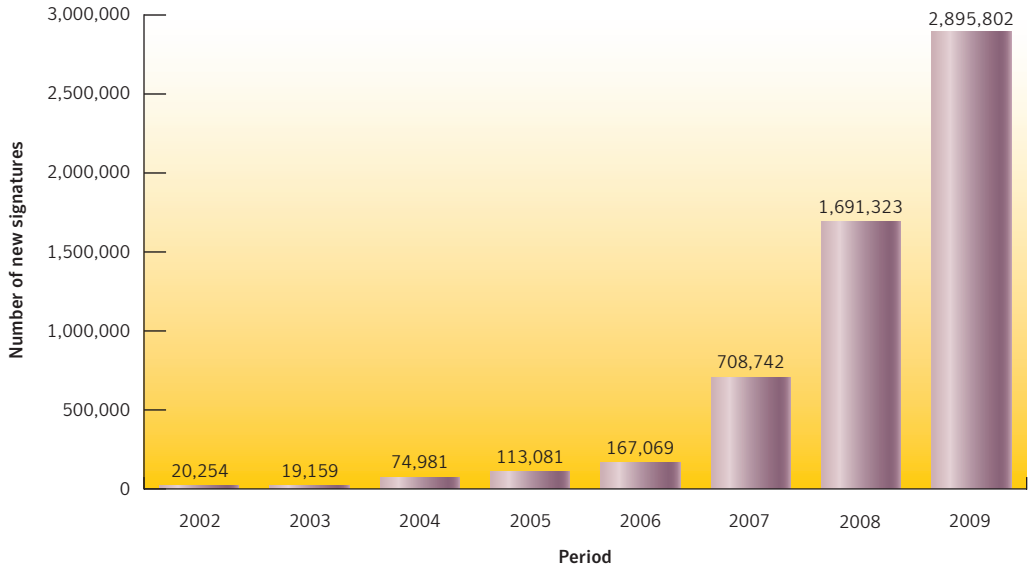

Figure 6. New malicious code signatures
Source: Symantec.

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.[90] 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. [91] 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.[92] 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.[93]

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.[94] 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.

[90] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 10
[91] Singletons are file instances that are seen on only one computer.
[92] http://securitywatch.eweek.com/botnets/playing_god_zeus_diy_botnet_kit_evolves.html
[93] http://www.krebsonsecurity.com/2010/01/money-mules-helped-to-rob-w-va-bank/
[94] Cumulative totals might not equal 100 percent due to rounding.

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.

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 6). 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 6. 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 7). 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 by 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 7. 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.[95] 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.[96]

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 8). 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 8. 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 9). 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.

[95] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf : p. 12
[96] 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 9. 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. India and Brazil are two countries specifically cited as countries expected to increase in their share of malicious activity.[97] 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 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 exposed confidential information or provide remote access. Three of the top 10 new threats directly exposed 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.

[97] 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 7). 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.

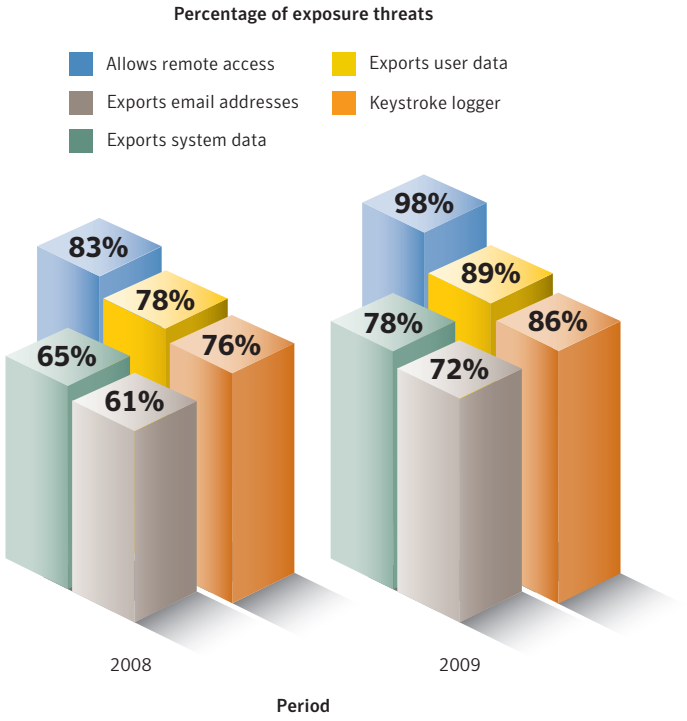

Figure 7. Threats to confidential information, by type
Source: Symantec

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[98], Gammima, Onlinegame,[99] and Lineage[100] 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.

[98] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[99] http://www.symantec.com/security_response/writeup.jsp?docid=2008-011012-0102-99
[100] http://www.symantec.com/security_response/writeup.jsp?docid=2005-011211-3355-99

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.[101] As a result, data should always be transmitted through secure channels such as SSH, SSL, and IPSec.[102]

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.[103] 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 10).[104] 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.

[101] 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.
[102] 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.
[103] 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.
[104] 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 10. 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[105] 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.[106]

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.

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.[107] Increased user awareness and greater vigilance and accuracy for email protection mechanisms may be a factor in this decrease. Another factor

[105] http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99
[106] TCP port 445 is the default port used to run CIFS on TCP.
[107] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 69

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.[108]

One specific example of the propagation of malicious code through email was through the Pandex botnet in 2009.[109] 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—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.

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.[110] 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.

[108] http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf : p. 30
[109] http://www.symantec.com/connect/blogs/2009-year-worth-learning
[110] Address space layout randomization is a security mechanism that randomizes data in memory to prevent the success of attacks that leverage memory corruption vulnerabilities, such as buffer overflows.

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 distinguish phishing from spam-based scams (such as the widely disseminated "419 scam" and other social engineering scams).[111] 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.[112] 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.

[111] 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
[112] http://news.bbc.co.uk/2/hi/technology/6676819.stm

This section will address the following metrics:

- Phishing activity by sector
- Phishing websites by government top-level domain
- Underground economy servers—goods and services available for sale
- Spam by category
- 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.[113] In the United States, eight out of 10 online households now bank online.[114] 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 11). 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.[115] 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 (as is discussed in the concurrent volume of the Symantec *Global Internet Security Threat Report*).[116]

[113] See http://www.ukpayments.org.uk/media_centre/press_releases/-/page/871/ and http://www.comscore.com/press/release.asp?press=2524
[114] http://www.javelinstrategy.com/lp/onlinebankingbillpayBrochure.html
[115] http://www.financialexpress.com/news/us-bank-collapse-toll-touches-94-so-far-this-year/520225/
[116] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf : p. 67

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 11: 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 8). 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 spear phishing 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.[117]

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

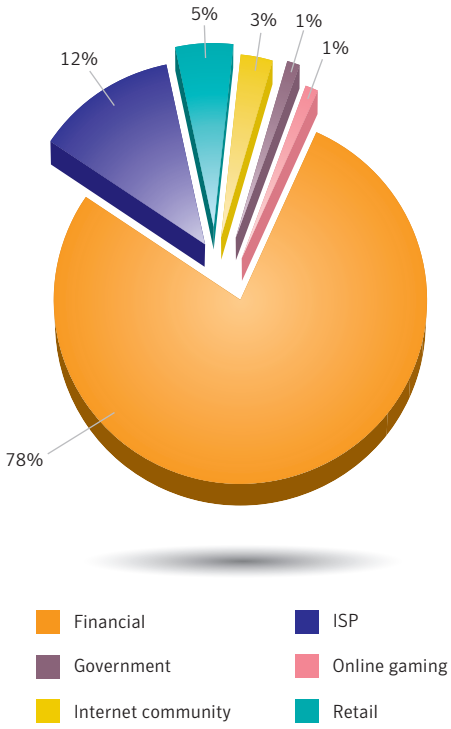

Figure 8: Phished sectors by volume of phishing URLs
Source: Symantec

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.[118] 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.

[118] 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.[119] 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.

Phishing websites by government top-level domains

This metric will assess the distribution of phishing websites that use government top-level domains (TLDs) by country in 2009.[120] Phishing websites may be hosted on domains that are registered to government entities, likely as a result of legitimate servers on these domains that have been compromised. In addition to hosting a phishing website, the compromised server may contain confidential or sensitive information that attackers could potentially access.

It should also be noted that while these phishing websites use government domain names, it is possible that they are not being hosted on government servers and that attackers are using spoofed domains. In addition, the website may be a legitimate site that has been compromised so that end users are being redirected to phishing/malicious sites, which could be an indication that governments are not protecting their TLDs sufficiently against misuse. As a result of this spoofing, it is difficult to assess the use of each country's TLD individually.

There are a number of reasons why phishers may want to use government TLDs for phishing websites. Primary among these is that using a government TLD adds credibility to phishing attacks that spoof government websites. Phishing websites spoofing these sites would likely be successful in the harvesting of personal information because many government agencies typically demand confirmation of identity from citizens in order to provide services, and many governments are providing an increasing number of services online. Furthermore, government websites are often high-traffic sites that attract a lot of attention, thereby making them attractive for phishers to spoof in order to attract a greater number of potential victims.

[119] http://www.coremetrics.com/company/2009/pr12-21-09-online_retail_sales.php
[120] In a domain name, the top-level domain is the part that is furthest to the right. For example, the "com" in symantec.com. There are two types of top-level domains: generic and country specific. Examples of generic domains are com, net, and org, while country-specific top-level domains include .cn for China, and .uk for the United Kingdom, as well as others.

Phishing websites spoofing government agencies would likely do so in order to obtain users' confidential information, which could then be used for identity theft and other fraudulent purposes. One common purpose for attacking this sector is to obtain personal information through fraudulent emails that referred to tax refunds. These attacks have been documented in both Canada and the United States.[121]

The top government TLD detected as being used by phishing lures in 2009 was .go.ro, with 15 percent of the total (table 12). This TLD is used for websites associated with the government of Romania. In 2008, this TLD ranked second and was used by 13 percent of government TLDs that were detected being used by phishing lures. Romania accounted for 1 percent of all malicious activity observed by Symantec on the Internet in 2009, making it the 19th ranked country for this consideration.

Government Top-level Domains Rank	Total Top-level Domains Rank	Top-level Domain	Percentage
1	88	.go.ro	15%
2	97	.go.th	12%
3	103	.go.id	10%
4	109	.gov.br	7%
5	118	.gov.co	6%
6	123	.gov.cn	5%
7	125	.go.kr	5%
8	130	.gov.ph	4%
9	142	.gov.bo	3%
10	145	.gov.in	3%

Table 12. Top government TLDs being used by phishing websites
Source: Symantec

The second most commonly used government TLD for phishing sites was .go.th, with 12 percent of the total. This is the TLD used by the government of Thailand. In 2008, .go.th was the most commonly used government TLD, accounting for 23 percent of the total. In 2009, Thailand ranked 21st for overall malicious activity, with 1 percent of the global total.

In 2009, the TLD for the government of Indonesia, .go.id, was the third-ranked government TLD used in phishing lures, accounting for 10 percent of the total. This is compared to 8 percent in 2008, when it was also the third-ranked government domain globally.

[121] Symantec State of Spam (URL forthcoming) and http://www.phishbucket.org/main/content/view/4135/103/

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.[122]

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 13). 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.[123]

Overall Rank		Item	Percentage		Range of Prices
2009	2008		2009	2008	
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 13. Goods and services advertised for sale on underground economy servers
Source: Symantec

[122] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
[123] 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.[124] 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.[125] 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 enough 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.[126]

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.

[124] 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.
[125] 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/
[126] 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.[127] 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-$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.

[127] 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.[128] 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.[129] 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.[130]

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

[128] http://news.bbc.co.uk/2/hi/8046492.stm
[129] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 76
[130] 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.[131]

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.[132] 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.

[131] http://www.krebsonsecurity.com/2010/01/texas-bank-sues-customer-hit-by-800000-cyber-heist/
[132] 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 9). 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.

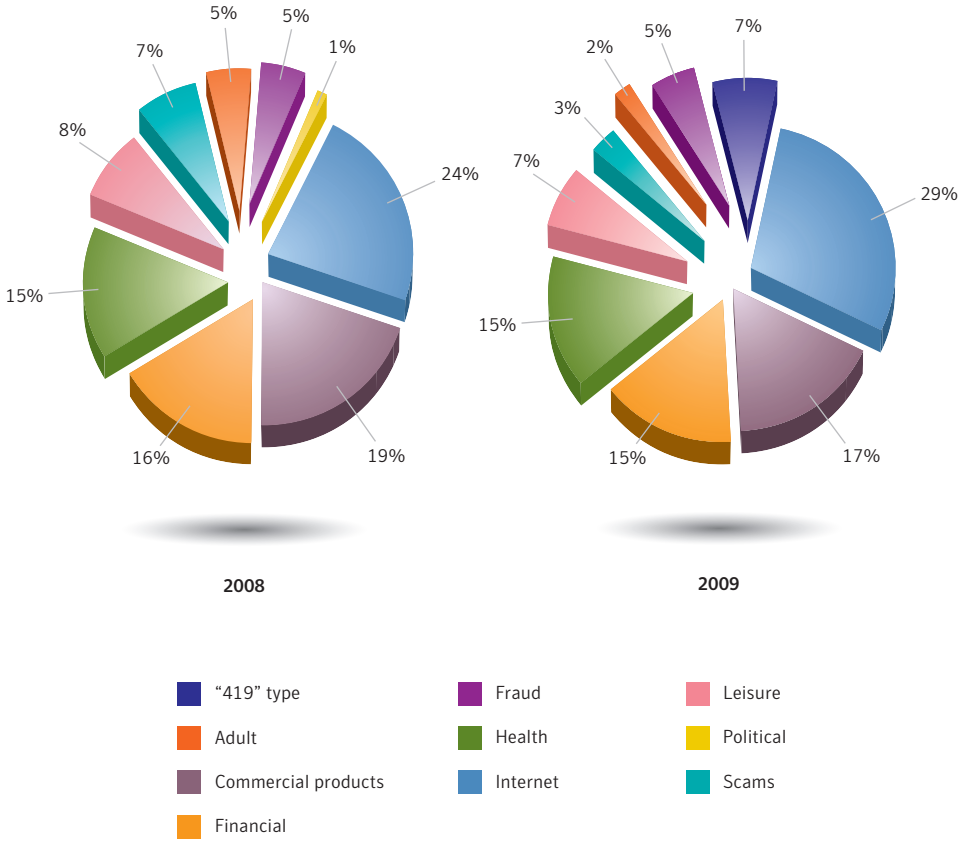

Figure 9. Spam by category
Source: Symantec

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.

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.

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.[133] 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 14). Rustock experienced similar growth, from less than 2 percent of botnet-related spam in 2008 to 18 percent in 2009.

[133] 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

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 14. Percentage of spam from botnets[134]
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.[135] 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 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,[136] making it less susceptible to a single point of failure such as a single rogue ISP.[137]

Other notable botnets that decreased considerably in 2009 were Gheg,[138] Cimbot, and Warezov_stration.[139] 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.

[134] Due to rounding totals may not equal 100 percent.
[135] http://www.ftc.gov/opa/2009/06/3fn.shtm
[136] 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.
[137] http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf : p. 12
[138] http://www.messagelabs.com/mlireport/MLIReport_2009.06_June_FINAL.pdf
[139] http://www.symantec.com/security_response/writeup.jsp?docid=2006-091012-5303-99

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.[140] 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.[141]

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.[142] 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.[143]

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.[144] So-called typo domains and homographic domains should also be monitored. [145] This can be done with the help of companies that specialize in domain monitoring; some registrars also provide this service.

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.

[140] 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.
[141] 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.
[142] Please 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
[143] Cf. http://www.antiphishing.org for information on the latest phishing threats.
[144] "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.
[145] 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".

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.[146] 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.

[146] 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.

Countries of origin for government-targeted attacks

Symantec identifies the country of origin of attacks by automatically cross-referencing source IP addresses of every attacking IP with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

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.

Attacks by type—notable critical infrastructure sectors

Symantec identifies attack types on notable critical infrastructure sectors that are determined by analysis of the IDS attack signatures. Attack types include backscatter, DoS, domain name system (DNS), shellcode/exploit, SMTP, Web (server), and Web (browser).

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.[147] 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 intrusion detection system (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.

[147] http://datalossdb.org

Appendix C—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 *Government 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.

Appendix D—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 the phishing data are received, Symantec spoof detection technology is used to verify that the website is a spoof site.

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.

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.

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 are 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 20970640