SYMANTEC ENTERPRISE SECURITY

symantec™

Confidence in a connected world.

Symantec Government Internet Security Threat Report

Trends for 2008

Volume XIV, Published April 2009

Marc Fossi
Executive Editor
Manager, Development
Security Technology and Response

Eric Johnson
Editor
Security Technology and Response

Trevor Mack
Associate Editor
Security Technology and Response

Dean Turner
Director, Global Intelligence Network
Security Technology and Response

Gary Kevelson
Global Manager
Symantec Cyber Threat Analysis Program

Andrew J. Rogers
Cyber Threat Analyst
Symantec Cyber Threat Analysis Program

Joseph Blackbird
Threat Analyst
Symantec Security Response

Mo King Low
Threat Analyst
Security Technology and Response

Teo Adams
Threat Analyst
Security Technology and Response

David McKinney
Threat Analyst
Security Technology and Response

Stephen Entwisle
Threat Analyst
Security Technology and Response

Marika Pauls Laucht
Threat Analyst
Security Technology and Response

Greg Ahmad
Threat Analyst
Security Technology and Response

Darren Kemp
Threat Analyst
Security Technology and Response

Ashif Samnani
Threat Analyst
Security Technology and Response

Volume XIV, Published April 2009

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. This volume will also provide an overview of observed activities on underground economy servers. 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 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 130 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.

Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 32,000 recorded vulnerabilities (spanning more than two decades), affecting more than 72,000 technologies from more than 11,000 vendors. Symantec also facilitates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 50,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 2.5 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 from around the globe. Over eight billion email messages, as well as over one 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 gives enterprises and consumers the 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 2008.

Executive Summary

The recent global economic crisis has shown how extensively interconnected the global economy has become. The repercussions of failing companies and industries have reached far beyond what many people might have expected. Even experienced practitioners find themselves in uncharted territories. This is spurring changing patterns in both international government and commercial relations. These are expanding in many new ways, some in response to the crisis, and others in support of intended growth.

Similarly, as the Internet and broadband interconnectivity continue to expand, so does the mutual risk inherent in these regional and global relationships.[1] One commonality demonstrated by the report data is that globalization continues to change traditional boundaries and alliances for both attackers and defenders.

Along with these issues, this summary will discuss the increasing sophistication of attackers and their tools against traditional defense mechanisms. In past reports, Symantec has identified that malicious activity has increasingly become Web-based, that attackers are targeting end users instead of computers, and that attackers are able to rapidly adapt their attack activities.[2] These trends are expected to continue, as are the increasingly sophisticated social engineering methods employed by attackers.

Attackers continue to diversify their range of threat options and in some cases have expanded the reach of their operations. As in previous years, Symantec continues to observe increasingly sophisticated attack techniques and the ability of attackers to rapidly adept their methods. In this reporting period, the increasing trend toward interoperability between threats, methods, and multistage attacks has continued. For example, Trojans often install additional back door threats that then download and install bots. These can then enable additional compromises, such as using the compromised computers as spam zombies. All of these threats work in concert to provide a coordinated and sophisticated network of malicious activity.

Threats due to data breaches and theft also continue to be dangerous, especially to governmental and critical infrastructure organizations, since these threats are often exploited for financial gain or intelligence gathering. As attackers refine their methods and consolidate their assets, they may be able to create global networks that support coordinated malicious activity.

Following a traditional network penetration approach sequence, successful Internet Control Message Protocol (ICMP) messages (otherwise known as pings) can be used to produce additional scanning attempts. Successful scans can then produce penetration attempts, which if properly executed can lead to malware deployment. If these attacks are identified as originating from multiple IP addresses, it would indicate more coordinated operations. This scenario would suggest that enhanced security intelligence could help to reduce the risk of further network compromises.

In the global and regional threat patterns observed by Symantec, attacks often target other computers within the same country or region.[3] In this reporting period, Symantec examined the top regions reporting malicious code infections, as well as the types of malicious code causing potential infections in each region. The regionalization of threats can cause differences between the types of malicious code being observed from one area to the next. For example, threats may use certain languages or localized events as part of their social engineering techniques. Because of the different propagation mechanisms used by different

[1] http://www.gao.gov/new.items/d08588.pdf : p. 1
[2] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xiii_gov_09_2008.en-us.pdf : p. 4
[3] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_gov_09_2007.en-us.pdf : p. 10

malicious code types, and the different effects that each malicious code type may have, information about the geographic distribution of malicious code can help network administrators improve their security efforts.

This is illustrated by potential malicious code infections. Symantec examines the top regions reporting potential malicious code infections, as well as the main types of malicious code causing potential infections in each region. Threats that steal confidential information can also be tailored to steal information that is more commonly available in some countries than in others. For instance, Trojans that attempt to steal account information for Brazilian banks are quite common in the Latin America region. Because of the increasing ability for attacks to be quite specifically and geographically targeted, governments should pay close attention to malicious events originating regionally.

The United States remained the top country for overall malicious activity in 2008, and again ranked first for a number of categories within this, including for malicious code, phishing website hosts, and originating attacks. Rounding out the top three countries in overall malicious activity were China and Germany, in second and third place, respectively. One notable change is the rise of Brazil from eighth rank in the previous report to fourth in 2008.

The most obvious explanation for a great deal of the attack patterns is the correlation between high-speed connectivity infrastructure in a country or region and the accompanying amount of malicious activity. An example of this is with spam bots, which typically require excessive bandwidth in order to propagate large amounts of email. Symantec has noted that spam bots are often concentrated in regions with well-established high-speed broadband infrastructures. High-bandwidth capacity networks may also enable attackers to hide attack and bot traffic more effectively, especially through HTTP-based command-and-control servers, where they can effectively hide malicious HTTP bot traffic within legitimate traffic—thus confounding efforts to filter for threats.

In 2008, China surpassed the United States for the largest number of broadband subscribers for the first time. This was likely a significant reason for China's continued prominence in many malicious code categories. Another reason for China's prominence is likely related to the fact that Internet users in China spend more of their leisure time online than users in any other country.[4] Online leisure activities are typically more likely to include activities that are popular and, in many instances, vulnerable attack targets. This includes social networking websites, online gaming sites, forums, blogs, and online shopping sites. Dynamic sites, such as forums are prime targets for attackers using bot-infected computers to host and propagate malicious content, as Web application and site-specific vulnerabilities can put these types of site at risk.

For attacks specifically targeting the government sector, 2008 marked the first time that the United States was not the top country of origin, as it was surpassed by China, which ranked first with 22 percent of the attacks on the government sector. China's rise in this category represented an increase from 8 percent in 2007, when it was ranked fourth. The United States ranked second, and Spain ranked third in this metric.

Malicious code attacks targeting governments on the Web can be motivated by a number of factors. Profit is often a motive because governments store considerable amounts of personal identification data, which if stolen can be exploited for profit. In addition, attacks may also be motivated by attempts to steal government-classified information.

[4] http://www.tnsglobal.com/_assets/files/TNS_Market_Research_Digital_World_Digital_Life.pdf

In 2008, some actions taken by governments were effective at reducing malicious threat activity. China initiated a large security effort to block address websites potentially most susceptible to fraud in an effort to increase online security for users ahead of the 2008 Beijing Olympic Games.[5] Thousands of websites were either shut down or blacklisted as part of this effort, including a substantial number of message forums, which are popular attack targets, as mentioned. Additionally, the Chinese government created a special response team to monitor systems for potential Internet attacks and malicious activity.[6] Lastly, many unlicensed Internet cafés there were also shut down and supervision was tightened on the cafés remaining to help address online security risks associated with the casual use of public computers.[7] Public computers tend to be more susceptible to attacks because of the significant amount of varied traffic on such computers. Public computers are frequently used by a great variety of people for many different activities such as email, online shopping, and gaming. The variety of usage and the likelihood that transient users are less aware of—or concerned with—security makes such computers attractive to attackers. Shutting down the Internet cafés in China thus removed possible channels for malicious activity.

Along with such actions taken by governments, the actions of regional commercial entities' were also effective at reducing security threats, and also demonstrate how interconnected the threat landscape has become. One example occurred when two ISPs in the United States were shut down by their upstream ISPs in September and November 2008. This resulted in a dramatic drop worldwide in both bot command-and-control servers and bot-infected computers. Bot network activity associated with spam distribution decreased substantially after both shutdowns.[8] Unfortunately, these slowdowns were only temporary, as the botnet controllers were able to reestablish their operations elsewhere soon afterward.

In this report period, Symantec also examined the SCADA (Supervisory Control and Data Acquisition) security threat landscape. This includes, but is not limited to, industries such as power generation, manufacturing, oil and gas, water treatment, and waste management. The security of SCADA technologies and protocols can be of concern because the disruption of related services can result in the failure of critical infrastructure. Due to the potential for disruption of critical services, these vulnerabilities may be the target of politically motivated or state-sponsored attacks.

Given their role in critical infrastructure and the severity of potential vulnerabilities, SCADA security is largely a private affair between SCADA vendors and the industries and government agencies that rely on these specific protocols and technologies. As such, Symantec does not report on any private research, although it does report on public research for the Symantec *Government Internet Security Threat Report*. The findings showed that SCADA technologies are affected by many of the same types of vulnerabilities that affect desktop and enterprise software. One noteworthy event took place in September 2008, when a security researcher publicly released exploit code for a SCADA vulnerability because the researcher believed that the reporting vendor did not adequately emphasize the risk of the vulnerability.[9]

During this reporting period, the most common attacks targeting government organizations were denial-of-service (DoS) attacks, representing a continued trend from the previous reporting period. This is problematic because much of the critical infrastructure that performs essential functions in many countries remains at risk to attackers who might choose to exploit operations with this type of attack. Sectors that were most often the subject of DoS attacks included the financial, biotech/pharmaceutical, and transportation industries. Within the transportation industry in particular, DoS attacks were the most

[5] See http://www.vnunet.com/vnunet/news/2207878/china-cracks-web-porn and http://english.gov.cn/2008-03/29/content_931872.htm
[6] http://www.infoworld.com/article/08/04/24/China-worries-hackers-will-strike-during-Beijing-Olympics_1.html
[7] http://www.theglobeandmail.com/servlet/story/RTGAM.20080212.wgtchina0212/BNStory/Technology/home
[8] See http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99 and http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html
[9] http://www.theregister.co.uk/2008/09/08/scada_exploit_released/

common attack by a significant margin, accounting for 74 percent of attacks in 2008, indicating that this industry may have been singled out and specifically targeted for this type of attack. The goal of attackers may be to cause large-scale disruptions in the services that this sector provides or these attacks may simply be out of spite due to dissatisfaction with those services.

The second most common type of attack against government networks was through Simple Mail Transfer Protocol (SMTP), the protocol through which the vast majority of email is transferred. If compromised, SMTP offers attackers an excellent access vector into internal network resources. While compromised email servers could be used to overwhelm networks with unauthorized bandwidth requests, the more likely motivation for compromising email servers lies in their usefulness for sending out spam, as well as harvesting email addresses for targeted phishing attacks. These attacks also offer the ability to spoof government communications and to obtain credentials to launch further attacks. Given how integral—and often trusted—email is that originates with government entities, these types of attacks offer the potential for compromising the integrity of information and communications within governments.

Although dropping from first to second in the attack-by-type ranking for the biotech/pharmaceutical and financial sectors, SMTP-based attacks remain a relatively large threat to these critical sectors, likely because of the value in spoofing their goods and services in attacks. Similarly, the manufacturing sector ranked very high for phishing website hosts, likely due to the fact that attackers rely upon the trust that users often have for well-known commercial brands.

Symantec also measures the level to which government and critical infrastructure organizations may have been compromised and are being used by attackers as launching pads for malicious activity. In 2008, the telecommunications sector again accounted for the highest proportion of attacks of this nature by a significant margin, with an overwhelming 97 percent of the total.

Attackers continue to target the telecommunications sector for a number of reasons. Organizations in this sector include ISPs and Web-hosting companies, which often have a large number of Internet-facing computers and broadband connections. In 2008, the majority of attacks against this sector were shellcode exploits.[10] This may indicate that attackers are attempting to take control of computers in this sector to use them to conduct malicious activity. Compromises to the servers or networks of these companies would also potentially expose a great number of their customers to a range of malicious attacks.

Moreover, governments and critical infrastructure organizations rely on the availability of public communication networks and the telecommunication sector for day-to-day operations. Since telecommunications organizations have a certain amount of control on the flow of data through networks, successful compromises of these networks could give attackers the ability to compromise targeted computers inside specific governmental or critical infrastructure organizations.

As mentioned, attacks targeting these large government repositories are often motivated by profit since governments store considerable amounts of personal identification that, if fraudulently obtained, can be sold on underground economy servers. This can also include sensitive information such as patent data, scientific research, and technology exports—all of which would be valuable information that could be sold to competing companies or other governments.

[10] Shellcode is a small piece of code used as the payload in the exploitation of a vulnerability.

One important and rising area of concern to governments is the increased use (and capacity) of removable media over the past few years. In 2008, 66 percent of potential malicious code infections propagated as shared executable files, up significantly from 44 percent in 2007. Shared executable files are the propagation mechanisms employed by viruses and some worms to copy themselves onto removable media. The 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 exploits developed for floppy disks can be easily modified for current removable media devices. Increasing the danger of this resurgence is that many organizations lack effective security measures to protect against such dangers. In a recent study, 59 percent of employees admitted to taking company information—such as email addresses, contact information of customers, employee records, and financial records—when leaving the organization.[11] Of those who admitted to taking data, 53 percent downloaded information onto a CD or DVD, 42 percent took data using a USB drive, and 38 percent sent attachments to a personal email account.

For data breaches that could lead to identity theft, the government sector continued to be prominent again in 2008, ranking second in both the number of breaches, with 20 percent, and in the number of identities exposed, with 17 percent. One example of a breach in 2008 occurred when confidential information on six million Chilean people was exposed after being illegally obtained from government databases by a hacker, who then publicly posted the information.[12] Although it would be unrealistic to think that all of this data would be exploited, the potential profit for the perpetrators of the attack is still substantial; for example, in 2008 Symantec observed advertised prices for full identities on underground economy servers for as much as $60 each.[13]

Symantec also assesses the distribution of phishing websites that use government top-level domains (TLDs).[14] In 2008, Thailand’s TLD accounted for the highest amount of phishing sites, followed by Romania and then Indonesia. As with most phishing attacks, profit seems to be the primary reason for phishing attacks using government TLDs. The more credible a phishing attack can appear, the more likely it is to succeed. People tend to trust that the content they are presented with on government websites is valid. Also, many governments are putting an increasing amount of services online and, as with online banking, people are becoming accustomed to providing sensitive information in online forms in order to receive services. Attackers may also embed these websites with malicious code designed to compromise the computers of any subsequent site visitors. The compromised computers could then be mined for any worthwhile data or used as a bot to send out spam and mount phishing campaigns. Social engineering exploits such as these are becoming very sophisticated and demonstrate the continued trend noted by Symantec toward focused attacks on end users. For example, in 2008, 95 percent of attacked vulnerabilities were identified as client-side vulnerabilities as opposed to server-side vulnerabilities.

Trends point to a maturing and self-sustaining market within the online underground economy, as fraud and identity theft continue to evolve. Within this, targeted phishing attacks on government users will likely remain popular due to the wealth of information data government databases contain and the potential to convert this data into profit through fraud. The valuation of the underground economy is a reliable indicator of the degree of compromise of information systems and networks throughout the world, and serves as a warning sign for government and critical infrastructure networks

[11] http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01

[12] See http://news.bbc.co.uk/1/hi/world/americas/7395295.stm and http://www.msnbc.msn.com/id/23678909/

[13] All figures are provided in U.S. dollars

[14] 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.

In 2008, Symantec observed heightened levels of malicious activity with specific increases in phishing, spam, bot networks, Trojans, and zero-day attacks. These threats coupled with the increased sophistication and coordinated activities of attackers may have further implications for government and critical infrastructure organizations, who should be particularly concerned with the ability of malicious code developers to target specific entities and websites.

Attackers will continue to rapidly adapt and engineer new techniques and strategies to circumvent security measures, and the identification, analysis, and trending of these techniques across the threat landscape are essential. It is becoming increasingly clear that security groups need to cooperate to develop effective countermeasures and intelligence to respond to the evolving threat landscape. The large increase in the number of new malicious code threats, coupled with the use of the Web as a distribution mechanism, also demonstrates the growing need for more responsive and cooperative security measures.

Highlights

Threat Activity Trends Highlights

- During this reporting period, 23 percent of all malicious activity measured by Symantec in 2008 was located in the United States; this is a decrease from 26 percent in 2007.
- The United States was the top country of attack origin in 2008, accounting for 25 percent of worldwide activity; this is a decrease from 29 percent in 2007.
- Telecommunications was the top critical infrastructure sector for malicious activity in 2008, accounting for 97 percent of the total; this is a slight increase from 96 percent in 2007 when it also ranked first.
- In 2008, Symantec documented six public SCADA vulnerabilities. This was a decrease from 2007 when there were 15 documented SCADA vulnerabilities.
- The education sector accounted for 27 percent of data breaches that could lead to identity theft during this period, more than any other sector and a slight increase from 26 percent in 2007.
- The financial sector was the top sector for identities exposed in 2008, accounting for 29 percent of the total and an increase from 10 percent in 2007.
- In 2008, the theft or loss of a computer or other data-storage devices accounted for 48 percent of data breaches that could lead to identity theft and for 66 percent of the identities exposed.
- Symantec observed an average of 75,158 active bot-infected computers per day in 2008, an increase of 31 percent from the previous period.
- China had the most bot-infected computers in 2008, accounting for 13 percent of the worldwide total; this is a decrease from 19 percent in 2007.
- Buenos Aires was the city with the most bot-infected computers in 2008, accounting for 4 percent of the worldwide total.
- In 2008, Symantec identified 15,197 distinct new bot command-and-control servers; of these, 43 percent operated through IRC channels and 57 percent used HTTP.
- The United States was the location for the most bot command-and-control servers in 2008, with 33 percent of the total, more than any other country.
- The top Web-based attack in 2008 was associated with the Microsoft® Internet Explorer® ADODB.Stream Object File Installation Weakness vulnerability, which accounted for 30 percent of the total.
- The United States was the top country of origin for Web-based attacks in 2008, accounting for 38 percent of the worldwide total.
- The United States was the country most frequently targeted by denial-of-service attacks in 2008, accounting for 51 percent of the worldwide total.
- The top country of origin for attacks targeting the government sector was China, which accounted for 22 percent of the total. This was an increase from 8 percent in 2007.
- The most common type of attack this period targeting government and critical infrastructure organizations was denial-of-service attacks, accounting for 49 percent of the top 10 in 2008.

Malicious Code Trends Highlights

- In 2008, the number of new malicious code signatures increased by 265 percent over 2007; over 60 percent of all currently detected malicious code threats were detected in 2008
- Of the top 10 new malicious code families detected in 2008, three were Trojans, three were Trojans with a back door component, two were worms, one was a worm with a back door component, and one was a worm with back door and virus components.
- Trojans made up 68 percent of the volume of the top 50 malicious code samples reported in 2008, a minor decrease from 69 percent in 2007.
- Five of the top 10 staged downloaders in 2008 were Trojans, two were Trojans that incorporated a back door component, one was a worm, one of was a worm that incorporated a back door, and one was a worm that incorporated a virus component.
- In 2008, 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 declined to 83 percent in 2008; this is a decrease from 91 percent in 2007, although such threats remained the most prevalent exposure type.
- In 2008, 78 percent of threats to confidential information exported user data and 76 percent had a keystroke-logging component; these are increases from 74 percent and 72 percent, respectively, in 2007.
- Propagation through executable file sharing continued to increase in 2008, accounting for 66 percent of malicious code that propagates—up from 44 percent in 2007.
- One percent of the volume of the top 50 malicious code samples modified Web pages in 2008, down from 2 percent in 2007.
- The percentage of documented malicious code samples that exploit vulnerabilities declined substantially, from 13 percent in 2007 to 3 percent in 2008.
- In 2008, eight of the top 10 downloaded components were Trojans, one was a Trojan with a back door component, and one was a back door.
- Malicious code that targets online games accounted for 10 percent of the volume of the top 50 potential malicious code infections, up from 7 percent in 2007.

Phishing, Underground Economy Servers, and Spam Trends Highlights

- The majority of brands used in phishing attacks in 2008 were in the financial services sector, accounting for 79 percent, down slightly from 83 percent identified in 2007.
- The financial services sector accounted for the highest volume of phishing lures during this period, with 76 percent of the total; this is considerably higher than 2007, when the volume for financial services was 52 percent.
- In 2008, Symantec detected 55,389 phishing website hosts, an increase of 66 percent over 2007, when Symantec detected 33,428 phishing hosts.
- In 2008, 43 percent of all phishing websites identified by Symantec were located in the United States; this is considerably less than 2007, when 69 percent of such sites were based there.
- The most common top-level domain used in phishing lures detected in 2008 was .com, accounting for 39 percent of the total; it was also the highest ranking top-level domain in 2007, when it accounted for 46 percent of the total.
- The top government top-level domain that was detected as being used by phishing lures in 2008 was .go.th, the TLD for websites associated with the government of Thailand.
- One particular automated phishing toolkit identified by Symantec was responsible for an average of 14 percent of all phishing attacks during 2008.
- Credit card information was the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 32 percent of all goods and services; this is an increase from 2007 when credit card information accounted for 21 percent of the total.
- The United States was the top country for credit cards advertised on underground economy servers, accounting for 67 percent of the total; this is a decrease from 2007 when it accounted for 83 percent of the total.
- The most common type of spam detected in 2008 was related to Internet- or computer-related goods and services, which made up 24 percent of all detected spam; in 2007, this was the second most common type of spam, accounting for 19 percent of the total.
- Symantec observed a 192 percent increase in spam detected across the Internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008.
- In 2008, 25 percent of all spam recorded by Symantec originated in the United States, a substantial decrease from 45 percent in 2007, when the United States was also the top ranked country of origin.
- In 2008, bot networks were responsible for the distribution of approximately 90 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 2008 that are of interest to governments and those in the critical infrastructure sector. The malicious activity discussed in this section not only includes threat activity, but also phishing, 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) 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
- Malicious activity by critical infrastructure sectors
- Top countries of origin for government-targeted attacks
- Attacks by type—notable critical infrastructure sectors
- SCADA vulnerabilities
- Data breaches that could lead to identity theft
- Data breaches that could lead to identity theft, by sector
- Data breaches that could lead to identity theft, by cause
- Bot-infected computers
- Bot command-and-control servers
- Top Web-based attacks
- Top countries of origin for Web-based attacks
- 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 website hosts, malicious code reports, spam zombies, and attack origin. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically more stable connections. The top three countries in this metric—the United States, China, and Germany—all have extensively developed and growing broadband infrastructures.[15] China, which passed the United States for the largest number of broadband subscribers for the first time in 2008, has 21 percent of the worldwide broadband subscriber total with 83.3 million subscribers. The United States is second with 20 percent, while Germany is fourth with 6 percent. Each country also experienced a growth of over 20 percent in broadband subscribers from 2007.

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

In 2008, the United States was the top country for overall malicious activity, making up 23 percent of the total (table 1). This is a decrease from 2007 when the United States was also first, with 26 percent. Within specific category measurements, the United States ranked first in malicious code, phishing website hosts, and attack origin.

2008 Rank	2007 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	United States	23%	26%	1	3	1	2	1
2	2	China	9%	11%	2	4	6	1	2
3	3	Germany	6%	7%	12	2	2	4	4
4	4	United Kingdom	5%	4%	4	10	5	9	3
5	8	Brazil	4%	3%	16	1	16	5	9
6	6	Spain	4%	3%	10	8	13	3	6
7	7	Italy	3%	3%	11	6	14	6	8
8	5	France	3%	4%	8	14	9	10	5
9	15	Turkey	3%	2%	15	5	24	8	12
10	12	Poland	3%	2%	23	9	8	7	17

Table 1. Malicious activity by country
Source: Symantec Corporation

The slight decrease in overall malicious activity for the United States can be attributed to the drop in spam zombies there. This is likely due to the shutdown of two U.S.-based Web hosting companies that were allegedly hosting a large number of bot C&C servers associated with spam distribution bot networks (botnets).[16] Spam activity decreased worldwide after both shutdowns. In one case, Symantec observed a 65 percent decrease in spam traffic in the 24 hours that followed.[17] Both companies allegedly hosted a large number of bot C&C servers for several large spam botnets: Srizbi,[18] Rustock,[19] and Ozdok (Mega-D).[20] Spam zombies that lack a critical command system are unable to send out spam.

China had the second highest amount of overall worldwide malicious activity in 2008, accounting for 9 percent; this is a decrease from 11 percent in the previous reporting period. Along with the fact that China has the most broadband subscribers in the world, the amount of time spent online by users there could contribute to the high percentage of malicious activity in China. The longer a user is online, the longer the computer is exposed to malicious attack or compromise, and Internet users in China spend more of their leisure time online than users in any other country.[21] Online leisure activities are also typically more likely to include activities on sites that may be vulnerable to attacks. This includes social networking websites, online gaming sites, forums, blogs, and online shopping sites. Dynamic sites, such as forums, for example, are prime targets for attackers using bot-infected computers to propagate and host malicious content since Web application and site-specific vulnerabilities can put these types of site at risk.

[16] http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html
[17] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf
[18] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
[19] http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99
[20] http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99
[21] http://www.tnsglobal.com/_assets/files/TNS_Market_Research_Digital_World_Digital_Life.pdf

The slight drop in China's percentage of malicious activity in 2008 was mainly due to the drop in phishing website hosts and bot-infected computers. China dropped from third for phishing website hosts in 2007 to sixth in 2008, with just under 3 percent of the global total; and, although China maintained its top ranking for bot-infected computers, its global share in this regard decreased from 19 percent in 2007 to 13 percent in 2008.

One possible cause for the decreases may be national initiatives to block websites potentially most susceptible to fraud in an effort to increase online security for users ahead of the 2008 Beijing Olympic Games. Thousands of websites were either shut down or blacklisted as part of this effort, including a substantial number of message forums,[22] which, as noted previously, are popular targets of attack from Web application and site-specific vulnerabilities. Thus, any reduction in the number of bot-infected computers should result in a corresponding drop in other attack activity categories, such as spam zombies, because these are often associated with bot-infected computers. China dropped from third in spam zombies in 2007, with 7 percent of the worldwide total, to fourth and 6 percent in 2008.

Another factor that may have contributed to the lower percentage of bot-infected computers in China in 2008 was that many unlicensed Internet cafés there were also shut down and supervision was tightened on the remaining cafés to help address online security risks associated with the casual use of public computers.[23] Public computers tend to be more susceptible to attacks because of the significant amount of varied traffic on such computer terminals. Public computers are frequently used by a great variety of people for many different activities such as email, online shopping, and gaming. The variety of usage and likelihood that transient users are less aware of—or concerned with—security makes such computers attractive to attackers.

In 2008, Germany again ranked third with 6 percent of all Internet-wide malicious activity, down slightly from 7 percent in 2007. In both years, Germany ranked highly in spam zombies and hosting phishing websites—activities that are often associated with bot networks. In 2008, Germany ranked fourth for bot C&C servers, with 5 percent of the total. This high number of bot C&C servers likely indicates that botnets are prominent in Germany, which would contribute to the high amount of overall malicious activity originating there. Also, spam zombies are often focused in regions with high broadband penetration and bandwidth capacity because these conditions facilitate sending out large amounts of spam quickly.

It is reasonable to expect that the United States, China and Germany will continue to outrank other countries in this measurement as they have done so for the past several reports. Beyond these three, however, countries such as Brazil, Turkey, Poland, India, and Russia are expected to continue to increase their share of overall malicious activity because they all have rapidly growing Internet infrastructures and growing broadband populations.[24] Countries that have a relatively new and growing Internet infrastructure tend to experience increasing levels of malicious activity until security protocols and measures are improved to counter these activities.

[22] See http://www.vnunet.com/vnunet/news/2207878/china-cracks-web-porn and http://english.gov.cn/2008-03/29/content_931872.htm
[23] http://www.theglobeandmail.com/servlet/story/RTGAM.20080212.wgtchina0212/BNStory/Technology/home
[24] http://www.point-topic.com

Malicious activity by critical infrastructure sectors

This metric will evaluate the amount of malicious activity originating from computers and networks that are known to belong to government and critical infrastructure sectors. To measure this, Symantec cross-references the IP addresses of known malicious computers with Standard Industrial Classification (SIC) codes[25] that are assigned to each industry and provided by a third-party service.[26] Symantec has compiled data on numerous malicious activities that were detected originating from the IP address space of these organizations. These activities include bot-infected computers, hosting phishing websites, spam zombies, and attack origins.

This metric indicates the level to which government and critical infrastructure organizations may have been compromised and are being used by attackers as launching pads for malicious activity. These attacks could potentially expose sensitive and confidential information, which could have serious ramifications for government and critical infrastructure organizations. Such information could be used for strategic purposes in the case of state- or group-sponsored attacks, especially since attackers who use compromised computers for malicious activity can mask their actual location.

In 2008, 97 percent of all malicious activity originating from critical infrastructure sectors originated from telecommunications organizations (table 2). This was an increase from 2007 when telecommunications accounted for 96 percent of the total. For each of the malicious activities in this metric, telecommunications ranked first by a significant margin.

2008 Rank	2007 Rank	Sector	2008 Percentage	2007 Percentage
1	1	Telecommunications	97%	96%
2	2	Manufacturing	1%	2%
3	3	Financial services	<1%	1%
4	4	Health care	<1%	<1%
5	5	Transportation	<1%	<1%
6	6	Utilities/energy	<1%	<1%
7	7	Military	<1%	<1%
8	8	Agriculture	<1%	<1%
9	9	Biotech/pharmaceutical	<1%	<1%
10	10	Law enforcement	<1%	<1%

Table 2. Malicious activity by critical infrastructure sector
Source: Symantec

[25] SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more, on this, please see http://www.sec.gov

[26] http://www.digitalenvoy.net

Attackers may be targeting the telecommunications sector for a number of reasons. Organizations in this sector include ISPs and Web-hosting companies and they often have a large number of computers that are directly connected to the Internet. These publicly accessible computers may present more opportunities for attackers to compromise because they do not have to break into a network to gain access to them. Organizations in this sector have a challenging task to manage these large numbers of Internet-facing computers and, hence, computers in telecommunications organizations likely represent attractive targets for attackers. As such, this likely contributes to the high amount of malicious activity originating from this sector. Also, Symantec observed that 84 percent of attacks against the telecommunications sector were shellcode exploits,[27] which may indicate that attackers are attempting to take control of computers in this sector and use them to conduct malicious activity.

Attackers may view telecommunications organizations as excellent platforms for launching subsequent attacks because organizations within this sector are likely to have extensive broadband infrastructures with high-bandwidth and high-traffic networks. This would enable an attacker to carry out large attacks, such as DoS attacks to disrupt services, which deny access to organizations/individuals that subscribe to their services, or other malicious activity, such as relaying spam. This is illustrated by the high percentage of spam zombies and bot-infected computers found in the telecommunications sector. High-bandwidth capacity networks may also allow an attacker to hide attack and bot traffic more effectively, especially for HTTP-based bot C&C servers, where HTTP bot traffic is virtually indistinguishable from regular traffic, making it difficult to filter.

Since organizations in the telecommunications sector likely have numerous servers, once an attacker gains access to the organization, he or she can potentially infect all websites that are hosted on those servers with malicious code for Web-based attacks, or compromise them for phishing attacks or malicious code delivery systems. In a recent example, attackers were able to gain access to a bill payment service website through the Internet domain registry and reroute all traffic to malicious sites hosted on servers in Ukraine.[28]

Government and critical infrastructure organizations rely on the availability of public communication networks and the telecommunication sector for day-to-day operations. Since telecommunications organizations typically control the flow of data through networks, attackers may compromise strategically located computers inside organizations. Computers within telecommunications organizations may effectively serve as platforms from which attacks can be launched against organizations served by telecommunications firms because they provide communications for other sectors as well, including government. As such, attackers who are seeking confidential or sensitive information may specifically target this sector. Successful compromise of computers in the telecommunications sector could allow an attacker to eavesdrop on or disrupt key communications in other sectors.

The manufacturing sector was the origin of the second highest amount of malicious activity during 2008, accounting for 1 percent of the total. This was a decrease from 2007, when it accounted for 2 percent of the total. Organizations in the manufacturing sector invest large amounts of time and money into research and development into new methods and products. As stated in the **“SCADA vulnerabilities”** discussion below, malicious activity in the manufacturing sector can be a national security concern due to the repercussions of disruptions to critical infrastructure. In this highly competitive sector, many organizations use websites as a tool to market and sell their products online. Attackers likely rely upon the trust that users

[27] Shellcode is a small piece of code used as the payload in the exploitation of a vulnerability.
[28] http://www.csoonline.com/article/474365/CheckFree_Warns_Million_Customers_After_Hack

have for these brands, as the manufacturing sector ranked high for phishing website hosts. Once an attacker compromises a manufacturer's website, visitors thinking they are browsing on a legitimate site may become victims of malicious activity such as downloaded Trojans or keystroke loggers.

Top countries of origin for government-targeted attacks

Attacks targeting governments can be motivated by a number of factors. 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. As a recent study discussed, attacks on government computer networks in the United States that resulted in a compromise or stolen information increased by 40 percent from 2007 to 2008.[29]

In 2008, China was the top country of origin for attacks that targeted the government sector, with 22 percent of the total (table 3), an increase from 8 percent in 2007 when it ranked fourth. For Internet-wide attacks in 2008, 13 percent of that total originated in China.

A number of media reports allege that attacks on government computer networks in countries such as the United States, India and Belgium had originated in China.[30] Nevertheless, 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 elsewhere than the country from where the attacks appear to originate.

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage
1	4	China	22%	8%
2	1	United States	12%	20%
3	2	Spain	6%	10%
4	3	France	5%	9%
5	8	United Kingdom	5%	4%
6	6	Italy	4%	7%
7	5	Germany	4%	8%
8	10	Brazil	3%	2%
9	19	Turkey	3%	1%
10	18	Russia	2%	1%

Table 3. Top countries of origin for government-targeted attacks
Source: Symantec

[29] http://www.usatoday.com/news/washington/2009-02-16-cyber-attacks_N.htm
[30] http://www.ft.com/cms/s/0/2931c542-ac35-11dd-bf71-000077b07658.html, http://timesofindia.indiatimes.com/India/Cyber_attacks_by_China_on_Indian_sites/articleshow/3010288.cms, and http://www.dofonline.co.uk/economy/chinese-espionage-alert-in-belgium5458.html

The United States ranked second in 2008 for attacks targeting government, with 12 percent of the total, a decrease from 20 percent in 2007. This drop is likely due to the shutdown of two ISPs in September and November 2008, which resulted in a dramatic drop in bot activity worldwide. Because bot-infected computers are used for large-scale attacks, such as DoS attacks, a significant drop in their numbers would result in a corresponding decrease in the number of malicious attacks detected.

The percentage of government-targeted attacks launched from the United States was less than half of its percentage for Internet-wide attacks, which accounted for 25 percent of that total in 2008. This indicates that the attacks originating from the United States were not specifically targeting government organizations, but were instead part of more general, widespread attacks.

Spain ranked third in this metric and accounted for 6 percent of attacks targeting government organizations in 2008, down from 10 percent in 2007. The 6 percent is twice the 3 percent of Internet-wide attacks that originated there, indicating that attacks originating in Spain may have been specifically targeting government organizations.

One reason for Spain's ranking here is due to the activities of a group of hackers located there. The group was arrested for compromising and defacing governmental websites in the United States, Asia, Latin America, and Spain.[31] Investigations show that the group was responsible for having disabled 21,000 Web pages over a two-year period.[32]

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 security administrators 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

[31] http://www.usatoday.com/tech/news/computersecurity/hacking/2008-05-17-hackers-spain_N.htm
[32] http://www.abc.net.au/news/stories/2008/05/18/2248032.htm

Government and critical infrastructure organizations

Government and critical infrastructure organizations are the target of a wide variety of attack types. The most common attack type seen by all sensors in the government and critical infrastructure sectors in 2008 was DoS attacks, which accounted for 49 percent of the top 10 attacks (figure 1). SMTP attacks were the second most common accounting for 44 percent of the top 10 attacks.

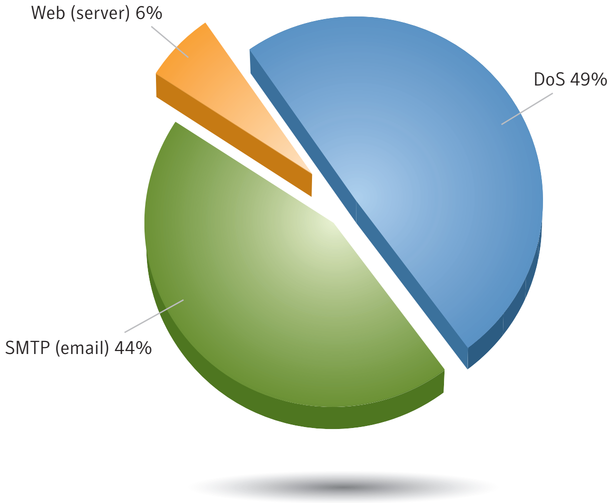

Figure 1. Top attack types, government and critical infrastructure[33]
Source: Symantec

DoS attacks are a threat to government and critical infrastructures because the purpose of such attacks is to disrupt the availability of high-profile websites or other network services, and make them inaccessible to users and employees. This could result in the disruption of internal and external communications, making it practically impossible for employees and users to access potentially critical information. Because these attacks often receive greater exposure than those that take a single user offline, especially for high-profile government websites, they could also result in damage to the organization’s reputation. A successful DoS attack on a government network could also severely undermine confidence in government competence, and impair the defense and protection of government networks.

DoS attacks can often be associated with political protests, since they are intended to render a site inaccessible in the same way that a physical protest attempts to block access to a service or location. They can also be associated with conflict whereby one country may attempt to block Web traffic or take websites offline. As such, the high percentage of DoS attacks may be an attempt to express disagreement with targeted organizations or countries.

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

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 in order to launch further attacks. These organizations heavily rely on email as a communication method and, as such, it is essential that email traffic be secured. Symantec recommends that administrators use secure email protocols, deploy anti-spam and antifraud solutions, and ensure that operating and email solutions are fully patched against all known vulnerabilities.

Top attacks by types, by sectors

DoS attacks were the most common type of attack observed by sensors deployed in the government, biotech/pharmaceutical, financial services, and transportation sectors in 2008 (figure 2). These attacks made up 48 percent of the top 10 attacks observed by government sensors, 54 percent in the biotech/pharmaceutical sector, 48 percent in the financial services sector, and 74 percent of the transportation sector.

As discussed above, it is likely these attacks were conducted to disrupt services in these sectors as a form of either protest or retaliation. Also, by denying access to these websites, these attacks could result in a significant loss of revenue for organizations in these sectors.

DoS attacks were by far the most common attack observed in the transportation sector. Since DoS attacks accounted for 49 percent of the attacks on government and critical infrastructure, this difference may indicate that attackers deploying these attacks are specifically targeting the transportation sector. Attackers may be using this type of attack to disrupt services and communications within the transportation sector.

Large-scale attacks of this nature may leave organizations unable to coordinate communications or relief efforts in the event of an emergency, or the inability to move supplies and goods for a military during a war or crisis. Also, because delays in the transportation sector often have a domino effect, in which delays in one city will cause delays in another due to scheduling, attacks on a relatively small part of this sector could have a significant effect on these situations.

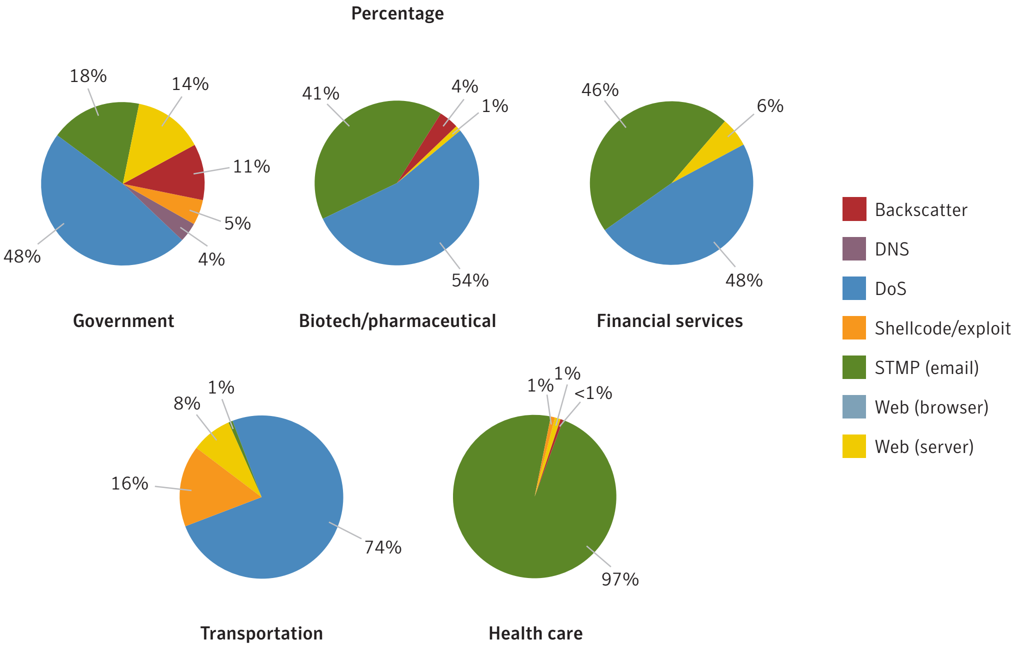

Figure 2. Top attack types, by sectors[34]
Source: Symantec

SMTP-based attacks were the most common attacks detected by sensors deployed in the health care sector in 2008, accounting for 97 percent of the top 10 attacks against the sector. These attacks against the health care sector may be from spammers trying to compromise email servers of legitimate companies in order to sell health care services and products. Malicious attackers may be able to use SMTP-based attacks to distribute confidential, misleading, or false information that could put patients and providers at risk. Also, by harvesting email addresses from such companies, attackers can use the trusted brand of that company to enhance their chances that their email is accepted as valid. This could, in turn, negatively effect the reputation of the targeted company.

It is worth noting that SMTP-based attacks fell from ranking first in 2007 to second in 2008 for the biotech/pharmaceutical and financial sectors, which may indicate that organizations in these sectors may be mitigating against these types of attacks by implementing better filters for Internet traffic and monitoring activity that enters the network. Although SMTP-based attacks did rank second for these two sectors, they still accounted for a large number of the top 10 attacks, likely for the same reasons as in the health care sector.

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.

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

This discussion is based on data surrounding publicly known vulnerabilities affecting SCADA technologies. The purpose of the metric is to provide insight into the state of security research as it affects 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 2008, Symantec documented six public SCADA vulnerabilities. This is fewer than the 15 public SCADA vulnerabilities documented by Symantec in 2007. There were more publicly reported SCADA vulnerabilities in 2007 due to multiple similar vulnerabilities affecting a single implementation that were reported in a single announcement.[35] Therefore, the difference between 2007 and 2008 does not appear to be a significant trend.

The number of public SCADA vulnerabilities is relatively small and represents the research efforts of a small community of specialized researchers. Security research in the field of SCADA often requires specialized knowledge and resources. Due to their role in critical infrastructure and the severity of potential vulnerabilities, SCADA security is often a private affair between industries that use SCADA protocols and technologies, the vendors themselves, and other stakeholders such as computer emergency response teams (CERTs) and government agencies. The close-knit nature of the SCADA industry means that vulnerability announcements are not necessarily made public. Information about vulnerabilities or general bugs is more likely to be exchanged in private between vendors, their customers, and other interested parties. These factors limit the number publicly disclosed SCADA vulnerabilities. The number of public vulnerabilities is not likely to increase until more security researchers become involved in this area of interest or until vendors change their policies about public vulnerability disclosure.

Information about SCADA-related incidents, whether accidental or malicious, has been tracked by organizations such as the British Columbia Institute of Technology (BCIT), which maintained, for a number of years, a non-public database of SCADA incidents called the Industrial Security Incident Database (ISID). Efforts such as the ISID have been able to provide credible incidence data that can be used to gauge the amount and severity of attack activity affecting SCADA environments. A Symantec-sponsored report assessing data in ISID was published in 2007.[36] In June of 2006, the database had tracked 105 legitimate incidents, with the earliest dating back to 1982. However, more recent data is not available because the ISID was not maintained after this point.[37]

In February of 2008, the SCADASEC-L mailing list was created to foster public discussion of SCADA security issues.[38] However, unlike other mainstream security mailing lists, SCADASEC-L discourages discussion of technical details surrounding vulnerabilities. The notion of the full-disclosure of security vulnerabilities is unpopular in SCADA security circles due to the elevated risk to critical infrastructure that is posed by vulnerabilities in SCADA technologies. This means that those affected by vulnerabilities are largely dependent on vendors reporting security issues as well as efforts by CERT organizations to disseminate

[35] http://www.securityfocus.com/bid/23059
[36] http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1823
[37] http://www.automationworld.com/news-4144
[38] http://www.infracritical.com/usage-scadasec.html

information about vulnerabilities. In September of 2008, a security researcher publicly released exploit code for a vulnerability in CitectSCADA because the researcher believed that the vendor reporting did not adequately emphasize the risk of the vulnerability.[39]

Governments have also expressed criticism toward the private sector regarding its ability to manage and prevent vulnerabilities that may affect critical infrastructure. In May of 2008, a government representative from the U.S. House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology criticized the North American Electric Reliability Corporation (NERC) for its handling of potential threats to the electrical grid.[40]

In December of 2006, Tenable Security announced the release of SCADA plug-ins for the Nessus vulnerability assessment tool.[41] This demonstrated converging interests between the SCADA community and the mainstream security community. From this point on, security researchers began to discover vulnerabilities in SCADA-related technologies. It has since been realized that SCADA technologies are affected by many of the same types of vulnerabilities that affect desktop and enterprise software.

For example, some functions are implemented as ActiveX® controls and are therefore prone to similar vulnerabilities that have been identified in other ActiveX controls in general. Many of the vulnerabilities documented in 2007 and 2008 affect ActiveX controls that implement functionality, such as OPC servers. This will allow a Microsoft Windows®-based computer to communicate with other applications and devices in a SCADA environment. Software such as this is more accessible to security researchers than other SCADA-related applications and hardware. Therefore, security researchers are able to discover vulnerabilities in these applications without requiring access to a complete SCADA environment.

Additionally, network-accessible devices may use either common or specialized networking protocols that are prone to attacks such as DoS attacks. 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.

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 and incoming/outgoing traffic should be limited to only those protocols that are required. 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. 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.

[39] http://www.theregister.co.uk/2008/09/08/scada_exploit_released/
[40] http://www.pcworld.com/businesscenter/article/146153/lawmakers_see_cyber_threats_to_electrical_grid.html
[41] http://blog.tenablesecurity.com/2006/12/nessus_3_scada_.html

Data breaches that could lead to identity theft

Identity theft continues to be a high-profile security issue, particularly for organizations that store and manage large amounts of personal information. Based on the most recent information available from 2007, roughly 8.4 million U.S. residents were victims of identity theft, which represents approximately 3 percent of the adult population.[42] 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 be costly for individuals to recover from the resulting identity theft, they can also be financially costly to organizations. In 2008, the average cost per incident of a data breach in the United States was $6.7 million,[43] an increase of 5 percent from 2007, and lost business amounted to an average of $4.6 million.[44] Also, organizations can be held liable for breaches and losses, which may result in fines or litigation.[45]

By the end of 2008, 44 states in the United States (along with the District of Columbia, Puerto Rico, and the Virgin Islands) had enacted legislation requiring notification of breaches involving personal information. The legislation regulates the responsibilities of organizations conducting business within the particular state after a data breach has occurred.[46] The laws require anyone who conducts business in the state to notify owners of the information exposed immediately after a security breach, with failure to do so resulting in possible civil action and fines.

Governments in other countries have also taken steps to embark on the issue of identity fraud, including Canada, Australia and New Zealand, who issued guidelines for dealing with privacy breach notification in 2007-2008.[47] Unlike legislation, guidelines may not have penalties associated with them, but they are a step toward creating accountability for data breaches that occur. Meanwhile, Australia is considering the recommendations by the Australian Law Reform Commission, in its review of the Privacy Act, to make data breach notification mandatory. [48]

In the United Kingdom, only government organizations are currently required to report all data breaches to the Information Commissioner's Officer (ICO) as part of the Data Protection Act, and there are no plans to implement breach notification laws.[49] Following the examples in the United States, recommendations have been made to the European Union by the European Network and Information Security Agency and the European Data Protection Supervisor to establish data breach notification laws.[50] Currently, the European Parliament states that organizations should report the breach but are not required to do so by law.[51] However, discussions are at the moment underway in Brussels, as part of the review of the European Telecommunications Regulatory Framework, on the possible introduction of a data breach notification law to the Privacy and Electronic Communications Directive for the European telecommunications sector.

[42] http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007
[43] All figures are in U.S. dollars unless otherwise noted.
[44] http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf
[45] http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml
[46] http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm
[47] http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp, http://www.privacy.gov.au/publications/breach_guide.html, and http://www.privacy.org.nz/the-privacy-act-and-codes/
[48] http://www.dpmc.gov.au/privacy/alrc.cfm and http://www.alrc.gov.au/media/2008/mr11108.html
[49] http://www.justice.gov.uk/docs/response-data-sharing-review.pdf, Recommendation 11
[50] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf and http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf
[51] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0452+0+DOC+XML+V0//EN&language=EN

There are other notable initiatives that exist in the United States for the safeguarding of personal information. They include the Red Flags Rules as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003, which requires all financial institutions and creditors to develop identity theft prevention programs,[52] and the Payment Card Industry Data Security Standards (PCI DSS), which lists a set of requirements for enhancing payment account data security such as network requirements, encryption transmission requirements, security assessments to eliminate security vulnerabilities, and maintaining security policies.[53] The updated version will include incorporating best practices and improving reporting requirements.[54] The added consideration of punitive costs may influence organizations to develop more robust security strategies, which may help reduce the number of breaches overall.

Data breaches that could lead to identity theft by sector

Using publicly available data, Symantec has determined the sectors that were most often affected by these breaches, as well as the most common causes of data loss.[55] This discussion will also explore the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data. An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.[56]

It should be noted that some sectors may 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.[57] 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.

In 2008, the education sector represented the highest number of known data breaches that could lead to identity theft, accounting for 27 percent of the total (figure 3). This is a slight increase from 2007 when the education sector also ranked first with 26 percent of the total.

[52] http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm
[53] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
[54] https://www.pcisecuritystandards.org/pdfs/08-18-08_2.pdf
[55] Open Security Foundation (OSF) Dataloss DB, see http://datalossdb.org
[56] An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.
[57] Cf. http://www.privacyrights.org/fs/fs6a-facta.htm and http://www.cms.hhs.gov/HealthPlansGenInfo/12_HIPAA.asp

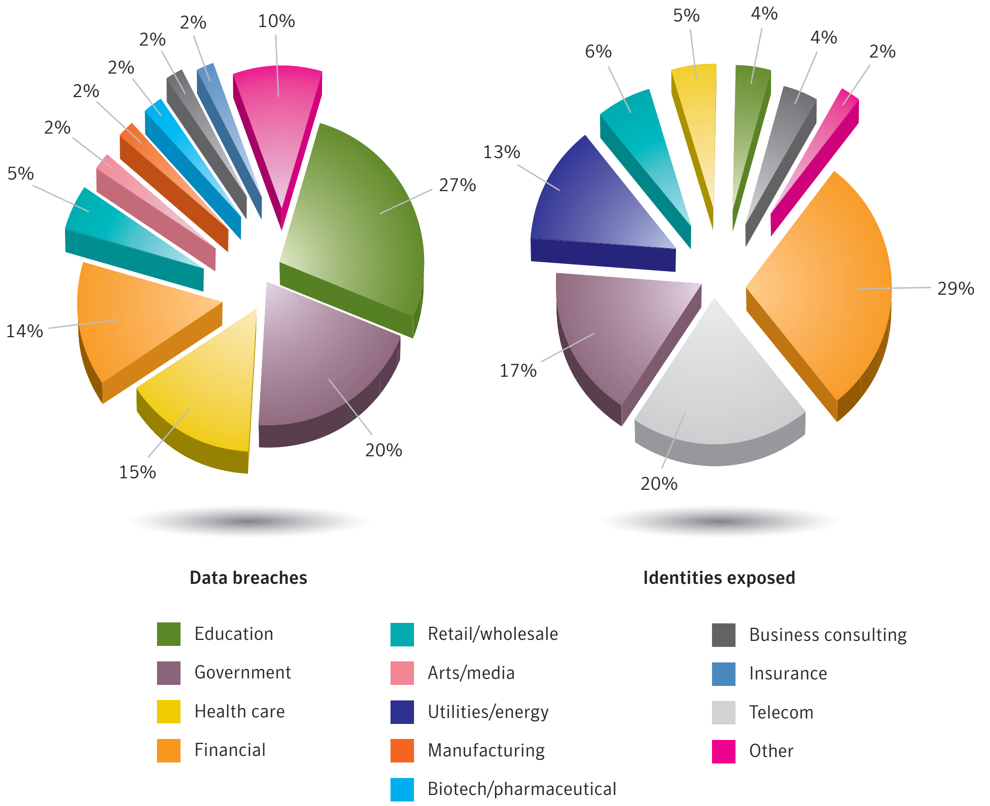

Figure 3. Data breaches that could lead to identity theft by sector and identities exposed by sector[58]
Source: Based on data provided by OSF DataLoss DB

Educational institutions store a large amount of personal information on students, faculty, and staff that could be used for the purposes of identity theft, including government-issued identification numbers, names, and addresses. Finance departments in these institutions also store bank account information for payroll and may also 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 within which sensitive personal identification information may be stored in separate locations and be accessible to many people. This may increase the opportunities for attackers to gain unauthorized access to this data since it may be more difficult to standardize the security, educate everyone with access to the data on the policies, and control access to these dispersed databases.

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

Despite the high number of data breaches that occurred in the education sector during 2008, it only accounted for 4 percent of all identities exposed during the period and ranked seventh (figure 1). This may be because the educational institutions have relatively smaller databases than those of financial or government institutions and, hence, fewer identities would be exposed in a data breach. One of the largest universities in the United States accounted for less than 80,000 students and employees, while financial and government institutions may store information on millions of people.[59]

Also, one-third of the data breaches in the education sector this period were caused by the theft or loss of computers or data-storage devices. As such, data breaches that occurred in the education sector in this reporting period were not as likely to result in wide-scale identity theft because they resulted in the exposure of fewer identities. These types of breaches only expose the limited amount of data that is stored on the devices.

In 2008, the government sector ranked second and accounted for 20 percent of data breaches that could lead to identity theft. This is a decrease from the previous year, when the government sector represented 23 percent of the total, though still ranking second. This trend is reinforced by the annual Federal Computer Security report card, where the number of government agencies with a failing grade decreased by almost half.[60] The health care sector ranked third in 2008, accounting for 15 percent of data breaches that could lead to identity theft. It also ranked third in 2007, accounting for 14 percent.

Government and health care organizations, like educational institutions, store large amounts of information that could be used for identity theft. Similar to the education sector, these organizations often consist of numerous autonomous departments that store sensitive personal information in separate locations and are accessible to numerous people. As a consequence, these organizations face the same security and control issues as educational institutions. Furthermore, health care organizations store sensitive medical information in addition to personal information, which could result in even more damaging breaches of privacy.

The government sector ranked third for identities exposed during 2008, accounting for 17 percent of the total while the health care sector ranked sixth, accounting for 5 percent of the total. As with the education sector, data breaches within the health care sector resulted in a relatively low number of identities exposed.

[59] http://www.osu.edu/osutoday/stuinfo.php
[60] http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf

Data breaches that could lead to identity theft, by cause

In 2008, the primary cause of data breaches that could facilitate identity theft 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.[61] Theft or loss made up 48 percent of all data breaches in 2008, a decrease from the previous reporting period when it accounted for 52 percent of all reported breaches (figure 4).

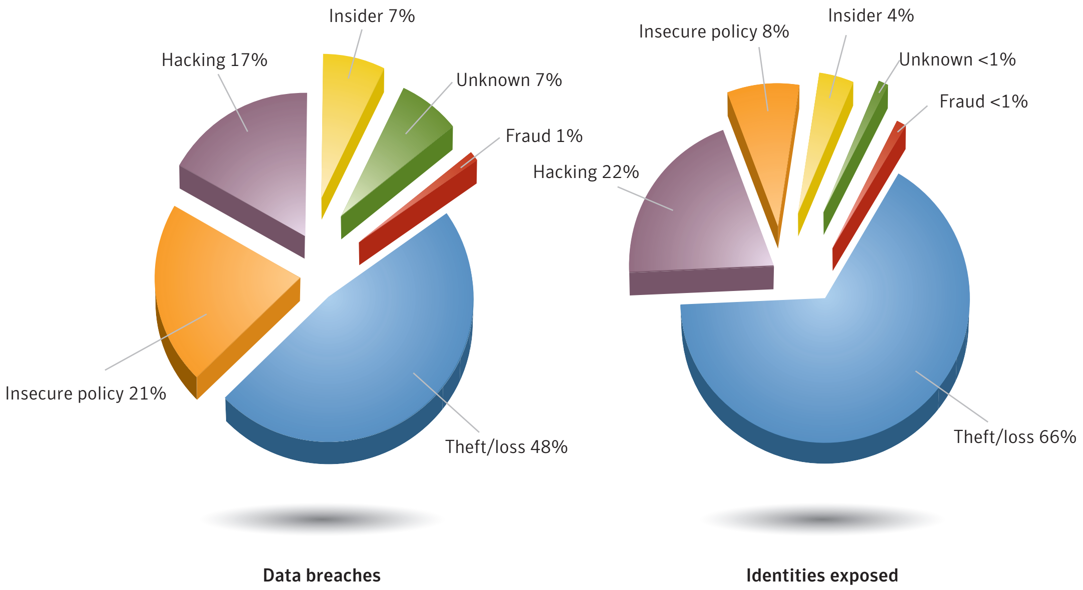

Figure 4. Data breaches that could lead to identity theft by cause and identities exposed[62]
Source: Based on data provided by OSF DataLoss DB

Theft or loss accounted for 66 percent of all identities exposed in 2008, more than any other cause (figure 4). This was a large increase from 2007, when the number of identities exposed from theft or loss accounted for 24 percent of the total. The main reason for this dramatic increase is that theft or loss was the cause for the three largest breaches that exposed the highest number of identities reported in 2008. These breaches were due to lost or missing disks and exposed personal information relating to an estimated 41 million people.

Although laptops and other storage devices, such as USB memory keys, portable hard drives, and disks, have become smaller, less expensive, and easier to use, their compact size and larger storage capability has increased the opportunity for theft, loss, or misplacement, as well as the potential amount of information breached; a single DVD disk can contain personal information on millions of people. In a recent survey, one in 10 people have lost a laptop, smart phone, or USB flash drive with corporate information stored on it.[63] It may be that the theft of a computer or data-storage device is opportunistic and motivated by the hardware itself and not necessarily its contents, and as such, may not lead to wide-scale identity theft, although there have been cases where information obtained from on a lost disk was discovered in advertisements in the underground economy.

[61] This cause will be referred to as theft or loss for the remainder of the report.
[62] Due to rounding, percentages might not equal 100 percent.
[63] http://www.rsa.com/press_release.aspx?id=9703

To protect against data theft or loss, organizations should restrict the use of outside personal storage devices within their network, monitor the usage of such hardware when permitted, and educate employees on proper usage. Organizations should also include reviews and audits of electronic documents used by employees upon leaving the company. In a recent study, 59 percent of employees admitted to taking company information, such as email addresses, contact information of customers, employee records, and financial records, when leaving the organization.[64] Of these former employees, 79 percent took the information without consent from the company. In 92 percent of the instances, the information was taken on disk, while 73 percent was on removable drives. It is worth noting that only 15 percent of the companies polled had conducted a review or audit of electronic documents taken by employees. Also, sensitive data should be strongly encrypted on any laptop or storage device that may be used outside of the enterprise.

The second most common cause of data breaches that could lead to identity theft during 2008 was insecure policy, which represented 21 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. In 2007, insecure policy also ranked second, accounting for 28 percent of such data breaches. This decrease in the number of data breaches may be due to organizations becoming more diligent and producing stronger security policies such as limiting access to sensitive information to required personnel and the documentation of document transfers. Insecure policy accounted for only 8 percent of exposed identities in 2008 and, thus, each breach exposed only a relatively small number of identities. Although breaches caused by insecure policy in 2008 were not likely to result in wide-scale identity theft, the breaches still exposed approximately 6.5 million identities.[65]

In 2008, hacking was the third leading cause of data breaches that could lead to identity theft, accounting for 17 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 2007, accounting for 14 percent of breaches that could facilitate identity theft. Hacking is more purpose-driven than insecure policy, theft, or loss: in 2008, over half of the breaches that exposed credit card information were due to hacking. Attackers can take advantage of site-specific and Web-application vulnerabilities to gain access to networks and steal personal information. For this discussion, Symantec considers hacking to be an intentional act with a defined purpose to steal data that can be used for purposes of identity theft or other fraud.

Hacking ranked second for identities exposed in 2008, with 22 percent; this is a large decrease from 2007, when hacking accounted for 62 percent of total identities exposed. The contributing factor for its high ranking in 2007 was a significant data breach in which data on over 94 million credit cards was stolen by attackers hacking into a company's database through unencrypted wireless transmissions and installing programs to capture credit card information.[66] It is estimated that between $63 million and $83 million in credit card fraud across 13 countries can be attributed to this single data breach.[67]

In 2008, two breaches contributed significantly to the high ranking of hacking in this metric: in the first, confidential information on six million Chileans was illegally obtained from government databases by a hacker who publicly posted the information afterward; in the second, credit card information from 4.2 million customers was stolen from a U.S.-based grocery chain by hackers monitoring the credit

[64] http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01
[65] http://datalossdb.org
[66] http://www.msnbc.msn.com/id/21454847/
[67] http://www.securityfocus.com/news/11493

authorization process.[68] Because of the motivation of attackers who use hacking to steal personal financial information, the impact of data breaches due to hacking are severe because they are likely to result in large-scale fraud and high financial cost to affected organizations, credit card issuers, and consumers.

Even though they constitute one of the most challenging issues faced by organizations, data breaches that could lead to identity theft are mostly preventable. For any department that manages or requires access to sensitive information, organizations should develop strong security policies such as strongly encrypting all data, ensuring there are controls in place that restricts access to such information to required personnel, and providing education and resources for all employees on proper security procedures. Network administrators should be closely monitoring network traffic and tracking all activity to ensure that there is no illegal access to databases, as well as testing security processes and systems regularly to ensure their integrity. Organizations should include these steps as part of a broader security policy, and ensure that any security policy is implemented and enforced to protect all sensitive data from unauthorized access.

Bot-infected computers

Bots are programs that are covertly installed on a user's machine in order to allow an attacker to remotely control the targeted system 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 new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft, all of which can have serious financial and legal consequences. Bots are also inexpensive and relatively easy to propagate. In 2008, Symantec observed underground economy advertisements for as little as $0.04 per bot. This is much cheaper than in 2007, when $1 was the cheapest price advertised for bots. Bot-infected computers with a decentralized bot C&C model are favored by attackers because they are difficult to disable, and most importantly, can be lucrative for their controllers. In one example, a botnet owner arrested in New Zealand admitted to earning $21,500 over a two-year span from his activities.[69]

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 2008, Symantec observed an average of 75,158 active bot-infected computers per day (figure 5), a 31 percent increase from 2007. Symantec also observed 9,437,536 distinct bot-infected computers during this period, a 1 percent increase from 2007.

[68] Cf. http://news.bbc.co.uk/1/hi/world/americas/7395295.stm or http://www.msnbc.msn.com/id/23678909/
[69] http://www.itworld.com/security/58670/botnet-master-sees-himself-next-bill-gates

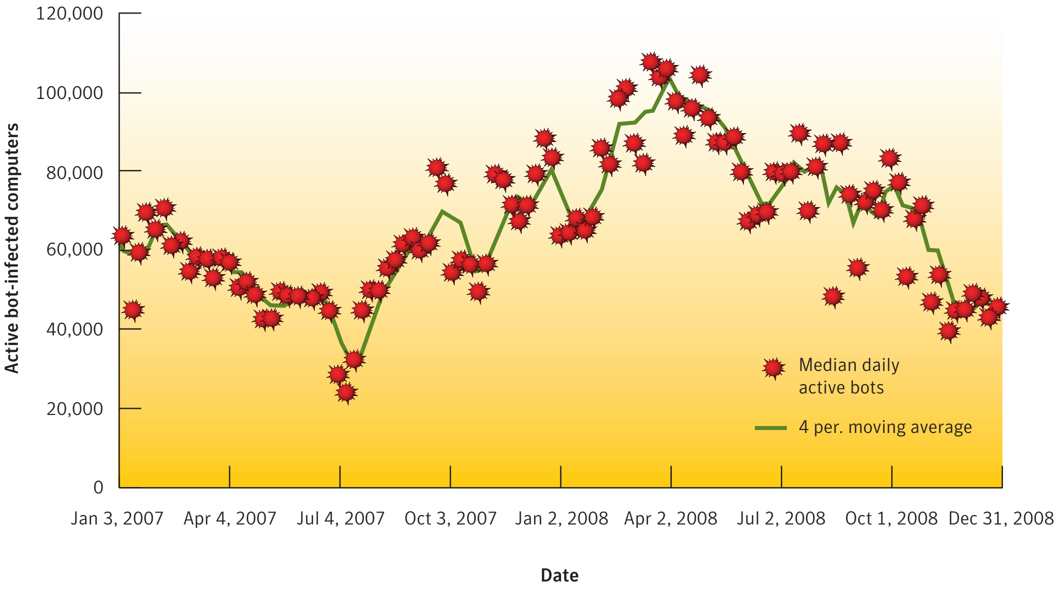

Figure 5. Active bot-infected computers, by day
Source: Symantec

The decrease in active bot-infected computers at the beginning of 2008 may be due to the reduction in size of the botnet associated with the Peacomm Trojan.[70] The number of bot-infected computers in the botnet was reduced to 5 percent of its previous estimated size, from 2 million bot-infected computers to 100,000.[71] In addition, as stated in "Malicious activity by country," the shutdown of two U.S.-based hosting companies responsible for hosting bot C&C servers for a number of major botnets likely contributed to the decrease in active bot-infected computers in September and November 2008. After the shutdown in September, major botnets, including Srizbi and Pandex,[72] were able to find alternate hosting, which resulted in an increase in bot-infected computers back to pre-shutdown levels. However, the shutdown in November severely crippled Srizbi and Ozdok, and as a consequence, competing botnets, including Pandex, were able to fill the void.[73]

Although the number of active bot-infected computers decreased at the end of the year, it is assumed that botnet owners will seek out new hosts to get their botnets back online, and it is expected that bot numbers will rise again in 2009.[74] One result of all the activity in 2008 is that this shows that botnets can be crippled by identifying and shutting down their bot C&C server hosts, but that this strategy is difficult to implement given the various global hosting options that botnet controllers have at their disposal.

[70] Also known as the Storm botnet.
[71] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 32
[72] http://www.symantec.com/security_response/writeup.jsp?docid=2007-042001-1448-99
[73] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 25–26
[74] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf

Bot command-and-control servers

Symantec tracks the number of bot C&C servers globally because these are what botnet owners use to relay commands to bot-infected computers on their networks. For the first time, in this volume of the Symantec *Government Internet Security Threat Report*, bot C&C servers controlled over HTTP are included in this analysis alongside IRC bot C&C servers.[75] This change in measurement was made due to the trend of botnet owners shifting away from traditional IRC bot C&C communication frameworks and toward managing their botnets through HTTP bot C&C servers. In 2008, Symantec identified 15,197 distinct new bot C&C servers (figure 6), of which 43 percent were over IRC channels and 57 percent over HTTP.

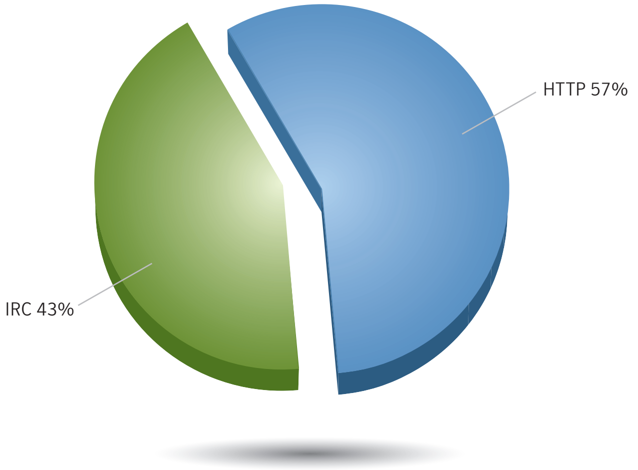

Figure 6. Bot command-and-control servers, by type
Source: Symantec

Botnet owners are moving away from traditional IRC-based botnets since they are easier to detect, track, filter, and block than botnets based on HTTP traffic. HTTP communications can be used to disguise botnet traffic among other Web traffic in order to make it difficult to distinguish malicious traffic from legitimate HTTP traffic. (Most HTTP bot transmissions are encrypted to avoid detection.) To filter the traffic, organizations would have to inspect the encrypted HTTP traffic and identify and remove bot-related traffic while still allowing legitimate traffic to pass through. Because of this, it is very difficult to pinpoint and disable a bot C&C structure. It is also unreasonable to block HTTP traffic since organizations depend on legitimate HTTP traffic to conduct day-to-day business. Botnet owners have also been switching away from using P2P for bot C&C server communications because such traffic is more easily detected due to the "noise" it creates in transmission. Moreover, many enterprises and other organizations also block P2P ports to prevent such high-bandwidth traffic from entering their networks.

[75] Not included in this measurement are bot C&C servers over P2P protocols; also, as this is the first report in which HTTP bot C&C servers are included in this analysis, 2007 comparisons are unavailable.

Symantec also observed an average of 42 new active bot C&C servers per day in 2008, of which 18 were IRC-based and 24 were HTTP (figure 7). The three largest botnets identified by Symantec in 2008—Srizbi, Rustock, and Pandex—are all HTTP-based.

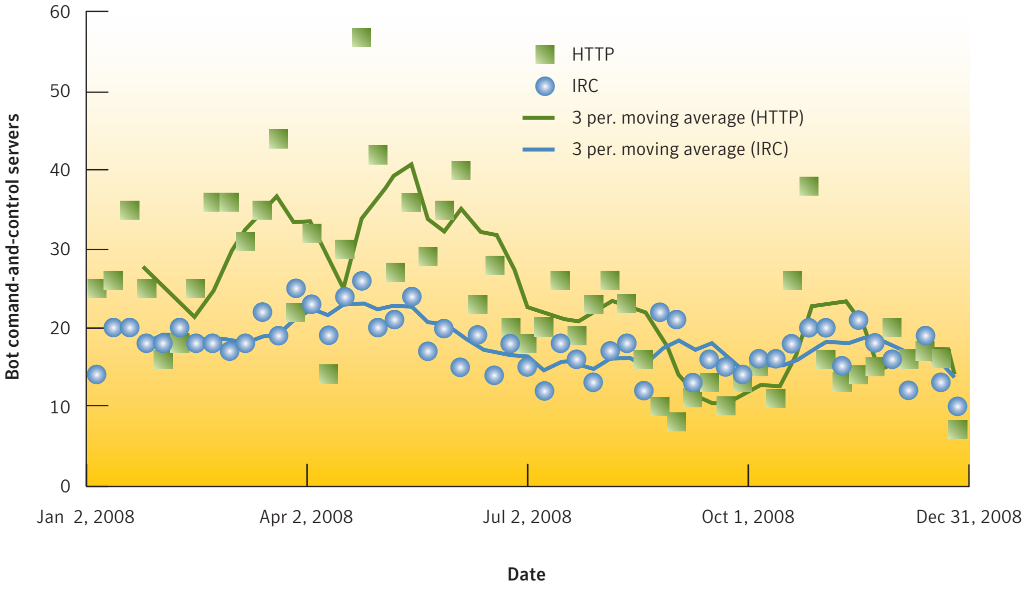

Figure 7. Bot command-and-control servers, by day
Source: Symantec

The drop in new and active HTTP bot C&C servers in February 2008 is likely due to bot C&C servers for a major HTTP-based botnet, Ozdok, going offline for 10 days during that month.[76] Also, the significant reductions that occurred in September and November 2008 are likely due to the shutdown of two U.S.-based ISPs, as was noted previously in this discussion. The September shutdown resulted in an immediate decrease in activity associated with the Srizbi and Pandex botnets.[77] As mentioned, it is assumed that these botnets found alternate hosting, which would explain the subsequent rise in activity.

The second shutdown in November resulted in a 30 percent decrease in overall botnet traffic and is thought to have severely weakened two of the largest botnets, Srizbi and Rustock.[78] The significant drop in new and active HTTP bot C&C servers in November 2008 may be because one of these ISPs was allegedly hosting a large number of bot C&C servers for Srizbi and Rustock, and bots were hard-coded to connect to these servers.[79] It was estimated that the Srizbi botnet had 300,000 bots prior to the shutdown[80] and the Rustock botnet had included over 150,000 bots.[81]

[76] http://www.scmagazineus.com/TRACE-Six-botnets-generate-85-percent-of-spam/article/107603/
[77] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 25
[78] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 26
[79] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf
[80] http://itknowledgeexchange.techtarget.com/security-bytes/srizbi-botnet-is-the-biggest-but-does-size-matter/
[81] http://www.scmagazineus.com/The-Rustock-botnet-spams-again/article/112940/

Top Web-based attacks

The widespread deployment of Web applications along with the ubiquity of easy-to-exploit Web application security vulnerabilities have resulted in the prevalence 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 are now focused on attacking and compromising websites in order 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. This metric will assess the top distinct Web-based attacks originating from compromised legitimate sites and malicious sites that have been created to intentionally target Web users.

The attacks discussed can involve social engineering to entice a victim to view a malicious website, but most attacks exploit trusted high-traffic websites. When the user visits a compromised website, a number of attack methods are used. Malicious content from the website can directly exploit a vulnerability in the browser, a browser plug-in, or a desktop application. An attack such as this may require nothing more than the user visiting the site from where the attack originates. In the case of a drive-by download, the attack will occur without any interaction required from the user.[82]

Attackers also use malicious websites for compromises, such as misleading the user to indirectly authorize a specific technology that then downloads malicious code, or prompting the user to click on a pop-up or banner ad. Attackers can also redirect all traffic from a legitimate website to a malicious website from which the user's computer will then be attacked. In all of these types of Web-based attacks, the user is unaware of the compromise. Once an attacker has compromised a website and injected malicious content, he or she can passively attack visitors of the compromised site. This type of attack is very efficient for attackers because they only have to compromise one Web page in order to affect multiple users. When a user visits a compromised Web page, the attack is carried out through the user's browser. The attack will either target vulnerabilities in the browser itself or it will target third-party applications that are activated by the browser.

All Web-based attack traffic goes through the HTTP or HTTPS protocols. The benefit of this for attackers is that it is unreasonable to block these protocols because legitimate organizations depend on them for their day-to-day business. In addition, filtering a large volume of HTTP traffic would significantly slow throughput traffic. HTTP traffic is also difficult to filter with intrusion detection/intrusion prevention systems (IDS/IPS) because it is difficult to distinguish malicious traffic from legitimate traffic, and HTTP traffic can be encrypted, thus enabling attacks to be obfuscated within legitimate traffic.

Attackers are not only employing manual methods to exploit these issues, but they are also using automated tools, such as Neosploit,[83] to exploit client-side vulnerabilities on a massive scale. Such toolkits are widely available and prepackaged so that people with minimal technical knowledge are able to use them effectively.

[82] 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.
[83] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=1

Another attraction of the Web for exploitation is the profusion of dynamic sites that use Web-based applications, such as forums, photo-sharing galleries, blogs, and online shopping applications. Dynamic sites are prime targets for attackers using bot-infected computers to propagate and host malicious content since Web application and site-specific vulnerabilities can put these types of site at risk.

Attackers are also especially attracted to large, popular websites with trusted reputations. This is not only because a successful compromise can reach a greater number of people (who tend to have an inherent trust for legitimate websites and are thus more susceptible to attack), but, as mentioned, it may be difficult to block attacks to these sites using security tools without disrupting legitimate traffic.

These developments and trends indicate that Web-based threats have not only become widespread, but that they also have increased in sophistication and severity. In particular, Symantec has noticed that botnets (such as Asprox,[84] which was initially used for phishing scams) are being redesigned to specifically exploit cross-site scripting vulnerabilities and inject malicious code into compromised websites.[85]

Many Web-based attacks exploit vulnerabilities that are considered medium severity. This means that they can compromise the account of the currently logged in user because the user does not require administrative privileges to run the affected applications. While the danger of client-side vulnerabilities may be limited by best practices, such as restricting Web applications to the administrative level, this is often unreasonable given how integral Web applications are to the delivery of content for many businesses. Medium-severity vulnerabilities affecting client or desktop applications are often sufficient for an attacker to mount successful malicious attacks on single clients, as well as at the enterprise level.

In 2008, the top Web-based attack was associated with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness,[86] which accounted for 29 percent of the total globally (table 4). The weakness 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 another vulnerability that bypasses Internet Explorer security settings to allow the attacker to execute malicious files installed by the initial security weakness. This issue was published on August 23, 2003, and fixes have been available since July 2, 2004. Since this was the top Web-based attack in 2008, this may indicate that many computers running Internet Explorer have not been patched or updated and are running with this exposed vulnerability.

Rank	Web-based Attack	Percentage
1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	30%
2	Acrobat PDF Suspicious File Download	11%
3	ANI File Header Size Buffer Overflow	7%
4	Adobe SWF Remote Code Executable	7%
5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	6%
6	SnapShot Viewer ActiveX File Download	5%
7	Microsoft Internet Explorer XML Core Services XMLHTTP Buffer Overload	4%
8	Quicktime RTSP URI Buffer Overload	3%
9	AOL SuperBuddy ActiveX Code Executable	3%
10	Microsoft Internet Explorer WebViewFolderIcon ActiveX Control Buffer Overflow	2%

Table 4. Top Web-based attacks
Source: Symantec

[84] http://www.symantec.com/security_response/writeup.jsp?docid=2007-060812-4603-99
[85] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 33
[86] Cf. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or http://www.securityfocus.com/bid/10514

A large number of exploits and malicious applications may depend on this vulnerability as a common way of compromising computers, in tandem with other known vulnerabilities. Therefore, the amount of attack activity is related to the cumulative number of exploits, attack toolkits, and worms targeting this vulnerability as one possible means of compromising computers. It is also likely that the large market share of Microsoft Internet Explorer plays a role in the popularity of this attack.[87] While the vulnerability was patched in 2004, there are likely still enough unpatched computers that are affected by this vulnerability for attackers to benefit.

The second most common Web-based attack in 2008 was related to malicious Adobe® Acrobat® PDF activity,[88] which accounted for 11 percent of Web-based attacks. Specifically, attempts to download suspicious PDF documents were observed. This may indicate attempts by attackers to distribute malicious PDF content to victims via the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious file would be designed to exploit an arbitrary vulnerability in an application that processes it, such as Adobe Acrobat Reader®. A successful attack could ultimately result in the compromise of the integrity and security of an affected computer. This attack is assumed to be popular to due the common use and distribution of PDF documents on the Web. Also, browsers can be set up to automatically render a PDF document by default. Specific exploit activity related to malicious PDF files was observed in 2008.[89]

In 2008, the third most common Web-based attack exploited the Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability,[90] accounting for 7 percent of Web-based attacks in 2008. The ANI (animated cursor file) handler is a default component of the Microsoft Windows operating system and is used by a significant number of widely used Microsoft applications as well as the Windows shell. If successfully exploited, the vulnerability allows an attacker to execute arbitrary code embedded in a malformed ANI file originating from the Web or other sources. This vulnerability was published on January 11, 2005, and fixes have also been available since that time. Exploit code was publicly available the following day. As with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness, the prominence of this type of attack indicates that computers in the region are likely not being sufficiently patched and updated.

Vulnerabilities such as those discussed here continue to generate a large amount of observed attack activity because they can be reliably exploited. 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 a large number malicious code variants and 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.

[87] http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0&qpmr=100&qpdt=1&qpct=3&qptimeframe=Y&qpsp=2008&qpnp=2
[88] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153
[89] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Pidief-the-Word-for-Exploits/ba-p/305564#A141
[90] Cf. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=21719 or http://www.securityfocus.com/bid/12233

Top countries of origin for Web-based attacks

This metric will assess the top countries of origin for Web-based attacks against users in 2008 by determining the location of computers from which the attacks occurred. Note that attackers, in order to hide their tracks, often redirect users through one or more servers that may be located virtually anywhere globally.

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

In 2008, computers from the United States were the leading source of Web-based attacks against users, accounting for 38 percent of the total (table 5). There are a number of factors that make the United States the top country of origin for Web-based attacks. This ranking may be due to the more than half a million websites that were compromised in May 2008 with malicious code that was hosted in Russia and the United States. Web forums hosted by PHP-based bulletin board applications were exploited to inject malicious JavaScript™ into forum content. These forums would then infect visitors with variants of the Zlob Trojan[91] disguised as a video codec installer. The exploit changes browser and DNS settings on the infected computer and enables additional attacks, including turning the infected computer into a zombie.[92] This attack follows the trend of attackers inserting malicious code into legitimate high-traffic websites where users are likely to be more trusting of the content, rather than attempting to lure users to visit specially designed malicious sites.

Rank	Country	Percentage
1	United States	38%
2	China	13%
3	Ukraine	12%
4	Netherlands	8%
5	Russia	5%
6	United Kingdom	5%
7	Canada	3%
8	Japan	2%
9	Latvia	1%
10	France	1%

Table 5. Top countries of origin for Web-based attacks
Source: Symantec

[91] http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[92] http://www.channelregister.co.uk/2008/05/13/zlob_trojan_forum_compromise_attack/

In 2008, China ranked as the second country of origin for Web-based attacks, with 13 percent of the worldwide total. The main reason for the high rank of China in 2008 is due to compromised websites relating to the 2008 Beijing Olympic Games. The games were one of the largest events of 2008 and attackers exploited the popularity of the event in their attempts to lure and compromise users, as has been seen previously with other major sporting and entertainment events.[93] One example is the Rustock botnet, which sent out emails with links to a news report about the games. Users were prompted to click a link in the email and visit a site, which then prompted them to download a missing codec in order to launch a video. Clicking to obtain the codec actually resulted in the installation of a Trojan.

Attackers may have also used social engineering to lure users to compromised websites under the guise of being associated with the 2008 Beijing Olympic Games, as attacks against Chinese-language websites increased significantly during the games.[94] The extent of these attacks was mitigated, however, by initiatives to increase online security for users ahead of the Games by shutting down or blacklisting thousands of websites potentially most susceptible to fraud, which are popular targets of attack from Web application and site-specific vulnerabilities. Also, thousands of websites in China were compromised when certain Web applications were infected with malicious JavaScript that was planted through the use of SQL-injection attacks.[95] Visitors to these compromised sites had their computers attacked and, if the attacks were successful, Trojans were downloaded onto the computers.[96]

Ukraine ranked third in 2008 for top country of origin for Web-based attacks, accounting for 12 percent of such attacks worldwide. The prominence of Ukraine in this metric is likely due to the compromise of the website of a U.S.-based electronic bill payment processing company.[97] The attackers were able to obtain account credentials to the company's domain using a phishing attack, and were then able to gain access to the company's website. Customers, thinking they were visiting the legitimate website, were redirected to a malicious website hosted on servers in Ukraine where they were attacked with a Trojan.[98] In addition to the compromise of the bill payment company's website, there were at least 71 domains that were redirected to the malicious Ukrainian server during this time.[99]

Of note, six of the top 10 countries for Web-based attacks in the Europe, Middle East, and Africa (EMEA) region were also in the top 10 countries of origin for Web-based attacks globally, and countries in the EMEA region accounted for 41 percent of the worldwide total, more than any other region. Exploit packs may be one of reasons behind the prominence of the EMEA region in this measurement. Many exploit packs, including MPack,[100] IcePack,[101] and Neosploit,[102] originated in Russia and it is likely that the Russians who developed these attack kits are responsible for much of their continued propagation. These attackers could possibly be compromising websites around the world and redirecting visitors to computers in EMEA that host the exploit code being used to target client-side vulnerabilities in Web browsers.

[93] http://news.bbc.co.uk/1/hi/technology/7548870.stm
[94] http://www.networkworld.com/newsletters/gwm/2008/090808msg1.html
[95] http://www.h-online.com/security/Chinese-websites-under-mass-attack--/news/110764
[96] Ibid.
[97] http://www.networkworld.com/news/2008/120508-network-solutions-phishing-came-before.html
[98] http://www.csoonline.com/article/474365/CheckFree_Warns_Million_Customers_After_Hack
[99] http://blog.kievukraine.info/2008/12/digging-deeper-into-checkfree-attack.html
[100] https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/vulnerabilities_exploits/article-id/93#M93
[101] https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/grab_bag/article-id/81
[102] http://blogs.zdnet.com/security/?p=1593

Also contributing to the prominence of the EMEA region this period were a number of high-profile Web-based attacks that occurred there. One example was in January 2008, when the embassy website of the Netherlands in Russia was compromised and visitors to the site were misled into installing malicious code.[103] Another example occurred in August 2008 when several hundred domains in the Netherlands were compromised and defaced.[104] A third case was when more than a thousand UK websites were compromised and users visiting these sites risked being infected with the Asprox Trojan.[105] The success of these attacks on government sites can be attributed, in part, to the inherent trust that visitors to such sites will have, making these visitors more liable to accept prompts to download files if requested.

Web-based attacks are a major threat to computer networks for both enterprises and end users. Attacks such as drive-by downloads are covert and very difficult to mitigate 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 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.

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.[106] 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. Also, 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.

[103] http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/
[104] http://blogs.zdnet.com/security/?p=1788
[105] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4381034.ece
[106] 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 prevents data breaches, but also mitigates 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.[107] Policies that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorized individuals should be put in place and enforced. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access. This would ensure that even if the computer or medium on which the data were 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.

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

Malicious Code Trends

Symantec also gathers malicious code intelligence from more than 130 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 section of the Symantec *Government Internet Security Threat Report* will discuss the following malicious code trends for 2008:

- New malicious code threats
- Geolocation by type of malicious code
- Threats to confidential information
- Propagation mechanisms
- Malicious code—protection and mitigation

New malicious code threats

Symantec monitors the proliferation of malicious code by examining the number of new malicious code signatures created to detect threats from period to period. Comparing new signatures against signatures created previously indicates how quickly new malicious code threats are being developed. Periods in which a significant number of new malicious code threats are created indicates how critical it is for both enterprises and home users to maintain updated antivirus signatures, and to implement and maintain robust security measures such as software patches.

In 2008, Symantec created 1,656,227 new malicious code signatures (figure 8). This is a 265 percent increase over 2007, when 624,267 new malicious code signatures were added. Although the percentage increase in signatures added is less than the fairly staggering 445 percent increase from 2006 to 2007, the overall number of malicious code signatures by the end of 2008 grew to 2,674,171. This means that of all the malicious code signatures created by Symantec, more than 60 percent of that total was created in 2008. Furthermore, Symantec blocked an average of more than 245 million attempted malicious code attacks worldwide each month in 2008.

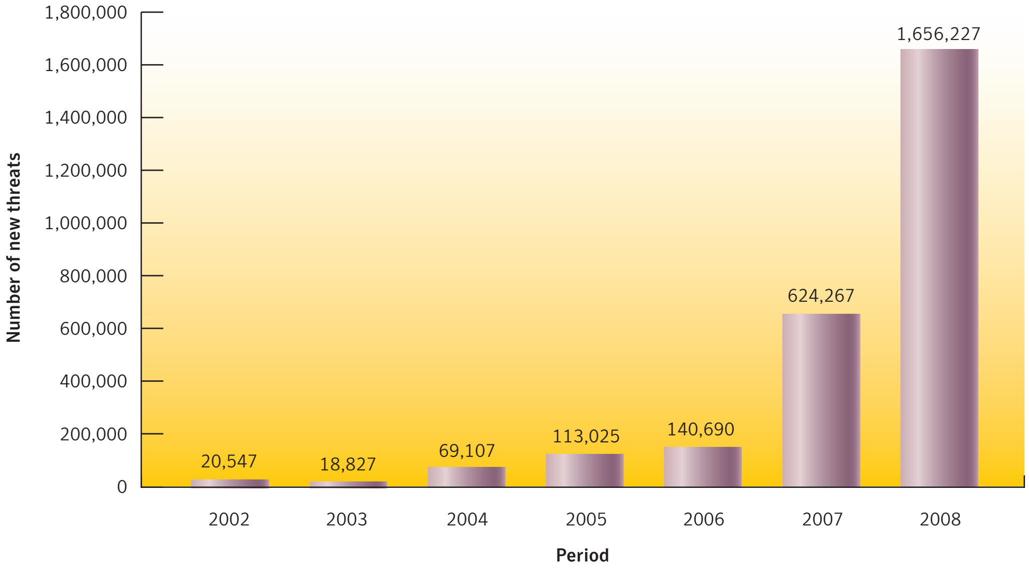

Figure 8. New malicious code signatures
Source: Symantec

Previous volumes of the Symantec *Global Internet Security Threat Report* have discussed the increasing professionalization of malicious code development.[108] The result is an increase in the speed and efficiency with which malicious code is "brought to market," which would enable an increased number of threats to be developed. A driving force behind the growing speed and efficiency of these developments is the demand for goods and services that facilitate online fraud. This is exemplified by the flourishing profitability of confidential information sales, as was discussed in the recently published Symantec *Report on the Underground Economy*.[109] For example, Symantec estimated the value of total advertised goods on underground economy servers between July 2007 and June 2008 to be $276 million.

Of particular value in the underground economy is malicious code that exposes confidential information. This is because confidential information is critical to several illegal practices, such as identity theft and credit card fraud. Symantec has determined that, in many instances, this code is being developed on a large scale by well-organized programmers, much as applications are developed in a legitimate software enterprise. The demand for malicious code in the underground economy is further illustrated by advertisements specific to such goods, with some advertisers selling the malicious code itself and others requesting the services of malicious code authors. Advertisements for malicious code authors are often looking for the one-time development of specific code to create new variants of existing threats, rather than developing entirely new threats. This is likely because variants of existing malicious code can be developed more easily, and can therefore be brought to market in the underground economy much more quickly.

[108] Cf. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 9 and http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 12
[109] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf : p. 6

Geolocation by type of malicious code

Symantec examines the top regions reporting potential malicious code infections as well as 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. For instance, Trojans that attempt to steal account information for Brazilian banks are quite common in the Latin America (LAM) region, while malicious code that steals online gaming account information is most frequently observed in the APJ region.[110] Because of the different propagation mechanisms used by different malicious code types, and the different 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 presented in this discussion represent proportional geographic percentages. Therefore, proportional percentage fluctuation from the previous period to the current period does not indicate a change in the absolute number of reports from a specific region.

In 2008, 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.[111] While there were small variances in some regions, the changes were not representative of significant shifts in the threat landscape. The proportion of reports from the EMEA region increased, which may indicate that the concentration of threats targeting countries in EMEA is growing faster than the concentration in other regions. This may also be a sign that the concentration of malicious code authors, or organizations employing those authors, is greater in EMEA than in other regions. One possible reason for a higher concentration in this region may be due to recent reports of politically motivated attacks during this period.[112] This sort of activity may have increased the demand for capable authors in EMEA.

Trojans

In 2008, 35 percent of Trojans were reported from the North America (NAM) region, 34 percent from EMEA, 24 percent from APJ, and 6 percent from LAM (table 6). Although the number of Trojans reported from NAM appears to have dropped significantly, this is mainly attributable to the proportional increase in Trojans reported from EMEA, indicating that a similar amount of Trojan activity was reported in both NAM and EMEA in 2008.

Region	2008 Percentage	2007 Percentage
NAM	35%	46%
EMEA	34%	28%
APJ	24%	22%
LAM	6%	4%

Table 6. Geolocation of Trojans
Source: Symantec

[110] Cf. http://www.comscore.com/press/release.asp?press=2504 or http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 81
[111] Cumulative totals might not equal 100 percent due to rounding.
[112] See http://blogs.zdnet.com/security/?p=1670 and http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

The previous edition of the Symantec *Global Internet Security Threat Report* discussed the continued concentration of Trojans in North America, and posited that attackers may consciously be moving toward Trojan attacks there because of successful efforts by North American-based enterprises and ISPs to thwart worm attacks.[113] In 2008, the number of Trojans reported in EMEA was similar to the number reported in NAM. While the increase in EMEA could be attributed to similar reasons as those given in the previous paragraph, the proportional increase in reports of other malicious code types in EMEA suggests that the increased activity is not a reaction to any specific mitigation efforts.

One possible explanation for the increase in EMEA is that there were a number of attacks against prominent government and corporate websites in the region during 2008.[114] For example, one attack that targeted the websites of both the United Nations and the UK government, among others, injected malicious code that was designed to load content from an attacker-controlled location into visitors' browsers.[115] Another separate attack successfully defaced the national Albanian postal service website.[116] Such attacks are a perfect beachhead for distributing malicious code because they target high-traffic websites of reputable organizations. Successful distribution of malicious code using this method of delivery may have contributed to the increased proportion of Trojans in EMEA in 2008.

Worms

Forty percent of the potential infections caused by worms in 2008 were reported from the APJ region, followed by EMEA with 36 percent, NAM with 13 percent, and LAM with 11 percent (table 7). The drop in proportion of worms in APJ is mainly attributed to the increase in EMEA and may indicate that worm activity in EMEA will eventually surpass that of APJ. The emergence of the Downadup worm may offset this, however, and cause the percentage of potential worm infections in APJ to rise in 2009 since that is where it has been initially concentrated.

Region	2008 Percentage	2007 Percentage
APJ	40%	44%
EMEA	36%	32%
NAM	13%	16%
LAM	11%	9%

Table 7. Geolocation of worms
Source: Symantec

Back door infections

EMEA accounted for the largest proportion of potential back door infections reported worldwide in 2008, with 39 percent of the total. APJ accounted for the second largest percentage, with 29 percent, followed by NAM at 23 percent, and LAM at 9 percent (table 8). As with the previously discussed types of potential malicious code infection, the proportional increase in reports from EMEA is the primary contributor to decreases in other regions. As is discussed elsewhere in this report, there are indications that back doors are increasingly being incorporated as secondary stages of multistage attacks. Because of this, the proportional increase of back doors in EMEA may be closely related to the observed increase of Trojans reported there.

[113] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 52
[114] http://news.cnet.com/8301-10789_3-9983940-57.html
[115] http://news.cnet.com/8301-10789_3-9925637-57.html
[116] http://albmasters.com/?p=3

Region	2008 Percentage	2007 Percentage
EMEA	39%	36%
APJ	29%	30%
NAM	23%	28%
LAM	9%	5%

Table 8. Geolocation of back door infections
Source: Symantec

While the regional percentages of potential back door infections can show fairly 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.

Viruses

The APJ region continued to hold the highest concentration of reported potential infections caused by viruses in 2008, with 41 percent of the worldwide total, although this is a decrease from its 53 percent share in 2007 (table 9). The EMEA region again ranked second, with its share growing to 38 percent in 2008 from 27 percent in 2007. The proportion of potential virus infections concentrated in NAM dropped to 15 percent in 2008 from 17 percent previously, while LAM increased to 6 percent this period from 4 percent previously.

Region	2008 Percentage	2007 Percentage
APJ	41%	53%
EMEA	38%	27%
NAM	15%	17%
LAM	6%	4%

Table 9. Geolocation of viruses
Source: Symantec

As was the case with the previous reporting period, the increased proportion of viruses in EMEA was linked to the greater proportion of worms reported from the region, which is because viral infection functionality is a common component incorporated into worms.[117] For example, the Mabezat worm includes a viral infection component and was heavily concentrated in the EMEA region in 2008 (it was one of the top 10 potential infections reported from the region).

[117] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 53

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 use in criminal activities such as identity theft. As mentioned in the previous Symantec *Government Internet Security Threat Report*, identity theft was the most common consumer complaint received by the United States Federal Trade Commission in 2007 by a significant margin and is likely to continue being a primary concern.[118] With the widespread use of online shopping and Internet banking, compromises that result in unauthorized access to confidential information can result in significant financial loss, particularly if credit card information or banking details are exposed.

Within organizations, exposure of confidential information can lead to significant data leakage. If it involves customer-related data, such as credit card information, it can severely undermine customer confidence as well as violate local laws.[119] Compromised computers can also contain sensitive information such as financial details, business plans, and proprietary technologies, which could also be leaked.

Government agencies are also at risk from threats to confidential information. If employee data is exposed by these threats, the data could be used to facilitate exfiltration of confidential data or identity theft, which could then lead to further security compromises. For instance, if the attacker gains access to a user’s personal and system information, he or she can use it to craft a targeted social engineering attack tailored to that particular user. Additionally, certain agencies—such as those dealing with health care, revenue and taxation, and pensions—may store personally identifiable information of citizens, including government-issued identification numbers, that could be used for identity theft or related fraud.

In 2008, 83 percent of confidential information threats had a remote access component (figure 9). This was a decrease from 91 percent in 2007. This decrease is mainly attributable to an increase in malicious code that exports user data or logs keystrokes, along with the decrease in the percentage of potential infections from back doors. Another reason may be that attackers are less interested in administering individual compromised computers than they are in simply gathering the available information, which can be accomplished without installing a back door.

[118] http://www.ftc.gov/opa/2008/02/fraud.shtm

[119] Many countries have implemented their own laws in this regard, such as the United Kingdom’s Data Protection Act, which can be found at http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

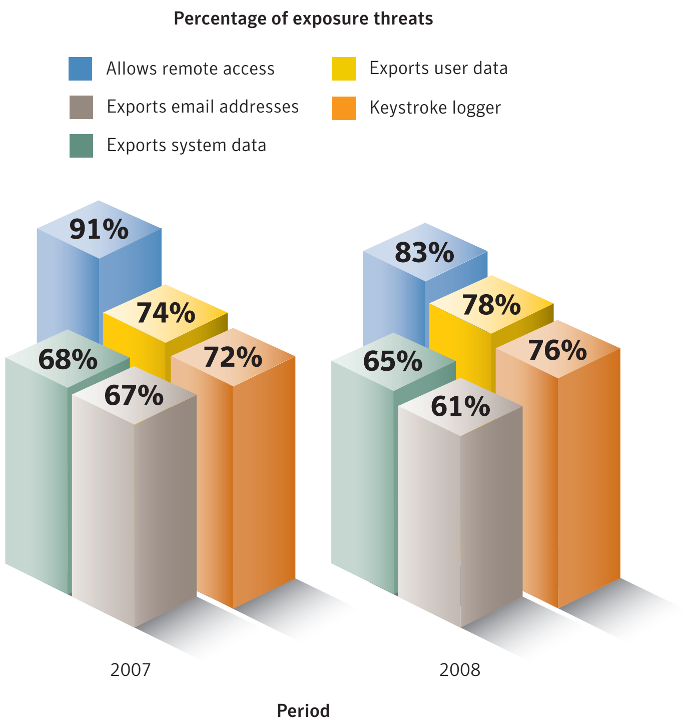

Figure 9. Threats to confidential information, by type
Source: Symantec

Malicious code that could export user data accounted for 78 percent of threats to confidential information in 2008, up from 74 percent in 2007. Such threats are useful because leaked data can be used to steal a user's identity or aid in further attacks. Increases in this type of exposure are not surprising considering the potential value of harvested information. The third highest exposure type, keystroke logging, further supports this.

Confidential information threats with a keystroke-logging capability made up 76 percent of threats to confidential information, up from 72 percent in 2007. Malicious code incorporating keystroke loggers that target online gaming account credentials continues to be popular. The Wowinzi worm is one such threat and was one of the top 10 new malicious code samples in 2008. Several Trojans and worms such as Gampass, Gammima,[120] and Mumawow[121] have been around for some time and are specifically designed to steal online gaming credentials, and they continue to account for a significant number of potential infections.

Organizations can take several steps to limit the exposure of confidential information by successful intrusions. Data leakage prevention solutions can prevent 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, as 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.[122] As a result, data should always be transmitted through secure channels such as SSH, SSL, and IPSec.

[120] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032206-2043-99
[121] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032015-4300-99
[122] 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.

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. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised via 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 2008, 66 percent of potential malicious code infections propagated as shared executable files, up significantly from 44 percent in 2007 (table 10).[123] Shared executable files are the propagation mechanisms employed by viruses and some worms to copy themselves onto removable media. The 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 exploits developed for floppy disks can be easily modified for current removable media devices.

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 policy 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.

2008 Rank	Propagation Mechanism	2008 Percentage	2007 Percentage
1	File-sharing executables	66%	44%
2	File transfer/email attachment	31%	32%
3	File transfer/CIFS	30%	26%
4	Remotely exploitable vulnerability	12%	15%
5	File sharing/P2P	10%	17%
6	File transfer/embedded HTTP URI/instant messenger	4%	3%
7	SQL	3%	3%
8	Back door/Kuang2	3%	3%
9	Back door/SubSeven	3%	3%
10	File transfer/instant messenger	2%	1%

Table 10. Propagation mechanisms
Source: Symantec

In 2008, 31 percent of malicious code that propagated did so in email attachments, a slight decrease from 32 percent in 2007. The previous volume of the Symantec *Government Internet Security Threat Report* stated that, despite a small increase for the reporting period, propagation through email attachments was surpassed by propagation through file sharing executables.[124] This was noted to likely be the result of diversification by malicious code authors. Although there was an increase again in 2008, the gap between the first and second ranked propagation mechanisms has widened substantially.

[123] Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.
[124] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 57

One possible reason for the diversification of propagation methods, as well as the resulting gap, is that malicious code authors may not be experiencing as much success with attacks using email attachments as in past years. Increased user awareness and prevention against email-based attacks may be a factor. However, the number of potential infections that use email-based propagation appears to be stable, which may be a result of attackers experiencing increased success with other propagation vectors and opting to use those instead. Despite such factors, email attachments continue to be a common and attractive propagation mechanism for malicious code.

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.

Malicious code that propagated by the CIFS protocol made up 30 percent of malicious code that propagated in 2008, up from 26 percent in 2007.[125] This indicates that this protocol continues to be a common and effective means for the propagation of malicious threats. The increase may be linked to the diversification of mechanisms discussed above. Two of the top 10 malicious code threats for 2008 employed this propagation mechanism. This includes the Fujacks worm,[126] a long-standing malicious code family in top 10 lists, and the Almanahe worm,[127] a modular threat that includes a viral component that has steadily increased in potential infections since its discovery early in 2007.

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. 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.[128]

An interesting decrease of note during 2008 was in the percentage of threats that propagate by exploiting remote vulnerabilities. While there was relatively stable activity in this type of threat through the majority of the year, that changed when the Downadup worm was discovered late in 2008. Downadup propagates by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability.[129] This worm has attracted a lot of attention because of its sophistication and aggressive infection routine. The first variant of Downadup is estimated to have infected over half a million computers, primarily in the APJ and LAM regions.[130] Symantec is monitoring its evolution to how Downadup affects the percentage of threats that propagate by exploiting remote vulnerabilities into 2009.[131]

[125] 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.
[126] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111415-0546-99
[127] http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99
[128] TCP port 445 is the default port used to run CIFS on TCP.
[129] http://www.securityfocus.com/bid/31874
[130] https://forums2.symantec.com/t5/Malicious-Code/W32-Downadup-Infection-Statistics/ba-p/376744
[131] Please see https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/225, https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/227, and https://forums.symantec.com/t5/Malicious-Code/Downadup-Small-Improvements-Yield-Big-Returns/ba-p/381717

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 address space layout randomization (ASLR).[132] 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.

[132] ASLR is a security mechanism that randomizes data in memory to prevent the success of attacks that leverage memory corruption vulnerabilities, such as buffer overflows.

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 an end user to enter his or her credentials into an online data entry field. This is one of the characteristics that distinguishes phishing from spam-based scams (such as the widely disseminated 419 scam and other social engineering scams).[133] 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.[134] Spam can also be used to deliver drive-by downloaders, which require no other end user interaction 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 2008; it will also discuss items that were offered for sale on underground economy servers during this time period, as 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 may 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. Specifically, statistics are gathered from enterprise customers' Symantec Brightmail AntiSpam servers that receive more than 1,000 email messages per day. This removes the smaller data samples (that is, smaller customers and test servers), thereby allowing for a more accurate representation of data.

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.

In addition to the Symantec Probe Network, phishing information is also gathered through the Symantec Phish Report Network, an extensive antifraud community of organizations and end users.[135] Members of the Symantec Phish Report Network contribute and receive fraudulent website addresses for alerting and filtering across a broad range of solutions.

[133] http://nortontoday.symantec.com/features/security_at_30.php
[134] http://news.bbc.co.uk/2/hi/technology/6676819.stm
[135] http://www.phishreport.net/

This section will address the following metrics:

- Phishing activity by sector
- Top countries hosting phishing websites and top targeted sectors
- Phishing websites by government top-level domains
- Underground economy servers—goods and services available for sale
- Spam by category
- 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 lures. These considerations are important for an enterprise because the use of its brand in phishing activity can significantly undermine consumer confidence in its reputation.

Previous volumes of the Symantec *Global Internet Security Threat Report* assessed phishing data based on the number of phishing websites that were targeted by the highest volume of phishing attacks.[136] However, in this volume, phishing activity will be assessed by sector according to the number of so-called phishing lures that are detected spoofing a company's brand. Phishing lures are URLs that lead end users to phishing websites and are usually delivered by spam email (also known as phishing email). Multiple lures can lead to the same phishing website.

Phishers are becoming increasingly adept at adapting their lures in order to direct end users to their phishing sites. For instance, in economically constrained circumstances, phishers may adopt lures that spoof well-known financial institutions and promise users access to low-interest loans. As a result, tracking phishing lures may give security analysts insight into what new tactics phishers are using.

The majority of brands used in phishing attacks in 2008 were in the financial services sector, accounting for 79 percent of the total, down slightly from the 83 percent reported in 2007 (table 11). The financial services sector also accounted for the highest volume of phishing lures during this period, at 76 percent, considerably higher than 2007 when the volume for financial services was 52 percent (figure 10).

It is likely that the increase in the percentage of phishing lures spoofing financial services is not so much due to an increase in the number of these lures, but to a drop in the number of lures spoofing Internet community-related brands, particularly social networking sites, as will be discussed later in this section. The rise in phishing lures that spoof financial services is reflected in the significant amount of credit card information that was offered on underground economy servers in 2008, as is discussed in the **"Underground economy servers"** discussion.

[136] 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.

Sector	2008 Percentage	2007 Percentage
Financial	79%	83%
ISP	8%	7%
Retail	4%	4%
Insurance	2%	2%
Internet community	2%	2%
Telecom	2%	<1%
Computer hardware	1%	1%
Government	1%	1%
Computer software	<1%	1%
Transportation	<1%	1%

Table 11. Unique brands phished, by sector
Source: Symantec

Phishing is often carried out for the purpose of financial gain. Brands and activities associated with the financial sector are most likely to yield data that could be used in financially motivated attacks, such as bank account credentials. As a result, it is not surprising that the majority of phishing activity detected in 2008 targeted brands in the financial sector.

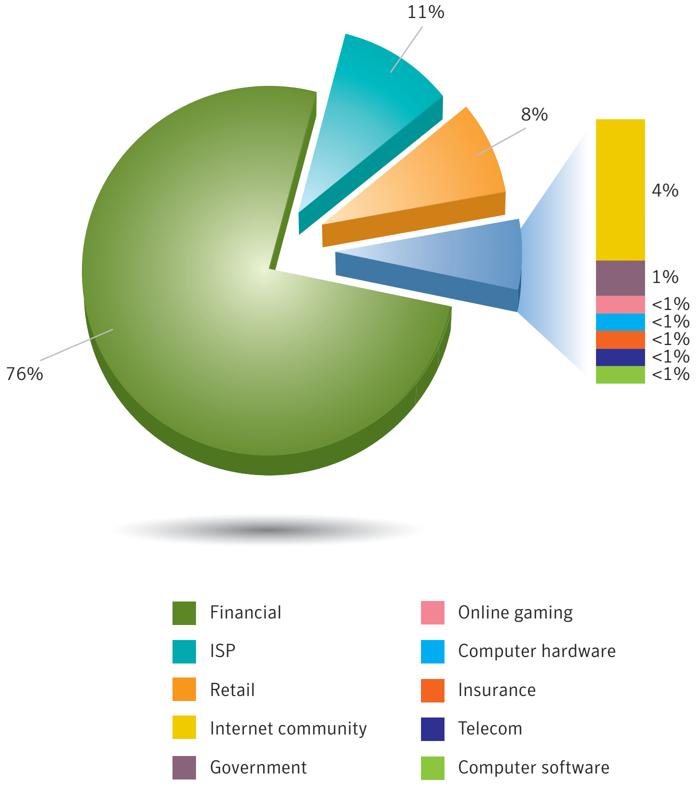

Figure 10. Phished sectors by volume of phishing lures
Source: Symantec

There are several items in the "Underground economy servers" discussion that illustrate the preponderance of financial services in phishing activity. The top two most frequently advertised items observed on underground economy servers during 2008 were credit card information and bank account credentials, in that order. Together, these two categories accounted for more than half of the goods and services advertised in 2008.

Many phishing attacks that spoof financial services brands will prompt users to enter credit card information or banking credentials into fraudulent sites. If this is done, the phishers can then capture and sell such information in the underground economy. This has been made easier for phishers because of the increasingly widespread acceptance of online banking. For example, 44 percent of Internet users in the United States perform some degree of online banking, as do 64 percent of users in Canada and 46 percent of those in France.[137] Because of this, end users may be more easily fooled into entering their information into fraudulent websites that mimic the brand of their financial services provider.

The 4 percent reduction in the number of financial sector brands being spoofed by phishing lures during 2008 may indicate increased awareness of phishing schemes and how to avoid falling victim to them. Information campaigns driven by specific financial institutions, as well as a heightened awareness of phishing schemes targeting financial services, have likely made it more difficult for phishers to carry out successful phishing attacks against companies offering those services. By the same token, it may also be a reflection of the fact that a number of financial institutions either ceased operations or changed their business offerings during 2008, thereby reducing the number of financial service brands available for phishers to spoof.[138]

ISPs were the second ranked sector for brands spoofed by phishing lures in 2007, making up 8 percent of the total. This is a 1 percentage point increase from 2007, when it also ranked second. The ISP sector also ranked second in the volume of phishing lures for 2008, accounting for 11 percent of the total, up from 4 percent in 2007. Again, the percentage increase in the volume of lures spoofing ISPs was likely due to a drop in the number of lures spoofing brands associated with Internet communities, as will be discussed shortly.

ISP accounts, which often include email accounts, can be valuable targets for phishers because people frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including email accounts. With a little effort on the part of the attacker, this information could provide access to other accounts, such as online banking accounts.

Attackers also sometimes use the free Web-hosting space that is often included in ISP accounts to put up phishing websites, or use the accompanying email accounts to send spam or launch further phishing attacks. Compromised ISP Web-hosting accounts can also be used to host Web-based exploits, which would give an attacker a greater number of potential targets. Compromised Web space can also be used to plant links to other websites that an attacker controls in order to boost the search engine rankings of those sites.

In addition, having access to an email account could allow the attacker to spam the victim's contact list—and likely enjoy greater success with this ploy because people tend to trust email from people they know. This assertion is enforced by email accounts/passwords and addresses being the third and fourth most common goods available on underground economy servers in 2008, respectively.

[137] http://www.comscore.com/press/release.asp?press=2524
[138] http://www.economist.com/finance/displayStory.cfm?story_id=12294688&source=features_box_main

The third most spoofed sector for 2008 was retail services, which accounted for 4 percent of organizations whose brands were spoofed by phishing attacks in 2008, the same percentage as 2007. The retail sector also ranked third in volume of phishing lures, accounting for 8 percent of the total for 2008, down from 12 percent recorded in 2007.

The retail sector is a logical target of phishers for several reasons. First, online retailers regularly conduct transactions that require the input of financial information, which could be fraudulently obtained and used for financial gain. By successfully mimicking a retailer's website, phishers will try to persuade users to attempt a purchase and enter their credit card information. They may also be able to persuade users to enter account information (such as usernames and passwords) that can then be used to access the account on the retailer's legitimate website. This can in turn be used to fraudulently order goods that are charged to the user's account. Many online stores give customers the option of storing credit card and billing information to facilitate the checkout process. Access to this information also gives phishers access to the victim's billing address, which is used by merchants as a security feature.

As has been mentioned previously, the volume of phishing lures spoofing brands associated with Internet communities, such as social networking sites, dropped significantly over the past year, from 31 percent in 2007 to only 4 percent in 2008. The previous two volumes of the Symantec *Global Internet Security Threat Report* discussed the rapid rise in lures targeting this sector and postulated that it was likely due to the increase in usage of these sites, as well as the fact that users associated with these communities generally tend to be trusted by other users.

Given the rapid rise of phishing activity targeting this sector in previous years, and the notable drop in volume in 2008, it is likely that companies in this sector have taken steps to either bolster security against phishing activity or limit its effectiveness. This could include increased network security measures and increased user awareness and education.

It is also likely that many of these communities have improved their ability to quickly identify phishing websites and have them taken down, reducing the window of exposure of end users to such websites. It may also be the case that phishers have concluded that there are more direct ways to obtain information that can be used for financial gain, such as spoofing brands associated with financial services organizations.

Top countries hosting phishing websites and top targeted sectors

This metric will assess the countries in which the most phishing websites were hosted in 2008. This data is a snapshot in time, and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also be noted that the fact that a phishing website is hosted in a certain country does not necessarily mean that the attacker is located in that country.

In 2008, 43 percent of all phishing websites detected by Symantec were located in the United States (table 12). This is considerably less than 2007, when 69 percent of phishing websites originated there. Of the phishing websites situated in the United States, 82 percent spoofed brands associated with financial services. This is in keeping with the Internet-wide average, since 76 percent of phishing websites detected across the Internet as a whole were associated with financial service organizations.

It is worth noting that of the top 10 countries for phishing websites in 2008, only the United States experienced a drop in activity. All other countries in the top 10 experienced growth (albeit relatively minor in most cases) or stayed relatively the same. Because the United States hosted such a vast majority of phishing websites in 2008, it is reasonable to conclude that the changes in percentage were due to a drop in the absolute number of these websites being hosted in the United States, rather than a rise in those situated in other countries. This could be related to the shutdown of ISPs that were being used for large volumes of spam activity.

Rank	Country	2008 Percentage	2007 Percentage	2008 Top Sector Targeted in Country	2008 Percentage of Lures Targeting Top Sector
1	United States	43%	69%	Financial services	82%
2	Poland	6%	1%	Financial services	94%
3	China	4%	3%	ISP	50%
4	France	4%	2%	Financial services	87%
5	South Korea	4%	4%	Financial services	88%
6	Russia	3%	2%	Financial services	60%
7	Germany	3%	3%	Financial services	79%
8	United Kingdom	3%	3%	Financial services	86%
9	Canada	3%	2%	Financial services	77%
10	Italy	2%	<1%	Financial services	67%

Table 12. Top countries hosting phishing websites and top targeted sectors
Source: Symantec

Of the phishing websites hosted in the United States in 2008, 82 percent targeted the financial services sector. As noted in “Phishing activity by sector,” attacks that spoof financial companies give phishers the best opportunity to attain information that can be used for financially rewarding attacks. In 2007, the Internet community sector was the sector most commonly spoofed by phishing websites based in the United States, accounting for 55 percent of the total, while financial services ranked second with 41 percent.

It is likely that phishers based in the United States have moved away from Internet community-based phishing websites due to countermeasures undertaken by companies in this sector to guard against phishing attacks—most likely through user-education campaigns. It may also be that phishers have moved toward financial services because this sector provides more opportunities for profit. With the current economic downturn, end users may be more susceptible to phishing attacks that advertise low interest rates for mortgages and credit cards or that claim to be associated with the administration of financial institutions that are undergoing some sort of restructuring or cessation.

Poland hosted the second highest percentage of phishing websites in 2008, with 6 percent of the total. This is a significant change from 2007, when Poland hosted just 1 percent of phishing websites and was only the fourteenth-ranked country in this category. Poland’s increased rank in 2008 may also be due to remotely situated attackers compromising computers in Poland to use them to host phishing websites, possibly due to recent crackdowns on fraudulent activity in other countries. For instance, in November 2007, the Russia-based operations of the Russian Business Network (RBN) were reportedly shut down.[139] The RBN reputedly specializes in the distribution of malicious code, hosting malicious websites, and other malicious activity, including the development and sale of the MPack toolkit. The RBN has been credited for

[139] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 11

creating approximately half of the phishing incidents that occurred worldwide last year, and reputedly associated with a significant amount of malicious Internet and computer activities in 2007. It is possible that when its operations in Russia were shut down, it relocated some of its operations to Poland, therefore contributing to the high number of phishing websites detected there in 2008.

China hosted the third highest percentage of phishing websites in 2008, with 4 percent of the total. This is up from fourth rank and 3 percent in 2007. The sector most commonly targeted by phishing websites hosted in China in 2008 was the ISP sector, which was spoofed by 50 percent of all known sites there. In 2007, the financial services sector was the sector most commonly spoofed by phishing websites based in China, with 44 percent of the total.

Of the top 10 countries for phishing websites, China was the only one in which the top targeted sector was ISPs. Financial services was the most commonly targeted sector for all of the other top 10 countries. As discussed previously in **"Phishing activity by sector,"** ISPs make valuable targets for phishers because of the potential wealth of personal information from the ISP accounts of end users that is often fairly easily accessed by skilled attackers and which provides many avenues for further malicious exploits.

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 2008. [140] 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 the 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. Instead, it is likely that they are using spoofed domains or the website is 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 insufficiently protecting their TLDs 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. Further, government websites are often high-traffic sites that attract a lot of traffic, thereby making them attractive for phishers to spoof in order to attract a high number of potential victims.

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 was to obtain personal information from end users through fraudulent emails that referred to tax refunds. These attacks have been documented in both Canada and the United States.[141]

[140] 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.

[141] http://www.phishbucket.org/main/content/view/4135/103/

The top government TLD detected as being used by phishing websites in 2008 was .go.th, with 23 percent of the total. This TLD is used for websites associated with the government of Thailand. In 2007, this TLD ranked 18th and was used by 2 percent of government TLDs that were detected being used by phishing lures.

Rank	Top-level Domain	Percentage
1	.go.th	23%
2	.go.ro	13%
3	.go.id	8%
4	.gov.co	7%
5	.go.ke	5%
6	.gov.br	4%
7	.gov.ph	4%
8	.gov.in	3%
9	.go.kr	3%
10	.gov.ec	3%

Figure 13. Top government TLDs being used by phishing websites
Source: Symantec

Thailand accounted for 1 percent of all malicious activity observed by Symantec on the Internet in 2008, making it the twenty-sixth ranked country for this consideration, although it was the seventeenth ranked country for spam zombies and eighteenth for phishing hosts for 2008.

The second most commonly used government TLD for phishing sites was .go.ro, with 13 percent of the total. This is the TLD used by Romanian government websites. In 2007, .go.ro was the fifth most commonly used government TLD, accounting for 6 percent of the total. Romania ranked 27th for overall malicious activity in 2008, with approximately 1 percent of that total.

The third most commonly used government TLD in phishing lures detected in 2008 was .go.id, with 8 percent. This is the TLD for the government of Indonesia. In 2007, .go.id ranked 19th for government TLDs used in phishing lures, accounting for approximately 2 percent of the total. Less than 1 percent of all malicious activity detected in 2008 originated in Indonesia, making it the 41st ranked country for the year.

Underground economy servers—goods and services available for sale

This discussion focuses on the most frequently advertised items for sale observed on underground economy servers. Underground economy servers are black market forums for the promotion and trade of stolen information and services. This information can include government-issued identification numbers, credit cards, credit verification values, debit cards, personal identification numbers (PINs), 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 occurs within channels on Internet Relay Chat (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.[142]

[142] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

The measure of goods and services available for sale is by distinct messages, which are considered to be 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 2008, the most frequently advertised item observed on underground economy servers was credit card information, accounting for 32 percent of all goods (table 14). This was an increase from 21 percent in 2007. Credit card information advertised on the underground economy consists of the credit card number and expiry date, and may also include the name on the card (or business name for corporate cards), billing address, phone number, CVV2 number, and PIN.[143] One reason for this ranking may be because there are many ways credit card information can be obtained for fraud. This includes phishing schemes, monitoring merchant card authorizations, the use of magnetic stripe skimmers, or breaking into databases and other data breaches that expose sensitive information.[144]

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	$0.06–$30
2	2	Bank account credentials	19%	17%	$10–$1000
3	9	Email accounts	5%	4%	$0.10–$100
4	3	Email addresses	5%	6%	$0.33/MB–$100/MB
5	12	Proxies	4%	3%	$0.16–$20
6	4	Full identities	4%	6%	$0.70–$60
7	6	Mailers	3%	5%	$2–$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of $200–$2000 per item
9	17	Shell scripts	3%	2%	$2–$20
10	8	Scams	3%	5%	$3–$40/week for hosting, $2–$20 design

Table 14. Goods and services available for sale on underground economy servers[145]
Source: Symantec

The frequent use of credit cards also influenced their high rank in 2008. For example, the 23.6 billion credit card transactions in the United States in 2007 represent a growth of 6 percent over the previous year.[146] High frequency use and the range of available methods for capturing credit card data would generate more opportunities for theft and compromise and, thus, lead to an increased supply on underground economy servers. Despite the economic slowdown of the last half of 2008, both the number of online purchases by credit card and the amount of purchases increased. Online spending for 2008 has been growing since the previous year with sales increased.

[143] Card Verification Value 2 (CVV2) is a three- or four-digit number on the credit card that is used for card-not-present transactions, such as purchases over the Internet or telephone. This is meant to improve security for credit cards and to verify that the person completing the transaction is in fact, in possession of the card.
[144] Magnetic stripe skimming devices are small machines designed to scan and retain data contained in the magnetic stripes on credit and debit cards.
[145] Descriptions and definitions for the goods and services discussed in this section can be found in Appendix D—Phishing and Spam Trends Methodology
[146] http://www.bis.org/publ/cpss85p2.pdf : table 7

Credit cards may also be popular on underground economy servers because using fraudulent credit card information for activities such as making online purchases is relatively easy. Online shopping can be easy and fast, and a final sale often requires only basic credit card information. Someone knowledgeable enough could potentially make many transactions with a stolen card before the suspicious activity is detected and the card is suspended. Once the purchases have been completed and the merchandise delivered, it can then be fenced for a profit. Also, online merchants who have yet to implement multi-level security features are likely attractive to criminals who wish to conduct fraudulent transactions without hassle.

Another factor that contributes to the popularity of credit cards is that they are typically sold in bulk packages on underground economy servers. Not only do advertisers offer discounts for bulk purchases or include free numbers with larger purchases, but having an extensive list of cards enables individuals to quickly try a new number if a card number does not work or is suspended. Also, having a larger number of credit cards numbers included should theoretically increase the likelihood of having active/valid cards in the bulk package.

The price range of credit cards in 2008 remained consistent with the prices from the previous year, ranging from $0.06 to $30 per card number. There were three main factors that influenced the price of credit cards: 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 rarity of the credit card information is often associated with the location of the issuing bank and the type of card. Information from regions such as Europe, Asia, and the Middle East is typically offered at higher prices than elsewhere because the supply of credit card information for these regions is rarer. For example, cards from countries such as Sweden or Belgium were the most costly, at an average of $20 each, while cards issued from the United States were the least expensive.

The lower price range for credit cards was also due to bulk purchase discounts offered by sellers. Credit cards are typically sold in bulk, with lot sizes from as few as 10 credit cards to as many as 5,000. Common bulk amounts and rates observed by Symantec during this reporting period were 100 credit cards for $150 ($1.50 each), 140 credit cards for $120 ($0.86 each), and 5,000 credit cards for $300 ($0.06 each).

As with other areas of the underground economy, the availability of the item seems to determine its price: an increase in supply will decrease the price of the goods. There are more credit cards in circulation in the United States than in any other country in the world—1.3 billion cards by the end of 2007, which is an average of over four credit cards per person.[147] In comparison, there were only 67 million credit cards in circulation in the United Kingdom, which is an average of one per inhabitant and only 5 percent of the U.S. total. This correlates with the originating location percentages of credit cards advertised on underground economy servers for this reporting period: cards issued by U.S.-based institutions accounted for 67 percent of the total, while cards from UK-based institutions accounted for 11 percent. This ratio also corresponds to advertised bulk package prices: UK cards were typically advertised at rates three to four times higher than U.S. cards.

[147] http://www.bis.org/publ/cpss85p2.pdf : tables 10 and 10b

The second most commonly advertised good on underground economy servers during 2008 was bank account credentials, accounting for 19 percent of all advertised goods. This was a slight increase from 17 percent observed in 2007. Bank account credentials may consist of account numbers, bank transit numbers, account holder names and/or company names, and may include online banking passwords. Also, most sellers advertised the type of account and the balances for the stolen bank accounts. Attackers can steal bank account credentials using the same methods as were outlined in the discussion of credit cards previously in this section.

The popularity of bank account credentials may be due to a shift toward online banking. As mentioned earlier, in the United States, 44 percent of Internet users perform some degree of online banking.[148] That number is even higher in Canada and France, where 64 percent and 46 percent of Internet users bank online, respectively.[149] The potential increased availability of such sensitive information would likely also result in an increase in attempts to steal banking credentials through phishing attempts or the use of malicious code such as banking Trojans. For example, Symantec observed an 86 percent increase in potential banking Trojan infections in the second half of 2007.

Bank account credentials are attractive to attackers because they offer the opportunity to withdraw currency directly. Withdrawing currency from a bank account has the advantage of a more immediate payout than with online purchases, which would need to be sold to realize a purely financial reward. Also, attackers have access to the full balances in the bank accounts, unlike credit cards where the credit limits imposed will not allow access to the maximum potential balances. Bank account balances advertised were also considerably higher than credit card limits; in 2008, the average advertised bank account balance was just over $176,000, while the average credit card limit was just over $3,400. It is likely that advertisers are skewing the average by promoting bank accounts with high balances, specifically from corporate accounts, to attract customers. Symantec observed advertisements with balances ranging from $3,000 to one with over $2.4 million. Beyond straightforward account cash outs, bank accounts can also be used as intermediary channels to launder money or to fund other online currency accounts that only accept bank transfers for payments.

The advertised price for bank account credentials varied as widely as it did in 2007, with prices ranging from $10 to $1,000, depending on the amount of funds available, the location of the account, and the type of account. Corporate and business accounts were advertised for considerably higher prices than those of personal bank accounts as they typically had higher balances on average. Symantec observed one EU business bank account—purportedly holding a balance of $400,000—being advertised for sale for $600. In addition, EU accounts were advertised at a considerably higher average price than their U.S. counterparts, which may be because EU accounts are rarer than U.S. accounts on underground economy servers. Furthermore, bank account credentials that bundled in additional information such as names, addresses, dates of birth, and mothers' maiden names were advertised at higher prices, presumably because this added information could potentially be used for further identity fraud.

[148] http://www.comscore.com/press/release.asp?press=2318
[149] http://www.comscore.com/press/release.asp?press=2524

Email accounts were the third most common item advertised for sale on underground economy servers in 2008, making up 5 percent of all advertised goods, an increase from 4 percent in 2007. Gaining possession of email passwords can allow access to email accounts, which can be used for sending out spam and/or for harvesting additional email addresses from contact lists. Recipients of the spam emails may be more trusting of emails coming from a known email address. Moreover, along with email, many ISPs include free Web space in their account packages, which many people rarely access. Once the ISP accounts are compromised, these free spaces can be used to host phishing sites or malicious code without the knowledge of the victims.

In addition, compromised email accounts will often provide access to additional sensitive personal information such as bank account data, student identification numbers, mailing address and phone numbers, or access to other online accounts (such as social networking pages, online stock accounts, etc.) that is stored in saved personal emails. From there, it is often simple for someone to use the password recovery option offered on most online registration sites and have a new password sent via email to gain complete access to these accounts. This danger is compounded by the fact that many people have of using the same password for multiple accounts. The fraudulently gained personal information can then be used to conduct identity theft and fraud.

The advertised prices of email accounts depended on the ISP of the account; larger ISPs that offered large amounts of Web space were advertised at higher prices than ones with smaller space. Web-based email accounts from various ISPs around the world were advertised, although the location used to register the account did not factor into the advertised price since users could obtain the same type of access worldwide. Accounts registered in Europe, the United States, and the Middle East were advertised at the same prices for this reporting period, ranging from $1 to $100 for each account.

The 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 seems to suggest that criminals are more focused on purchasing goods that allow them to make large quantities of money quickly on underground economy servers rather than on exploits that require more time and resources, such as scam pages and email lists for spamming. This trend is likely to continue until steps are taken to make it more difficult to obtain and use this financial information.

As part of their best practices to help prevent fraud, credit card companies, credit card issuers, and banks have been taking more secure measures to verify and authenticate users, such as multi-factor authorization or using technologies such as chip and PIN on the credit cards they issue.[150] By instituting effective multi-factor authentication and multi-level security systems, banks and credit card companies can make it more difficult for criminals to exploit stolen financial information. Also, security features such as Smart Card-based credit cards using the EMV standard for security verification,[151] or credit cards with chip & PIN technology for card-present transactions can make it more difficult for criminals to obtain and use financial information.

[150] http://www.chipandpin.co.uk/reflib/Consumer_digi-guide_Post_14_Feb_FINAL.PDF

[151] EMV is a standard for authenticating credit and debit card payments. The name originates from the initial letters of Europay, MasterCard, and VISA, who together developed the standard. Cf. http://www.emvco.com/about_aspx

Another technology currently being tested in the United Kingdom for card-not-present transactions, such as online shopping, are credit cards with one-time codes. To complete the transaction, credit card holders enter their PIN into the built-in keypad on the back of the card. Once the correct PIN is entered, the card will display a six-digit one-time code to be used to authenticate the transaction.[152] This code would be unique for each specific transaction. Even if the card is stolen or lost, a criminal would need the PIN to use the card.

Moreover, consumers who fear identity theft and payment fraud may be moving toward Internet-based payment services and other non-credit card electronic payment services. These types of services have become more popular because they do not expose the credit or debit card information that is used to set up the accounts and, as with some credit card issuers, often offer full protection from unauthorized transactions. In addition, they allow people without credit cards to make online purchases.

Nonetheless, even though consumers seem to be moving toward other non-credit card electronic payment services for online payments, credit cards are still the most popular payment method. People may prefer to use credit cards over other payment options because of the added bonuses sometimes associated with using them, such as zero liability, flight points, cash-back options, travel options, or dividend bonuses. In the United States, the value of credit card transactions for 2006 was estimated at just over $2.1 trillion—the equivalent of nearly $7,000 for each person in the United States.[153]

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 weed out particular spam attacks, such as those that are determined to be potential fraud attacks.

The most common type of spam detected in 2008 associated with Internet- or computer-related goods and services, which made up 24 percent of all detected spam (figure 11). In 2007, this was the second most common type of spam, accounting for 19 percent of the total. This type of spam is typically used to promote Web hosting and design, as well as other online commodities such as phishing and spam toolkits. Since phishing and spam toolkits cannot typically be advertised by legitimate means, such as through banner ads on websites, spam may be the most effective way to promote them.

The increase in spam associated with Internet- or computer-related goods and services is reflected in the items that were most commonly available on underground economy servers in 2008, as discussed in **“Underground economy servers”** previously. Email addresses, which are usually purchased for the sake of spamming, were the fourth most commonly advertised good.

[152] http://www.visaeurope.com/pressandmedia/newsreleases/press377_pressreleases.jsp
[153] http://www.bis.org/publ/cpss85p2.pdf : tables 9 and 9d

Furthermore, scams ranked tenth in items for sale on underground economy servers in 2008. Scams advertised on these servers consist of creating scam Web pages, creating and disseminating scams, or hosting scam pages. Fraudsters promote these items, and buyers can often find them advertised on underground economy servers. This spamming activity in turn adds to the growth of the underground economy servers. Some of the phishing scams result in the harvesting of credit card and bank account credentials, which are then sold on underground economy servers.

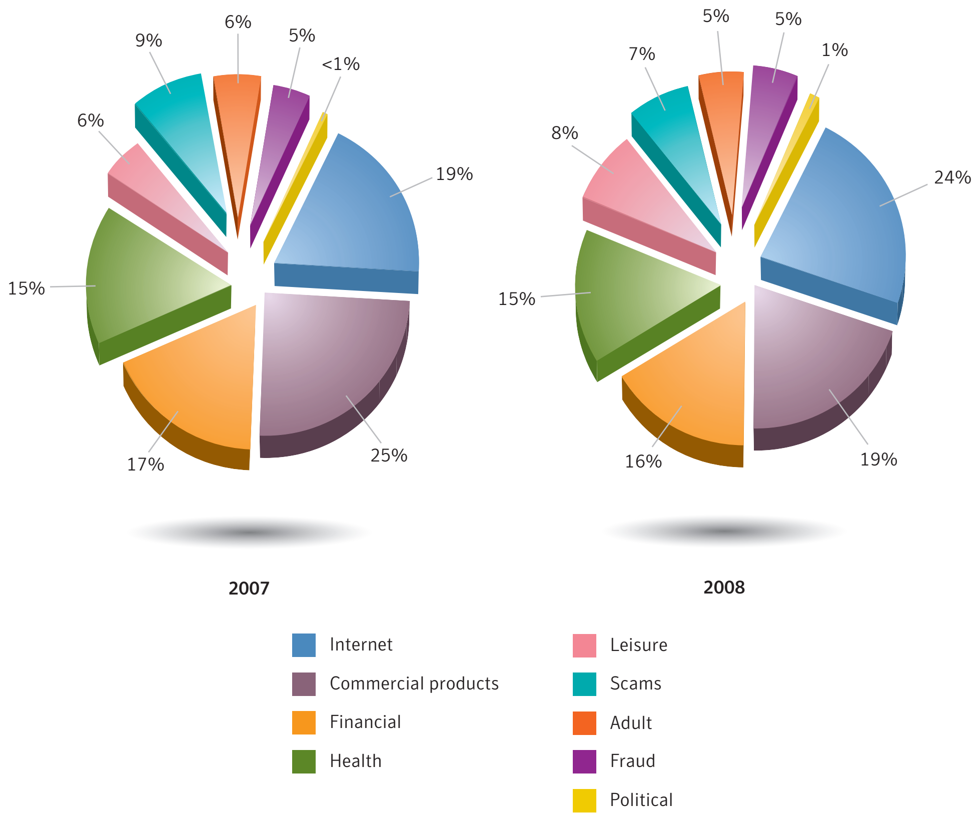

Figure 11. Top spam categories
Source: Symantec

The second most common type of spam detected in 2008 was related to commercial products, which made up 19 percent of all spam detected by Symantec sensors. In 2007, commercial spam was the most common type of spam, accounting for 25 percent of the total. Commercial products spam usually consists of advertisements for commercial goods and services. Such spam is frequently used to sell designer goods such as watches, handbags, and sunglasses. The profits from the sale of these products can be substantial given that the goods sold are often cheaply made counterfeits.

For 2008, Internet-related spam and commercial-products spam not only switched places from the previous year, but also percentages. Symantec believes this may be the result of the economic downturn. It is possible that, with the drop in consumer confidence, people are less inclined to buy the types of goods and services advertised by commercial-product spam.

Spam related to financial services made up 16 percent of all spam detected in 2008, making it the third most common type of spam during this period. Financial services spam contains references or offers related to money, the stock market, or other financial "opportunities." This is almost unchanged from 2007, when financial services spam was also the third most common type of spam, with 17 percent of the total. While it might be expected that spam offering stock market tips or other financial opportunities would drop off during a period of market uncertainty, it is likely that such a drop-off would be negated by an increase in spam offering such recession-related enticements as low-interest loans and easy access to credit.

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.[154] 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.[155]

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.[156] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, and provide a means to report suspected phishing sites.[157]

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.[158] So-called typo domains and homographic domains should also be monitored.[159] 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.

[154] 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.

[155] 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.

[156] Cf., 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

[157] Cf. http://www.antiphishing.org for information on the latest phishing threats.

[158] "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.

[159] 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".

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

Users should review bank, credit card, and credit information frequently. This can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[160] 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. Also, 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.

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

Appendix A—Symantec 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.
- Turn off and remove services that are not needed.
- 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.
- Always keep patch levels up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, email, and DNS services.
- 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.
- 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.
- Isolate infected computers quickly to prevent the risk of further infection within the organization.
- Perform a forensic analysis and restore the computers using trusted media.
- 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.
- 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.
- Educate management on security budgeting needs.
- Test security to ensure that adequate controls are in place.
- 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.
- 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.

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 by using Symantec Security Check at www.symantec.com/securitycheck.
- Deploy an antiphishing solution. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
- 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.
- 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 as a consequence 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 Activity Trends Methodology

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.

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.[161] 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 well-coordinated and aggressive fashion at some point in time during the reporting period.

[161] http://datalossdb.org

Bot command-and-control servers

Symantec tracks the number of new bot C&C servers detected worldwide. Only IRC and HTTP bot C&C server trends will be evaluated in the methods botnet owners are using to communicate with their bot-infected computers.

Top Web-based attacks

To evaluate this metric, Symantec identifies each distinct attack delivered via 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 based 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.

Top 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.

Appendix C—Malicious Code Trends Methodology

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

Symantec developed the Symantec AntiVirus research Automation (SARA) technology to help detect and eradicate computer viruses. This technology 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 Methodology

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. Over eight billion email messages, 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 Symantec Phish Report Network (PRN) is an extensive antifraud community whose members contribute and receive fraudulent website addresses for alerting and filtering across a broad range of solutions. These sites are categorized according to the brand being phished and its sector. PRN members and contributors send in phishing attacks from many different sources. This includes a client detection network that detects phishing websites as the clients visit various websites on the Internet. It also includes server detection from spam emails. The sender confirms all spoofed websites before sending the address of the website into the PRN. After it is received by the PRN, Symantec spoof detection technology is used to verify that the website is a spoof site. Research analysts manage the PRN console 24 hours a day, 365 days of the year, and manually review all spoof sites sent into the PRN to eliminate false positives.

Top countries hosting phishing websites and top targeted sectors

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

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.

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

04/09 20016966