SYMANTEC ENTERPRISE SECURITY

symantec.

Confidence in a connected world.

# Symantec Internet Security Threat Report

## Trends for 2008

Volume XIV, Published April 2009

## Executive Summary

The Symantec *Internet Security Threat Report* consists primarily of four reports: the *Global Internet Security Threat Report*; the *EMEA Internet Security Threat Report*, for the Europe, the Middle East, and Africa (EMEA) region; the *APJ Internet Security Threat Report*, for the Asia-Pacific/Japan (APJ) region; and the *Government Internet Security Threat Report*, which focuses on threats of specific interest to governments and critical infrastructure sectors. Together, these reports provide a detailed overview and analysis of Internet threat activity, malicious code, and known vulnerabilities. Trends in phishing and spam are also assessed, as are observed activities on underground economy servers.

This summary will discuss current trends, impending threats, and the continuing evolution of the Internet threat landscape based on data for 2008 discussed within the four reports. This summary will also discuss how regional differences can affect malicious activity globally.

There are a number of trends noted in previous volumes of the Symantec *Internet Security Threat Report* that continued in 2008: malicious activity has increasingly become Web-based; attackers are targeting end users instead of computers; the online underground economy has consolidated and matured; and attackers are able to rapidly adapt their attack activities.[1]

Symantec recently examined these trends along with the continued consolidation of malicious activities in the online underground economy in the Symantec *Report on the Underground Economy*.[2] That report found that the underground economy is geographically diverse and able to generate millions of dollars in revenue for (often) well-organized groups. The underground economy is also increasingly becoming a self-sustaining

[1] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
[2] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

**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

**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

**Candid Wueest**
Threat Analyst
Security Technology and Response

**Paul Wood**
Senior Analyst
MessageLabs Intelligence, Symantec

**Dan Bleaken**
Threat Analyst
MessageLabs Intelligence, Symantec

**Greg Ahmad**
Threat Analyst
Security Technology and Response

**Darren Kemp**
Threat Analyst
Security Technology and Response

**Ashif Samnani**
Threat Analyst
Security Technology and Response

system where tools specifically developed to facilitate fraud and theft are freely bought and sold. These tools are then used for information theft that may then be converted into profit to fund the development of additional tools.

Based on the data and discussions presented in the current Symantec *Internet Security Threat Report*, this summary will examine the primary methods being used to compromise end users and organizations, who is generating these attacks, and what these attackers are after. Finally, this summary will look at emerging trends that Symantec believes will become prevalent in the immediate future.

## How users are being compromised

Web-based attacks are now the primary vector for malicious activity over the Internet. The continued growth of the Internet and the number of people increasingly using it for an extensive array of activities presents attackers with a growing range of targets as well as various means to launch malicious activity.[3] Within this activity, Symantec has noted that most Web-based attacks are launched against users who visit legitimate websites that have been compromised by attackers in order to serve malicious content.

Some of the common techniques used by attackers to compromise a website include exploiting a vulnerable Web application running on the server (by attacking through improperly secured input fields), or exploiting some vulnerability present in the underlying host operating system. In 2008 alone, there were 12,885 site-specific vulnerabilities identified (figure 1) and 63 percent of vulnerabilities documented by Symantec affected Web applications. Attackers can exploit these vulnerabilities in a website or underlying application to modify the pages served to users visiting the site. This can include directly serving malicious content from the site itself, or embedding a malicious iframe on pages that can redirect a user’s browser to another Web server that is under the attacker’s control.[4] In this way, the compromise of a single website can cause attacks to be launched against every visitor to that site.

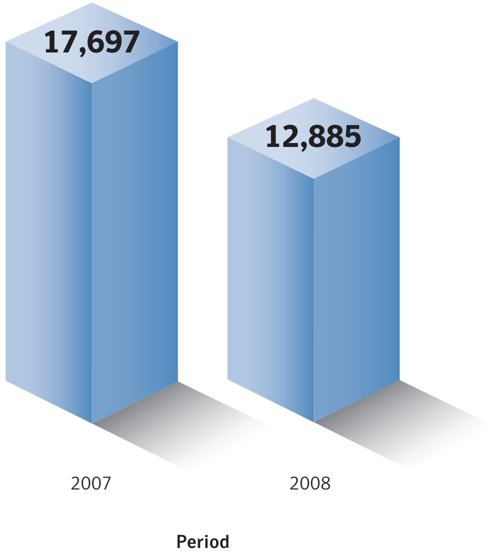

**Figure 1. Site-specific vulnerabilities**
*Source: Based on data provided by the XSSed Project*[5]

[3] http://www.verisign.com/static/043939.pdf
[4] An iframe is an HTML element that can include Web content from other pages or Web servers to be rendered when the user visits the original page. This tag can be constructed so that it is effectively invisible and the user will not see any of the embedded content when viewing the original page.
[5] Data was provided by the XSSed Project, a site devoted to tracking and verifying reports of site-specific cross-site scripting vulnerabilities: http://www.xssed.com.

In the case of a popular, trusted site with a large number of visitors, this can yield thousands of compromises from a single attack. 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.[6] Another separate attack successfully defaced the national Albanian postal service website.[7] These types of attacks provide an optimal beachhead for distributing malicious code because they target high-traffic websites of reputable organizations.

In order to compromise the largest possible number of websites with a single mechanism, attackers will attempt to compromise an entire class of vulnerability by searching for commonalities within them and generically automating their discovery and exploitation. This allows attackers to compromise websites with the efficiency commonly found in network worms.

The lengthy and complicated steps being pursued to launch successful Web-based attacks also demonstrate the increasing complexity of the methods used by attackers. While a single high-severity flaw can be exploited to fully compromise a user, attackers are now frequently stringing together multiple exploits for medium-severity vulnerabilities to achieve the same goal. An indication of this is that eight of the top 10 vulnerabilities exploited in 2008 were rated as medium severity.

Many enterprises and end users will often make patching high-severity vulnerabilities a top priority, while medium- and low-severity vulnerabilities may be ignored. This could result in the possibility of more computers remaining exposed for longer periods to these vulnerabilities. For example, of the 12,885 site-specific cross-site scripting vulnerabilities identified by Symantec in 2008, only 394 (3 percent) are known by Symantec to have been fixed.[8]

These developments and trends indicate that Web-based threats have not only become widespread, but that they have also increased in sophistication. In particular, Symantec has noticed that some botnets (such as Asprox,[9] which was initially used for phishing scams) are being redesigned to specifically exploit cross-site scripting vulnerabilities in order to inject malicious code into compromised websites.[10]

In many cases, medium-severity vulnerabilities are sufficient to mount successful attacks if attackers are able to execute arbitrary code and perform actions such as accessing confidential information or making network connections. This is made possible because many end users do not require administrative privileges to run or modify the targeted applications. While the danger of client-side vulnerabilities may be limited by best practices, such as restricting Web applications at the administrative level, this is often unrealistic 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 individual end users as well as at the enterprise level.

That said, however, a single high-severity vulnerability was the top attacked flaw in 2008. Previous editions of the Symantec *Internet Security Threat Report* noted that there has been a decrease in the volume of network worms, partly due to a lack of easily exploitable remote vulnerabilities in default operating system components. Many network worms exploited such vulnerabilities in order to propagate. Highly successful worms—such as CodeRed,[11] Nimda,[12] and Slammer[13]—all exploited high-severity vulnerabilities in remotely

[6] http://news.cnet.com/8301-10789_3-9925637-57.html
[7] http://albmasters.com/?p=3
[8] For the purpose of this report, the term cross-site scripting encapsulates two broad classes of vulnerability; this includes traditional cross-site scripting and a category known as HTML injection (or persistent cross-site scripting).
[9] http://www.symantec.com/security_response/writeup.jsp?docid=2007-060812-4603-99
[10] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 33
[11] http://www.symantec.com/security_response/writeup.jsp?docid=2001-071911-5755-99
[12] http://www.symantec.com/security_response/writeup.jsp?docid=2001-091816-3508-99
[13] http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99

accessible services to spread. These worms prompted changes in security measures, such as the inclusion of personal firewall applications in operating systems that are turned on by default. This helped protect users from most network worms, even if the vulnerability being exploited was not immediately patched.

The high-severity vulnerability in question was a zero-day vulnerability that was discovered in late 2008 in the Microsoft® Windows® Server Service RPC Handling component that allowed remote code execution.[14] Because remote communication with this service is allowed through the Windows firewall when file and print sharing is turned on, many users would have to apply the patch to be protected from exploitation attempts. Soon after, a new worm called Downadup (also known as Conficker) emerged that exploited this vulnerability.[15] Downadup was able to spread rapidly, partially due to its advanced propagation mechanisms and its ability to spread through removable media devices.[16] By the end of 2008 there were well over a million individual computers infected by Downadup. Once Downadup has infected a computer, it uses a Web or peer-to-peer (P2P) update mechanism to download updated versions of itself, or to install other malicious code onto the compromised computer.

Downadup has been particularly prolific in the APJ and Latin America (LAM) regions.[17] These regions are also where some of the highest software piracy rates are recorded.[18] Because pirated versions of software are frequently unable to use automated update mechanisms for security patches (in case they are detected and disabled), it is likely many computers in these two regions have not been patched against Downadup. Software piracy rates are often high in many emerging markets with rapidly growing Internet and broadband infrastructures.[19]

From the data gathered for this reporting period, Symantec has also noted other significant malicious activities occurring in countries with rapidly emerging Internet infrastructures. For example, while the United States is still home to a large amount of threat activity and continues to be the top ranked country for malicious activity—mainly due to its extensive broadband penetration and significantly developed Internet infrastructure—Symantec has noted a steady increase in malicious activity in countries not previously associated with such activities. One result of this trend is that these countries can appeal to attackers as potential bases for hosting phishing websites, spam relays, and other malicious content, possibly because rapidly growing ISPs in these areas may have difficulty monitoring and filtering the growing volume of traffic across their networks.

Attackers are also organized enough to implement contingency plans in case their activities are detected. By relocating their activities to a variety of countries, attackers can minimize the chances of being partially or completely shut down. This is demonstrated by events after the shutdown of a U.S.-based ISP toward the end of 2008.[20] It seems that the bot controllers generating much of the attack activity from this ISP had alternative hosting plans.[21] As a result, although Symantec noted a significant drop in malicious activity after the shutdown, particularly in spam, the numbers returned to previous levels soon afterward. It became apparent that the botnet controllers had been able to successfully relocate enough of their bot command-and-control (C&C) servers to other hosts, and were thus able to rebuild their botnets back up to previous numbers. Given that the affected botnets were three of the world's largest, it is not surprising that new locations were quickly found to host these servers due to the significant profits such botnets are able to generate.

[14] http://www.securityfocus.com/bid/31874
[15] http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
[16] https://forums2.symantec.com/t5/Malicious-Code/Downadup-Attempts-at-Smart-Network-Scanning/ba-p/382114 - A233
[17] https://forums2.symantec.com/t5/Malicious-Code/Downadup-Geo-location-Fingerprinting-and-Piracy/ba-p/380993 - A228
[18] http://arstechnica.com/old/content/2008/01/bsa-piracy-economic-impact-is-tens-of-billions-of-dollars.ars
[19] http://findarticles.com/p/articles/mi_m0EIN/is_2008_May_14/ai_n25411795
[20] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 7
[21] http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/

## What attackers want

More than ever before, attackers are concentrating on compromising end users for financial gain. In 2008, 78 percent of confidential information threats exported user data, and 76 percent used a keystroke-logging component to steal information such as online banking account credentials. Additionally, 76 percent of phishing lures targeted brands in the financial services sector (figure 2) and this sector also had the most identities exposed due to data breaches. Similarly, 12 percent of all data breaches that occurred in 2008 exposed credit card information. In 2008 the average cost per incident of a data breach in the United States was $6.7 million—which is an increase of 5 percent from 2007—and lost business amounted to an average of $4.6 million.[22]

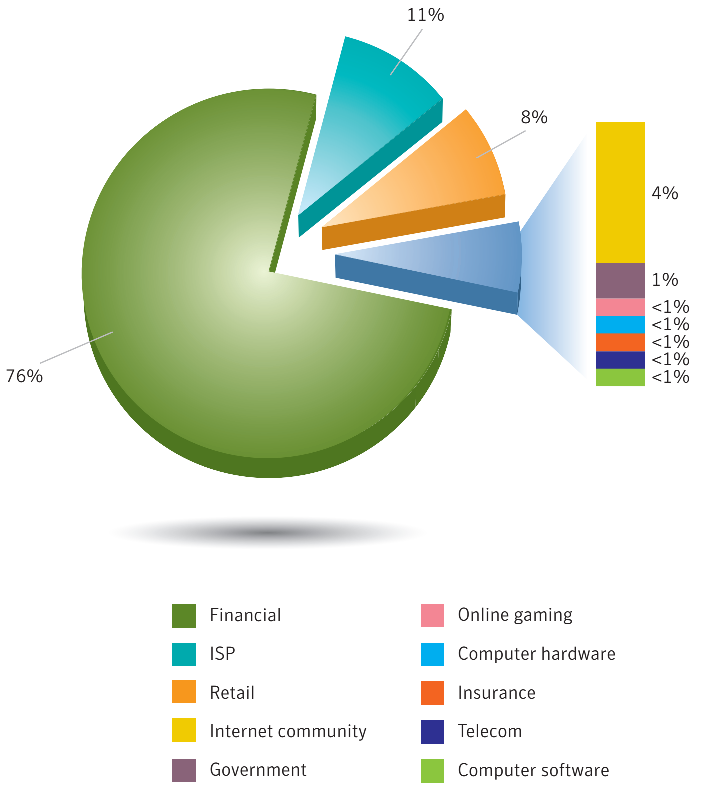

**Figure 2. Phished sectors by volume of phishing lures**
*Source: Symantec Corporation*

[22] http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf

Once attackers have obtained financial information or other personal details—such as names, addresses, and government identification numbers—they frequently sell that data on the underground economy.[23] The most popular item for sale on underground economy servers in 2008 was credit card information, accounting for 32 percent of the total (table 1). This is likely due to the fact that there are numerous ways for credit card information to be stolen, and that stolen card data can be easily cashed out. This is because the underground economy has a well-established infrastructure for monetizing such information, again indicating the increased sophistication of the underground economy. Also, because of the large quantity of credit card numbers available, the price for each card can be as low as 6 cents when they are purchased in bulk. Some groups in the underground economy also specialize in manufacturing blank plastic cards with magnetic stripes destined to be encoded with stolen credit card and bankcard data. The manufacture and distribution of these cards requires a well-organized level of sophistication since the cards are often produced in one country, imprinted, and then shipped to the countries from where the stolen data originated.

| 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 1. Goods and services available for sale on underground economy servers**
*Source: Symantec*

One result that Symantec has drawn from the observance of increased professionalization in the underground economy is that the coordination of specialized and, in some cases, competitive groups for the production and distribution of items such as customized malicious code and phishing kits has led to a dramatic increase in the general proliferation of malicious code. In 2008, Symantec detected 1,656,227 malicious code threats (figure 3). This represents over 60 percent of the approximately 2.6 million malicious code threats that Symantec has detected in total over time.

[23] The underground economy comprises various forums, such as websites and Internet Relay Chat (IRC) channels, which allow criminals to buy, sell, and trade illicit goods and services. For more information see: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

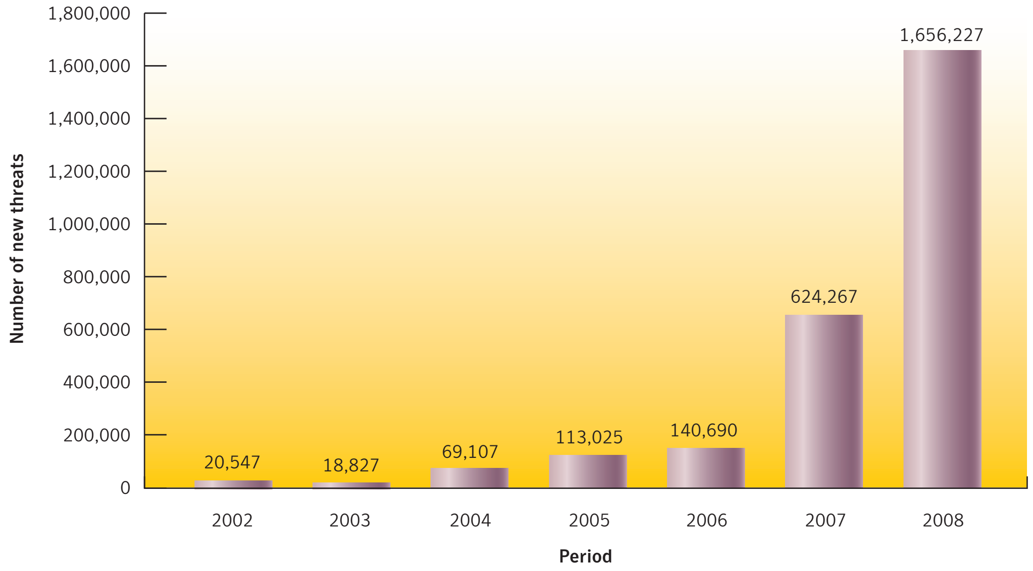

**Figure 3. New malicious code threats**
*Source: Symantec*

A prime example of this type of underground professional organization is the Russian Business Network (RBN). The RBN reputedly specializes in the distribution of malicious code, hosting malicious websites, and other malicious activity. The RBN has been credited with creating approximately half of the phishing incidents that occurred worldwide last year. It is also thought to be associated with a significant amount of the malicious activities on the Internet in 2007.

Since that time there have been two significant cases of ISPs that were shut down because of malicious activity. These ISPs were hosting malicious code, phishing websites, bot C&C servers, and spam relays. This includes the instance noted above, when Symantec saw a 65 percent drop in spam and a 30 percent decrease in bot activity within 24 hours of one particular ISP being taken offline.[24] While it may seem remarkable that the shutdown of a single ISP can result in such drastic decreases in malicious activity within a short time period, as noted, malicious activity is increasingly organized and attackers are now readily prepared for contingencies that might affect their operations. Much of the malicious activity was simply shifted to other locations. In this instance, the ISP even resurfaced briefly to afford the group an opportunity to update the botnets under their control.[25]

In this increasingly sophisticated Internet threat landscape, there is a growing impetus for greater cooperation to address the high degree of organization of groups creating threats on the Internet. This was demonstrated by the aggressive spread of the Downadup worm in the latter months of 2008 and into 2009. Due to its multiple propagation mechanisms, the worm was able to spread rapidly. More worrisome is the fact that the worm contains an update mechanism that could allow new versions of the worm or other threats, such as a bot, to be installed on compromised computers. To combat its rapid spread and aggressive profile, a coalition was formed by stakeholders involved in Internet security.[26] The success of this coalition of identifying how the worm operates, slowing its growth, and limiting its potential danger demonstrates the benefits of increased cooperation among Internet security stakeholders.

[24] Cf. http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 7
and http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 26
[25] http://www.pcworld.com/businesscenter/article/154554/spammers_regaining_control_over_srizbi_botnet.html
[26] https://forums2.symantec.com/t5/Malicious-Code/Coalition-Formed-in-Response-to-W32-Downadup/ba-p/388129 - A241

## Conclusion

Changes in the current threat landscape—such as the increasing complexity and sophistication of attacks, the evolution of attackers and attack patterns, and malicious activities being pushed to emerging countries—show not just the benefits of, but also the need for increased cooperation among security companies, governments, academics, and other organizations and individuals to combat these changes. Symantec expects malicious activity to continue to be pushed to regions with emerging infrastructures that may still lack the resources to combat the growing involvement of organized crime in the online underground economy. The onus will be on organizations, institutions, and other knowledgeable groups to come together for the benefit of the affected regions. Internet threat activity is truly global, and malicious activity allowed to flourish in one area could quickly spread worldwide.

With the increasing adaptability of malicious code developers and their ability to evade detection, Symantec also expects that overt attack activities will either be abandoned or pushed further underground. For example, if the effort to set up malicious ISPs outweighs the return for attackers before being taken offline, it is likely that attackers will abandon this approach for other attack vectors in order to continue to evade detection and potential apprehension or prosecution. This has already been seen with the use of HTTP and P2P communication channels in threats such as Downadup. Because of the distributed nature of these control channels, it is much more difficult to disable an entire network and locate the individual or group behind the attacks.

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. While antivirus signature scanning, heuristic detection, and intrusion prevention continue to be vital for the security of organizations as well as end users, newer technologies, such as reputation-based security, will become increasingly important.

The focus of threats in 2008 continued to be aimed at exploiting end users for profit, and attackers have continued to evolve and refine their abilities for online fraud. While some criminal groups have come and gone, other large organizations persist and continue to consolidate their activities. These pseudo-corporations and their up-and-coming competitors will likely remain at the forefront of malicious activity in the coming year.

## *Global Internet Security Threat Report*, Volume XIV Highlights

The following section provides highlights of the security trends that Symantec observed in 2008 that are included in the current volume of the Symantec *Global Internet Security Threat Report*.

### *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.
- 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, 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.

***Vulnerability Trends Highlights***

- Symantec documented 5,491 vulnerabilities in 2008; this is a 19 percent increase over the 4,625 vulnerabilities documented in 2007.
- Two percent of vulnerabilities in 2008 were classified as high severity, 67 percent as medium severity, and 30 percent as low severity. In 2007, 4 percent of vulnerabilities were classified as high severity, 61 percent as medium severity, and 35 percent as low severity.
- Eighty percent of documented vulnerabilities were classified as easily exploitable in 2008; this is an increase from 2007, when 74 percent of documented vulnerabilities were classified as easily exploitable.
- Of any browser analyzed in 2008, Apple® Safari® had the longest window of exposure (the time between the release of exploit code for a vulnerability and a vendor releasing a patch), with a nine-day average; Mozilla® browsers had the shortest window of exposure in 2008, averaging less than one day.
- Mozilla browsers were affected by 99 new vulnerabilities in 2008, more than any other browser; there were 47 new vulnerabilities identified in Internet Explorer, 40 in Apple Safari, 35 in Opera™, and 11 in Google® Chrome.
- There were 415 browser plug-in vulnerabilities identified in 2008, fewer than the 475 identified in 2007. ActiveX® technologies still constituted the majority of new browser plug-in vulnerabilities, with a total of 287; however, this is substantially down from the 399 ActiveX vulnerabilities identified in 2007.
- Memory corruption vulnerabilities again made up the majority of the type of vulnerabilities in browser plug-in technologies for 2008, with 271 vulnerabilities classified as such.
- In 2008, 63 percent of vulnerabilities affected Web applications, an increase from 59 percent in 2007.
- During 2008, there were 12,885 site-specific cross-site scripting vulnerabilities identified, compared to 17,697 in 2007; of the vulnerabilities identified in 2008, only 3 percent (394 vulnerabilities) had been fixed at the time of writing.
- In 2008, Symantec documented nine zero-day vulnerabilities, compared to 15 in 2007.
- The top attacked vulnerability for 2008 was the Microsoft Windows® Server Service RPC Handling Remote Code Execution Vulnerability.
- In 2008, 95 percent of attacked vulnerabilities were client-side vulnerabilities and 5 percent were server-side vulnerabilities, compared to 93 percent and 7 percent, respectively, in 2007.

### *Malicious Code Trends Highlights*

- In 2008, the number of new malicious code signatures increased by 165 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 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 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 33,428 phishing hosts were detected.
- In 2008, 43 percent of all phishing websites identified by Symantec were located in the United States, 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; this was the second most common type of spam in 2007, 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, 29 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 for spam.
- In 2008, bot networks were responsible for the distribution of approximately 90 percent of all spam email.

## *Government Internet Security Threat Report*, Volume XIV Highlights

The following section provides a summary of the threat activity that Symantec observed taking place in government and infrastructure sectors in 2008. This includes only highlights specific to the Symantec *Government Internet Security Threat Report* that are not also included in the Symantec *Global Internet Security Threat Report* highlights, listed above.

### *Threat Activity Trends Highlights*

- 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.
- 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.
- In 2008, Symantec documented six public SCADA vulnerabilities. This was a decrease from 2007 when there were 15 documented SCADA vulnerabilities.

### *Phishing, Underground Economy Servers, and Spam Trends Highlights*

- 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.

## *EMEA Internet Security Threat Report*, Volume XIV Highlights

The following section provides highlights of the security trends that Symantec observed in the Europe, the Middle East, and Africa (EMEA) region in 2008.

### *Threat Activity Trends Highlights*

- Germany ranked first for malicious activity in EMEA during 2008 with 14 percent, a slight drop from 18 percent in the previous period.
- Twenty-eight percent of attacks targeting EMEA in 2008 originated in the United States, the top ranked country, compared to 22 percent in 2007.
- Symantec observed an average of 32,188 active bots per day in the EMEA region in 2008, a 47 percent increase from 2007, when 21,864 active bots were detected.
- Spain was the top ranked country in EMEA for bot infections in 2008, with 15 percent of the total.
- Lisbon was the top city for bot infections in EMEA in 2008, accounting for 5 percent of all bot infections in the region.
- In 2008, Symantec identified 5,147 distinct new bot command-and-control servers in EMEA, of which 40 percent were through IRC channels and 60 percent on HTTP.
- Russia was the top country for bot command-and-control servers in EMEA, with 20 percent of the regional total.
- The most common Web-based attack in 2008 against users in EMEA was associated with the Adobe SWF Remote Code Executable vulnerability, which accounted for 22 percent of the regional total.
- In 2008, Ukraine was the top country of origin for Web-based attacks in the EMEA region, accounting for 31 percent of the regional total.

### *Malicious Code Trends Highlights*

- Trojans were the most common type of malicious code in EMEA during 2008, accounting for 66 percent of the top 50 potential infections in the region—a minor increase from 64 percent in 2007.
- The United Kingdom was the top ranked country for back doors and Trojans; Egypt was the top ranked country for viruses; and Saudi Arabia was the top ranked country for worms.
- The Vundo Trojan was the top malicious code sample by potential infection in EMEA during the current reporting period, unchanged from 2007; it was also the top ranked sample globally.

- The Brisv worm, which modifies multimedia files to open malicious URLs, was the top new malicious code family reported in 2008 in the EMEA region, as well as globally.
- In EMEA during 2008, 87 percent of confidential information threats had remote access capabilities, compared to 94 percent in 2007.
- The most common propagation method for malicious code was through shared executable files, accounting for 65 percent of potential infections in EMEA—a substantial increase from 37 percent in 2007.
- In 2008, 1 percent of the volume of the top 50 samples in EMEA had the capability to modify Web pages, unchanged from 2007.

### *Phishing and Spam Trends Highlights*

- Poland hosted the highest percentage of phishing websites to which EMEA users were directed by phishing lures in 2008, with 18 percent of all known lures. The financial services sector was the sector most targeted by these lures in Poland.
- The highest percentage of spam detected in EMEA in 2008 originated in Russia, which accounted for 14 percent of the regional total.
- The most common top-level domain used in phishing lures detected in EMEA in 2008 was .com, which accounted for 25 percent of the total

## *APJ Internet Security Threat Report*, Volume XIV Highlights

The following section provides highlights of the security trends that Symantec observed in the Asia-Pacific/Japan (APJ) region in 2008.

### *Threat Activity Trends Highlights*

- China ranked first for malicious activity within APJ in 2008, with 41 percent of the total; China also ranked first in 2007, with 42 percent of the total.
- In 2008, the United States ranked first for originating attacks targeting the APJ region, with 28 percent of the total; this is an increase from 24 percent in 2007, when it also ranked first.
- Symantec observed an average of 11,683 active bot-infected computers per day in the APJ region in 2008, which is a 3 percent increase from the 11,329 recorded in 2007.
- China had the most bot-infected computers in the APJ region during this period, with 58 percent of the total—down from 66 percent in 2007.
- Taipei was the top city for bot infections in the APJ region in 2008, accounting for 9 percent of all bot infections in the APJ region.
- In 2008, Symantec identified 3,567 distinct new bot command-and-control servers in the APJ region, of which 30 percent were controlled through IRC channels and 70 percent were managed over HTTP.
- China was the top country for bot command-and-control servers in the APJ region, with 63 percent of the regional total.
- The most common Web-based attack in 2008 against users in the APJ region was associated with the Adobe SWF Remote Code Executable vulnerability, which accounted for 32 percent of the regional total.
- In 2008, China was the top country of origin for Web-based attacks in the APJ region, accounting for 79 percent of the regional total.

### *Malicious Code Trends Highlights*

- Trojans were the most common type of malicious code in 2008 in the APJ region, accounting for 55 percent of the volume of the top 50 potential infections in the region—an increase from 46 percent in 2007.
- Worms accounted for 43 percent of malicious code in the APJ region in 2008, compared to 29 percent globally.
- In 2008, China was the top country for back doors and Trojans in the APJ region, while India was the top country for viruses and worms.
- The Gampass Trojan was the top malicious code sample by potential infection in the APJ region in 2008—unchanged from 2007.

- The Brisv worm was the top new malicious code family in the APJ region in 2008.
- In 2008, 82 percent of confidential information threats detected in the APJ region exported user data, compared to 85 percent in 2007.
- The most common propagation method for malicious code in the APJ region in 2008 was through shared executable files, which accounted for 65 percent of potential infections, a slight increase from 63 percent in 2007.

***Phishing and Spam Trends Highlights***

- China hosted the highest percentage of phishing websites in 2008, with 35 percent of the regional total; in 2007, China ranked second with 28 percent.
- In 2008, China had the highest percentage of spam detected in APJ, with 22 percent; this is down slightly from 24 percent in 2007, when China also ranked first for spam origin.
- The most common TLD used in phishing lures detected in APJ in 2008 was .com, accounting for 30 percent. In 2007, .com was the second most common TLD in APJ after .cn.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

## 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