



Confidence in a connected world.

Symantec Internet Security Threat Report

Trends for January–June 07

Volume XII, Published September 2007

Executive Summary

The Symantec *Internet Security Threat Report* provides a six-month update of worldwide Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It will also assess trends in phishing and spam activity. This summary of the *Internet Security Threat Report* will alert readers to current trends and impending threats. It will also offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from January 1 to June 30, 2007.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network tracks attack activity across the entire Internet. It consists of over 40,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products.

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the BugTraq™ mailing list, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.¹ Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 22,000 vulnerabilities (spanning more than a decade) affecting more than 50,000 technologies from over 8,000 vendors. The following discussion of vulnerability trends is based on a thorough analysis of that data.

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Senior Editor
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Marc Fossi
Analyst
Symantec Security Response

Joseph Blackbird
Analyst
Symantec Security Response

David McKinney
Analyst
Symantec Security Response

Ronald Bowes
Analyst
Symantec Security Response

Nicholas Sullivan
Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Ollie Whitehouse
Security Architect—Advanced
Threat Research
Symantec Security Response

Zulfikar Ramzan
Analyst—Advanced Threat
Research
Symantec Security Response

Jim Hoagland
Principal Software Engineer
Symantec Security Response

Chris Wee
Manager, Development
Symantec Security Response

Contributors

David Cowings
Sr. Manager of Operations
Symantec Business Intelligence

Dylan Morss
Manager
Symantec Business Intelligence

Shravan Shashikant
Principal Business Intelligence
Analyst
Symantec Business Intelligence

¹ The BugTraq mailing list is hosted by SecurityFocus (<http://www.securityfocus.com>). Archives are available at <http://www.securityfocus.com/archive/1>

Symantec Internet Security Threat Report

Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity. These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers. Members of the network contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

The Symantec *Internet Security Threat Report* is grounded principally on the expert analysis of data provided by all of these sources. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity. By publishing the Symantec *Internet Security Threat Report*, Symantec hopes to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

Over the past several reporting periods, Symantec has observed a fundamental change in the threat landscape. Attackers have moved away from nuisance and destructive attacks towards activity that is motivated by financial gain. Today's attackers are increasingly sophisticated and organized, and have begun to adopt methods that are similar to traditional software development and business practices.

In the previous *Internet Security Threat Report*, Symantec reported that global, decentralized networks of collaborative malicious activity were beginning to appear. Furthermore, distinct regional threat patterns were beginning to emerge. In response to these trends, Symantec launched three additional reports: the *EMEA Internet Security Threat Report* for 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 focused on threats and trends that were of specific interest to organizations in the government and critical infrastructure sectors.²

For the first time, Symantec is providing an executive summary that provides highlights from all four reports to give audiences a more concise analysis of how the threat landscape has evolved. It is also intended to draw attention to key findings that not only show regional differences, but show how activity in these regions is both reflective of and contributing to global patterns of malicious activity.

Today, the threat landscape is arguably more dynamic than ever. As security measures are developed and implemented to protect the computers of end users and organizations, attackers are rapidly adapting new techniques and strategies to circumvent them. The ensuing changes have been evident over the first six months of 2007. Based on the data collected during that period, Symantec has observed that the current security threat landscape is characterized by the following:

- Increased professionalization and commercialization of malicious activities
- Threats that are increasingly tailored for specific regions
- Increasing numbers of multistaged attacks
- Attackers targeting victims by first exploiting trusted entities
- Convergence of attack methods

² Critical infrastructure industries include telecommunications, manufacturing, financial services, military, health care, transportation, government, aerospace, legal, biotech/pharmaceutical, agriculture, and law enforcement.

The remainder of this executive summary will explore these concepts in greater depth. It will also discuss the implications of the trends for end users and organizations. Where possible, this discussion will also include the strategies necessary for end users, administrators, and enterprises to protect themselves against these threats.

Increased professionalization and commercialization of malicious activities

As attack activity has become more profit-driven, many aspects of it have become professionalized and commercialized. This is a reflection of the burgeoning underground economy. In Volume IX of the *Internet Security Threat Report* (March 2006), Symantec predicted that the trade of malicious code in popular forums such as IRC, Web sites, and black-market auction sites would continue to grow.³ While this prediction has been borne out, the rate of growth has exceeded most predictions. To meet the needs of what has become a multi-billion dollar criminal industry,⁴ the development and distribution of many malicious activities has become professionalized and commercialized over the past two years.

MPack was one of the notable security threats that emerged in the first half of 2007. It is a commercially available black-market attack toolkit that can launch exploits for browser and client-side vulnerabilities against users who visit a malicious or compromised Web site. Symantec believes that MPack was professionally written and developed.⁵ The reliability and robustness of MPack implies that it benefited from professional development. Furthermore, there is evidence that MPack was selling online for US\$1,000.⁶

Another indication of the commercialization of malicious activity has been the emergence of phishing toolkits. A phishing toolkit is a set of scripts that allow an attacker to automatically set up phishing Web sites that spoof the legitimate Web sites of different brands, including the images and logos associated with those brands. These scripts also help to generate corresponding phishing email messages.

Phishing kits are beginning to be used on a widespread basis. One indicator of a phishing toolkit is the hosting of a number of phishing Web sites on a single IP address. During the first half of 2007, 86 percent of all phishing Web sites reported to Symantec were hosted on only 30 percent of phishing IP addresses. Furthermore, a look at the three most widely used phishing toolkits reveals that they alone were responsible for 42 percent of all phishing attacks detected in the first half of 2007 (figure 1).

³ Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 19

⁴ <http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf>

⁵ http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

⁶ http://www.symantec.com/enterprise/security_response/weblog/2007/07/mpack_clearance_sale.html

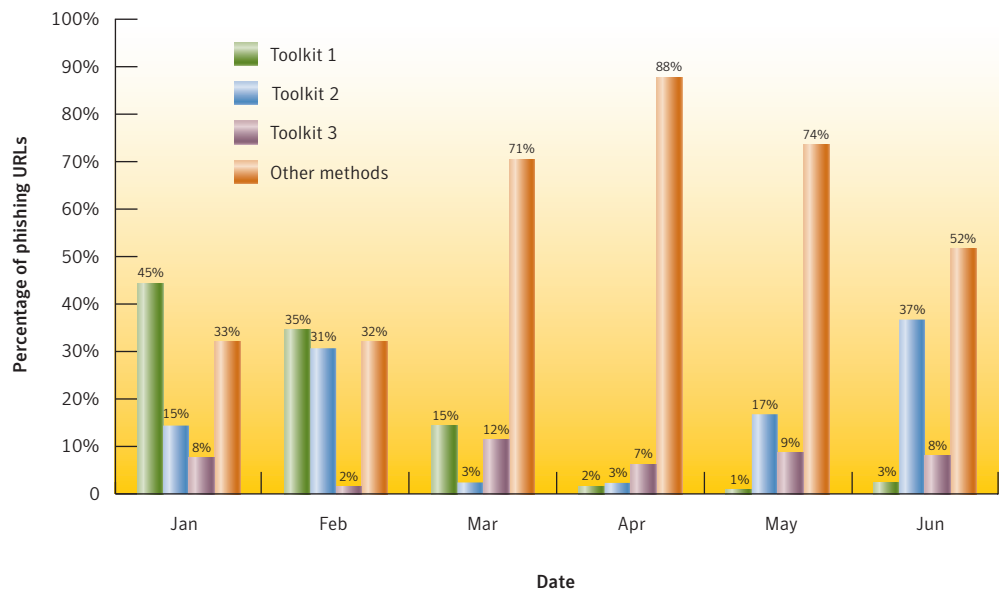


Figure 1. Use of automated phishing toolkits, January–June 2007

Source: Symantec Corporation

Further evidence supporting Symantec’s belief that malicious activity is becoming a more professional and commercial endeavor is the presence of an increasing number of underground economy servers. Underground economy servers are used by criminals and criminal organizations to sell stolen information, typically for subsequent use in identity theft. This data can include government-issued identification numbers, credit cards, bank cards and personal identification numbers (PINs), user accounts, and email address lists.

During the first six months of 2007, the United States was the top country for underground economy servers, accounting for 64 percent of the total known to Symantec. Germany had the second most economy servers during this period, accounting for 12 percent of the worldwide total. Sweden ranked third, accounting for nine percent of worldwide underground economy servers.

During the first half of 2007, credit cards were the item most frequently advertised for sale on underground economy servers, making up 22 percent of all goods advertised (table 1). During this period, Symantec observed 8,011 distinct credit cards being advertised for exchange on underground economy servers; however, this is only a small proportion of the credit cards sold across the Internet as a whole. Eighty-five percent of credit cards advertised for sale on underground economy servers known to Symantec were issued by banks in the United States.

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	\$0.50-\$5
2	Bank Accounts	21%	\$30-\$400
3	Email Passwords	8%	\$1-\$350
4	Mailers	8%	\$8-\$10
5	Email Addresses	6%	\$2/MB-\$4/MB
6	Proxies	6%	\$0.50-\$3
7	Full Identity	6%	\$10-\$150
8	Scams	6%	\$10/week
9	Social Security Numbers	3%	\$5-\$7
10	Compromised UNIX® Shells	2%	\$2-\$10

Table 1. Breakdown of goods available for sale on underground economy servers

Source: Symantec Corporation

Threats are increasingly tailored for specific regions

Attackers are increasingly turning their attention to creating threats that are regional in nature. While there has always been a degree of this type of activity, recent analysis indicates that attackers are currently focusing more on targets that share a common language, infrastructure, and/or online activity. Whereas earlier threat activity was predominantly global in nature, the expansion of broadband Internet into areas that have traditionally not been served by high-speed connectivity has given attackers new targets for attack activity.

In previous volumes of the *Internet Security Threat Report*, Symantec has observed that a rapid increase in broadband often coincides with a rapid increase in malicious activity.⁷ In part, this is due to the reality that new broadband users may not be aware of the necessary precautions required to protect their computers. It is also likely because rapidly expanding Internet service providers (ISPs) are likely to focus their resources on meeting growing demand at the expense of implementing adequate security measures, such as port blocking and ingress and egress filtering. As a result, these ISPs may have security infrastructures that are underdeveloped relative to their needs.

As broadband moves into new areas and develops a stronger regional presence, more potential targets appear online for attackers. The regionalization of attack activity is particularly evident in the distribution of certain types of malicious code. During this period, 44 percent of all potential Trojan infections were reported from North America, while 37 percent were reported from the EMEA region (figure 2). This is significantly higher than the 15 percent reported from the APJ region and the four percent from Latin America.

⁷ For example, please see the Symantec *Government Internet Security Threat Report* (September 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf : p. 43

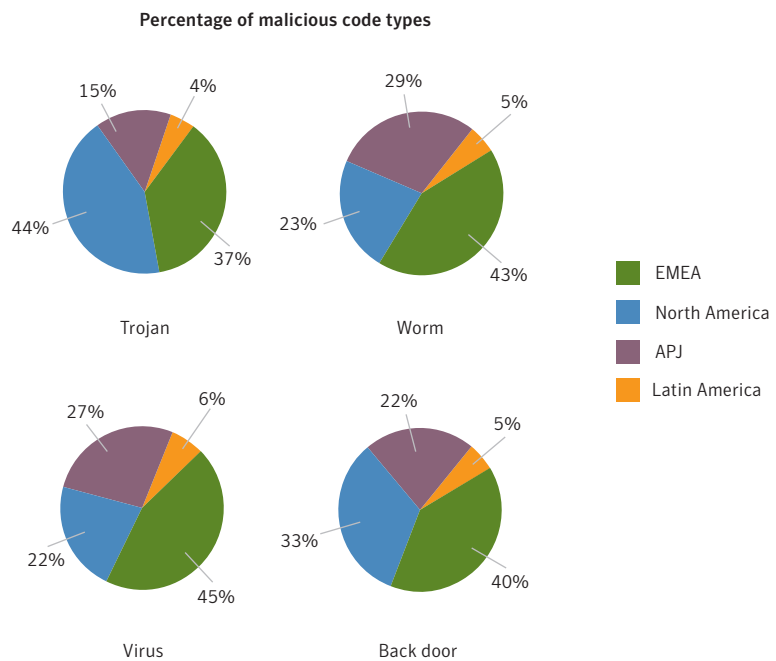


Figure 2. Location of malicious code by type
 Source: Symantec Corporation

The concentration of Trojans in North America may be indicative of enterprises and ISPs taking more active steps to prevent the propagation of worms.⁸ On the other hand, it could reflect a conscious decision by attackers to move towards Trojans in reaction to the success of network-perimeter defenses—such as intrusion detection/intrusion prevention systems (IDS/IPS) and firewalls—that have been implemented by ISPs to thwart worm attacks, but which have little effect on Trojans.

During this period, EMEA accounted for 43 percent of all potential infections caused by worms, while North America only accounted for 23 percent. This may indicate that defenses implemented by North American ISPs are successfully limiting the spread of network worms. These defenses likely include antivirus filtering at the email gateway to limit mass-mailing worms.

One reason for the regionalized distribution of worms is that some worms use region-specific subject lines and text in their email messages. For example, the Rontokbro worm, which was the fifth most common worm in EMEA during this period, emails messages written in Indonesian.⁹ However, this worm was seen more in India than in any other country. There is a great deal of commerce between India and Indonesia,¹⁰ which means that it is highly likely that many enterprise users in Indonesia communicate with counterparts in India by email. Since Rontokbro sends its email messages to all the addresses it gathers from files on a compromised computer, it stands to reason that this worm was sent to many Indian users from business contacts in Indonesia.

⁸ Such steps likely include more aggressive blocking and filtering of email attachments at the email gateway to prevent the propagation of mass-mailing worms, and port blocking to prevent the spread of network worms.
⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99
¹⁰ <http://www.hindu.com/2005/11/24/stories/2005112405871200.htm>

Symantec Internet Security Threat Report

The Sober.AA mass-mailing worm was another example of a regionally targeted worm. It used German and English email messages to propagate.¹¹ During this reporting period, Sober.AA was in the top 50 malicious code samples in EMEA, but not worldwide.

By the same token, many of the worms that were prominent in the APJ region during this period were tailored specifically toward users in the region. For example, the Antinny worm,¹² which was one of the top ten malicious code samples observed in the region, propagated over Winny, a Japanese peer-to-peer (P2P) file-sharing program. Other worms, such as Looked.BK,¹³ also caused significant numbers of potential infections in the APJ region but not elsewhere. Looked.BK specifically disabled security applications that issued security warnings in Chinese.

The EMEA region accounted for the highest percentage of potential infections by viruses during this reporting period, with 45 percent of the total. The APJ and North America regions accounted for 27 and 22 percent of viruses respectively, while Latin America only accounted for six percent. The prevalence of viruses in EMEA may be related to the high number of worms reported there during this period. Many worms are incorporating a viral component that causes them to be classified as both worms and viruses.

One reason for the increase in regional attack behavior is that some attacks are targeting particular activities that are more popular in some regions than others. For instance, online gaming is becoming an increasingly common target for attackers. Online gaming appears to be particularly popular in the APJ region, particularly in China and South Korea. There were 30 million Internet gamers in China alone by the end of 2006,¹⁴ and the online game market in that country alone is expected to grow by 35 percent.¹⁵

During the first six months of 2007, the Gampass Trojan had the most potential infections of any malicious code sample in the APJ region.¹⁶ This Trojan targets users of the Lineage, Ragnarok Online, Rohan, and Rexue Jianghue games. These games are more popular in the APJ region than the rest of the world.¹⁷ The most potential infections of Gampass during this period were reported in mainland China and Taiwan. In total, 84 percent of worldwide potential infections by Gampass during this period originated in that region.

Sample	Type	Game(s) Targeted
Gampass	Trojan	Configurable for many
Lineage	Trojan	Lineage
Dowiex	Virus, Trojan	World of Warcraft

Table 2. Top three malicious code samples targeting online gaming sites

Source: Symantec Corporation

¹¹ http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-043010-5416-99

¹² http://www.symantec.com/security_response/writeup.jsp?docid=2003-080817-4045-99

¹³ http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99

¹⁴ <http://abcnews.go.com/Technology/wireStory?id=3386396>

¹⁵ <http://uk.reuters.com/article/internetNews/idUKSHA27160820070628>

¹⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99

¹⁷ http://news.com.com/Consumers+Gaming+their+way+to+growth+Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html

Increasing number of multistaged attacks

Traditional attack activity has consisted of a single compromise aimed at gaining unauthorized access to the computer or the data stored upon it. However, current attack techniques have become much more sophisticated. Symantec is seeing considerable attack activity that incorporates multistaged attacks. These are attacks in which an initial, low-profile compromise is used to establish a beachhead from which subsequent attacks are launched.

In part, the use of multistaged attacks is indicative that previous attack methods—such as wide-scale network worms and denial of service (DoS) attacks—are no longer as effective as they once were. In order to overcome strong network defenses, such as IDS/IPS and firewalls, attackers have adopted stealthier attack techniques, such as multistaged attacks that use Trojans for the initial compromise. The clearest example of the multistaged approach is malicious code known as staged downloaders.

Staged downloaders, sometimes called modular malicious code, are threats that download and install other malicious code onto a compromised computer. These threats allow an attacker to change the downloadable component to any type of threat that suits his or her objectives. As the attacker’s objectives change, he or she can change any later components that will be downloaded to perform the requisite tasks.

During the first six months of 2007, 28 of the top 50 malicious code samples were staged downloaders. Although down slightly from the 29 samples in the second half of 2006, during this period, 79 percent of potential malicious code infections were some form of staged downloader. The most widely reported new malicious code family during this period was a staged downloader known as the Peacomm Trojan.¹⁸ Peacomm downloads and installs other files, such as the Mespam¹⁹ and Abwiz.FTrojans,²⁰ the latter of which can send confidential information to the remote attacker and/or be used to relay spam.

Rank	Sample	Type	Download Mechanism
1	Zlob	Trojan	Redirects browser to malicious Web page
2	Vundo	Trojan	Downloads files from remote addresses
3	Mixor.Q	Worm	Downloads files from remote addresses
4	Anicmoo	Trojan	Downloads files from remote addresses
5	Skintrim	Trojan	Downloads files from remote addresses
6	Metajuan	Trojan	Downloads files from remote addresses
7	Stration	Worm	Downloads files from remote addresses
8	Wimad	Trojan	Uses Microsoft® Windows Media® Digital Rights Manager to trick user into downloading files
9	Nebuler	Trojan	Downloads files from remote addresses
10	Secup	Trojan	Displays fake security alerts to trick user into downloading files

Table 3. Top staged downloaders
 Source: Symantec Corporation

¹⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
¹⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2007-020915-2914-99
²⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2006-032311-1146-99

Symantec Internet Security Threat Report

Another example of multistaged attacks is the MPack kit. MPack, which was discovered in May 2007, exploits vulnerabilities in Web browser plug-ins, specifically a QuickTime® vulnerability,²¹ a WinZip ActiveX component,²² and various other plug-in vulnerabilities such as the Microsoft WebViewFolderIcon issue.²³ During the current reporting period, the MPack kit was used to install malicious code on thousands of computers.²⁴ Legitimate Web sites were compromised and were modified to include code to redirect the user's browser to a malicious MPack server. The MPack server then attempted to exploit one of a number of vulnerabilities to install the first stage of a multistaged downloader on the compromised computer.

Malicious code samples that expose confidential information on the infected computer are another example of the multistaged approach. After the initial infection, the threat can employ one of several capabilities to send confidential information to the attacker. For instance, a keystroke logger can be used to record keystrokes on a compromised computer and either email the log to the attacker or upload it to a Web site under the attacker's control.

Keystroke logs can contain any account information the user may have typed while the computer was infected, including log-on credentials for different types of accounts, such as online banking and trading accounts, as well as ISP accounts. The attacker can then use this information as a stepping stone to launch further attacks or conduct identity theft. Confidential information threats with keystroke logging capability made up 88 percent of threats to confidential information in this period, up from 76 percent in the second half of last year.

Phishing activity targeting ISPs, and their customers, is also related to multistaged attacks. Eleven percent of brands used in phishing attacks in the first half of 2007 belong to organizations in the ISP sector, making it the second ranked sector during this period (figure 3).

As noted in the previous edition of the *Internet Security Threat Report*, ISP accounts can be valuable targets for phishers.²⁵ People frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including their email accounts.²⁶ Thus, information gleaned through phishing attacks may provide access to other accounts, such as online banking.

²¹ <http://www.securityfocus.com/bid/21829>

²² <http://www.securityfocus.com/bid/21060>

²³ <http://www.securityfocus.com/bid/19030>

²⁴ http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

²⁵ Symantec *Internet Security Threat Report*, Volume XI (March 2007):

http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 69

²⁶ http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf

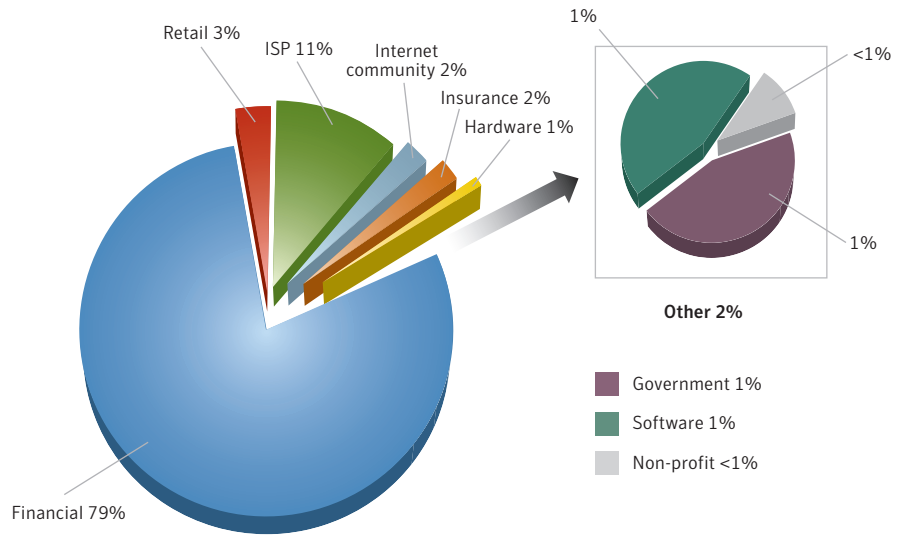


Figure 3. Brands phished by sector
 Source: Symantec Corporation

In part, the use of multistaged attacks is a natural step in the evolution of the end objective of attacks. Over the past two years, attack activity has been increasingly motivated by financial gain. Most attacks are now driven by a quest for data or information that can be used directly for fraud or theft—such as credit card numbers or bank account information—or that can be used indirectly to create the necessary conditions for fraudulent activities. The most obvious example of the latter is identity theft.

Many of the multistaged attacks that Symantec is now seeing are designed to obtain unauthorized, confidential information. In some cases, this requires several steps. Previous attack methods, such as wide-scale network worms and DoS attacks, were not as effective in meeting these objectives. Instead, smaller scale, staged attacks are required. The first stage of these attacks is often targeted specifically for the region or industry in which the attacks take place, which enhances the chances of successful compromise. Once that has been accomplished, subsequent stages can be downloaded to obtain the sought-after information, which can then be used for fraudulent purposes. As long as attacks are financially motivated, it is likely that these smaller-scale, multistaged attacks will be favored by attackers.

Attackers targeting victims by first exploiting trusted entities

One of the characteristics of the threat landscape that has emerged over the last few years is that attackers are no longer actively seeking out their intended victims. Instead, they are attempting to entice their victims to come to them. That is, instead of trying to break into the computers of targeted users, attackers are now compromising trusted sites and/or applications. When the end user visits that site or uses that application, the attacker is able to compromise the user's computer, often by directing the user to a malicious Web site or by downloading a Trojan onto the user's computer.

This trend has been made possible by the increased deployment of Web applications and Web 2.0 technologies. Web applications are technologies that use a browser for their user interface, rely on HTTP as the transport protocol, and reside on Web servers. Examples of Web-based applications include content management systems, e-commerce suites (such as shopping cart implementations), Weblogs, and Web-based email.

Web 2.0 technologies rely in large part on the user-as-publisher model of interaction. They allow for user-created content to be developed and implemented by large groups of individuals. Popular applications of Web 2.0 technologies include social networking sites and wiki sites, both of which allow users to easily collaborate to create content.

Over the past several years, as Web applications have been more widely deployed, they have been increasingly targeted by attackers as a simple means to circumvent network security measures, such as IDS/IPS and firewalls. Social networking sites have proven fruitful for attackers because they give attackers access to large numbers of people, many of whom implicitly trust that the site—and the content on it—are secure. Attackers are increasingly targeting social networking sites as Web users are becoming wary of unsolicited email attachments and other enticements.

Attackers have found that attacks can be launched from sites that users are likely to trust, which can be easily compromised due to the prevalence of Web application vulnerabilities in those sites. During the current reporting period, 61 percent of all vulnerabilities disclosed were Web application vulnerabilities (figure 4). This has serious implications for end users because they can no longer place their trust in well known sites.

Symantec Internet Security Threat Report

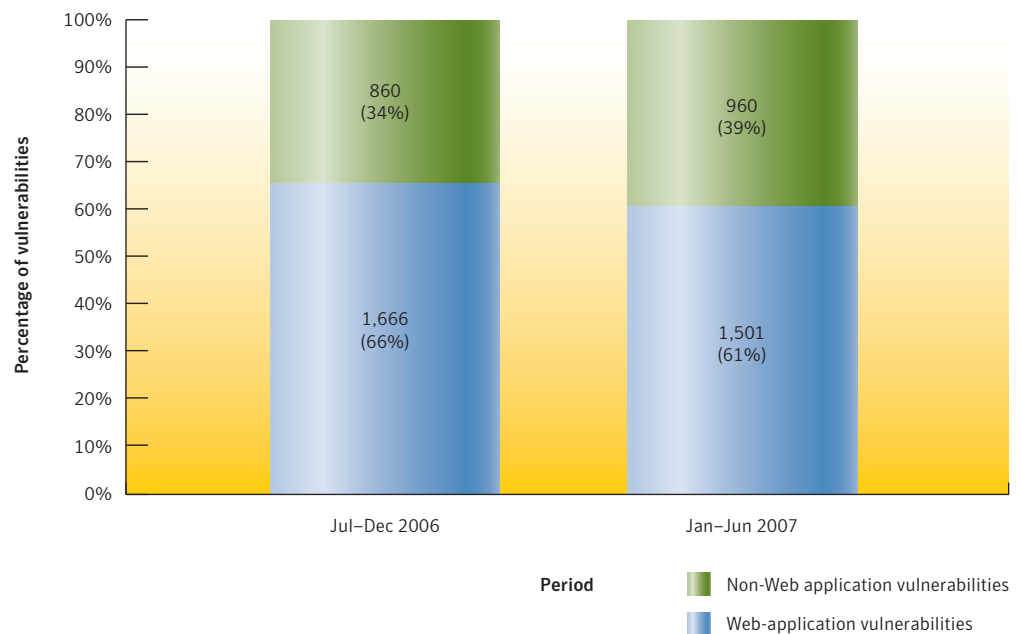


Figure 4. Web application vulnerabilities

Source: Symantec Corporation

There were also a number of instances in which attackers compromised trusted sites in order to lie in wait for unsuspecting users. For instance, many Trojans are now being installed via Web pages that exploit Web browser vulnerabilities and browser plug-in vulnerabilities. In the first half of 2007, Symantec documented 237 vulnerabilities in Web browser plug-ins, over three times the number of plug-in vulnerabilities from the previous reporting period. Two high-profile examples that exploit this type of vulnerability are the Metajuan²⁷ and Vundo²⁸ families of Trojans, both of which Symantec detected in the first half of 2007. As the Web browser has become the default application in a Web 2.0 world, these plug-ins and their vulnerabilities have provided an expanded attack surface.

In Volume X of the *Internet Security Threat Report*, Symantec predicted that Web 2.0 technologies would present new opportunities for attackers to exploit.²⁹ This prediction appears to have been borne out. Attackers will often take advantage of the implied trust between the community of users to compromise individual users and/or Web pages, or to create malicious Web pages themselves.

Attacks against trusted sites are often highly valued by attackers because they can be used to expose confidential user information, such as usernames, passwords, and online account information. Such information could then be used directly for identity theft or fraud, or indirectly to access sites from which to launch further attacks, such as hosting phishing sites using compromised ISP/Web hosting credentials.

²⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2007-030112-0714-99

²⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99

²⁹ Symantec *Internet Security Threat Report*, Volume X (September 2006):

http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf : p. 27

Information gleaned from a successful phishing attack against a social networking site account could be used to propagate malicious code to other users of the network, steal information from other user accounts, or gather addresses for spamming. For example, during the first six months of 2007, a prominent social networking site was one of the top ten brands targeted by phishing.

Another example of the shift in attacker strategy is in the distribution of some malicious code samples. Traditionally, malicious code was delivered to an intended target, often as mass-mailed email attachments. Increasingly, however, malicious code samples, such as Trojans, are installed by attackers who lure users into visiting Web pages that exploit vulnerabilities in the user's browser or its components. The malicious code itself does not directly exploit any vulnerabilities in this scenario but, instead, is installed on a computer through the exploitation of a vulnerability. During the first half of 2007, 18 percent of the 1,509 documented malicious code instances were installed on computers using this method.³⁰ While this is lower than the 23 percent of the 1,318 malicious code instances documented in the second half of 2006, the sites being targeted have the potential to reach larger numbers of users, thus increasing the chances of widespread propagation.

Convergence of attack methods

Traditionally, the *Symantec Internet Security Threat Report* has analyzed and discussed security activity as separate distinct activities, namely Internet attacks, vulnerabilities, malicious code, phishing and spam, and other malicious activities. While this report continues to maintain that structure, over the past two reporting periods, it has become increasingly apparent that, while these threats were often used separately in the past, attackers are now consolidating diverse attack methods to create global networks that support coordinated malicious activity. That is, Symantec is noticing a convergence of the various components of attack activity that is due to the increased interconnectivity and cross-functionality of the various malicious activities.

M-Pack is a good example of this convergence. Symantec classifies M-Pack as malicious code, specifically a Trojan. However, in order to install it on a user's computer, the attacker must first generate traffic to the M-Pack servers. This can be accomplished in a number of ways, the first of which is by compromising legitimate Web sites to cause users' browsers to be redirected when they visit those sites. Alternatively, the attacker may send links to the malicious Web servers in spam messages. These servers, in turn, redirect the user's browser to the M-Pack server. In some cases, attackers have set up "typosquatting" domains that direct users to the M-Pack servers.³¹

Once the user is redirected to an M-Pack server, it exploits one of several vulnerabilities in the Web browser or various browser plug-ins in order to download and install a Trojan on the computer. This Trojan is the first stage in a multistaged downloader, which in turn downloads and installs additional threats on the compromised computer.

Like M-Pack, other Trojans exhibit this convergence of threats. Once installed on a computer, they can be used to view confidential information that can subsequently be used in identity theft or fraud. They can also be used to launch phishing attacks and/or host phishing Web sites. Finally, they can be used as spam zombies.

³⁰ It should be noted that the number of documented malicious code instances differs from the number of malicious code submissions. Documented malicious code instances are those that have been analyzed and documented within the Symantec malicious code database.

³¹ Typosquatting is the practice of registering domain names that are similar to that of a legitimate domain that may include a common misspelling. For example a typosquatting domain for google.com may be gogle.com.

Symantec Internet Security Threat Report

Bots also exemplify this trend. They allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Bots can be used by external attackers to perform DoS attacks against an organization's Web site. Furthermore, once on an organization's network, they can be used to attack other organizations' Web sites. Bots can be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft or other fraudulent activities. They can also be used to distribute spam and phishing attacks.

As attackers have become increasingly financially motivated, this convergence of activities has allowed them to optimize the capabilities of the broad spectrum of attack methods. This suggests that exploit code developers, malicious code authors, spammers, and phishers may be collaborating for mutual gain. It also indicates that a new type of attacker has emerged who is versed in all of these different types of attacks and extremely flexible in his or her attack methodology.

As attacks converge and become more complex than before, it is important to provide complete protection for computers and enterprise networks. In the past different groups were often responsible for various aspects of enterprise network protection—desktop protection, server and network operations, antivirus groups, and antispam teams. It is now imperative that these groups work more closely together and share information as a single threat can affect them all.

Symantec Internet Security Threat Report, Volume XII Highlights

The following section will offer a brief summary of the security trends that Symantec observed in Volume XII of the *Internet Security Threat Report*. This summary includes all of the metrics that are included in the main report.

Global Attack Trends Highlights

- The United States was the country targeted by the most DoS attacks, accounting for 61 percent of the worldwide total in the first half of 2007.
- The United States was the top country of attack origin in the first six months of 2007, accounting for 25 percent of the worldwide attack activity.
- During this period, the United States accounted for 30 percent of all malicious activity during the period, more than any other country.
- Israel was the country with the most malicious activity per Internet user in the first six months of 2007, followed by Canada and the United States.
- Four percent of all malicious activity detected during the first six months of 2007 originated from IP space registered to Fortune 100 companies.
- The education sector accounted for 30 percent of data breaches that could lead to identity theft during this period, more than any other sector.
- Theft or loss of computer or other data-storage medium made up 46 percent of all data breaches that could lead to identity theft during this period.
- The United States was the top country for underground economy servers, accounting for 64 percent of the total known to Symantec.
- Credit cards were the most common commodity advertised on underground economy servers known to Symantec, accounting for 22 percent of all items.
- Eighty-five percent of credit cards advertised for sale on underground economy servers known to Symantec were issued by banks in the United States.
- Symantec observed an average of 52,771 active bot-infected computers per day in the first half of 2007, a 17 percent decrease from the previous period.
- China had 29 percent of the world's bot-infected computers, more than any other country.
- The United States had the highest number of bot command-and-control servers, accounting for 43 percent of the worldwide total.

Symantec Internet Security Threat Report

- Beijing was the city with the most bot-infected computers, accounting for seven percent of the worldwide total.
- The average lifespan of a bot-infected computer during the first six months of 2007 was four days, up from three days in the second half of 2006.
- Home users were the most highly targeted sector, accounting for 95 percent of all targeted attacks.

Global Vulnerability Trends Highlights

- Symantec documented 2,461 vulnerabilities in the first half of 2007, three percent less than the second half of 2006.
- Symantec classified nine percent of all vulnerabilities disclosed during this period as high severity, 51 percent were medium severity, and 40 percent were low. In the second half of 2006, four percent of newly disclosed vulnerabilities were high severity, 69 percent were medium severity, and 27 percent were low severity.
- Sixty-one percent of vulnerabilities disclosed during this period affected Web applications, down from 66 percent in the second half of 2006.
- Seventy-two percent of vulnerabilities documented in this reporting period were easily exploitable. This is a decrease from 79 percent in the previous reporting period.
- In the first half of 2007, all operating systems except Hewlett Packard HP-UX® had shorter average patch development times than in the second half of 2006.
- Hewlett-Packard HP-UX had an average patch development time of 112 days in the first half of 2007, the highest of any operating system. Sun had the highest average patch development time in the second half of 2006, with 145 days.
- The average window of exposure for vulnerabilities affecting enterprise vendors was 55 days. This is an increase over the 47-day average in the second half of 2006.
- Symantec documented 39 vulnerabilities in Microsoft Internet Explorer®, 34 in Mozilla browsers, 25 in Apple Safari, and seven in Opera. In the second half of 2006, 54 vulnerabilities were disclosed for Internet Explorer, 40 for Mozilla browsers, four for Apple Safari, and four for Opera.
- Apple® Safari™ had an average window of exposure of three days in the first half of 2007, the shortest of any browser reviewed during this period. Mozilla browsers had the shortest average window of exposure in the second half of 2006, two days.
- Symantec documented six zero-day vulnerabilities in the first half of 2007, down from the 12 that were reported during the second half of 2006.
- Ninety-seven vulnerabilities were documented in Oracle®, more than any other database during the first half of 2007. Oracle also had the most database vulnerabilities in the second half of 2006, with 168.
- There were 90 unpatched enterprise vendor vulnerabilities in the first half of 2007, which is down from the 94 documented in the second half of 2006. Microsoft had the most unpatched vulnerabilities of any enterprise vendor during both of these periods.

Symantec Internet Security Threat Report

- In the first half of 2007, Symantec documented 237 vulnerabilities in Web browser plug-ins. This is a significant increase over 74 in the second half of 2006, and 34 in the first half of 2006.
- During the first half of 2007, 89 percent of plug-in vulnerabilities disclosed affected ActiveX components for Internet Explorer. ActiveX components accounted for 58 percent of plug-in vulnerabilities in the second half of 2006.
- Symantec found that more than 50 percent of medium- and high-severity vulnerabilities patched by operating system vendors affected Web browsers or had other client-side attack vectors during this and the previous reporting period. Apple was the sole exception, with 49 percent of the vulnerabilities examined in the first half of 2007 affecting browsers or having client-side attack vectors.

Global Malicious Code Trends Highlights

- Of the top ten new malicious code families detected in the first six months of 2007, four were Trojans, three were viruses, one was a worm, and two were worms with a virus component.
- In the first half of 2007, 212,101 new malicious code threats were reported to Symantec. This is a 185 percent increase over the second half of 2006.
- During the first half of 2007, Trojans made up 54 percent of the volume of the top 50 malicious code reports, an increase over the 45 percent reported in the final six months of 2006.
- When measured by potential infections, Trojans accounted for 73 percent of the top 50 malicious code samples, up from 60 percent in the previous period.
- During this period, 43 percent of worm infections were reported in the EMEA region.
- North America accounted for 44 percent of Trojans reported this period.
- Threats to confidential information made up 65 percent of the top 50 potential malicious code samples by potential infection reported to Symantec.
- Threats with keystroke-logging capacity made up 88 percent of confidential information threats during this period, as did threats with remote access capability, such as back doors. This is an increase from 76 percent and 87 percent respectively over the previous period.
- Forty-six percent of malicious code that propagated did so over SMTP, making it the most commonly used propagation mechanism.
- During the first half of 2007, 18 percent of the 1,509 documented malicious code instances exploited vulnerabilities.
- Thirty-five percent of infected computers reported more than one infection in the first half of 2007.
- Eight of the top ten staged downloaders this period were Trojans and two were worms.
- Seven of the top ten downloaded components were Trojans and three were back doors.
- Malicious code that targets online games made up five percent of the top 50 malicious code samples by potential infection.
- Lineage and World of Warcraft were the two most frequently targeted online games in the first half of 2007.

Symantec Internet Security Threat Report

Global Phishing Highlights

- The Symantec Probe Network detected a total of 196,860 unique phishing messages, an 18 percent increase over the last six months of 2006. This equates to an average of 1,088 unique phishing messages per day for the first half of 2007.
- Symantec blocked over 2.3 billion phishing messages, an increase of 53 percent over the last half of 2006. This means that Symantec blocked an average of roughly 12.5 million phishing emails per day over the first six months of 2007.
- Organizations in the financial services sector accounted for 79 percent of the unique brands that were used in phishing attacks during this period.
- The brands of organizations in the financial services sector were spoofed by 72 percent of all phishing Web sites.
- Fifty-nine percent of all known phishing Web sites were located in the United States, a much higher proportion than in any other country.
- Three phishing toolkits were responsible for 42 percent of all phishing attacks observed by Symantec in the first half of 2007.
- Eighty-six percent of all phishing Web sites were hosted on only 30 percent of IP addresses known to be phishing Web servers.

Global Spam Highlights

- Between January 1 and June 30, 2007, spam made up 61 percent of all monitored email traffic. This is a slight increase over the last six months of 2006 when 59 percent of email was classified as spam.
- Sixty percent of all spam detected during this period was composed in English, down from 65 percent in the previous reporting period.
- In the first half of 2007, 0.43 percent of all spam email contained malicious code compared to 0.68 percent in the second half of 2006. This means that one out of every 233 spam messages blocked by Symantec Brightmail AntiSpam™ in the current reporting period contained malicious code.
- Spam related to commercial products made up 22 percent of all spam during this period, the most of any category.
- During the first six months of 2007, 47 percent of all spam detected worldwide originated in the United States compared to 44 percent in the previous period.
- In the first six months of 2007, 10 percent of all spam zombies in the world were located in the United States, more than any other country.
- In the first half of 2007, 27 percent of all spam blocked by Symantec was image spam.

Government Internet Security Threat Report Executive Summary

The following section will offer a brief summary of the security activity that Symantec observed taking place in government and infrastructure sectors during the first half of 2007. This summary includes all of the metrics that are included in the *Government Internet Security Threat Report*.

Government Attack Trends Highlights

- Between January 1 and June 30, 2007, the United States was the top country for malicious activity, accounting for 30 percent of activity detected worldwide.
- Israel had the most malicious activity per Internet user, followed by Canada and the United States.
- In the first six months of 2007, 90 percent of all malicious activity originating from critical infrastructure sectors originated from telecommunications organizations.
- During this reporting period, the government sector accounted for 26 percent of data breaches that could lead to identity theft, making it the second highest sector for this consideration.
- 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.
- Hacking was responsible for 73 percent of identities exposed during the period.
- The United States was the target of the most DoS attacks, accounting for 61 percent of all attacks during this period.
- Between January 1 and June 30, 2007, Symantec observed an average of 52,771 active bot-infected computers per day, a 17 percent decrease from the previous reporting period.
- The lifespan of the average bot-infected computer was four days, an increase from three days in the second half of 2006.
- China had the highest number of bot-infected computers during the first half of 2007, accounting for 29 percent of the worldwide total.
- The United States had the most known command-and-control servers worldwide, accounting for 43 percent of the worldwide total.
- The United States was the top country of attack origin, accounting for 25 percent of worldwide attack activity, a decrease from 33 percent during the last half of 2006.
- The top country of origin for attacks detected by sensors based in the government sector in the first half of 2007 was the United States, which accounted for 19 percent of the total.
- The majority of attacks seen by all sensors in the government and critical infrastructure sectors in the first six months of 2007 were SMTP-based attacks, which accounted for 36 percent of the top attacks.

Symantec Internet Security Threat Report

Government Vulnerability Trends Highlights

- Of the five operating systems tracked in the first six months of 2007, Microsoft had the shortest average patch development time at 18 days, based on a sample set of 38 patched vulnerabilities.
- Symantec documented six zero-day vulnerabilities during this period, down from 12 zero-day vulnerabilities in the second half of 2006.
- In the first half of 2007, Symantec documented 90 unpatched enterprise vulnerabilities that were published during this period.

Government Malicious Code Trends Highlights

- In the first six months of 2007, threats to confidential information made up 65 percent of potential infections by the top 50 malicious code samples. This is an increase over the 53 percent of potential infections in the second half of 2006.
- Eighty-eight percent of confidential information threats had remote access capabilities, up slightly from 87 percent last period.
- Eighty-eight percent of confidential information threats had keystroke-logging capabilities, up from 76 percent in the second half of 2006.
- In the second half of 2007, 46 percent of malicious code that propagated did so in email attachments.
- In the current period, the United States was the country with the highest number of multiple malicious code infections in the world, followed by China and Japan.
- Between January and June of 2007, 44 percent of Trojans were reported from North America, while 37 percent were reported from the EMEA region.
- EMEA accounted for 43 percent of potential infections caused by worms. This was followed by the APJ region, which accounted for 29 percent of potential worm infections.
- EMEA accounted for 45 percent of potential virus infections this period, followed by APJ, which accounted for 27 percent of virus infections worldwide.
- EMEA accounted for 40 percent of all potential back door infections worldwide, and North America accounted for 33 percent.

Government Phishing Trends Highlights

- Seventy-nine percent of organizations whose brands were used in phishing attacks in the first six months of 2007 were in the financial services sector, down from 84 percent in the second half of 2006.
- The financial services sector also accounted for 72 percent of the volume of all phishing Web sites, up from 64 percent in the previous period.
- In the first half of 2007, 59 percent of all known phishing Web sites were located in the United States, compared to 46 percent in the previous six-month reporting period.
- During the first six months of 2007, 23 percent of the unique government domains used to host phishing Web sites were located in Thailand.

EMEA Internet Security Threat Report Executive Summary

The following section will offer a brief summary of the security activity that Symantec observed taking place during the first half of 2007 in the EMEA region. This summary includes all of the metrics that are included in the *EMEA Internet Security Threat Report*.

EMEA Attack Trends Highlights

- Over the first six months of 2007, the United States was the country of origin of the most attacks against EMEA-based computers, accounting for 35 percent of attacks detected by sensors in the region.
- Over the first six months of 2007, the United Kingdom was the EMEA country most frequently targeted by DoS attacks, accounting for 46 percent of attacks in the region during this period.
- Between January 1 and June 30, 2007, Symantec observed an average of 18,616 active distinct bot-infected computers per day in the EMEA region, down from the 21,707 seen during the previous reporting period. Symantec also detected 52,771 active bots per day worldwide, so the EMEA region accounted for about 41 percent of active bots on an average day.
- Between January 1 and June 30, 2007, Germany had the highest number of bot-infected computers in the EMEA region, accounting for 23 percent of the total. This is an increase from 16 percent in the second half of 2006, when Germany was ranked second in EMEA for bot-infected computers.
- Madrid, Spain was the EMEA city with the highest number of bot-infected computers during the first six months of 2007, as it was in the previous reporting period.
- The home user sector was by far the most highly targeted sector in the EMEA region, accounting for 99.4 percent of all targeted attacks, which is unchanged from the previous period.
- In the first six months of 2007, Germany accounted for 19 percent of malicious activity in the EMEA region, the most of any country. This was the same percentage and rank as in the second half of 2006.
- Israel had the most malicious activity per Internet user in EMEA, followed by Poland and Spain.

EMEA Malicious Code Highlights

- During the first six months of 2007, Trojans were the most common malicious code type in EMEA, accounted for 68 percent of malicious code reports received from the region.
- The United Kingdom was the top EMEA country for potential infections of back doors and Trojans.
- India was the top EMEA country for potential infections of viruses and worms.
- The top reported malicious code sample for the EMEA region was the Netsky.P mass-mailing worm, which was the second most common malicious code sample in the second half of 2006.
- The most prevalent new malicious code family reported in the EMEA region during the first six months of 2007 was the Metajuan Trojan, which was the third most frequently reported new malicious code family worldwide this period.

Symantec Internet Security Threat Report

- Threats to confidential information made up 61 percent of the volume of the top 50 malicious code causing potential infections from the EMEA region, less than the worldwide percentage of 65 percent.
- Threats that allow remote access, such as back doors, made up 87 percent of confidential information threats by volume of reports.
- Email attachments were used by 49 percent of the propagating malicious code samples detected in the EMEA region during this period, making it the most common propagation mechanism in the region. It also accounted for 46 percent of the volume of the propagating samples worldwide.

EMEA Phishing Trends Highlights

- During the first six months of 2007, Germany was home to the highest percentage of phishing Web sites in EMEA with 22 percent of the region's total. It was the second highest country in the world for phishing Web sites after the United States.
- Karlsruhe, Germany was the city with the most phishing Web sites in the EMEA region in the first six months of 2007, as it was in the previous period.

APJ Internet Security Threat Report Executive Summary

The following section will offer a brief summary of the security activity that Symantec observed taking place during the first half of 2007 in the APJ region. This summary includes all of the metrics that are included in the *APJ Internet Security Threat Report*.

APJ Attack Trends Highlights

- The United States was the country of origin of the most attacks against APJ-based computers, accounting for 29 percent of attacks detected there.
- China was targeted by 74 percent of attacks in the APJ region during this period, an increase over the 63 percent seen during the previous period.
- Symantec observed an average of 15,447 active distinct bot-infected computers per day in the APJ region, 29 percent of the worldwide total of 52,771.
- China had the most bot-infected computers in APJ, accounting for 78 percent of the total, up from 71 percent during the second half of 2006.
- Beijing was the APJ city with the most bot-infected computers during the first six months of 2007, as it was in the previous reporting period.
- The home user sector received 97 percent of all targeted attacks, down from 98 percent in the second half of 2006.
- China accounted for 42 percent of malicious activity in the APJ region, the most of any country, up from 39 percent in the previous reporting period.
- Sri Lanka had the most malicious activity per Internet user, followed by Bangladesh and Taiwan.

APJ Malicious Code Trends Highlights

- Trojans accounted for 51 percent of the volume of malicious code reports from the APJ region. During the same period, they made up 73 percent of the volume of malicious code reports worldwide.
- China was the top APJ country for all malicious code types with the exception of worms, for which type Japan was the top reporting country.
- The top reported malicious code sample for the APJ region was the Gampass Trojan. Eighty-four percent of worldwide potential infections of Gampass originated from this region.
- The most prevalent new malicious code family reported in the APJ region during this period was the Fubalca worm.
- Threats to confidential information made up 57 percent of potential infections by the top 50 malicious code samples in the APJ region.

Symantec Internet Security Threat Report

- Of all threats to confidential information in APJ, 79 percent could be used to export user data and 78 percent had a keystroke-logging component.
- SMTP was most common propagation mechanism in the APJ region, as it was used by 37 percent of propagating malicious code during this period.

APJ Phishing Trends Highlights

- Japan was home to the highest percentage of phishing Web sites in the APJ region, but only the eighth highest number in the world.
- Taipei was the city with the most phishing Web sites in the APJ region in the first six months of 2007, as it was in the previous reporting period.

Future Watch

This section of the *Internet Security Threat Report* will discuss emerging trends and issues that Symantec believes will become prominent over the next six to twenty-four months. These forecasts are based on emerging research that Symantec has collected during the current reporting period and are speculative in nature. In discussing potential future trends, Symantec hopes to provide organizations and end users with an opportunity to prepare themselves for rapidly evolving and complex security issues. This section will discuss potential security issues associated with the following:

- Malicious code and virtual worlds
- Automated evasion processes—hide and seek for the security generation
- Advanced Web threats—laundering origins through the Web
- Diversification of bot usage

Malicious code and virtual worlds

A persistent virtual world (PVW) is a simulated online environment in which users are able to create personas known as avatars. These avatars are able to interact with each other in a simulated reality environment, 24 hours a day, seven days a week. Second Life is probably the best known example of a PVW.

Virtual worlds often serve as environments in which numerous online users interact in massively multiplayer online games (MMOGs).³² Popular examples of MMOGs include World of Warcraft and Lineage, both of which allow thousands of players to interact online simultaneously. PVWs and MMOGs are extremely popular, and have been widely adopted in areas like China and South Korea. Symantec believes that as the use of these virtual environments expands, a number of security concerns will emerge.

One simple reason for this is that the main audience of PVWs and MMOGs are early adopters, people who frequently use computers already. As MMOGs become more mainstream, and more commonly played by novice computer users, attack tactics targeting these environments will likely become more effective. The general population (that is, casual players) is probably an audience that attackers will start targeting more.

Many PVWs and MMOGs allow players to conduct real-money transactions (RMTs) in virtual worlds. Players can use credit cards or other payment methods to purchase virtual credits and then exchange those credits with players in other countries, where they may be withdrawn back into local currencies. These RMTs give rise to a de facto international monetary system. There are even exchanges in place for trading (virtual) currency across virtual worlds or different games.³³

These markets (also referred to as secondary economies) are currently unregulated and are still too small to attract serious attention from law enforcement and securities regulators. Symantec believes that these characteristics could allow criminals to use them for illicit activities. For example, because of the anonymity offered by PVWs, in which all identities are virtual, criminals may be able to launder money through the use of RMTs.

³² For the purposes of this discussion, MMOGs also include massively multiplayer online role-playing games (MMORPG), which some people consider to be distinct from MMOGs.

³³ <http://games.slashdot.org/article.pl?sid=07/06/14/100255&tid=209>

Symantec Internet Security Threat Report

To facilitate this, a criminal enterprise could open several thousand MMOG accounts. Each account could be used to trade with other players in the purchase or sale of in-game assets, the funds from which would ultimately be withdrawn from the accounts in question. Since thousands of accounts may engage in millions of transactions, each with small profits or losses, it would be difficult to trace the true source of the funds when they are withdrawn. These transactions can be conducted worldwide without the oversight that typically accompanies international bank remittances. In fact, in February 2007, China's central bank and finance ministries called upon companies to stop trading QQ coins and virtual currencies, presumably to curb the unregulated exchange of currency.³⁴

Furthermore, Sparter has created an inter-game currency trading exchange called Gamer2Gamer that permits players to sell their MMOG wares and currencies.³⁵ Currently, Blizzard Entertainment's World of Warcraft, Turbine's Lord of the Rings Online, Sony Online Entertainment's EverQuest II, and CCP's EVE Online games are supported. Availability of such platforms will further encourage the use of PVWs and MMOGs by attackers as money laundering vehicles.

Symantec also believes that attackers will use PVWs and MMOGs to trick victims into installing malicious software under the pretense that the software improves functionality in the virtual world. For example, virtual worlds have embraced the concept of scripted bots that serve, entertain, and protect avatars within the virtual environment. This could provide attackers with an opportunity to compromise the environment itself.

Although most MMOGs are designed to be played by players, automated tools can be used to enhance play and avoid some tedious, repetitive activities. The downloading and use of these tools presents an opportunity to attackers to incorporate malicious programs such as keystroke loggers and password and information stealers, which the user may unknowingly install on their computer. Symantec has already observed malicious code that attempts to steal information and passwords from players, such as *infostealer.wowcraft*.³⁶ Symantec expects that, as in-game toolkits become more popular and are used by more players, attackers will shift their efforts to infecting in-game extensions.

MMOG players and "residents" of virtual communities may also be targeted by phishers and spammers. For instance, users in these environments may receive emails that claim to be from a game's administrators that direct users to spoofed Web sites that are designed to capture account information, such as the player's username and password. The phisher will thus have access to the legitimate player's account, from which they can then distribute the player's assets to other avatars, or sell the account to another player. Despite this risk, the allure of purchasing an established account, with an existing high playing level and established assets at a relative discount (compared to spending thousands of hours playing the game, gaining that level and accumulating similar assets) continues to entice buyers.

Similar to phishing, Symantec also expects to see an increase in the amount of spam that is sent over in-game channels. Spammers will try to collect character names from Web sites that display the standings of the game, or they may use automated scripts to collect player names. Once spam arrives via in-game communications—which may consist of instant messaging clients that are built into the game environment itself—it could be used to deliver phishing attacks or malicious code, or to direct users to malicious Web sites.

³⁴ http://online.wsj.com/public/article/SB117519670114653518-dn8gNfQ5f7FniF4G8iQ_gbzDKug_20080328.html

³⁵ <http://www.shacknews.com/onearticle.x/47408>

³⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2005-073115-1710-99

Automated evasion processes—hide and seek for the security generation

Current antivirus engines are not solely behavior based. Some detect malicious files using static signatures, which simply involve searching for a unique string in a particular file. Others use dynamic analysis, which requires executing the potentially malicious code in a controlled environment. To develop these signatures, antivirus vendors must first acquire malicious code samples through means such as customer submissions, honey pots, or zoo submissions.³⁷ The samples must then be analyzed, after which signatures are produced and deployed to customers.

The longer a malicious code writer's newest creation goes undetected, the greater the likelihood it will propagate successfully. As malicious code writers put more effort into their creations, the need to evade detection increases. As a result, they have developed numerous evasion mechanisms.

Historically, polymorphism³⁸ and metamorphism,³⁹ as well as packers,⁴⁰ have been used to evade detection, thereby increasing the effective lifetime of malicious code. However, advances in detecting polymorphic and metamorphic threats and in unpacking malicious code have enabled antivirus vendors to produce signatures that are capable of catching most variations. Malicious code authors have thus been forced to adopt new tactics.

Some of the new techniques center on the distribution point, the point where the malicious code is hosted, such as a Web server. With the significant decline of network-based worms over the past several years (as is discussed in the "Malicious Code Trends" section of this report), current malicious code frequently relies on the exploitation of client-side vulnerabilities. These exploits often use the staged downloader model in which an initial Trojan is installed on the machine and then downloads the most up-to-date version of the malicious code from a distribution point.

Symantec has observed malicious code authors employing numerous techniques to protect the Web servers that are used as distribution points. The most basic is to configure a distributing Web server to serve only one copy of the malicious code per IP address, after which it serves up only a benign executable. The purpose of this is to evade detection and acquisition by security companies who would require samples of the original Trojan in order to produce signatures. This delay in the ability of security companies in acquiring samples increases the chances the malicious code will spread further before detection.

This would have two different consequences. On the one hand, computers behind a Web-proxy or a network address translation device are less likely to become infected since all the computers behind one of these devices share a single IP address. On the other hand, a computer security researcher or malicious code analyst trying to investigate the infection will have trouble obtaining a sample. This difficulty occurs because the same technique could be used to deliberately block IP addresses registered to certain organizations such as antivirus vendors, security consultancies or computer emergency response teams. This phenomenon occurred recently during the MPack Trojan incidents.⁴¹ Malicious code distributors can accomplish these aims either through blacklisting of known IP address ranges or programmatically relying on WHOIS data and performing a keyword search.⁴² Symantec expects the prevalence of this defense technique to be more widely deployed in the future due to documented success in instances where it has been used previously.

³⁷ Malicious code that is developed "in the zoo" is developed in a controlled laboratory environment.

³⁸ A polymorphic virus is one that can change its byte pattern when it replicates, thereby avoiding detection by simple string-scanning antivirus techniques. In essence, polymorphic viruses make changes to their code to avoid detection.

³⁹ Metamorphic code evolution describes a method used by malicious code writers that allows a piece of malicious code to change itself autonomously.

⁴⁰ Run-time packing utilities, also known as run-time packers, are traditionally used to make files smaller. Malicious code writers use them to make antivirus detection more difficult.

⁴¹ http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-052712-1531-99

⁴² WHOIS data stores the name of the person or company who registers a domain and owns IP address space.

Another, more worrisome, technique is known as x-morphism. Borrowing from an idea originally presented by IBM, the concept is simple: the distribution point can serve up a different copy of the malicious code to each visitor. In this scenario, the malicious code no longer has to carry its own metamorphic or polymorphic engine. Instead, the server retains the engine. With this approach, the polymorphic and metamorphic methods that are used to change each instance are hidden, thus making it difficult to produce signatures that reliably work on all variants. Another option available to the malicious code distributor is that the remote site can host a copy of the original source code so any x-morphism can occur in the higher-level programming language before compilation, after which compiler optimization can be used to further obfuscate the sample.

Advanced Web threats—laundering origins through the Web

As the number of available Web services increases and as browsers continue to converge on a uniform interpretation standard for scripting languages such as JavaScript, Symantec expects the number of new Web-based threats to continue increasing. One interesting class of threats includes those that circumvent the same origin policy (SOP) in Web browsers.⁴³

One concept that lends itself to SOP circumvention is the mash-up. Mash-ups involve a Web service that collects data from other Web services and then aggregates that data into one view. If data collected from two separate origins is “mashed” through an appropriate Web service, then the end user’s Web browser receives the two pieces of data through the same web site. As a result, they appear to have the same origin, even though they may originate from two different sources. Therefore, JavaScript code from one of the origins can obtain and modify properties of the data obtained through the second origin after the two pieces of data have been mashed.

Similar functionality can also be provided by non-transparent Web proxies, like Google Translate. Such proxies generally act as a channel that funnels any content a user desires. Because the content is funneled, from the browser’s perspective, the content appears as if it originated from the proxy, when really it might have originated elsewhere. This distinction is important since it might lift restrictions associated with the SOP.

For example, Jikto is a tool that leverages such proxies to scan sites for Web vulnerabilities.⁴⁴ The site being scanned and the site containing the scanning code are both loaded through the same proxying service. Therefore, from the Web browser’s perspective, they appear to have the same origin, although their actual origins are likely different. As a result, the scanning code can successfully make requests to and read the responses from the site being scanned without being encumbered by the SOP.

Jikto is written entirely in JavaScript so it can run in the user’s browser. Any user who visits a page containing the appropriate Jikto source will inadvertently perform a vulnerability scan on a different Web site. That site’s Web logs will trace back to the user, and not necessarily to the Web server on which the Jikto source was located. Therefore, since the vulnerability scan is actually being performed by an end user, the attacker’s location will be effectively hidden.

Symantec expects that research will continue into novel techniques for SOP circumvention. It is still unclear whether the vulnerabilities found will be exploited in the wild on a wide-scale basis.

⁴³ The same origin policy dictates that a document or script loaded from one origin (defined with respect to the domain, protocol, and port number) cannot access or modify a document obtained from a different origin. Note that a document or script from one origin can issue a request for a document or script from another origin; however, the first document or script cannot actually read the contents of the other document or script.

⁴⁴ http://news.com.com/2100-1002_3-6169034.html

Diversification of bot usage

Bots are programs that are covertly installed on a user's machine in order to allow an unauthorized user to control the computer remotely. They allow an attacker to remotely control the targeted system through a communication channel such as IRC. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a bot network, 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 capabilities by downloading new code and features. They can be used by external attackers to perform DoS attacks against an organization's Web site. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious business and legal consequences. Bots can be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft. They can also be used to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications.

Bots tend to be "early adopters" of new functionality because, due to their design, they can easily incorporate new code across widely dispersed bot networks. As such, they can be used as test environments, deploying new malicious functionalities on a variety of targets before making widespread use of them. Because of this capability, Symantec believes that bots and bot networks will likely be used in an increasingly diverse number of ways in the near future.

For instance, bots may be used in client-side phishing attacks against the legitimate owner or users of an infected computer. Malicious code on an infected computer could be used to mimic the legitimate Web site of an organization whose brand is being used in the phishing attack. As a result, the intended victim could be tricked into disclosing personal identity information, which could subsequently be used in fraudulent activity. This approach allows phishers to bypass some traditional phishing protection mechanisms. Further, a phisher using this technique would not have to rely on a Web site that could be taken down if detected.

In another example, bots can give attackers specific access to infected computers that attackers can then use to their advantage. Bot owners may extract location-identifying information such as domain names from infected computers and subsequently advertise that they control a computer within a specific organization. Parties with interest in the targeted organization might pay for the use of the compromised computer to gather information or to conduct attacks. This approach could greatly increase the risk a bot infection poses to an organization.

In a final example of possible new malicious functionality, bots may be used to artificially increase apparent traffic to certain Web sites. In a twist on the traditional concept of click fraud, bots may be used to hijack browsers, steering them toward sites that allow users to submit and vote upon or recommend Web sites. The idea behind this is to falsely improve search engine ratings, giving the impression of high traffic to a particular site, thereby driving traffic to that site. This could be then used to generate advertising revenue or to serve malicious code, which can then be used in subsequent fraudulent activities.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

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

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, BugTraq, and Symantec Brightmail AntiSpam are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Apple and QuickTime are trademarks of Apple Inc., registered in the U.S. and other countries. Safari is a trademark of Apple Inc. Microsoft, ActiveX, Internet Explorer, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Sun, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Other names may be trademarks of their respective owners.
09/07 12755155