SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Internet Security Threat Report

Trends for July–December 07

Volume XIII, Published April 2008

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 also assesses trends in phishing and spam activity. This summary of the *Internet Security Threat Report* will alert readers to current trends and impending threats that Symantec has observed for the six-month period from July 1 to December 31, 2007.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network encompasses worldwide security intelligence data gathered from a wide range of sources, including more than 40,000 sensors monitoring networks in over 180 countries through Symantec products and services such as Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, and from other third-party sources. Symantec gathers malicious code reports from over 120 million client, server, and gateway systems that have deployed its antivirus product, and also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 25,000 recorded vulnerabilities (spanning more than two decades) affecting more than 55,000 technologies from over 8,000 vendors. Symantec also operates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

As well, the Symantec Probe Network, a system of over two million decoy accounts in more than 30 countries, attracts email from around the world to gauge global spam and phishing activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers whose members contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The Symantec *Internet Security Threat Report* gives enterprises and consumers essential information to effectively secure their systems now and into the future.

Dean Turner
Executive Editor
Director, Global Intelligence Network
Symantec Security Response

Marc Fossi
Manager, Development
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Trevor Mack
Associate Editor
Symantec Security Response

Joseph Blackbird
Threat Analyst
Symantec Security Response

Stephen Entwisle
Threat Analyst
Symantec Security Response

Mo King Low
Threat Analyst
Symantec Security Response

David McKinney
Threat Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

The Symantec *Internet Security Threat Report* consists of four reports: the *Global Internet Security Threat Report,* 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 focuses on threats and trends that are of specific interest to organizations in government and critical infrastructure sectors.

This *Internet Security Threat Report Executive Summary* brings together the common threads represented in these four reports to provide an analysis of the continuing evolution of the Internet threat landscape. It is also intended to draw attention to key findings that not only show regional differences, but also show how activity in these regions affects global malicious activity.

As security administrators and end users adapt new measures to resolve security threats, attackers must create new and innovative ways to attain their objectives. As a result, the threat landscape is constantly shifting. The ensuing changes have been evident over the last six months of 2007. Based on the data collected during this period, Symantec has observed that the current security threat landscape is predominantly characterized by the following:

- Malicious activity has become Web-based
- Attackers targeting end users instead of computers
- Underground economy consolidates and matures
- Rapid adaptability of attackers and attack activity

Malicious activity has become Web-based

In the past, traditional attack activity primarily used widespread, broadcast attacks aimed at computers deployed on networks. However, as administrators and vendors fortified perimeter defenses with tools such as firewalls and intrusion detection/prevention systems (IDS/IPS), attackers responded by adopting new tactics. Instead of trying to penetrate networks with high-volume broadcast attacks, attackers have adopted stealthier, more focused techniques that target individual computers through the World Wide Web. This may be driven, in part, by the fact that compromises that affect computers on enterprise networks are increasingly likely to be discovered and shut down. On the other hand, activity that takes place on end users' computers and/or Web sites is less likely to be detected. As a result of these considerations, Symantec has observed that the majority of effective malicious activity has become Web-based: the Web is now the primary conduit for attack activity.

Site-specific vulnerabilities are perhaps the most telling indication of this trend. These are vulnerabilities that affect custom or proprietary code for a specific Web site. During the last six months of 2007, 11,253 site-specific cross-site scripting vulnerabilities were documented.[1] This is considerably higher than the 2,134 traditional vulnerabilities documented by Symantec during this period.

These vulnerabilities are a concern because they allow attackers to compromise specific Web sites, which they can then use to launch subsequent attacks against users. This has shown to be an effective strategy for launching multistage attacks and exploiting client-side vulnerabilities.

[1] As documented by the XSSed project: http://www.xssed.com/about

Symantec has also observed that attackers are particularly targeting sites that are likely to be trusted by end users, such as social networking sites. This increases the likelihood that the attacks will be successful because a user is more likely to allow a trusted site to execute code on his or her computer, or to open a file downloaded from a trusted site. Attackers targeting trusted sites can also steal user credentials or launch mass attacks because they may allow attacks to propagate quickly through a victim's social network. This is one reason for the shift to site-specific vulnerabilities.

Site-specific vulnerabilities are also popular with attackers because so few of them are addressed in a timely manner. Of the 11,253 site-specific cross-site scripting vulnerabilities documented during this period, only 473 had been patched by the administrator of the affected Web site. Of the 6,961 site-specific vulnerabilities in the first six months of 2007, only 330 had been fixed at the time of writing.[2] In the rare cases when administrators do fix these vulnerabilities, they are relatively slow to do so. In the second half of 2007, the average patch development time was 52 days, down from an average of 57 days in the first half of 2007.[3]

Another indication of the emergence of the Web as an attack vector is the continued growth in browser plug-in vulnerabilities (figure 1). Browser plug-ins are technologies that run inside the Web browser and extend the browser's features. They can include plug-ins that allow additional multimedia content from Web pages to be rendered in the browser, such as ActiveX®. In the second half of 2007, Symantec documented 239 browser plug-in vulnerabilities, compared to 237 during the first six months of the year.

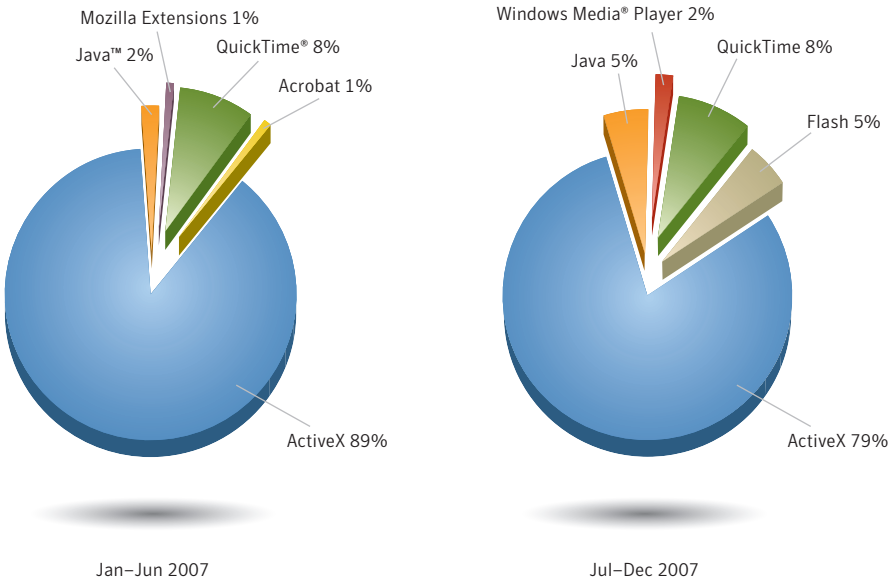

Figure 1. Browser plug-in vulnerabilities
Source: Symantec Corporation

[2] This report was written at end of 2007.
[3] The average patch development time for site-specific cross-site vulnerabilities can be determined by measuring elapsed time between the publication date of the vulnerability and the patch date by the maintainer of the affected Web site.

These vulnerabilities have remained popular because they are a very effective means of conducting Web-based attacks. Attackers will often compromise a Web site by exploiting site-specific vulnerabilities and then use that site to launch shotgun attacks to exploit browser plug-in vulnerabilities.[4] The attacker can then install malicious software—such as Trojans, back doors, and bots—on the compromised computer.

The MPack toolkit that emerged in the first half of 2007 was an example of this complementary exploitation of vulnerabilities. MPack 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]

In August 2007, Symantec observed in-the-wild exploitation of a specific browser plug-in vulnerability, the Microsoft® DirectX® ActiveX Vulnerability.[6] An exploit for this vulnerability was later incorporated into the IcePack Web-attack toolkit.[7] In the last six months of 2007, Symantec has also detected zero-day exploitation of many ActiveX vulnerabilities in the wild, including vulnerabilities in GlobalLink,[8] Real Networks RealPlayer,[9] and SSReader Ultra Star Reader.[10] A significant ActiveX vulnerability was also discovered in December 2007 that affected many HP laptops.[11]

Malicious code has also evolved to reflect the recent emphasis on Web-based attacks. One signifier of this has been the emergence of malicious code that alters Web pages on compromised computers. By modifying Web pages, particularly home pages, attackers may be able to alter code on the compromised computer or redirect the browser to malicious Web sites that can further compromise the user's computer.

Of the top 10 new malicious code families detected during this reporting period, two modify Web pages. In the last six months of 2007, seven percent of the volume of the top 50 malicious code samples modified Web pages, up from three percent in the first half of the year (figure 2). In the second half of 2006, none of the top 50 malicious code samples attempted to modify Web pages on a compromised computer. It is likely that the success of threats like the MPack kit has encouraged attackers to use Web pages to install malicious code in recent months.

[4] A shotgun attack is one that attempts to compromise a victim by exploiting multiple vulnerabilities. Attackers choose this method to improve the likelihood of successful compromise since the victim may be patched against some of the vulnerabilities, or there may be other factors that impact the reliability of the attack. Sophisticated shotgun attacks also employ browser version detection to avoid attacking clients that do not run vulnerable versions of affected applications.
[5] http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html
[6] http://www.securityfocus.com/bid/25279
[7] http://explabs.blogspot.com/2007/09/new-exploit-this-weekend.html
[8] http://www.securityfocus.com/bid/26244
[9] http://www.securityfocus.com/bid/26130
[10] http://www.securityfocus.com/bid/26247
[11] http://www.securityfocus.com/bid/26950

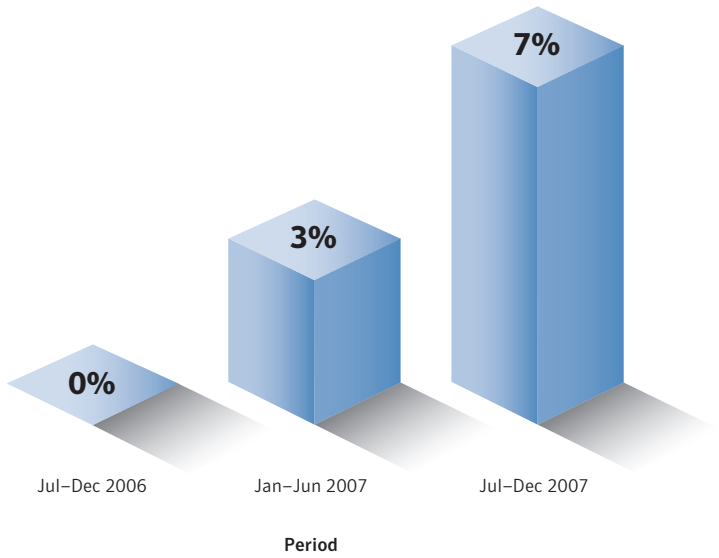

Figure 2. Malicious code that modifies Web pages
Source: Symantec Corporation

The most widely reported new malicious code family during this reporting period, the Invadesys worm,[12] also alters Web pages on compromised computers. Users frequently store the pages for personal Web sites on their local drive and upload any modified pages. Web pages that are infected by Invadesys could be uploaded to the user's hosting provider the next time he or she uploads page modifications. This could result in visitors to the user's site being compromised when they view an infected page.

Another indication of the emergence of the Web as the target of malicious activity is the predominant malicious code type. For the past few years, worms have been the most common form of malicious code. Worms propagate by sending themselves in high volumes of email messages or by exploiting vulnerable network services. This typically creates "noise" on the network, increasing the likelihood that network administrators will detect the threats and take remedial action. However, over the past year or so, attackers have adopted stealthier attack techniques, particularly multistage attacks that use Trojans to initially compromise a targeted computer, which are less likely to be detected. This has resulted in a decline in the use of worms.

During the current reporting period, Trojans made up 71 percent of the top 50 potential malicious code infections, a slight decrease from the 73 percent in the first half of 2007 (figure 3). Worms made up only 22 percent of the top 50 potential malicious code infections during this period, unchanged from the first half of the year.

[12] http://www.symantec.com/security_response/writeup.jsp?docid=2007-111215-5430-99

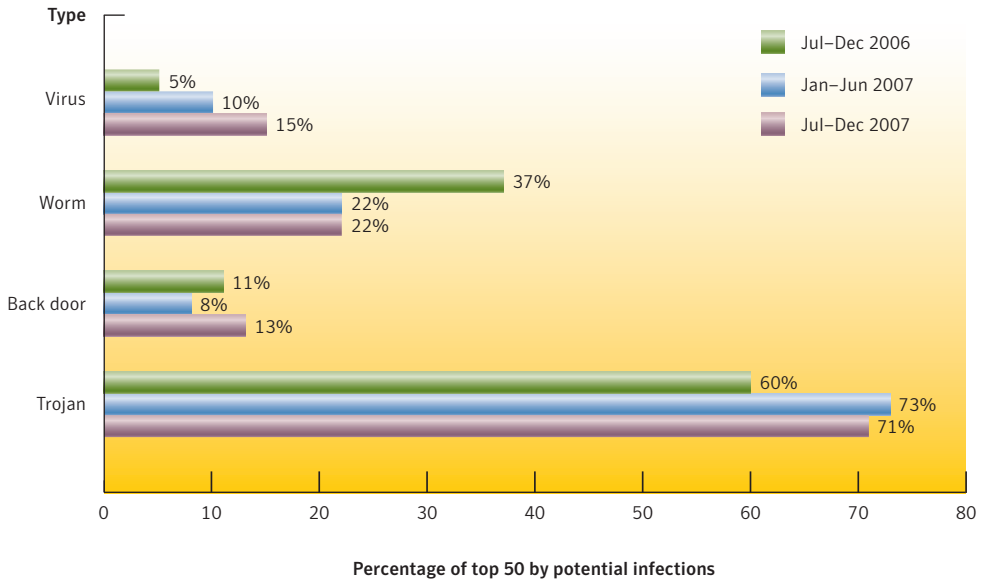

Figure 3. Malicious code types by potential infections
Source: Symantec Corporation

Phishing is a malicious activity that is commonly carried out over the Web. A phishing Web site is a site that is designed to mimic the legitimate Web site of an organization, often an online bank or e-commerce retailer, in order to fool a user into disclosing personal information associated with that organization, such as banking credentials, account information and so on. This information is usually used in fraudulent activities for financial gain.

In the last six months of 2007, Symantec observed 87,963 phishing hosts, which are computers that can host one or more phishing Web sites. This is an increase of 167 percent from the first half of 2007, when Symantec detected only 32,939 phishing Web hosts. Between the second half of 2006 and the second half of 2007, Symantec observed a dramatic increase of 559 percent in detected phishing Web site hosts.

Globally, 66 percent of all phishing Web sites identified by Symantec were located in the United States. The majority of brands used in phishing attacks in the last six months of 2007 were in the financial services sector, accounting for 80 percent, virtually unchanged from the 79 percent reported in the previous period. The financial services sector also accounted for the highest volume of phishing Web sites during this period, at 66 percent, down from 72 percent in the first half of 2007 (figure 4). Since most phishing activity pursues financial gain, successful attacks using brands in this sector are most likely to yield profitable data, such as bank account credentials, making this sector an obvious focus for attacks.

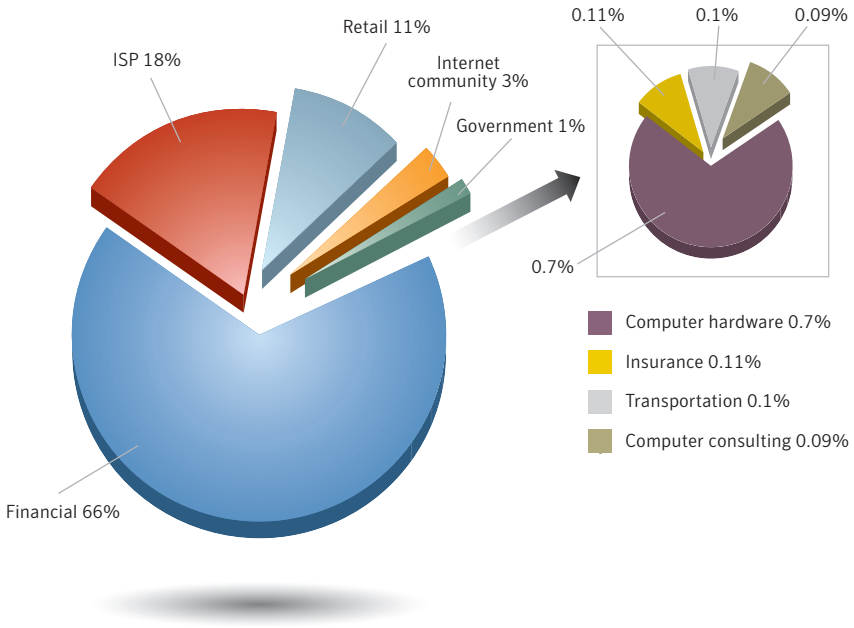

Figure 4. Phished sectors by volume of phishing Web sites
Source: Symantec Corporation

The drop in the volume of phishing Web sites spoofing financial services organizations was likely due to a rise in phishing attempts targeting ISPs. The ISP sector accounted for the second highest volume of phishing attacks during this period, accounting for 18 percent, a significant increase from three percent in the first half of the year.

ISP accounts can be valuable targets for phishers because people frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including email accounts.[13] This information may provide access to other accounts, such as online banking. Additionally, attackers could use the free Web-hosting space often included in these accounts to put up phishing sites, or use the accompanying email accounts to send spam or launch further phishing attacks.

Attackers targeting end users instead of computers

Increasingly, Symantec has observed that malicious activity has moved away from targeting computers and towards targeting end users themselves. Specifically, attackers are targeting confidential end-user information that can be used in fraudulent activity for financial gain. This is a byproduct of the move towards financially motivated malicious activity that the Symantec *Internet Security Threat Report* has observed over the past two years.[14]

Many threats to confidential information are designed specifically to target end users. For instance, a keystroke logger targets any and all credentials and sensitive information typed in by the user. It affects the user's confidential information directly rather than affecting the computer or system on which the information is stored or transmitted.

[13] http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf
[14] For instance, please see the 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. 4

In the last six months of 2007, threats to confidential information made up 68 percent of the volume of the top 50 malicious code samples causing potential infections (figure 5). This is an increase over the 65 percent reported in the first half of 2007 and the 53 percent from the second half of 2006.

Threats to confidential information are a particular concern because of their potential for use in criminal activities. With the widespread use of e-commerce, particularly online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

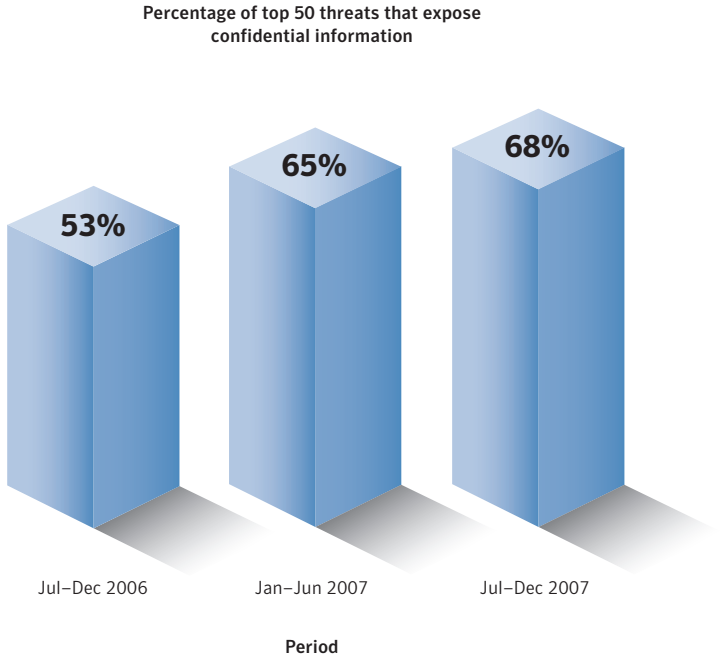

Figure 5. Threats to confidential information by volume
Source: Symantec Corporation

Underground economy servers are black market forums used by criminals and criminal organizations to advertise and trade stolen information and services typically for use in identity theft. The distribution of goods and services advertised on underground economy servers illustrates the growing focus on end users and their financial and personal information, such as bank account credentials, credit card information, and identities.

Over the last six months of 2007, Symantec observed that data related to identities, credit cards, and financial details accounted for 44 percent of the goods advertised on underground economy servers this period. Bank accounts were the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 22 percent of all items, an increase from the first half of 2007, when they represented 21 percent of the total (table 1).

One reason for the continued popularity of bank account credentials may be partly due to the increase in the number of banking Trojan infections in the second half of 2007. The number of potential banking Trojan infections increased 86 percent from the previous reporting period, which likely increased the number of bank account credentials stolen and their availability on underground economy servers during this period.

One prominent example of a banking Trojan detected during this reporting period was the Silentbanker Trojan.[15] This malicious code can be used to steal a user's online banking credentials and divert legitimate transactions. It includes sophisticated mechanisms to steal funds from a user's online banking account. Silentbanker is also able to modify information in the transaction summary Web page that the bank displays to the user, fooling the user into thinking that the transaction has been successfully completed.

Underground economy consolidates and matures

In the previous volume of the Symantec *Internet Security Threat Report*, one of the recurrent themes that Symantec discussed was the increased professionalization and commercialization of malicious activities.[16] During this reporting period, this tendency has continued to the point that Symantec believes that it has evolved into a mature, consolidated underground economy. This economy is characterized by a number of traits that are present in more orthodox economies, including:

- Specialization of production of goods and services
- Outsourcing of production
- Multivariate pricing
- Adaptable business models

Specialization of production of goods and services

The specialization of production of goods and services is an indication of a mature, consolidated economy. Specialized production of goods and services means that individuals will focus on one specific task or job, which is generally done for two reasons: because an economy has evolved enough that individuals can successfully specialize in a specific area; and to take advantage of the economic efficiencies presented when one individual or group performs only one activity.

In the previous *Internet Security Threat Report*, Symantec noted that malicious threats that attackers had previously performed separately were consolidating across the globe into networks of coordinated malicious activity. This has been made possible by the specialized production of those malicious goods and services.

In the last six months of 2007, Symantec detected 499,811 new malicious code threats (figure 6). This is a 136 percent increase over the previous period when 212,101 new threats were detected and a 571 percent increase over the second half of 2006. In total, Symantec detected 711,912 new threats in 2007 compared to 125,243 threats in 2006, an increase of 468 percent. This brings the overall number of malicious code threats identified by Symantec to 1,122,311 as of the end of 2007. This means that almost two-thirds of all malicious code threats currently detected were created during 2007.

[15] http://www.symantec.com/security_response/writeup.jsp?docid=2007-121718-1009-99
[16] Symantec Executive Summary, *Internet Security Threat Report*, Volume XII (September 2007), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf : p. 3

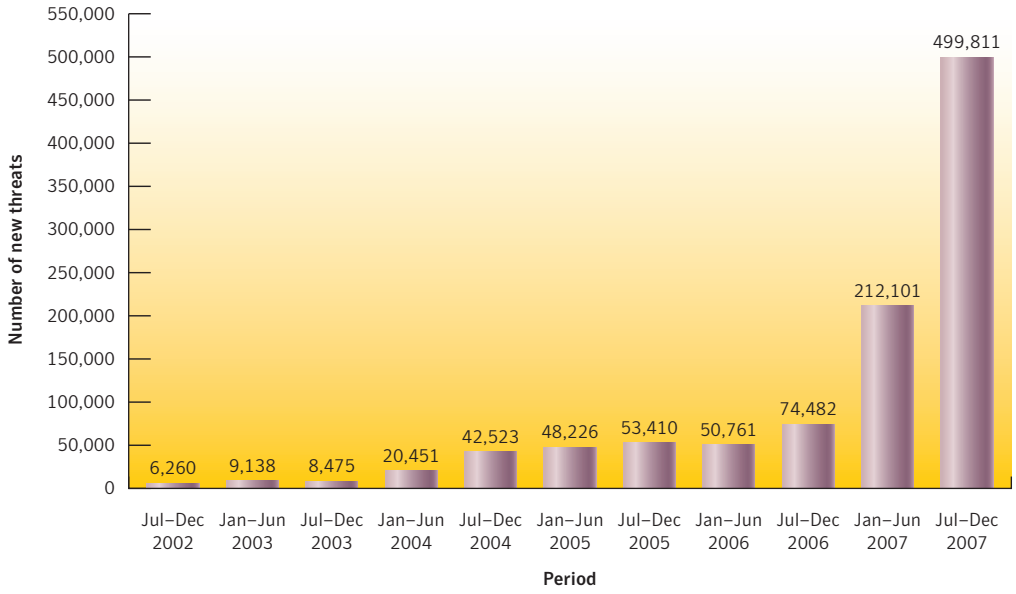

Figure 6. New malicious code threats
Source: Symantec Corporation

The significant increase in new threats over the past year is likely due to the emergence of specialized malicious code authors and the existence of organizations that employ programmers dedicated to the production of these threats. This is reflective of increased professionalization of malicious activity, which has created sufficient demand to create a niche of professional malicious code developers.

A group of specialized programmers can create a larger number of new threats than can a single malicious code author, bringing about economies of scale and, therefore, an increased return on investment. Many of these threats can be used for financial gain by performing actions such as stealing confidential information that can be sold online. These proceeds can then be used to pay the programmers to continue creating new threats. The combination of these factors results in a high volume of new malicious code samples that threaten users online.

Another example of specialization of goods and services is the apparent rise of certain countries as leading centers of specific malicious activities. For example, during this reporting period, Romania was home to the third most phishing Web sites globally, accounting for five percent of all phishing Web sites detected, and the most phishing Web sites in EMEA, with 46 percent of the region's total. Although it ranked thirty-fifth worldwide and sixteenth in EMEA for overall malicious activity, it was the fifteenth ranked country in the world for phishing hosts and had the tenth highest number of phishing hosts in EMEA.

Thus it would seem that the amount of phishing activity based in Romania is disproportionately high relative to the overall malicious activity originating there. These figures would indicate that phishing is the most common malicious activity originating in Romania, suggesting that attackers there may be specializing in that activity. This is borne out by numerous reports that indicate that Romania has become a growing source of online fraud.[17] There is a well-established tradition of computer skills in the country dating back to the early 1980s.[18] Combined with the slow economic growth in Romania since the fall of communism, and the ensuing lack of employment opportunities, this may have led to an increase in phishing activity based there.[19]

Outsourcing of production

The specialized production of malicious goods and services is often made possible by the development of an outsourcing model of malicious activity. Outsourcing is the practice of having people or organizations outside the organization perform certain services. This is usually done to maximize economic efficiencies or to acquire skills that may not otherwise be available to the organization.

As was discussed in the previous section, there was a significant increase in new malicious code threats that Symantec detected over the past two reporting periods. It is reasonable to assume that this is the result of outsourcing, in which the malicious code authors are paid to create new samples.

Automated phishing toolkits are another example of outsourcing. A phishing toolkit is a set of scripts that allows 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. Phishing toolkits are developed by groups or individuals and are sold in the underground economy. These sophisticated phishing kits are typically difficult to obtain and expensive, and are more likely to be purchased and used by well organized groups of phishers, rather than average users.

The three most popular phishing toolkits that Symantec tracked for this reporting period were responsible for 26 percent of all phishing attacks observed by Symantec (figure 7).[20] This is a decrease from the first half of 2007, when the three most popular phishing toolkits were responsible for 42 percent of all phishing attacks. Furthermore, two of the three most popular phishing toolkits tracked by Symantec in the first half of 2007 were no longer commonly used in the second half of the year and, as such, are not discussed here.

[17] http://news.bbc.co.uk/2/hi/technology/3344721.stm
[18] http://news.bbc.co.uk/2/hi/technology/3344721.stm
[19] http://bucharest.usembassy.gov/US_Citizen_Services/Visiting_Living/Corruption.html
[20] Unlike legitimate software, where naming plays a large role in marketing the product, phishing toolkits often become popular based on who has produced them. As a consequence, phishing toolkits discussed here cannot be named specifically.

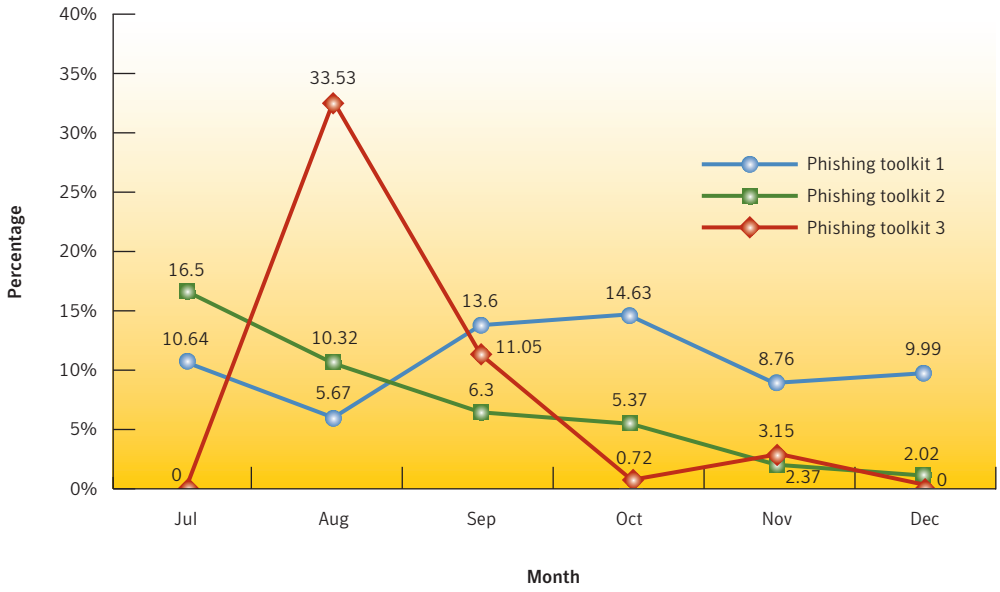

Figure 7. Use of automated phishing toolkits
Source: Symantec Corporation

These numbers indicate that the popularity of phishing toolkits changes quickly, which reflects the need for phishers to adapt in order to avoid detection by antiphishing software. This is likely the driving factor behind the dramatic upward spike and subsequent decline of Phishing toolkit 3 during this period. Its drop in popularity between August and October probably occurred because the phishing kit was identified by antiphishing software, and so became ineffective and had to be replaced. The change in phishing toolkits during this reporting period also indicates that the number of toolkits is increasing and that attackers are using a greater number of different toolkits, resulting in the total amount of attacks being distributed over more toolkits.

Multivariate pricing

The underground economy now appears to be characterized by pricing that is affected by a number of market forces, particularly supply and demand. The price range of credit cards in the last half of 2007 remained consistent with the prices from the first half of the year, ranging from $0.40 to $20 USD per card number (table 1).

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	$10–$1000
2	1	Credit cards	13%	22%	$0.40–$20
3	7	Full identities	9%	6%	$1–$15
4	N/A	Online auction site accounts	7%	N/A	$1–$8
5	8	Scams	7%	6%	$2.50/week–$50/week for hosting, $25 for design
6	4	Mailers	6%	8%	$1–$10
7	5	Email addresses	5%	6%	$0.83/MB–$10/MB
8	3	Email passwords	5%	8%	$4–$30
9	N/A	Drop (request or offer)	5%	N/A	10%–50% of total drop amount
10	6	Proxies	5%	6%	$1.50–$30

Table 1. Breakdown of goods and services available for sale on underground economy servers
Source: Symantec Corporation

Two of the main factors affecting the cost of credit cards on underground economy servers were the location of the issuing bank and the rarity of the card. Cards from the European Union cost more than those from the United States. One reason for the higher prices may be due to the availability of credit cards. It is estimated that there are approximately eight times the number of credit cards in circulation in the United States than the European Union.[21] Rarer cards, such as those from smaller countries or smaller credit card companies, were typically twice as expensive as their more popular counterparts.

Credit cards issued by banks in the United States constituted 62 percent of the total credit cards advertised in the last half of 2007. This represents a drop from 85 percent in the first half of 2007, but is still significantly higher than cards from other countries. The ready supply of cards from the United States has likely driven down prices relative to those of other countries.

Symantec observed that the cost of full identities depended on the location of the identity. As with bank accounts and credit cards, EU identities were advertised at prices 50 percent higher than U.S. identities. This would indicate that demand for these identities was higher than for those based in the United States. Along with their availability, this may also be due to the flexibility of their use, since citizens in the European Union are able to travel and conduct business freely throughout the region without a passport. This flexibility may be useful to attackers and criminals who could use the identities easily across all EU countries.

Another pricing phenomenon that Symantec saw on underground economy servers during this reporting period is bulk pricing. In order to take advantage of economic efficiencies and entice buyers, sellers will offer reduced prices on larger volumes of goods for sale. Some bulk amounts and rates observed by Symantec during the last six months of 2007 were 50 credit card numbers for $40 USD ($0.80 each), and 500 credit card numbers for $200 USD ($0.40 each). This is a decrease from the bulk rates advertised in the first half of 2007, when the lowest bulk purchase price identified was $1 USD each for 100 cards.

[21] http://www.ecb.int/stats/payments/paym/html/index.en.html and http://www.bis.org/publ/cpss78p2.pdf

As well, identities were available in bulk, at $100 USD for 50 items. Full identities were the third most common item advertised for sale on underground economy servers, making up nine percent of all advertised goods, an increase from six percent in the first half of 2007. The popularity of full identities may be due to their versatility, ease of use, and inclusion of additional information on individuals.

Pricing on the underground economy also appears to be subject to value-added incentives. For instance, bank account information for accounts that included higher balances, such as business accounts, and EU accounts, were advertised for considerably more. Furthermore, in some cases, bank accounts that bundled in personal information—such as names, addresses and dates of birth—were advertised at higher prices than those without this extra information.

Adaptable business models

A mature, consolidated economy is characterized by the development and implementation of specific business models that are suitable to the prevailing conditions in the economy. Symantec has observed that organizations and individuals currently operating within the underground economy appear willing and able to change their business models or adopt new ones in response to changes in the threat landscape.

This change of business model is apparent in the sale of credit cards on underground economy servers. During the current reporting period, credit cards were the second most commonly advertised item on underground economy servers, accounting for 13 percent of all advertised goods. This was a decrease from 22 percent in the first six months of 2007 (table 1).

The decrease in credit cards being advertised may be due to several reasons. With several recent high-profile reports on lost credit card data, credit card companies may be more diligent in monitoring customers' credit card activities and quicker to inform customers of suspicious transactions, subsequently reducing the window of opportunity for criminals to exploit stolen credit cards. It is also becoming more difficult to cash out credit cards as many wire transfer companies and currency exchange services do not accept them as a form of payment for all countries.[22]

Because of this, attackers may be seeking different sources of financial information. Likely as a result, bank account credentials, including account numbers and authentication information, were the most frequently advertised item during this period, making up 22 percent of all goods. This was a slight increase from 21 percent in the first half of 2007.

[22] http://www.asianagold.com/faq.html

Rapid adaptability of attackers and attack activity

The threat landscape is arguably more dynamic than ever. This is driven by rapid adaptability of attackers and attack activity in response to security measures that are continually developed to protect the computers of end users and organizations.

In some cases, this adaptability takes the form of geographic mobility, particularly in the case of attackers who may relocate their operations in order to seek digital safe havens. For instance, one of the most noteworthy Internet security news items of the second half of 2007 centered on the Russian Business Network (RBN). The RBN is a suspected criminal organization specializing in the distribution of malicious code, hosting malicious Web sites, and other malicious activity, specifically the development and sale of the MPack toolkit. It has been implicated in widespread malicious activity over the past two years.[23]

According to some reports, Russian organizations may be responsible for up to 60 percent of phishing activity on the Internet.[24] The third ranked top-level domain (TLD) used by phishing Web sites in the EMEA region during this period was .ru, which was used by seven percent of the total. The .ru TLD is assigned to the country domain of Russia. Only two percent of global phishing Web sites used this TLD. Furthermore, only about 0.5 percent of Internet-wide Web sites use this TLD, indicating that phishing Web sites using this TLD were heavily concentrated in the EMEA region. In the first half of the year, Russia hosted eight percent of phishing Web sites, the fifth highest total in the EMEA region. Many of these likely employed the .ru TLD, leading to its prominence in this category.

RBN was reported to have dropped offline in November 2007, in response to pressure from upstream Internet service providers.[25] However, it appears to have re-emerged in China briefly soon after.[26] As a result, it is likely that phishing Web sites using the .ru TLD will diminish over the foreseeable future. The rapid relocation of the RBN indicates that malicious groups are actively anticipating and planning for the need to adapt on the fly. This includes the deployment of back-up servers to which they can turn when law enforcement agencies or ISPs threaten to shut down existing operations.

Some attackers may relocate to regions in which security practices, legislation and/or infrastructure are not particularly well developed. Symantec has noted that, in areas where broadband connectivity is new or is rapidly expanding, ISPs may be more focused on meeting growing demand than on ensuring that adequate security measures are in place.[27] Furthermore, in these areas, users and administrators are less likely to be familiar with best security practices. Because Internet infrastructure either was not existent or is still relatively new in these areas, adequate legislation and law enforcement measures may not yet be in place.

The movement of attackers into potentially under-secured areas may result in regionalization of attack activity. For instance, several countries that have not traditionally been associated with malicious activity featured prominently in various categories during this reporting period. One example is Romania, which had a surprisingly high number of phishing Web sites during this reporting period, as was discussed previously.

[23] http://www.zdnet.com.au/news/security/soa/Infamous-porn-and-phishing-ISP-rolls-Bank-of-India/0,130061744,339281722,00.htm
[24] http://www.smh.com.au/news/security/the-hunt-for-russias-web-crims/2007/12/12/1197135470386.html
[25] http://www.theregister.co.uk/2007/11/08/rbn_offline/
[26] http://www.scmagazineus.com/Is-this-the-end-of-the-Russian-Business-Network/article/96289/ and http://www.pcworld.com/article/id,139465-page,1-c,privacysecurity/article.html
[27] For instance, please see the 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. 36

Another example of attackers adapting to the deployment of new or rapidly expanding technologies is the Farfli Trojan,[28] which was the third most commonly reported new malicious code family in the last half of 2007. This Trojan changes the search settings for the Maxthon and TheWorld Web browsers,[29] two Web browsers that have a smaller market share than browsers that are typically more commonly targeted by attackers.

The targeting of these two browsers also illustrates the tendency towards regionalization of attacks. Both browsers have been developed and maintained by Chinese companies, which may indicate that the author of the Trojan is specifically targeting Chinese users. Further, since the Trojan changes the search settings to use a popular Chinese search engine, this may also indicate that Chinese users are being targeted.

Effective security measures implemented by vendors, administrators, and end users have forced attackers to adopt new tactics more rapidly and more often. Symantec believes that such a change is currently taking place in the construction and use of bot networks.

Between July 1 and December 31, 2007, Symantec observed an average of 61,940 active bot-infected computers per day, a 17 percent increase from the previous reporting period.[30] Symantec also observed 5,060,187 distinct bot-infected computers during this period, a one percent increase from the first six months of 2007. However, despite this increase, the number of bot command-and-control servers detected by Symantec during this period dropped. In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers, 11 percent less than the previous reporting period, when 4,622 bot command-and-control servers were identified (figure 8).

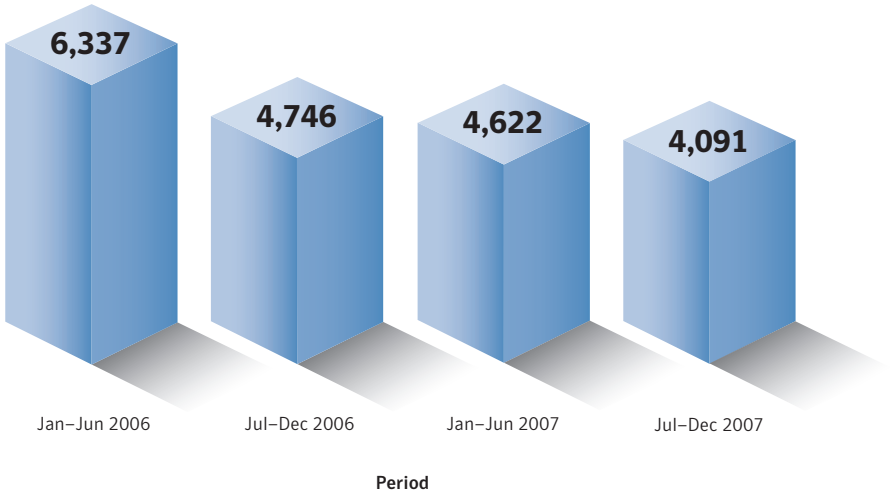

Figure 8. Bot command-and-control servers
Source: Symantec Corporation

[28] http://www.symantec.com/security_response/writeup.jsp?docid=2007-072901-5957-99
[29] Maxthon and TheWorld are Web browsers that make use of the Internet Explorer® and Firefox rendering engines. As a result, they behave in a similar manner to these browsers and are also susceptible to the same vulnerabilities.
[30] An active bot-infected computer is one that carries out at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days. A distinct bot-infected computer is a distinct computer that was active at least once during the period.

Attackers appear to be shifting away from traditional IRC bot command-and-control communications. Instead, they are adopting a decentralized command-and-control architecture, thus making their bot networks more difficult to detect and disable.[31] For example, the Peacomm (also known as Storm Trojan)[32] and Nugache[33] Trojans establish peer-to-peer (P2P) networks for bot communication. P2P-based bot network owners typically use a fast-flux domain name service scheme,[34] in which control of the bot network is diffused through a number of computers within the network. Because P2P bot networks do not have a centralized command-and-control server, they can be broken up into smaller pieces for more stealthy operations, making them very difficult to detect and disable. As is discussed in the "Future Watch" section of this report, Symantec expects this trend to continue.

Another example of attackers' ability to change tactics to adapt to new circumstances is the change in zero-day vulnerabilities that were observed in the second half of 2007.[35] Symantec documented nine zero-day vulnerabilities in the second half of 2007, compared to six zero-day vulnerabilities in the first half of 2007. All the zero-day vulnerabilities documented during this period targeted specific, regionally oriented third-party applications for Microsoft Windows®. Eight of the nine zero-day vulnerabilities were also client-side in nature, the majority of which affected ActiveX components. Seven of the nine targeted popular Japanese and Chinese language applications such as JustSystem Ichitaro, Lhaz, GlobalLink, SSReader Ultra Star Reader, and Xunlei Web Thunder.

Thus, it appears that attackers are exploiting zero-day vulnerabilities in regionalized versions of globally deployed applications such as Microsoft Office. It is likely that there is an active community of attackers based in the respective regions who have discovered that it is economically efficient to focus on users within their own region, instead of exploiting vulnerabilities with a higher profile on the global scale.

This makes sense because it is in attackers' best interest to strike a balance between vulnerabilities that affect a large user base versus lower profile attacks that are less likely to draw public attention. High profile vulnerabilities are more likely to be patched or mitigated by organizations, whereas there is a greater likelihood that lower profile vulnerabilities will remain unpatched for a longer period.

Some new tactics are targeting well established technologies. For instance, the most reported new malicious code family in EMEA during the last half of 2007 was the Pidief family.[36] Instances of malicious code belonging to this family were the fourth most commonly reported family globally. Pidief exploits a vulnerability in Adobe PDF Reader. Several factors may explain its high ranking for this period. Organizations within EMEA may be more resistant, on average, to the typical malicious code threat. There may be more widespread deployment of technologies such as gateway filtering and more user awareness in the region than exists, on average, within the global Internet community as a whole. As well, PDF documents are widely used and trusted within corporate environments, creating the potential for widespread propagation through the vector.

The process of rapid adaptation has been made more pronounced by the fact that many threats now have built-in adaptability. For instance, staged downloaders have historically used Trojans as the first component. However, during this reporting period, this role was also filled by viruses like Mumawow,[37] which downloads other threats onto a compromised computer. Previously, worms and Trojans were the primary malicious code types that were used as the first stage of multistage attacks. This shows that attackers are experimenting and evolving their techniques. Since attackers are always looking for new ways to compromise computers, it is not surprising that they have varied their methods by using viruses.

[31] http://www.darkreading.com/document.asp?doc_id=117924
[32] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
[33] http://www.symantec.com/security_response/writeup.jsp?docid=2006-043016-0900-99
[34] http://news.zdnet.com/2100-1009_22-6222896.html
[35] A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the vendor prior to exploitation, and the vendor had not released a patch at the time of the exploit activity.
[36] http://www.symantec.com/security_response/writeup.jsp?docid=2007-102310-3513-99&tabid=2
[37] http://www.symantec.com/security_response/writeup.jsp?docid=2007-061400-4037-99

The increasing use of firewalls has limited the ability of network worms to propagate and effective file-attachment blocking has also slowed the distribution of mass-mailing worms. However, there has been an increase in the use of removable media in both home and enterprise environments.[38] USB drives are increasingly used to transfer files that are too large to email or that consume too much bandwidth over the network. These devices are prime targets for traditional file-infector viruses to use for propagation.

The most common means of propagation for malicious code during this period was the sharing of executable files, which was used by 40 percent of malicious code that propagates, a significant increase from 14 percent in the first half of 2007 (table 2). During this period, this propagation mechanism was usually employed by viruses and some worms that copy themselves to removable media. However, in the past, it was associated with physical sharing of files, the traditional method employed by the original file infector viruses. Although current removable drives differ from floppy disks, the principle remains the same, enabling attackers to adapt old propagation techniques for new purposes.

Rank	Propagation Mechanism	Current	Previous
1	File sharing executables	40%	14%
2	File transfer/email attachment	32%	30%
3	File transfer/CIFS	28%	15%
4	File sharing/P2P	19%	20%
5	Remotely exploitable vulnerability	17%	12%
6	SQL	3%	<1%
7	Back door/Kuang2	3%	2%
8	Back door/SubSeven	3%	2%
9	File transfer/embedded HTTP URI/Yahoo! Messenger	2%	<1%
10	Web	1%	1%

Table 2. Propagation mechanisms
Source: Symantec Corporation

The file sharing vector lost popularity among malicious code authors when the use of floppy disks declined and attackers shifted towards more widely used file transfer mechanisms such as email and shared network drives. However, as the storage capacity of removable drives has increased and their usage has become more widespread, attackers have again begun to employ this propagation technique.

The renewed prominence of this vector is largely due to the increased storage capacity and use of removable media, such as USB keys and portable hard drives. These high-capacity and highly portable storage devices allow individuals to easily exchange large amounts of data. As is discussed in the "Future Watch" section of this report, Symantec speculates that as these devices continue to increase in popularity, attackers and malicious code authors will target them more frequently, adapting their methods to take advantage of the new opportunities these technologies may offer.

[38] http://www.macsimumnews.com/index.php/archive/worldwide_demand_remains_strong_for_mp3_portable_media_players

Global Internet Security Threat Report Highlights

The following section provides a summary of the security trends that Symantec observed in the current *Global Internet Security Threat Report*.

Global Attack Trends

- During this reporting period, the United States accounted for 31 percent of all malicious activity, an increase from 30 percent in the first half of 2007.
- The United States was the top country of attack origin in the second half of 2007, accounting for 24 percent of worldwide activity, a decrease from 25 percent in the first half of 2007.
- The education sector accounted for 24 percent of data breaches that could lead to identity theft during this period, more than any other sector. This was a decrease from the previous reporting period, when it accounted for 30 percent of the total.
- Government was the top sector for identities exposed, accounting for 60 percent of the total, a significant increase from 12 percent in the first half of 2007.
- Theft or loss of computer or other data-storage medium was the cause of the most data breaches that could lead to identity theft during this reporting period, accounting for 57 percent of the total. It accounted for 61 percent of the identities exposed in the second half of 2007, more than any other sector.
- The United States was the top country for hosting underground economy servers, accounting for 58 percent of the total identified by Symantec, a decrease from the first half of 2007, when it accounted for 64 percent of the total.
- Bank accounts were the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 22 percent of all items, an increase from the first half of 2007, when they accounted for 21 percent of all times.
- Symantec observed an average of 61,940 active bot-infected computers per day in the second half of 2007, an increase of 17 percent from the previous period.
- The average lifespan of a bot-infected computer during the last six months of 2007 was four days, unchanged from the first half of 2007.
- The United States had the most bot-infected computers, accounting for 14 percent of the worldwide total, a slight increase from 13 percent in first half of 2007.

- Madrid was the city with the most bot-infected computers, accounting for three percent of the worldwide total.
- In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers. This is an 11 percent decrease from the previous reporting period, when 4,622 bot command-and-control servers were identified. Of these, 45 percent were located in the United States, more than any other country.
- The United States was the country most frequently targeted by denial-of-service attacks, accounting for 56 percent of the worldwide total. This is a decrease from 61 percent reported in the first half of 2007.

Global Vulnerability Trends

- Not including site-specific vulnerabilities, Symantec documented 2,134 vulnerabilities in the second half of 2007, 13 percent less than the first half of 2007.
- Three percent of vulnerabilities documented in this period were classified as high severity, 61 percent as medium, and 36 percent as low. In the first half of 2007, nine percent of documented vulnerabilities were considered high severity, 51 percent medium, and 40 percent low.
- Fifty-eight percent of vulnerabilities documented in the second half of 2007 affected Web applications, down from 61 percent in the first half of 2007.
- Seventy-three percent of vulnerabilities documented in this period were classified as easily exploitable, compared to 72 percent in the first half of 2007.
- All operating system vendors except Apple and Sun had shorter average patch development times than in the previous reporting period. Microsoft had the shortest patch development time, at six days; Sun™ had the longest patch development time, at 157 days.
- Over half of patched medium- and high-severity operating system vulnerabilities for Microsoft, HP®, and Sun in the second half of 2007 were browser and client-side vulnerabilities. During the first half of 2007, browser and client-side vulnerabilities composed the majority of patched operating system vulnerabilities for all vendors but Apple®.
- The window of exposure for enterprise vendors was 46 days in the last six months of 2007, compared to 55 days in the previous six months.
- Safari had the shortest window of exposure of any browser in the last six months of 2007, with an average exposure of less than one day from a sample set of 18 patched vulnerabilities. Safari™ also had the shortest window of exposure during the first six months of 2007, an average of three days from a sample set of 13 patched vulnerabilities.
- During the second half of 2007, there were 88 vulnerabilities reported in Mozilla browsers, 22 in Safari, 18 in Internet Explorer, and 12 in Opera. In the previous six month period, Internet Explorer was subject to 39 vulnerabilities, Mozilla to 34, Safari to 25, and Opera to seven.

- Symantec documented 239 browser plug-in vulnerabilities in the last six months of 2007, compared to 237 during the first six months. During the second half of 2007, 79 percent of these vulnerabilities affected ActiveX components, compared to 89 percent in the first half.
- In the second half of 2007, 58 percent of all vulnerabilities affected Web applications. This is less than the 61 percent in the first half of 2007.
- Symantec identified 11,253 site-specific cross-site scripting vulnerabilities in the last six months of 2007, compared to 6,961 in the first half (though with measurement beginning only in February).
- Symantec documented nine zero-day vulnerabilities in the second half of 2007, all of which affected third-party applications for the Windows platform. There were six zero-day vulnerabilities in the first half of 2007.
- Eighty-eight vulnerabilities that affected enterprise vendors in the second half of 2007 remain unpatched at the end of the reporting period. This is an increase over the 81 unpatched enterprise vulnerabilities in the first half of 2007. Microsoft had the most unpatched vulnerabilities in both reporting periods.
- Symantec documented 92 vulnerabilities that affected security products during the second half of 2007, down from 113 in the first half of the year. Of the 92 vulnerabilities, 15 were classified as high severity, 48 as medium, and 29 as low.

Global Malicious Code Trends

- In the second half of 2007, 499,811 new malicious code threats were reported to Symantec, a 136 percent increase over the first half of 2007.
- Of the top 10 new malicious code families detected in the last six months of 2007, five were Trojans, two were worms, two were worms with a back door component, and one was a worm with a virus component.
- During the second half of 2007, Trojans made up 71 percent of the volume of the top 50 malicious code samples, a decrease from 73 percent in the first six months of 2007.
- Forty-three percent of worms originated in the Europe, Middle East, and Africa (EMEA) region.
- North America accounted for 46 percent of Trojans for this period.
- Threats to confidential information made up 68 percent of the volume of the top 50 potential malicious code infections reported to Symantec.
- Of all confidential information threats detected this period, 76 percent had a keystroke logging component and 86 percent had remote access capabilities, a decrease for each from 88 percent in the previous period.
- Forty percent of malicious code that propagated did so through executable file sharing, a significant increase from 14 percent in the first half of 2007, making this the most commonly used propagation mechanism during this period.

- Seven percent of the volume of the top 50 malicious code samples modified Web pages this period, up from three percent in the previous period.
- During the second half of 2007, 10 percent of the 1,032 documented malicious code samples exploited vulnerabilities. This is lower than the 18 percent proportion of the 1,509 malicious code instances documented in the first half of 2007.
- Seven of the top 10 staged downloaders this period were Trojans, two were worms, and one was a worm with a viral infection component.
- Of the top 10 downloaded components for this period, eight were Trojans and two were back doors.
- Malicious code that targets online games made up eight percent of the volume of the top 50 potential malicious code infections, up from five percent in the previous period.

Global Phishing Trends

- The Symantec Probe Network detected a total of 207,547 unique phishing messages, a five percent increase over the first six months of 2007. This equates to an average of 1,134 unique phishing messages per day for the second half of 2007.
- Eighty percent of all unique brands used in phishing attacks were in the financial sector, compared to 79 percent in the previous period.
- During this period, 66 percent of all phishing Web sites spoofed financial services brands, down from 72 percent in the first half of 2007.
- In the second half of 2007, 66 percent of all phishing attacks detected by Symantec were associated with Web sites located in the United States. Two social networking sites together were the target of 91 percent of phishing attacks with Web sites hosted in the United States.
- The most common top-level domain used in phishing Web sites for this period was .com, accounting for 44 percent; the second most common top-level domain used by phishing Web sites was .cn, accounting for 23 percent.
- Symantec observed 87,963 phishing hosts worldwide this period, an increase of 167 percent from the 32,939 observed in the first half of the year.
- Sixty-three percent of all phishing hosts identified were in the United States, a much higher proportion than in any other country.
- Three phishing toolkits were responsible for 26 percent of all phishing attacks observed by Symantec in the second half of 2007.

Global Spam Trends

- Between July 1 and December 31, 2007, spam made up 71 percent of all email traffic monitored at the gateway, a 16 percent increase over the last six months of 2006, when 61 percent of email was classified as spam.
- Eighty percent of all spam detected during this period was composed in English, up from 60 percent in the previous reporting period.
- In the second half of 2007, 0.16 percent of all spam email contained malicious code, compared to 0.43 percent of spam that contained malicious code in the first half of 2007. This means that one out of every 617 spam messages blocked by Symantec Brightmail AntiSpam™ contained malicious code.
- Spam related to commercial products made up 27 percent of all spam during this period, the most of any category and an increase from 22 percent in the previous period.
- During the last six months of 2007, 42 percent of all spam detected worldwide originated in the United States, compared to 50 percent in the previous period.
- The United States hosted the most spam zombies of any country, with 10 percent of the worldwide total, representing no change from the first six months of 2007.
- In the second half of 2007, the daily average percentage of image spam was seven percent. This is down from a daily average of 27 percent during the first six months of 2007.

Government Internet Security Threat Report Highlights

The following section provides a summary of the security activity that Symantec observed taking place in government and infrastructure sectors in the second half of 2007. This includes only highlights from the *Government Internet Security Threat Report* that are not also included in the *Global Internet Security Threat Report* highlights, listed above.

Government Attack Trends

- Telecommunications was the top critical infrastructure sector for malicious activity in the last half of 2007, accounting for 95 percent of the total. This is an increase from 90 percent in the first half of 2007.
- The top country of origin for attacks targeting the government sector was the United States, which accounted for 21 percent of the total. This is an increase from the first half of 2007 when the United States accounted for 19 percent of the total.
- Denial-of-service attacks were the most common attack type targeting government and critical infrastructure organizations, accounting for 46 percent of the top ten attacks. This is a decrease from the first half of 2007, when denial-of-service attacks accounted for 35 percent of the total and ranked second.

Government Phishing Trends

- The most common government TLD used in phishing Web sites for this period was gov.br, used by Web sites that are registered to the government of Brazil, with 19 percent of the total.

EMEA Internet Security Threat Report Highlights

The following section will offer a brief summary of the security trends that Symantec observed during the second 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

- Germany was the top ranked country for total malicious activity in EMEA, with 18 percent of the regional total, a slight drop from 19 percent in the previous period.
- Fifty-two percent of attacks targeting EMEA in the last six months of 2007 originated in the United States, the top ranked country, compared to 35 percent in the previous reporting period.
- During this period, the United Kingdom was the top ranked country in EMEA for denial-of-service attacks, with 32 percent of the total, down from 46 percent in the first half of the year.
- Symantec observed an average of 25,344 active bots per day in EMEA for the last six months of 2007, an increase from the first half of the year when there were 18,616 active bots observed.
- For the second period in a row, Germany was the top ranked country in EMEA for bot infections, with 18 percent of the total, a decrease from 23 percent in the first half of 2007.
- Madrid was the top city for bot infections in EMEA in the second half of 2007, as it was for the previous two reporting periods.

EMEA Malicious Code Trends

- Trojans were the most common type of malicious code, with 68 percent of the top 50 regional potential infections, the same percentage as in the first half of the year.
- The United Kingdom was the top reporting country for back doors, Trojans, viruses, and worms.
- The Vundo Trojan was the top malicious code sample by potential infection in EMEA during the current reporting period; it was also the top ranked sample globally.
- The top new malicious code family reported in EMEA this period was Pidief, a Trojan that exploited a vulnerability in PDF-reading software.
- In the last six months of 2007, 67 percent of the malicious activity observed in EMEA was considered a threat to confidential information, an increase from the 61 percent observed in the previous period.
- In the last six months of 2007 in EMEA, 91 percent of confidential information threats had remote access capabilities, compared to 87 percent in the previous six months.

- During the current reporting period, the most common propagation method for malicious code was through email attachments, making up 37 percent of potential infections in EMEA, a decline from 49 percent in the previous reporting period.
- For the last six months of the year, five percent of the volume of the top 50 submissions in EMEA had the capability to modify Web pages content, unchanged from the first half of 2007.

EMEA Phishing and Spam Trends

- During the last six months of 2007, Romania was home to the most phishing Web sites in EMEA with 46 percent of the region's total. The most commonly spoofed brand for phishing Web sites hosted in Romania was a social networking site.
- In the second half of 2007, the most common top-level domain used by known phishing Web sites situated in the EMEA region was .com, which was used by 24 percent of the total.
- The highest source of spam in EMEA this period was the United Kingdom, with 15 percent of the region's total, the same percentage and rank as the previous reporting period.

APJ Internet Security Threat Report Highlights

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

- With 38 percent of the total, China ranked first for malicious activity within APJ for this period. In the first half of the year, China ranked first with 42 percent of the total.
- China was the top source of attacks in APJ, with 32 percent of the regional total, up from 18 percent in the previous period.
- China was the country targeted by the most denial-of-service attacks in the APJ region, with 44 percent of the total, a significant decrease from 74 percent in the previous period.
- Symantec observed an average of 7,640 active bot-infected computers per day in the APJ region, a 52 percent decrease from the 15,447 recorded in the previous reporting period.
- Symantec identified 901,648 distinct bot-infected computers in the APJ region, which is 18 percent of the 5,060,187 distinct bot-infected computers detected worldwide during this period. It is 49 percent less than the 1,782,416 active bot-infected computers that Symantec identified in the APJ region during the first half of 2007.
- China had the most bot-infected computers in the APJ region during this period, with 43 percent of the total, down from 78 percent of the regional total in the first half of 2007.
- Kuala Lumpur had the most bot infections in the APJ region in the last half of 2007, a significant rise from seventh rank in the first half of the year.

APJ Malicious Code Trends

- Trojans were the top type of malicious code causing potential infections in APJ, amounting to 47 percent of the volume of the top 50 by potential infections.
- China was the top country for all four types of malicious code during this period.
- The top malicious code sample reported for the last six months of 2007 within the APJ region was the Gampass Trojan.
- The most widely reported new malicious code family during this reporting period, both in APJ and worldwide, was the Invadesys worm.
- For the last six months of 2007, confidential information threats made up 51 percent of malicious code reports, a slight decrease from the 57 percent reported in the first six months of the year.

- The top propagation vector in APJ during this period was executable file sharing, which was employed by 55 percent of regional threats. In the first half of 2007, this vector was used by 33 percent of regional threats and ranked third.
- For the last six months of 2007, 18 percent of malicious code samples originating in the APJ region had the ability to modify Web pages, substantially higher than the 5 percent recorded in the first half of 2007.

APJ Phishing and Spam Trends

- During the last six months of 2007, China was home to the highest percentage of phishing Web sites in APJ, with 69 percent of the region's total.
- The most common top-level domain used by phishing Web sites in the APJ region during this period was .cn, which was used by 37 percent of phishing sites in the region.
- Twenty-four percent of all spam detected from the APJ region during this period originated in China, the most of any country in the region and the same percentage as originated there in the first half of the year.

Future Watch

This section of the Symantec *Internet Security Threat Report Executive Summary* will discuss emerging trends and issues that Symantec believes will become prominent over the next six to 24 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:

- Increasing use of whitelisting technologies
- Portable media and shrink-wrapped devices
- The decline of IRC-controlled bot networks
- Increase in threats attempting to influence U.S. election results

Increasing use of whitelisting technologies

For the past few years, Symantec has observed a significant increase in the number of new malicious code threats targeting users and computer systems. As of the end of 2007, the number of malicious code threats that Symantec had identified stood at 1,122,311. Of this total, 711,912 threats were identified in 2007 alone, a 468 percent increase over the 125,243 threats identified in 2006. When adware, spyware and misleading applications are included, Symantec speculates that the ratio of non-malicious software to malicious software being distributed may be reaching a tipping point.

To combat malicious threats, security technologies have traditionally relied on blacklisting, a technique that removes, blocks, or quarantines malicious code or unwanted applications based on a list of known characteristics. This approach has proven to be successful, as the number of malicious, or unwanted, software programs has traditionally been lower than the number of non-malicious, or desired, software programs. But using new sensor technology deployed by Symantec that measures the prevalence of different software applications around the world, the initial results indicate that the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications.

For example, Symantec measured the adoption rate of applications and found that out of 54,609 unique applications deployed on Microsoft Windows PCs, 65 percent were malicious. Furthermore, Symantec observed that while legitimate applications were distributed to thousands of users, the majority of unique malicious code applications had been distributed to five users or less, indicating that malicious code and other unwanted programs continue to be targeted in nature.

While these results are preliminary, Symantec speculates that levels of malicious code and unwanted programs will continue to rise and exceed the quantity of legitimate software released and that, rather than relying on just the traditional blacklisting approach of identifying bad applications, security techniques will need to focus on whitelisting known or certified “good” applications. Security technologies will likely need to adopt this model in order to economically and effectively write signatures for a smaller set of legitimate programs, which will allow security vendors to provide consumers and enterprises with adaptive solutions that reflect changes in the threat landscape.

Portable media and other small storage devices

Portable media such as USB flash thumb drives, portable audio and video players, and other small storage devices such as digital picture frames have experienced a rapid growth in availability, distribution and storage capabilities.[39] Not unlike earlier portable storage methods, such as the 3.5 inch floppy disk, today's mobile storage options represent a serious security concern, not only as an attack target, but also in their ability to act as a distribution system for malicious code, such as viruses, worms and Trojans. With some of these devices having Internet connectivity, Symantec speculates that, as these devices continue to increase in popularity, attackers and malicious code authors will target these devices more frequently, even during the manufacturing process.

Increasingly, multi-function devices such as cellular telephones and audio players contain flash drives and small, high-storage hard drives that enable the easy portability of large amounts of data. The result is an expansion of the network endpoint, since unauthorized devices can be connected to enterprise systems and authorized devices can be connected to unauthorized systems and networks. This has resulted in an increased attack surface and a higher number of potentially viable entry points for malicious code and attacks.

A recent survey has suggested that over 43 percent of enterprises have little or no measures in place to address permissions or restrictions on removable media within their networks. Moreover, less than 17 percent use endpoint security measures to address the issue.[40] With increases in data theft and data leakage, these devices represent a viable attack vector for attackers as they attempt to steal as much information from as many sources as possible.

While the risks associated with Internet-connected devices are well documented, the risks of malicious code being introduced during the manufacturing process of these devices are not. Symantec is concerned that attackers could introduce malicious code at one or more points during their manufacture and distribution. Media players, cellular phones, and other digital devices with storage mediums may have various components created by different manufacturers before final assembly and shipping. The longer the manufacturing supply chain during this process, the greater the opportunity for malicious code to be embedded in the devices directly. In some instances, the transfer of malicious code to storage media could accidentally occur from an infected PC at a manufacturing facility. It is also possible that attackers could deliberately target machines at a manufacturing facility to enhance the chances that, once final assembly and delivery is completed, their malicious code will be delivered to the end user out-of-the-box. A recent example is a number of digital picture frames that were found to contain an older Trojan program and distributed by a major U.S.-based retailer.[41] In another case, some units of a media player manufactured in China and imported by a Dutch company were found to have the Fujacks[42] worm.[43]

[39] http://www.us-tech.com/RelId/669342/ISvars/default/New_Production_Technologies_fo.htm
[40] http://www.secprodonline.com/articles/47976/
[41] http://www.securityfocus.com/news/11499/1
[42] http://www.symantec.com/security_response/writeup.jsp?docid=2007-010509-0134-99
[43] http://www.pcworld.idg.com.au/index.php/id;527648929

The decline of IRC-controlled bot networks

For the past several years, Symantec has reported on the number of bot-infected computers controlled via command-and-control servers through Internet Relay Chat (IRC). Over the past several reporting periods, Symantec has observed a steady decrease in the number of command-and-control servers using the IRC protocol, while the numbers of bot-infected computers has remained relatively steady. Although the decline in IRC bot networks (botnets)[44] has been expected for some time, it has only begun to manifest itself relatively recently through better detection solutions and methods. As a result, Symantec speculates that attackers are accelerating their shift away from IRC control channels to newer, stealthier control methods, using protocols such as HTTP and peer-to-peer (P2P).

Traditional IRC-controlled botnets rely on a client-server model of control, where commands to individual bot-infected computers are relayed through a central server controlled by an attacker or group of attackers. By employing IRC for this traffic, ISPs and security organizations are more readily able to identify patterns in the traffic to allow for their identification and, once identified, the command-and-control servers can be shut down, effectively disabling the botnet. This has resulted in a significant drop in identified IRC command-and-control servers over the past two reporting periods.[45] As a result, threats such as the Peacomm (Storm worm),[46] along with the recent Mega-D[47] and MayDay[48] examples, are becoming increasingly popular threats that represent advancements in botnet organization and implementation.

Peacomm and Mega-D are botnet threats that use P2P networks in order to communicate. Unlike IRC-controlled botnets, the hosts in a P2P botnet get their instructions from other hosts in the same network; essentially creating a headless botnet whereby shutting down one host will not result in the collapse of the network itself. To reduce the likelihood of detection, these threats employ encrypted communications between the hosts, increasing the difficulty of differentiating between legitimate and malicious traffic. As bots become more difficult to detect due to encryption, attackers are likely to increase their use of botnets for launching Internet attacks, distributing malicious code, transferring stolen confidential information, and conducting other criminal transactions.

MayDay extends this concept by using several different communications channels, including Web browser proxy settings and the Internet Control Message Protocol (ICMP), along with P2P. Its ability to use secure Web browser proxies to bypass security controls in enterprise environments makes MayDay potentially more dangerous than many other potential threats. Although most of these threats are currently used to distribute spam, their botnet capabilities could also allow them to distribute malicious code, steal confidential information and launch attacks on other systems.

Symantec speculates that more advanced botnet threats will begin to emerge that employ stealth methods such as steganography.[49] In bot communications, steganography would allow bot masters[50] to place command instructions in public forums, and even go so far as to direct bots to use search engines in order to search for particular embedded words or symbols hidden in forums, which could then lead to specifically crafted Web sites that relay further instructions. In combination with other communication methods, such as using DNS queries and replies to transmit commands and data,[51] and HTTP headers,[52] bots and botnets are entering a new phase that will likely see traditional IRC bot networks decline in longevity and popularity.

[44] Botnet is a term used to refer to collections of bot-infected computers acting in concert and under the control of an individual or group.
[45] During the current reporting period, Symantec observed a decrease of 11 percent in identified command-and-control servers from the previous reporting period.
[46] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
[47] http://security4all.blogspot.com/2008/02/new-kid-on-block-mega-d-overtakes-storm.html
[48] http://www.symantec.com/enterprise/security_response/weblog/2008/02/mayday_mayday_a_botnet_is_here.html
[49] Steganography is a deliberate attempt to obfuscate communications by ensuring that only the sender and receiver know the meaning of the keys words, usually hidden in public texts, images or Web sites.
[50] Bot masters or bot herders are individuals or groups that control collections of bot-infected computers.
[51] DNS queries and replies could be used by bot masters to issues commands to bot hosts by setting up specific DNS servers to reply to DNS lookup queries from compromised hosts or by having special DNS records contain commands.
[52] An example of this type of bot is Trojan.Zlob discussed in detail at http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99

Increase in threats attempting to influence election results

On November 4, 2008, United States citizens will go to the polls to elect a new president, as well as representatives for the Senate, the House of Representatives, and other gubernatorial offices. In the run-up to the elections, Symantec has observed a number of threats designed to take advantage of the widespread coverage the election has generated.[53] As election day draws near, Symantec expects to see an increase in phishing attempts, scams and malicious code that exploit election themes and target individual candidates or their campaigns.

In the Symantec *Internet Security Threat Repor*t, Volume XI,[54] examining seasonal variations in phishing showed that phishing attacks often increase around notable events, such as international sporting events and the deadline for taxes. Throughout 2007 and into 2008, the candidates in the forthcoming U.S. elections have increased their use of (and reliance on) the Internet as part of their campaigns through Web sites,[55] email campaigns, and viral and social marketing.[56] Along with candidates increasingly relying on the Web to bolster their campaigns, they are also using these sites to raise campaign funds. Symantec speculates that phishers will increasingly target these campaigns and sites as the election approaches.

Symantec also expects increased efforts on the part of attackers to compromise political Web sites in an attempt to alter messaging and distribute false or misleading information about a candidate or his or her policies. Though past attacks have been attributed to denial-of-service attacks,[57] the increase in site-specific vulnerabilities noted in the current Symantec *Global Internet Security Threat Report* could mean a focused effort to compromise candidates' Web sites.[58] In one possible scenario, these sites might be compromised and potentially made to host malicious code,[59] which in turn could compromise users' computers and result in significant negative media coverage.

In connection with attempts to compromise political Web sites, Symantec expects to see an increase in the amount of malicious code that uses election themes. As Trojans such as Peacomm[60] have shown, major news events have been used to aid in the propagation of various types of malicious code. For most Trojans, successful propagation relies on social engineering[61] and the curiosity of end users. With the increased attention surrounding the 2008 elections, it is likely that more Trojans will attempt to use social engineering themes pulled from campaigns and media headlines to entice users. Other types of malicious code or unwanted software are also likely to target candidates and their Web sites, including viruses, adware, and spyware, as attackers attempt to capitalize on the increased attention of users on electoral issues during the campaign season.

Another area of concern during the upcoming election is the opportunity presented to phishers to mimic campaign Web sites and solicit fraudulent donations. As noted previously, political candidates have embraced the Web as a medium for distributing campaign information, and in the case of several candidates, have used their Web sites to solicit donations.[62] In addition to the usual phishing schemes, there is additional concern around the ability for attackers to host phishing Web sites that mimic one candidate but actually divert funds to another candidate.[63] Phishing continues to represent one of the fastest growing fraud areas online today. As a result, Symantec expects to see an increasing focus on election-themed phishing activities and its resultant fraud up to the U.S. elections in November.

[53] http://www.symantec.com/enterprise/security_response/weblog/2008/02/you_know_its_election_year_whe.html and http://blog.washingtonpost.com/securityfix/2008/02/fake_prez_campaign_video_sprea.html
[54] http://www.symantec.com/business/theme.jsp?themeid=threatreport
[55] http://asia.cnet.com/blogs/cyberpersia/post.htm?id=63001963
[56] http://www.cs.washington.edu/homes/pedrod/papers/iis04.pdf
[57] http://news.bbc.co.uk/2/hi/technology/3961557.stm
[58] Barack Obama, Hillary Clinton and John McCain all have extensive profiles on popular social networking sites. For more on site-specific vulnerabilities, please see the current volume of the *Global Internet Security Threat Report*, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 41
[59] http://www.securityfocus.com/bid/27533/discuss
[60] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
[61] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html
[62] http://blog.wired.com/27bstroke6/2007/10/online-campaign.html
[63] http://www.symantec.com/enterprise/security_response/weblog/2007/10/cybercrime_politics.html

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 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

04/08 13585534-1