SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec EMEA Internet Security Threat Report

Trends for July–December 07

Volume XIII, Published April 2008

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

Volume XIII, Published April 2008

Symantec EMEA Internet Security Threat Report

Contents

Overview

The Symantec *EMEA Internet Security Threat Report* provides a six-month update of Internet threat activity that Symantec has observed in the Europe, Middle East, and Africa (EMEA) region. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It also discusses numerous issues related to online fraud, including phishing and spam. This volume covers 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, analyse, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The Symantec *EMEA Internet Security Threat Report* gives enterprises and consumers essential information to effectively secure their systems now and into the future.

Highlights

The following section will offer a brief summary of the security trends that Symantec observed during the second half of 2007 based on data provided by the sources listed above. These highlights include all of the metrics that are discussed in the *EMEA Internet Security Threat Report*.

Attack Trends Highlights

- Germany ranked first for malicious activity in EMEA during the second half of 2007, 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 the average was 18,616 active bots per day.
- 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.

Malicious Code Highlights

- Trojans were the most common type of malicious code, accounting for 68 percent of the top 50 potential infections in the region, 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, which exploits a vulnerability in PDF 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 61 percent 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.
- In the second half of 2007, five percent of the volume of the top 50 samples in EMEA had the capability to modify Web pages, unchanged from the first half of 2007.

Phishing and Spam Trends Highlights

- In the second half of 2007, Romania was home to the most phishing Web sites in EMEA, with 46 percent of the regional 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.

Attack Trends

The malicious activity discussed in this section includes not only attack activity, but also phishing Web sites hosted, malicious code, spam zombies, bot-infected computers, and command-and-control server activity. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activity can be found in their respective sections of this report.

This section of the *EMEA Internet Security Threat Report* will analyse the following attack activities that Symantec observed in EMEA between July 1 and December 31, 2007:

- Malicious activity by country
- Top countries of attack origin
- Top countries targeted by denial of service attacks
- Bot-infected computers
- Bot-infected computers by country
- Bot-infected computers by city
- Attacks—protection and mitigation

Malicious activity by country

This metric will assess the countries in which the most malicious activity took place or originated in EMEA. To determine this, Symantec compiles geographical data on numerous malicious activities, including bot-infected computers, bot command-and-control servers, phishing Web site hosts, malicious code incidents, spam relay hosts, and Internet attacks.

To determine the proportion of Internet-wide malicious activity that originated in each country, the mean of the proportion of all the considered malicious activities that originated in each country was calculated. This average determined the proportion of overall malicious activity that originated from the country in question and was used to rank each country within the EMEA region. This section will discuss those findings.

Germany ranked first for malicious activity in EMEA during the second half of 2007, with 18 percent, a slight drop from 19 percent in the previous period (table 1). It is not surprising that, within the region, the country with the highest number of broadband subscribers has the greatest proportion of malicious activity. As was seen in the previous reporting period, Germany ranks first in all categories except malicious code, which reflects its dominance in broadband subscribers and overall Internet usage within EMEA.

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	Germany	18%	19%	1	1	1	3	1	1
2	2	United Kingdom	11%	11%	6	2	4	1	8	3
3	3	France	9%	9%	5	6	3	6	4	4
4	5	Spain	8%	8%	2	10	9	4	6	2
5	4	Italy	8%	8%	3	4	7	5	3	5
6	6	Poland	5%	5%	4	13	8	10	5	6
7	9	Turkey	5%	3%	7	8	20	12	2	7
8	8	Netherlands	5%	4%	15	5	2	9	19	10
9	10	Russia	4%	3%	9	9	5	17	7	14
10	11	Sweden	3%	2%	17	3	6	16	34	9

Table 1. Malicious activity by country, EMEA
Source: Symantec Corporation

Hosts based in the United Kingdom were responsible for the second highest proportion of malicious activity in EMEA during this period, with 11 percent of the total, unchanged from the previous six months. The only category in which the United Kingdom ranked first is for malicious code activity, which may correlate to its rank as the top country for Trojans and back door submissions, the two most prevalent classes of malicious code.

One area of change for the United Kingdom is in its ranking for hosted phishing sites, which dropped to fourth this period from second in the previous period. The Office of Fair Trading (OFT),[1] the department of the UK government responsible for consumer protection, has been working to increase awareness of phishing and other Internet scams since 2005.[2] The private sector is also working to combat the problem. For example, a campaign in 2007 by Nationwide Building Society involved the formation of an anti-fraud group devoted to the implementation of new solutions to automatically track phishing Web sites.[3] The result of these initiatives may have contributed to the reduction in phishing activity in the United Kingdom. Because awareness of phishing by end-users and customers may reduce the success for operators of phishing sites, they may be compelled to use other attack methods, such as keystroke loggers, resulting in a reduction in the number of detected phishing hosts.

Malicious code trends may be influencing phishing activity. Historically, many phishing sites were hosted on compromised servers, where they would run until they were detected and taken offline. To be successful, phishing sites must remain undetected for some time because there is a delay between the transmission of phishing email messages, for example, and users actually visiting the site. The increased vigilance in detecting and removing these Web sites may have contributed to the decline in phishing site rank for the United Kingdom.

[1] http://www.oft.gov.uk/
[2] http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=2585
[3] http://www.computing.co.uk/computing/news/2188055/nationwide-cracks-phishing

As well, Symantec is observing the increasing use of malicious code that modifies Web pages. Attackers may be adopting this tactic because they can no longer as easily create and maintain phishing sites through traditional means, such as by compromising a Web server. One example is the discovery and break-up of a major phishing case that included over 10,000 Web sites that had been compromised and used for phishing attacks.[4]

France again ranked third in malicious activity for this period, with nine percent of the regional total. For bot activity, it dropped to fifth for this period, from third previously. For attack activity, it dropped from third to fourth. For phishing hosts, France went up from fifth in the first half of 2007 to third in this period.

The new French president, Nicolas Sarkozy, elected in May 2007, has taken a strong stance against illegal peer-to-peer (P2P) file sharing. The French anti-file sharing initiative,[5] sponsored by industries and endorsed by Sarkozy, may affect how ISPs operating in France respond to security incidents in the future. According to the plan, ISPs bear the responsibility of enforcing copyright protection within their networks. This will necessitate the use of advanced content monitoring technologies to detect and stop transmission of pirated media by their customers. The deployment of these technologies will likely come at great expense and effort, and may add increased pressure on the security response resources of the ISPs. The initiative is new and the consequences may not be seen for some time. The UK government is pushing for a similar plan for ISPs operating there.[6]

Germany, the United Kingdom and France are the EMEA countries with the most broadband subscribers and well-established Internet communities and it is not surprising that they also have the biggest share of malicious activity within EMEA.

Top countries of attack origin

Measurement of the top countries targeting the region for attacks is based on aggregate IDS and firewall event data collected through the Symantec Global Intelligence Network. These events include intrusions, attempted intrusions and reconnaissance activity. This activity is initiated by both attackers targeting specific individuals or organisations, and automated attacks—such as bots and other types of malicious code—that may not be targeting specific Internet addresses.

Fifty-two percent of attacks targeting EMEA countries in the last six months of 2007 originated in the United States (table 2), a substantial increase from 35 percent in the previous period. This is more than double the 24 percent of attacks that originated in the United States worldwide for this period.

Malicious activity usually affects computers that are connected to high-speed broadband Internet because broadband connections provide larger bandwidth capacities than other connection types, and the connections are frequently continuous. It is thus not surprising that the United States had the most malicious activity as it has the most established broadband infrastructure in the world: 94 percent of U.S. households have access to available broadband connections, and its 65.5 million broadband subscribers represent over 20 percent of the world's total, more than any other country.[7]

The proportional increase in attacks from the United States targeting EMEA in this period, however, may also be due to a decrease in activity originating in China. As well, the percentage of attacks on EMEA originating in Norway decreased from 13 percent in the first six months of 2007 to two percent during this period.

[4] http://www.itpro.co.uk/security/news/123003/italian-police-arrest-phishing-gang.html
[5] http://arstechnica.com/news.ars/post/20071125-the-insanity-and-genius-of-frances-anti-file-sharing-plan.html
[6] http://www.guardian.co.uk/technology/2008/feb/22/filesharing?gusrc=rss&feed=technology
[7] http://point-topic.com/content/operatorSource/profiles2/usa-broadband-overview.htm

Current Rank	Previous Rank	Country	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage
1	1	United States	52%	35%	24%
2	2	United Kingdom	11%	15%	5%
3	3	China	5%	14%	10%
4	36	Slovenia	4%	<1%	1%
5	5	Germany	4%	5%	2%
6	8	Canada	3%	1%	5%
7	6	Italy	3%	3%	1%
8	4	Norway	2%	13%	1%
9	7	France	2%	2%	1%
10	9	Spain	1%	1%	1%

Table 2. Top countries of attack origin, EMEA

Source: Symantec Corporation

The United Kingdom ranked second for originating attacks on EMEA, with 11 percent, a decrease from 15 percent in the previous period. In the last six months of 2007, five percent of attacks worldwide originated in the United Kingdom. As noted in the previous volume of the *EMEA Internet Security Threat Report*, the difference in proportions between attacks originating in the United Kingdom targeting EMEA and attacks with global targets indicate that much of the attack volume originating in the United Kingdom is targeting EMEA.

China again ranked third for originating attacks on EMEA this period, with five percent of the total, although this is substantially less than the 14 percent recorded in the first half of the year. The five percent of attacks targeting EMEA originating in China is also less than its 10 percent total for worldwide attacks. Overall, there has been a decline in attacks originating in China.

One reason for this drop may be that there was a noticeable decrease in the number of active bots in China in the second half of 2007, which is attributable to a significant reduction in the availability of many Web sites, forums, and blogs in China for several months during this period.[8] Symantec believes that, because of their scalability, bots are responsible for much of the malicious attack activity that is observed, and any serious reduction in the number of bots should result in a corresponding drop in total attack activity. Although the proportion of attacks originating in China dropped, perception of China as a source of attacks in the region remains; in the second half of 2007, sources in the governments of both the United Kingdom[9] and France[10] claimed to have directly observed attacks from China.

Slovenia ranked fourth for originating attacks targeting EMEA, with four percent of the total. This is noteworthy since it was not ranked in the top 10 previously. This is much higher than Slovenia's one percent share of attacks globally, and indicates that attacks originating in Slovenia are targeting the EMEA region specifically.

[8] http://www.msnbc.msn.com/id/21268635/
[9] http://www.guardian.co.uk/technology/2007/sep/04/news.internet
[10] http://www.theregister.co.uk/2007/09/12/french_cyberattacks/

Six of the top 10 countries targeting EMEA are situated in the region. Previously, the *EMEA Internet Security Threat Report* has attributed this to several factors. Many targets, such as businesses, governmental organisations and even individuals, have a higher profile locally, making them natural targets for attackers based in the region. Linguistic and cultural similarities throughout the region may also contribute to intra-regional attack volumes.

Top countries targeted by denial of service attacks

This metric will assess the geographic location of targets of DoS attacks. Insight into the locations targeted by these attacks is valuable in determining global trends in DoS attack patterns. It may also help administrators and organisations in affected countries to take the necessary steps to protect against or minimise the effects of such attacks.

DoS attacks are a major threat to Internet-dependent organisations, as a successful attack can render Web sites or other network services inaccessible to customers and employees. This could result in the disruption of organisational communications, a significant loss of revenue, and/or damage to the organisation's reputation. Furthermore, as discussed in previous volumes of the *Internet Security Threat Report*, criminals have been known to use DoS attacks in extortion schemes.[11]

The United Kingdom was again the top country in EMEA targeted by DoS attacks in the second half of 2007, with 32 percent of the regional total (table 3). This is down from the 46 percent recorded in the first half of the year. It was speculated in previous volumes that hacktivism,[12] specifically in response to legislation outlawing DoS attacks, might be responsible for DoS attacks.[13] While the decrease may be indicative of a decline of hacktivists activity, the United Kingdom's 32 percent is still a very large share relative to the other countries. One widely reported incident occurred in May 2007, when access to the Web site of the Daily Telegraph newspaper was blocked by a DoS attack.[14] Other attacks, including extortion attacks, have been reported in the United Kingdom in the past.

[11] http://networks.silicon.com/webwatch/0,39024667,39118605,00.htm
[12] Malicious activity carried out for a social, political, or religious cause that the attacker(s) identify with, rather than for fun or commercial reasons
[13] http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/
[14] http://technology.timesonline.co.uk/tol/news/tech_and_web/article1824601.ece

Current Rank	Previous Rank	Country	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage
1	1	United Kingdom	32%	46%	6%
2	2	Germany	12%	10%	2%
3	4	France	10%	7%	2%
4	3	Netherlands	7%	7%	1%
5	5	Italy	5%	4%	1%
6	8	Russia	5%	2%	1%
7	6	Spain	4%	3%	1%
8	7	Sweden	3%	2%	1%
9	9	Ireland	2%	2%	<1%
10	12	Belgium	2%	<1%	<1%

Table 3. Top countries targeted by DoS attacks, EMEA
Source: Symantec Corporation

Germany ranked second for this period, increasing to 12 percent from 10 percent in the previous period. Again, hacktivism may be responsible for Germany's position here, since new legislation implementing the EU Framework Decision on Attacks against Information Systems went into effect in Germany in August 2007.[15] The law clarified and extended the criminality of offences considered cybercrime. There was considerable concern in the security research community about the implications of this law, because it could be interpreted to make possession or use of security tools a criminal offence.[16] Several German security research groups, such as Phenoelit, took their content offline because it could be considered illegal under the new law.[17] The increase in DoS attacks within Germany may be evidence of retaliation by hackers against this new legislation.

France replaced the Netherlands this period as the third ranked country targeted by DoS attacks in EMEA, with an increase to 10 percent, up from seven percent in the first six months of 2007. Given that the United Kingdom, France, and Germany have the most established Internet infrastructures in EMEA, it is natural for these three countries to rank high in DoS attacks, especially considering that the Web has become a major platform for personal, business and government purposes in these countries, and the disruption of Internet services is of real consequences.

Bot-infected computers

Bots are programs that are covertly installed on a user's machine to allow an unauthorised user to remotely control the targeted system through a communication channel, such as IRC, P2P, or HTTP. These channels allow the remote attacker to control a large number of compromised computers in a bot network (botnet), which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up DoS attacks against an organisation's Web site, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft, all of which can have serious financial and legal consequences.

[15] http://www.securityfocus.com/columnists/448
[16] http://www.oreillynet.com/sysadmin/blog/2007/08/german_antihacker_law_starts_t.html
[17] http://www.phenoelit.de/202/202.html

Symantec identifies bot-infected computers based on coordinated scanning and attack behaviour that is observed in network traffic. The bot-infected computers identified have attempted to exploit vulnerabilities in network services to propagate and may include bot-infected computers that are part of botnets controlled by various communication channels such as IRC, P2P, or HTTP. This behavioural matching will not catch every bot-infected computer, specifically bot-infected computers that have used non-traditional propagation methods, and may identify other malicious code or individual attackers behaving in a coordinated way like a bot network. However, this behavioural matching will identify many of the most coordinated and aggressive bot-infected computers.

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. In the second half of 2007, Symantec observed an average of 25,344 active bots per day in the EMEA region (figure 1). This is a greater number than seen in either of the two previous reporting periods, when 18,616 active bots were detected in the first half of 2007, and 21,707 in the last half of 2006. In the second half of 2007, active bots in the EMEA region accounted for 41 percent of global bot activity.

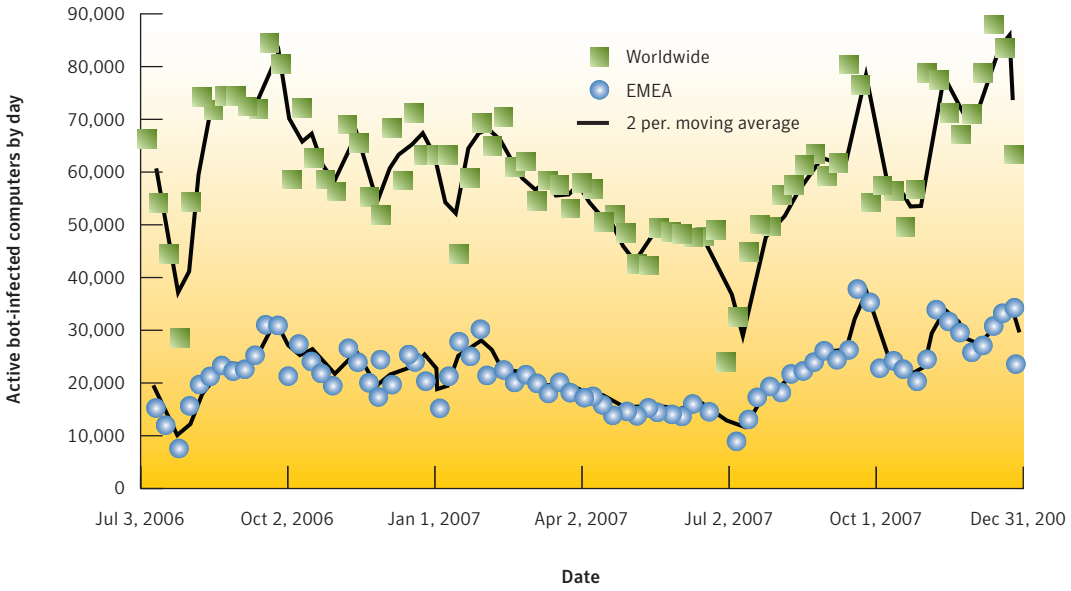

Figure 1. Active bot-infected computers by day, EMEA and Global
Source: Symantec Corporation

A distinct bot-infected computer is a computer that has been determined to be active at any point in the reporting period. There were 2,885,129 distinct bot-infected computers recorded in the EMEA region in the last six months of 2007. This is 38 percent more than the 2,084,189 observed in EMEA in the previous reporting period. The rise in the detection of distinct bot-infected computers in EMEA this period is likely attributable to an overall increase in broadband subscriptions in EMEA countries during this time. Along with continued growth in Western Europe, broadband subscriptions are rapidly increasing in many Eastern European countries; for example, Russia ranked eighth globally for broadband growth last period.[18] This increase may also be due to the shorter lifespan of bots because of improved detection rates in countries

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

such as Germany, where the average lifespan of a bot is one day, compared to an average of three days in EMEA overall. This forces botnet controllers to actively seek out new, replacement bots, driving the overall number of distinct bots higher for the period.

To reduce exposure to bot-related attacks, end users should employ defence-in-depth strategies,[19] including the deployment of antivirus software and a firewall. Creating and enforcing policies that identify and limit applications that can access the network may also help to limit the spread of bot networks. Users should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Users should never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known.

Bot-infected computers by country

Recognizing the ongoing threat posed by botnets, Symantec tracks the distribution of bot-infected computers worldwide as well as regionally. For regions, Symantec calculates the number of computers globally that are known to be infected with bots, and assesses which countries within the region are home to highest percentages of these computers. A high percentage of infected machines could mean a greater potential for bot-related attacks, as well as indicating the level of patching and security awareness in the region.

For EMEA, Germany ranked first for bot-infected computers detected in the last six months of 2007, with 18 percent of the regional total (table 4), a decrease from 23 percent in the first six months of the year. The reduction may be due to the increased enforcement of laws against cybercrime in Germany after the implementation of the EU Framework Decision on Attacks against Information Systems in August of 2007, mentioned previously. The law clarified the criminality of unauthorised access to computer systems and DoS attacks. Prior to the passing of the legislation, the German penal code may not have considered DoS attacks against non-commercial targets illegal. The law also specifically criminalised access to computer systems. Prior to the passage of the law, unauthorised access to computer systems may have been technically legal if it could not be proven that there were other, specifically criminal aspects to the incident. As noted in the previous volume of the *EMEA Internet Security Threat Report*, the high proportion of bot activity in Germany is likely due to the high number of broadband subscribers there, rather than poor security awareness or a lack of response capability.[20]

[19] Defence-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defence-in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.
[20] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_emea_09_2007.en-us.pdf : p. 12

Current Rank	Previous Rank	Country	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage	Average Lifespan (days)	Command-and-Control Percentage
1	1	Germany	18%	23%	10%	1	22%
2	2	Spain	14%	15%	7%	3	3%
3	4	Italy	10%	9%	6%	3	6%
4	7	Poland	10%	6%	6%	3	2%
5	3	France	9%	11%	5%	3	6%
6	5	United Kingdom	7%	9%	4%	4	11%
7	9	Turkey	6%	2%	3%	2	5%
8	6	Israel	5%	6%	3%	3	2%
9	11	Russia	3%	2%	1%	7	5%
10	8	Portugal	3%	2%	1%	2	1%

Table 4. Bot-infected computers by country, EMEA
Source: Symantec Corporation

Spain was the second ranked country in the second half of 2007, with 14 percent of bot-infected computers detected, down slightly from 15 percent in the previous period. In the previous report, it was noted that Spain had the fifth highest number of broadband connections added between May 2006 and May 2007. Spain also recently ranked tenth for total broadband connections globally.[21]

Italy ranked third for malicious activity in EMEA this period, up from fourth in the first half of 2007. In the same period one year ago, Italy was ranked sixth. This rise over the past 12 months may reflect increasing broadband subscription rates and the growing deployment of FTTH within the country.[22]

In Volumes XI and XII of the *Internet Security Threat Report*, Symantec speculated that the number of new users adopting high-speed Internet in a country may be a significant factor in the rate of bot infections. Rapidly growing ISPs may be focused on growth and slow to implement effective measures to protect against threats such as botnets. In many countries, ISPs and law enforcement are still developing their own response to the problem of bot activity in their region.

For example, Botswana's cybercrime bill passed its second parliamentary reading on December 3, 2007 and it may become law in 2008.[23] The bill defines offences associated with cybercrime activity, such as unauthorised system access or interference. It also specifies jurisdiction parameters, allowing for a framework to be built for cooperation with other governments in dealing with incidents. This law may be a response to a serious incident in 2006 involving a local bank in Botswana, in which attackers allegedly compromised the systems of a local bank and transmitted funds to South Africa.[24] Further raising the profile of cybercrime within Botswana was that it was identified as a source of click-fraud activity, which may indicate local cyber-criminals or an unusually high pattern of infection with malicious code designed to commit click-fraud.[25]

[21] Point Topic World Broadband Statistics: Q3 2007 report
[22] http://point-topic.com/content/operatorSource/profiles2/italy-broadband-overview.htm
[23] http://allafrica.com/stories/200712040992.html
[24] http://www.mmegi.bw/2007/October/Friday5/30.php
[25] http://www.mmegi.bw/2007/September/Friday14/29.php

Another example is in Estonia, where the government is attempting to amend its penal code so that cyber-attacks can be considered terrorism, which would allow for imposing harsher punishment.[26] This is likely a response to the DoS attacks in Estonia in May 2007, and meant to serve as deterrence to such attacks in the future.[27]

User awareness is another factor. Broadband users are often unaware of the malicious dangers on the Internet until they are directly affected, and only then do they implement security solutions such as antivirus and personal firewalls. Moreover, subscribers may be foregoing extra premium security options from their ISP to reduce monthly costs, increasing their risk of exposure to malicious activities.

Bot-infected computers by city

Madrid was the top ranked city for bot-infected hosts in the last six months of 2007, the same position it has held in the previous two periods (table 5). One possible reason for this is the high proportion of bot activity in Spain, as it ranks second in EMEA behind only Germany. Also, as discussed in Volume XII of the *EMEA Internet Security Threat Report*, the continued prominence of Madrid in this metric is likely due to much of Spain's Internet infrastructure and ISPs being concentrated in Madrid, as opposed to Germany, where ISPs are spread more evenly across the country.[28]

Another reason may stem from fibre-to-the-home (FTTH) trials conducted in Madrid.[29] With FTTH, also known as FTTP (fibre-to-the-premises), the fibre-optic cable is connected directly to the end-point, in contrast to traditional broadband connections where the transmission to the end-point occurs over telecommunications infrastructure not originally designed for high-capacity data transmission, such as the telephone network. Since botnet operators seek bots with two important properties—that they are online as continuously as possible and that they have high-bandwidth connections—FTTH connections are ideal targets since they have superior bandwidth capacity, typically higher average speeds and the possibility of continuous connections.

Current Rank	Previous Rank	City	Country	Current Regional Percentage	Previous Regional Percentage
1	1	Madrid	Spain	7%	8%
2	7	Ankara	Turkey	6%	2%
3	20	Cagliari	Italy	3%	1%
4	9	Warsaw	Poland	3%	2%
5	12	Wroclaw	Poland	3%	2%
6	3	Rome	Italy	2%	3%
7	8	Lisbon	Portugal	2%	2%
8	4	Milan	Italy	2%	3%
9	13	Rabat	Morocco	2%	2%
10	11	Moscow	Russia	2%	2%

Table 5. Bot-infected computers by city, EMEA
Source: Symantec Corporation

[26] http://www.baltictimes.com/news/articles/18815/
[27] http://news.bbc.co.uk/2/hi/europe/6665145.stm
[28] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_emea_09_2007.en-us.pdf : p. 14
[29] http://www.ecommercetimes.com/story/60791.html?welcome=1202749024

Beyond Spain, FTTH may be an important trend to watch in EMEA and elsewhere. This technology is the next step in broadband connectivity, bringing much higher bandwidth capacity to both personal and commercial users. The technology is growing, although the level of deployment varies among countries in the EMEA region. Many telecommunications companies are conducting trials and phasing in deployment city by city. For this reason, it is important to look at bot-infected computers by city, since FTTH connections will be appealing targets for botnet controllers. Trials or deployment of FTTH services in cities may affect bot activity because botnet operators may target these cities in an attempt to secure these high-bandwidth hosts.

Ankara, Turkey jumped to second for this reporting period, up from seventh in the first half of 2007. The concentration of bot activity in Ankara may be because a major Ankara-based ISP is working to roll out fibre-optic lines to increase bandwidth availability in the country.[30]

Cagliari, the capital city of Sardinia, Italy, significantly increased in rank for bot activity by city this period, from twentieth in the last period to third for the second half of 2007. Its rise may be due to recent ownership changes to the major ISPs providing service there and the possible subsequent challenges to providing effective security.[31]

[30] http://www.point-topic.com
[31] http://www.iht.com/articles/2007/04/29/business/italia.php

Attacks—protection and mitigation

There are a number of measures that enterprises, administrators, and end users can take to protect against malicious activity. Organisations should monitor all network-connected computers for signs of malicious activity, including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organisations should employ defence-in-depth strategies, including the deployment of antivirus software and a firewall. Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

Symantec recommends that organisations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorised communications are not taking place.[32] Organisations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users. In addition, the egress filtering is one of the best ways to mitigate a DoS attack. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. By creating and enforcing policies that identify and restrict applications that can access the network, organisations can minimise the effect of malicious activity, and hence, minimise the effect on day-to-day operations.

[32] Ingress traffic refers to traffic that is coming into a network from the Internet or another network. Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

Malicious Code Trends

Symantec gathers malicious code data from over 120 million desktops that have deployed Symantec's antivirus products in consumer and corporate environments. The Symantec Digital Immune System, and Scan and Deliver technologies allow customers to automate this reporting process. In previous editions of the Symantec *Internet Security Threat Report*, the number and volume of threats analysed were based upon the number of malicious code reports received from enterprise and home users. This report will also examine malicious code according to potential infections. This allows Symantec to determine which malicious code sample was attempting to infect computers and the number of potential infections in EMEA.

This section of the *EMEA Internet Security Threat Report* will analyse the following malicious code threats that Symantec observed in EMEA between July 1 and December 31, 2007:

- Malicious code types
- Geolocation by type
- Top malicious code samples
- Top new malicious code families
- Threats to confidential information
- Propagation mechanisms
- Malicious code that modifies Web pages
- Malicious code—protection and mitigation

Malicious code types

The proportions of potential malicious code infections reported in EMEA closely correlate with the numbers observed globally. For example, between July 1 and December 31, 2007, Trojans made up 68 percent of the volume of the top 50 potential infections in EMEA and 71 percent globally (figure 2). For Trojans, the percentages are also virtually the same for this reporting period as in the first half of the year, when the volume of Trojans made up 68 percent of the top 50 potential infections in EMEA and 73 percent globally.

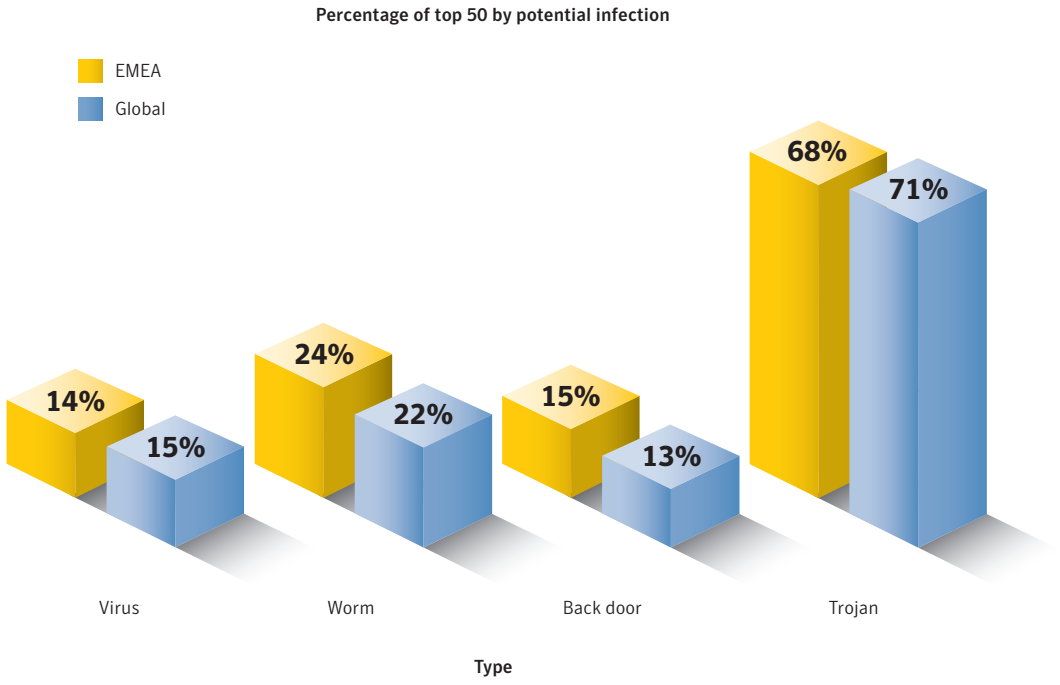

Figure 2. Potential infections by type, EMEA
Source: Symantec Corporation

Trojans remain popular for the same reasons speculated in the previous volume of the *EMEA Internet Security Threat Report*. First, they do not produce the often disruptive network noise associated with other types of malicious code. For example, mass-mailing worms produce a lot of email communication, while worms that attack network services can cause service outages or consume large amounts of bandwidth. Trojan attacks, on the other hand, are more point-to-point and harder to identify through the same type of network noise detection. Trojans can also expose confidential information, and can be used to install other malicious programs. Furthermore, they can often be used to download subsequent malicious code modules, which can then be used for further attack activity. Commonly known as staged downloaders, these Trojans are becoming increasingly common. Staged downloaders are small, specialised Trojans that establish a beachhead on a compromised computer in order to download and install other malicious programs, such as back doors or other Trojans. Many of these Trojans are installed using Web browser vulnerabilities and zero day vulnerabilities in other applications.

Worms made up 24 percent of potential infections originating in EMEA, compared to 22 percent observed globally. This is also very close to proportions observed in the previous six months when 26 percent of potential infections in EMEA were classified as worms, with a slightly larger gap between the proportions of worms seen in EMEA and the global volume. Worms are on the decline, partly because of a lack of major vulnerabilities through which they can propagate. Increased blocking by ISPs, deployment of security patches, antivirus use and operating system upgrades will reduce the worm submission count by attrition, and older, still-propagating worms should slowly die out.

Geolocation by type

This metric examines top countries for potential malicious code infections in EMEA by malicious code type. Because of the different propagation mechanisms used by different malicious code types, and the different affect that each may have, the geographic distribution of malicious code can indicate where network administrators in different regions may want to increase their security measures.

Along with ranking first for other three malicious code types in this metric, the United Kingdom was the top country for back doors in EMEA this period (table 6). The remaining two top countries for back doors in EMEA were Germany in second, and France in third. As these countries have the highest number of broadband connections and the most well-established Internet communities, it is not surprising that they are the top three countries for back doors, which are one of the most common classes of malicious code. It is worth noting that Vundo[33] and Virut,[34] two of the top 10 malicious code samples seen in the United Kingdom during the second half of 2007, had back door components.

Rank	Top Country
1	United Kingdom
2	Germany
3	France

Table 6. Location of back doors, EMEA
Source: Symantec Corporation

For Trojans, the top three countries were, in order, the United Kingdom, Germany, and Italy (table 7). Again, as with the first two countries and France, Italy has a high number of broadband connections and its appearance here is not surprising.

Rank	Top Country
1	United Kingdom
2	Germany
3	Italy

Table 7. Location of Trojans, EMEA
Source: Symantec Corporation

[33] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[34] http://www.symantec.com/security_response/writeup.jsp?docid=2007-092718-3700-99

The top three ranked countries for viruses this period were the United Kingdom, Egypt and Poland (table 8). The high rank of the latter two countries may have to do with the high rates of piracy in each. File infection is characteristic of the virus class of malicious code. One way that viruses spread is through pirated software as executable files from disreputable sources are copied and shared. According to a recent study, the piracy rate in Poland is 57 percent, while in Egypt it is 63 percent.[35] Additionally, Egypt and Poland are both experiencing high growth in broadband deployment.[36] Lack of security awareness and a lack of protective measures, such as gateway filters, by ISPs may contribute to the propagation of viruses through vectors such as CIFS file shares. The increasing availability and use of high-volume portable storage devices, such as USB keys and portable hard drives, may also contribute to the re-emergence of classic viruses.

Rank	Top Country
1	United Kingdom
2	Egypt
3	Poland

Table 8. Location of viruses, EMEA
Source: Symantec Corporation

The top three countries for worms this period were the United Kingdom, Germany and Spain (table 9). The United Kingdom and Germany are the two EMEA countries with the highest number of broadband users. Spain ranked second for attacks in the malicious activity by country ranking, and those attacks may be related to the high submission rate for worm samples.

Rank	Top Country
1	United Kingdom
2	Germany
3	Spain

Table 9. Location of worms, EMEA
Source: Symantec Corporation

Top malicious code samples

The top malicious code sample in EMEA in the second half of 2007 was Vundo, a Trojan with a back door component (table 10). Vundo was also the top sample causing potential infections globally this period. In the first half of the year, it ranked second in EMEA. The United Kingdom was the top country for potential infections caused by Vundo in both this and the previous period.

The second ranked sample for this report, the Zlob Trojan, ranked third in the first half of 2007. Both of these malicious code instances are staged downloaders and can augment their functionality with updates downloaded from remote locations on the Internet. Vundo also attempts to generate revenue from infections through its adware component.

[35] http://w3.bsa.org/globalstudy//upload/2007-Global-Piracy-Study-EN.pdf
[36] http://www.point-topic.com

Regional Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact
1	Vundo	Trojan, back door	United Kingdom	Spain	N/A	Displays advertisements, downloads and installs additional threats
2	Zlob	Trojan	Germany	France	N/A	Downloads and installs additional threats
3	Fujacks	Worm, virus	United Arab Emirates	Ethiopia	CIFS	Modifies HTML files
4	Netsky	Worm	Spain	Poland	SMTP, P2P	Keystroke logger targets www.e-gold.com
5	Rontokbro	Worm	United Arab Emirates	France	SMTP	Performs DoS attacks
6	Virut	Virus, back door	United Kingdom	Poland	CIFS	Downloads and installs additional threats
7	Metajuan	Trojan	United Kingdom	Spain	N/A	Downloads and installs additional threats
8	Rahack	Worm	Germany	Austria	CIFS	Modifies HTML files
9	Licum	Worm, virus	Italy	Germany	CIFS, remote vulnerability	Downloads and installs additional threats
10	Adclicker	Trojan	United Kingdom	Italy	N/A	Clicks advertisements to generate revenue

Table 10. Top malicious code samples, EMEA
Source: Symantec Corporation

The third most common sample, Fujacks[37] is a file infector that also modifies HTML files, a recent trend that Symantec has observed and continues to monitor. When Fujacks runs on a computer, it scans the file system for common file extensions associated with Web content, such as .html and .aspx. It then appends invisible iframe code to these files that will redirect the browser that renders them to a Web site to download additional malicious code. An iframe is an HTML element that can include Web content from other pages or Web servers to be rendered when the user visits the original page. This tag can be constructed so that it is effectively invisible and the user will not see any of the embedded content when viewing the original page.

Top new malicious code families

The most reported new malicious code family in EMEA during the second half of 2007 was Pidief (table 11).[38] Instances of malicious code belonging to this family were the fourth most commonly reported globally. Pidief is interesting because it exploits a vulnerability in Adobe PDF reader software.[39] Several factors may explain the high rank of Pidief for this period. Organisations within EMEA may be more resistant, on average, to typical malicious code threats as there may be more widespread deployment of security technologies such as gateway filtering and more user awareness in the region than across the Internet as a whole. Furthermore, PDF documents are widely used and trusted within corporate environments, resulting in a vector for propagation which may be, for now, very successful.

[37] http://www.symantec.com/security_response/writeup.jsp?docid=2007-010509-0134-99
[38] http://www.symantec.com/security_response/writeup.jsp?docid=2007-102310-3513-99
[39] http://www.securityfocus.com/bid/25748

Regional Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact
1	Pidief	Trojan	United Kingdom	Germany	N/A	Exploits Adobe Acrobat vulnerability to lower security settings and download other threats
2	Neeris	Worm, back door	Spain	United Kingdom	IM	Allows remote access
3	Scrimge	Worm, back door	Spain	United Kingdom	IM	Allows remote access
4	Blastclan	Worm	United Arab Emirates	Egypt	CIFS	Disables security applications
5	Farfli	Trojan	France	Italy	N/A	Downloads other threats and modifies Internet Explorer® start page
6	Ascesso	Trojan	Germany	United Kingdom	N/A	Downloads other threats and sends spam
7	Fakeavalert	Trojan	United Kingdom	Germany	N/A	Displays fake antivirus alerts and lowers security settings
8	Mimbot	Worm	United Kingdom	Italy	MSN Messenger	Allows remote access
9	Mabezat	Worm, virus	Saudi Arabia	Oman	SMTP, CIFS	Encrypts data files
10	Vispat	Worm	Italy	Belgium	SMTP	Modifies Internet Explorer start page and lowers security settings

Table 11. Top new malicious code families, EMEA

Source: Symantec Corporation

Neeris,[40] which spreads over the MSN instant messaging network, was the second most commonly seen new family of malicious code in EMEA for this period. It ranked seventh globally. The prominence of Neeris in the EMEA region relative to its rank globally is due its use of European languages in its propagation attempts. To spread, Neeris sends messages to users on a victim's contact list in Spanish, French, German, Italian and English.

The third most widely reported new malicious code family was Scrimge,[41] another instance of malicious code that attempts to spread through the MSN network. Like Neeris, variants of the Scrimge family send messages with file transfer requests to the contacts of infected users to propagate. Various languages are used, depending on the variant. For example, Scrimge[42] sends messages in different languages, including English and French. The Scrimge family ranked sixth globally for this period.

[40] http://www.symantec.com/security_response/writeup.jsp?docid=2007-091208-1650-99
[41] http://www.symantec.com/security_response/writeup.jsp?docid=2007-081716-1758-99
[42] http://www.symantec.com/security_response/writeup.jsp?docid=2007-092816-1332-99&tabid=2

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats may expose sensitive data such as system information, confidential files and documents, or logon credentials. Some malicious code threats, such as back doors, can give a remote attacker complete control over a compromised computer. Threats to confidential information are a particular concern because of their potential for use in criminal activities. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

Within the enterprise, exposure of confidential information can lead to significant data leakage. If it involves customer-related data—such as credit card information—customer confidence in the enterprise can be severely undermined. Moreover, it can also violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies, could also be leaked from compromised computers. It should be noted that threats that expose confidential information may employ more than one method to do so; as a result, cumulative percentages discussed in this metric may exceed 100 percent.

During this reporting period, for all types of confidential information exposure classifications, proportions observed in EMEA closely correlate with global numbers. Of the top 50 threats in EMEA, 67 percent of malicious code instances are considered threats to confidential information, compared to 68 percent reported globally. In the first half of 2007, 61 percent of threats in EMEA were classified as threats to confidential information.

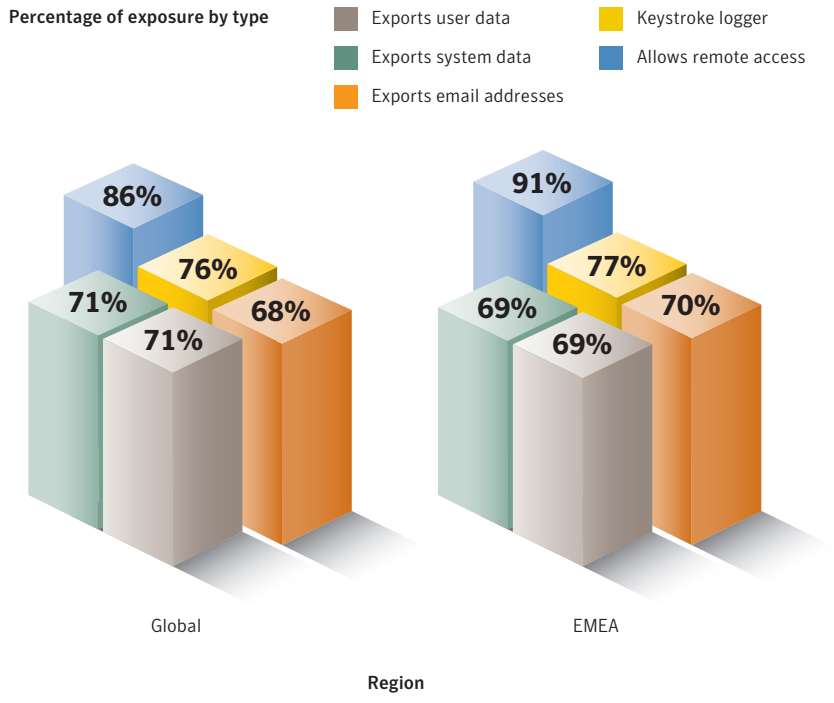

Figure 3. Threats to confidential information, EMEA and Global
Source: Symantec Corporation

Sixty-nine percent of the threats to confidential information reported in EMEA for this period were classified as threats that can export user data, compared to 71 percent globally (figure 3). This is a decrease from the first half of the year both in EMEA and globally, when the percentages were 77 percent and 80 percent, respectively.

Instances of malicious code that have the capability to transmit system data made up 69 percent of all threats to confidential information reported in the EMEA region this period, compared to 71 percent globally. In the previous reporting period, 78 percent of threats originating in EMEA had this capability, compared to 76 percent worldwide. These forms of data leakage can enable an attacker to steal a user's identity or launch further attacks. An attacker with access to a user's personal and system data can use it to craft a targeted social engineering attack as though it were originating from that particular user.

Seventy percent of threats to confidential information in EMEA this period had the ability to extract and transmit email addresses, compared to 68 percent globally. In the first half of 2007, the numbers were 75 percent in EMEA and 76 percent worldwide. These email addresses may be used in spamming operations or sold in bulk to other individuals or groups.

Seventy-seven percent of the threats to confidential information reported in EMEA during this period had a keystroke logger component, compared to 76 percent globally. This is a decline from the previous period, when the proportions were 86 percent in EMEA and 88 percent worldwide. Keystroke loggers are popular tools because they allow an attacker to steal credentials from any interface or Web site, without specific customisation. The increasing use of two-factor identification by online banks, which can limit the usefulness of keystroke loggers in obtaining useful credentials from compromised hosts, may explain the decline.

Instances of malicious code that facilitated remote access made up 91 percent of confidential-information threats reported in EMEA for this period, compared to 86 percent globally. In the first half of the year, 87 percent of potential infections in EMEA had back door capabilities, compared to 88 percent globally.

Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), Simple Mail Transfer Protocol (SMTP), Common Internet File System (CIFS), P2P, and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised via a back door server and using it to upload and install itself.

This metric will discuss some of the propagation mechanisms used by malicious code samples in EMEA during the first six months of 2007. It should be noted that many malicious code samples employ multiple propagation mechanisms in an effort to increase the probability of successful propagation. As a result, cumulative percentages included in this discussion may exceed 100 percent.

Email attachments remained the most commonly used vector of propagation within EMEA for the last six months of 2007, with 37 percent of all samples using this vector (table 12). This is a decline from the first half of the year, when 49 percent of all samples were classified as propagating through email attachments. This may be due to the decline in submissions of NetSky, a mass-mailing worm that also propagates over P2P file sharing networks. The prominence of email attachments as a propagation vector is not surprising because email is one of the most widely used applications on the Internet. Furthermore, the current volume of samples using this propagation vector include all the existing and still-spreading instances of malicious code which use mass-mailing spam as their propagation mechanism.

Regional Rank	Propagation Mechanism	Regional Percentage	Global Percentage
1	File transfer/email attachment	37%	32%
2	File sharing executables	27%	40%
3	File transfer/CIFS	26%	28%
4	File sharing/P2P	25%	19%
5	Remotely exploitable vulnerability	24%	17%
6	SQL	4%	3%
7	Back door/Kuang2	4%	3%
8	Back door/SubSeven	4%	3%
9	File transfer/MSN instant messenger	4%	1%
10	File transfer/HTTP/embedded URI/Yahoo! Messenger	2%	2%

Table 12. Top propagation vectors, EMEA
Source: Symantec Corporation

Executable files are the second ranked propagation vector in EMEA, with 27 percent of the volume. Commonly associated with file infector viruses, this vector ranked fifth in the first half of the year. It is worth noting that the proportion for EMEA is much lower than the 40 percent of total submission volume that was observed globally.

The third most commonly seen propagation vector in this period was Windows® file sharing, or CIFS. In the second half of 2007, 26 percent of samples originating in EMEA propagated over CIFS shares. This is close to the 28 percent observed globally. In the previous report, this vector ranked sixth, with 18 percent of the regional volume. The increase in rank for CIFS as a propagation vector in EMEA for the second half of 2007 may be because this vector is used by several instances of the top 10 malicious code samples observed this period, including Fujacks, Virut, Rahack, and Licum.

A vector to continue watching for in EMEA is IM. It is a successful propagation vector because there is more trust built into the social networks of IM systems than there is with email. Some of the samples that use local European languages have likely been successful for this reason. Two of the three top new families in EMEA this period propagate over IM networks. Another interesting trend is propagation through Web-applications and modification of Web pages. This class of malicious code is seen by Symantec as on the rise, and accurately capturing this trend may require definition of new propagation vectors in the future.

Malicious code that modifies Web pages

For the first time, in this volume of the *EMEA Internet Security Threat Report,* Symantec is examining malicious code samples that modify Web pages on a compromised computer. Only threats that modify pages in order to propagate or redirect users were examined. Those that simply deface the pages by adding text or simple images are not included in this metric.

In May 2007, a new attack kit called MPack was observed in the wild.[43] This kit compromised Web pages, typically through the insertion of iframes, to redirect users to an MPack server that attempted to exploit Web browser and plug-in vulnerabilities and install malicious code on computers.[44] This kit experienced great success because it took advantage of users visiting trusted legitimate Web pages that had been compromised. Since the Web browser is a primary gateway to the Internet, Web pages that users visit frequently—such as online forums and other Internet communities—are a valuable attack vector.

During this reporting period, five percent of malicious code samples within EMEA could modify Web pages (figure 4), the same proportion observed in the first half of 2007. Globally, seven percent of samples had the ability to modify Web pages this period, compared to three percent in the previous period. There are unique dynamics with this class of attacks: compromised Web sites often only attract users who can read the language of the site, putting constraints on and directing attacks in ways that may not be seen with other classes of malicious code, such as typical mass email propagation. This may explain the different proportions seen between the regional and global volume, especially when compared to the proportions seen in the previous period.

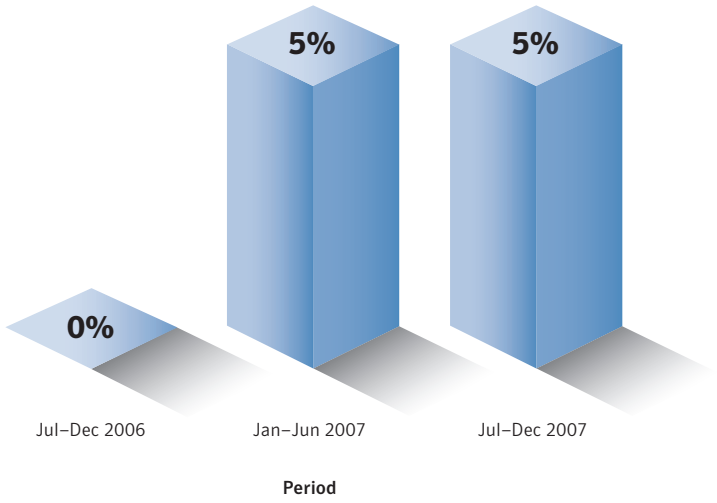

Figure 4. Malicious code that modifies Web pages, EMEA
Source: Symantec Corporation

[43] http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-052712-1531-99
[44] http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

One instance of malicious code designed to seek out and modify HTML, the Fujacks worm, was in the top 10 new malicious code samples in EMEA for this period, and was most commonly reported in the United Arab Emirates and Ethiopia. Like MPack, this worm adds an invisible iframe to HTML documents on the compromised host. It then redirects users' browsers to a malicious Web site, which could then exploit vulnerabilities in the users' Web browser to download and install further threats.

During this period, there was at least one major incident involving malicious code designed to modify Web pages. In August 2007, Italian police uncovered a large-scale phishing operation that had allegedly compromised over 10,000 Web sites, which were being used to launch phishing attacks and targeting users of the Italian post office and various financial institutions in Europe.[45] According to reports, once credentials were obtained, the group attempted to transfer funds to PostePay cards belonging to members of the group. The group allegedly used MPack or a variant to carry out these attacks.

In many cases, the Web pages modified by malicious code do not reside on Web servers. However, users who maintain their own Web sites often keep a copy of the site on their own computer. When they want to update their Web site, they will upload pages to their Web hosting providers. These updated pages could likely include the modifications made by the malicious code, which would be included in the upload. As a result, other users who trust the compromised user's site would be at risk.

Malicious code—protection and mitigation

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications—such as HTTP, FTP, SMTP, and DNS servers—and that are accessible through a firewall or placed in a DMZ. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of IPS technologies can prevent exploitation of browser and plug-in vulnerabilities through signatures and behaviour-based detection in addition to ASLR.

End users should employ defence-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

[45] http://www.itpro.co.uk/security/news/123003/italian-police-arrest-phishing-gang.html

Phishing Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organisation, often for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to commit fraudulent acts.

The data provided in this section is based on statistics derived from the Symantec Probe Network, a system of over two million decoy accounts in more than 30 countries that attracts email from around the world to gauge global spam and phishing activity. It encompasses more than 600 participating enterprises worldwide, attracting email that is representative of traffic that would be received by over 250 million mailboxes. The Probe Network consists of previously used email addresses as well as email accounts that have been generated solely to be used as probes.

This section of the Symantec *EMEA Internet Security Threat Report* will discuss the following phishing activity that Symantec detected in the EMEA region between July 1 and December 31, 2007:

- Top countries hosting phishing Web sites and top targets phished
- Phishing Web site top-level domains
- Phishing—protection and mitigation

Top countries hosting phishing Web sites and top targets phished

A phishing Web site is a site that is designed to mimic the legitimate Web site of the organisation whose brand is being spoofed, often an online bank or e-commerce retailer. In many cases, it is set up by the attacker to capture a victim's authentication information or other personal identification information, which can then be used in identity theft or other fraudulent activity.

This section of the Symantec *EMEA Internet Security Threat Report* will discuss the EMEA countries in which the most phishing Web sites were hosted, and the type of service offered by the organisations whose brands were most frequently spoofed. Readers should note that phishing Web sites differ from phishing hosts, which are computers that can host one or more phishing Web sites, and which are discussed in the "Malicious activity by country" metric in the "Attack Trends" section of this report.

The data discussed in this section is a snapshot in time and, therefore, does not have insight into changes in the locations of certain phishing Web sites throughout the period. It should also be noted that just because a phishing Web site is hosted in a certain country, it does not necessarily mean that the attacker is located in the same country.

During the last six months of 2007, Romania was home to the most phishing Web sites in EMEA (table 13) with 46 percent of the total. Globally, Romania ranked third for hosting phishing Web sites during this period, with five percent, behind only the United States and China.

Regional Rank	Global Rank	Country	Regional Percentage	Type of Organisation
1	3	Romania	46%	Social networking site
2	5	France	8%	Online auction site
3	6	Germany	8%	Online payment system
4	7	Italy	7%	Online auction site
5	9	Sweden	6%	Telecommunications site
6	10	Netherlands	6%	Social networking site
7	11	Russia	4%	Online auction site
8	13	United Kingdom	3%	Online payment system
9	14	Poland	2%	Social networking site
10	17	Spain	1%	Online auction site

Table 13. Top countries hosting phishing Web sites and top targets, EMEA
Source: Symantec Corporation

The presence of Romania in this position is somewhat surprising, as it ranked only sixteenth in EMEA and thirty-fifth worldwide for malicious activity during this period. However, for phishing hosts it ranked tenth in EMEA and fifteenth worldwide, which would indicate that phishing is the most common malicious activity originating in Romania. This is borne out by numerous reports that indicate that Romania has become a growing source of malicious activity, particularly online auction fraud.[46] There is a well-established tradition of computer skills in the country dating back to the early 1980s.[47] Combined with the slow economic growth in Romania since the fall of communism, this has led to an increase in on-line fraud.[48]

The most commonly spoofed Web site in Romania was a social networking site, which accounted for 98 percent of the top 10 brands phished by Web sites hosted in Romania. These sites are relatively easy to phish because they are generally trusted by users. As a result, phishing attacks spoofing them may have a good chance of success.[49] In fact, in five of the top 10 countries for hosting phishing Web sites globally during this reporting period, social networking sites were the most commonly spoofed sites.

Spoofed social networking pages can include links to malicious downloads that require users to enter confidential information, such as authentication information or credit card information, that can subsequently be used for fraudulent purposes. Further, in some cases, phishers may be able to upload content, such as Flash videos, onto a spoofed social networking page that will allow the attacker to hijack the page of anyone who visits the spoofed page.[50]

France ranked second for hosting phishing Web sites in EMEA this period, with eight percent. Worldwide, France ranked fifth, with one percent. France had the third highest amount of malicious activity in EMEA this period. France's ranking in several other malicious code categories could contribute to the high number of phishing Web sites hosted there. In EMEA this period, France had the fourth highest number of spam zombies, which are compromised computers used to relay spam messages, some of which could

[46] http://news.bbc.co.uk/2/hi/technology/3344721.stm
[47] http://news.bbc.co.uk/2/hi/technology/3344721.stm
[48] http://bucharest.usembassy.gov/US_Citizen_Services/Visiting_Living/Corruption.html
[49] http://www.symantec.com/enterprise/security_response/weblog/2006/09/contextaware_phishing_realized.html
[50] http://www.symantec.com/enterprise/security_response/weblog/2006/07/myspace_shockwave_flash_hack.html

include links to phishing Web sites. It had the fifth highest number of bot-infected computers in EMEA, which could contribute to the number of phishing Web sites because a computer that is compromised by a bot can be used to host phishing sites. France also had the third highest number of phishing hosts in EMEA during this period. Since phishing hosts can host one or more phishing Web sites, this would likely contribute to a high number of phishing Web sites.

In addition to these considerations, at the end of 2007, France had the third highest number of domain names in the EMEA region.[51] The higher number of domain names will not, in and of itself, contribute to a higher number of phishing Web sites, but it will likely indicate a higher probability of phishing Web sites, if only as a percentage of the higher number of domain names.

During this period, France had only the eighth highest number of Web-hosting companies in the world, despite the high number of domains, suggesting that these Web-hosting companies were relatively large. Large Web-hosting companies may be susceptible to hosting phishing Web sites because those sites may be able to exist for a long period in time in relative obscurity and undetected by the hosting provider.

The top target of phishing Web sites hosted in France was an online auction site. These sites are commonly targeted for fraudulent activity as they are a forum for the sale of goods and may, as a result, involve significant financial transactions. They can be used by fraudsters in a number of ways. A genuine user's online auction account could be hijacked by phishers who can then use it to post fraudulent listings for which an unsuspecting buyer pays money while receiving no goods in return. Another method would be to divert the legitimate user to a spoofed online auction page into which the target would be asked to enter credit card information, which could then be used for fraudulent financial gain.

Between July 1 and December 31, 2007, Germany ranked third for hosting phishing Web sites in EMEA, with eight percent, and sixth worldwide, with one percent. Germany ranks first in Web domains in EMEA by a wide margin.[52] This means that there is a significant chance that many of these domains were used as phishing Web sites. This is supported by the fact that the .de domain name, which is assigned to the country domain of Germany, was the second highest top level domain used by phishing Web sites in EMEA during this reporting period.

Germany also had the second most Web-hosting companies in the EMEA region, behind only the United Kingdom.[53] Web-hosting companies can be used to host phishing Web sites in two ways. First, they can employ the hosting company to host a Web site legitimately, but use that site for phishing. Second, they can compromise legitimate Web sites hosted by the company and use them for phishing purposes. A high number of Web hosting companies increases the number of potential hosts for phishers to use, legitimately or not, for phishing purposes.

The top target of phishing Web sites in Germany during this period was an online payment system. This is a secure third-party payment service that allows users to pay for on-line goods and services without entering their credit card or banking information into e-commerce Web sites that may not be secure. As part of this process, users' accounts contain their credit card information. Phishing attempts that spoof these Web pages will often attempt to fool the user into using his or her account information, which will allow phishers to access their credit card information or to use the victim's account to make purchases online.

[51] http://www.webhosting.info/domains/
[52] http://webhosting.info/domains/countrystats
[53] http://www.webhosting.info/webhosts/globalstats

Phishing Web site top-level domains

The domain name system was developed to translate the unique IP addresses assigned to computers on the Internet from complicated series of numbers into familiar words. IP addresses are translated into domain names by domain name servers. End users are thus able to navigate the Internet using names rather than IP addresses.

The highest level of domain names is the top-level domain (TLD). Examples include .com (which is generally used by businesses but available to anyone), .edu (which is used by organisations in the education sector), and .org (which is predominantly used by non-profit organisations).

Understanding the TLDs that are most commonly used in phishing Web sites may help end users, security administrators, and organisations to understand which TLDs may be most prone to hosting phishing Web sites, which could help alert them to potentially malicious sites. It may also help security analysts further identify which countries or sectors are hosting the most phishing Web sites. Readers should note that this is the first reporting period for which Symantec tracked this data; therefore, period-to-period comparisons are not possible.

In the second half of 2007, the most common TLD used by known phishing Web sites situated in the EMEA region was .com, which was used by 24 percent of the total (table 14). This is not surprising, as .com is the most common TLD on the Internet and is used by approximately 74 percent of all registered general top-level domain.[54] During this reporting period, it was used by 44 percent of phishing Web sites detected worldwide.

While .com was originally employed to designate a Web site that is used by a commercial organisation, it has expanded to include many different types of organisations, as well as individuals. It is an unrestricted TLD, meaning that anyone can register a domain name using it, thus making it easy for phishers to use. As it is the most commonly used TLD, and is thus familiar to users, .com may be inherently more trusted than other less widely employed TLDs, thereby making it more effective for phishing Web sites.

Rank	Top-level Domain	Regional Percentage	Global Percentage
1	.com	24%	44%
2	.de	9%	2%
3	.ru	7%	2%
4	.net	6%	6%
5	.fr	5%	1%
6	.cn	4%	23%
7	.es	4%	1%
8	.org	4%	3%
9	.tk	3%	1%
10	.pl	3%	1%

Table 14. Phishing Web sites by top-level domain, EMEA
Source: Symantec Corporation

[54] http://www.icannwiki.org/Domain_Statistics

The percentage of phishing Web sites using the .com TLD in EMEA is somewhat lower than the worldwide numbers, indicating that phishing Web sites using this TLD are less concentrated in EMEA than globally and, thus, are not targeting users in the EMEA region specifically. Furthermore, the proportion of phishing Web sites using this TLD in the EMEA region was significantly lower than those across the Internet as a whole. This may indicate that phishers in the EMEA region are using phishing sites that are hosted on local TLDs, such as those indicating specific countries. This suggests that phishing Web sites located in EMEA are likely targeting clients and customers of regional organisations, such as local financial organisations. Spoofing the brands of local organisations, and using local TLDs, would allow phishers to craft the phishing messages in the local language, thereby increasing the credibility of the fraudulent Web site and enhancing its chances of success.

The comparatively low number of .com TLDs in EMEA phishing Web sites may also be due to the distribution of TLDs across the Internet. By far the majority of domain names using .com are situated in the United States.[55] It is therefore logical that the number of phishing Web sites using this TDL is lower in EMEA than elsewhere.

During the last six months of 2007, .de was the second most common TLD used by phishing Web sites in the EMEA region, accounting for nine percent of the total. Only two percent of all registered Web sites globally use this TLD, making it the seventh most commonly used TLD. This would indicate that phishing Web sites using .de are concentrated in EMEA and, thus, are targeting users in the EMEA region specifically.

The .de domain name is assigned to Germany and this indicates that these phishing Web sites are located on address space registered in that country. However, readers should note that not all countries require a domain registrant to be situated in the country. As a result, there is not necessarily a correlation between the use of a TLD and the involvement of a national of that country being involved in that activity. The .de TLD is currently used by less than one percent of domain names across the Internet as a whole.[56] The number of phishing Web sites using this TLD is highly concentrated in the EMEA region and, thus, targeting users in the EMEA region, most likely those in Germany itself. During the current reporting period, Germany had the third highest number of phishing Web sites in EMEA, and in the first six months of the year it had the highest number. It is likely that many of these employed the .de TLD.

As of January 2008, Germany had the highest number of Web domains in the EMEA region and the second highest number in the world.[57] Germany also had the second highest number of Web-hosting companies in EMEA during this period.[58] The high number of phishing Web sites using the .de TLD is likely a reflection of Germany's high ranking in these two considerations. That having been said, the high number of phishing Web sites using the .de TLD does not necessarily mean that the phishers using these sites are located in Germany. Rather, it may be that phishers in indeterminate locations have compromised Web sites or ISPs located in Germany to host their phishing Web sites or are hosting their phishing Web sites on German domains.

[55] http://www.webhosting.info/registries/country_stats/US
[56] http://populicio.us/toptlds.html
[57] http://webhosting.info/domains/countrystats
[58] http://www.webhosting.info/webhosts/globalstats

The third most common 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 the country domain assigned to Russia. Only two percent of global phishing Web sites used this TLD. Furthermore, only about 0.5 percent of Internet-wide Web sites use .ru, 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 in the EMEA region, the fifth highest total. Many of these likely employed the .ru TLD, leading to its prominence in this category.

The disproportionately high number of phishing Web sites using .ru in the EMEA region is also likely due to the involvement of organised criminals conducting phishing activity based in Russia. According to some reports, Russian organisations may be responsible for up to 60 percent of phishing activity on the Internet.[59] Prominent amongst these is the Russia Business Network (RBN), which has been implicated in widespread malicious activity over the past two years.[60] The RBN reputedly specialises in the distribution of malicious code, hosting malicious Web sites, and other malicious activity, specifically the development and sale of the MPack toolkit. This organisation illustrates the professionalisation of malicious activities and the burgeoning underground economy that Symantec has discussed in previous volumes of the *Internet Security Threat Report*. RBN was reported to have dropped offline in November 2007.[61] As a result, it is likely that phishing Web sites using the .ru TLD will diminish over the foreseeable future.

Phishing—protection and mitigation

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA). Although this will likely remain the primary point of filtering for phishing, organisations can also use IP-based filtering upstream, as well as HTTP filtering.

DNS block lists also offer protection against potential phishing emails.[62] Organisations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.[63]

To protect against potential phishing activity, administrators should always follow Symantec best practices as outlined in Appendix A of this report. Symantec also recommends that organisations educate their end users about phishing.[64] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, and should provide a means to report suspected phishing sites.[65]

Organisations can also employ Web-server log monitoring to track if and when complete downloads of their Web sites, logos, and images are occurring. Such activity may indicate that someone is attempting to use the legitimate Web site to create an illegitimate Web site for phishing.

[59] http://www.smh.com.au/news/security/the-hunt-for-russias-web-crims/2007/12/12/1197135470386.html
[60] http://www.zdnet.com.au/news/security/soa/Infamous-porn-and-phishing-ISP-rolls-Bank-of-India/0,130061744,339281722,00.htm
[61] http://www.theregister.co.uk/2007/11/08/rbn_offline/
[62] A DNS block list (sometimes referred to as a black list) is simply a list of IP addresses that are known to send unwanted email traffic. It is used by email software to either allow or reject email coming from IP addresses on the list.
[63] Spoofing refers to instances where phishers forge the "From:" line of an email message using the domain of the entity they are targeting with the phishing attempt.
[64] For instance the United States Federal Trade Commission has published some basic guidelines on how to avoid phishing. They are available at: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
[65] A good resource for information on the latest phishing threats can be found at: http://www.antiphishing.org

Organisations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[66] So-called typo domains[67] and homographic domains[68] should also be monitored. This can be done with the help of companies that specialise in domain monitoring; some registrars also provide this service.

The use of antiphishing toolbars and components in Web browsers can also help protect users from phishing attacks. These measures notify the user if a Web page being visited does not appear to be legitimate. This way, even if a phishing email reaches a user's inbox, the user can still be alerted to the potential threat.

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

Users should review bank, credit card, and credit information frequently. This can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[69] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[66] "Cousin domains" refers to domain names that include some of the key words of an organisation's domain or brand name; for example, for the corporate domain "bigbank.com", cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.
[67] Typo domains are domain names that use common misspellings of a legitimate domain name, for example the domain "symatnec.com" would be a typo domain for "symantec.com".
[68] A homographic domain name uses numbers that look similar to letters in the domain name, for example the character for the number "1" can look like the letter "l".
[69] http://www.fbi.gov/majcases/fraud/internetschemes.htm

Spam Trends

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts. It could also cause a loss of service or degradation in the performance of network resources and email gateways. This section of the *EMEA Internet Security Threat Report* will discuss developments in spam activity in the EMEA region between July 1 and December 31, 2007.

The data used in this analysis is based on data returned from the Symantec Probe Network as well as data gathered from a statistical sampling of the Symantec Brightmail AntiSpam customer base. Specifically, statistics are gathered from enterprise customers' Symantec Brightmail AntiSpam servers that receive more than 1,000 email messages per day. This removes the smaller data samples (that is, smaller customers and test servers), thereby allowing for a more accurate representation of data.

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attacks. An attack can consist of one or more messages. The goal of the Probe Network is to simulate a wide variety of Internet email users, thereby attracting a stream of traffic that is representative of spam activity across the Internet as a whole. For this reason, it is continuously optimised in order to attract new varieties of spam attacks. This is accomplished through internal production changes that are made to the network, which thus affect the number of new spam attacks it receives as a whole.

The following metric will be discussed for this report period:

- Top countries of spam origin

Top countries of spam origin

The nature of spam makes it difficult to identify the location of people who are sending spam. Many spammers try to redirect attention away from their actual geographic location. In an attempt to bypass DNS block lists, they build coordinated networks of bot-infected computers, which allow them to send spam from sites that are distant from their physical location. Following this logic, the region from which the spam originates may not correspond with the region in which the spammers are located.

This discussion is based on data gathered by customer installations of Symantec Brightmail AntiSpam. This data includes the originating server's IP address, against which frequency statistics are summarised. Each IP address is mapped to a specific country and charted over time.

The top source of spam in EMEA this period was the United Kingdom, with 15 percent of the regional total (table 15).[70] This is the same percentage of EMEA-based spam that originated in the United Kingdom in the first half of 2007. The amount of spam originating in the United Kingdom is in close proportion to the overall amount of malicious activity that originated there during this reporting period, which was 11 percent.

[70] The previous *EMEA Internet Security Threat Report* listed this number as 25 percent; however, due to methodological changes over the past six months, figures for the previous reporting period have been revised.

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage
1	1	United Kingdom	15%	15%
2	2	Russia	12%	6%
3	5	Poland	10%	11%
4	6	Germany	10%	9%
5	9	Spain	7%	5%
6	3	Italy	6%	7%
7	8	France	6%	7%
8	7	Turkey	5%	2%
9	10	Netherlands	3%	3%
10	4	Israel	3%	3%

Table 15. Top countries of spam origin, EMEA
Source: Symantec Corporation

Spam can be sent by either using a compromised computer as a spam server itself, which is known as a spam zombie, or by using it to send mail through legitimate mail servers using the server itself or the computer user's email account. The United Kingdom was only the eighth ranked country for spam zombies in the EMEA region during this period, accounting for five percent of the total. As a result, it is likely that most of the spam originating in the United Kingdom is being sent by compromised computers and relayed through legitimate email servers.

The second highest volume of spam detected being sent from the EMEA region during this period originated in Russia, which accounted for 12 percent of the total. This is an increase over the first six months of 2007 when only six percent of EMEA spam originated there.

Symantec observed a 231 percent increase in the number of spam zombies detected in Russia during the current reporting period. Despite this rapid increase, only seven percent of EMEA spam zombies were located in Russia, making it the seventh ranked country in the region. Therefore, the number of spam zombies in Russia was low compared to the amount of spam originating in there. Russia was only ranked ninth for bot-infected computers in EMEA during this period, so it is unlikely that the high volumes of spam originating there were tied to bot-infected computers.

Given Russia's prominence in the "Phishing Web site by top-level domain" metric, it is likely that the high volume of spam originating there is related to other malicious activities. For instance, it is possible that this is due to the activity of the Russian Business Network (RBN), also discussed in the above mentioned metric. This group, which is referred to as both an ISP and an online service provider, likely used its own servers to launch high volumes of spam messages. Many of these would be malicious messages that would entice unknowing users to click on a malicious link that would take them to a Web site that could harvest confidential information to be used in phishing activity. As the group appears to have been shut down, or at least relocated, it is likely that spam activity originating in Russia will return to lower levels in ensuing reporting periods.

Poland had the third highest volume of spam in the EMEA region in the last six months of 2007, accounting for 10 percent of the region's total, down slightly from 11 percent in the first six months of the year. In the first six months of 2007, Poland had the third highest volume of spam in the EMEA region, accounting for eight percent of the region's total, both of which are very close to the current period's numbers. It was also the country of origin for eight percent of spam detected in EMEA in the last six months of 2006, so it appears that the percentage of spam originating in Poland is fairly stable.

Poland had the fifth highest number of spam zombies in the EMEA region during this period, with seven percent of the total. It also had the fourth highest number of bot-infected computers in the EMEA region during this period, with 10 percent of the total, which is proportionate to the amount of spam originating there. It is likely that these two factors were responsible for the volume of spam originating in Poland during this period.

Appendix A—Symantec Best Practices

Enterprise Best Practices

- Employ defence-in-depth strategies, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated antivirus, firewalls, intrusion detection, and intrusion protection systems on client systems.
- Turn off and remove services that are not needed.
- If malicious code or some other threat exploits one or more network services, disable or block access to those services until a patch is applied.
- Always keep patch levels up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
- Enforce an effective password policy.
- Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files.
- Isolate infected computers quickly to prevent the risk of further infection within the organisation. Perform a forensic analysis and restore the computers using trusted media.
- Train employees to not open attachments unless they are expected and come from a known and trusted source, and to not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- Ensure that emergency response procedures are in place. This includes having a backup-and-restore solution in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Educate management on security budgeting needs.
- Test security to ensure that adequate controls are in place.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software. Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organisation are deployed on desktop computers.

Consumer Best Practices

- Consumers should use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Consumers should ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Consumers should ensure that passwords are a mix of letters and numbers, and should change them often. Passwords should not consist of words from the dictionary.
- Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Consumers should keep virus definitions updated regularly. By deploying the latest virus definitions, consumers can protect their computers against the latest viruses known to be spreading in the wild.
- Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- Consumers should deploy an antiphishing solution. They should never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.
- Consumers can get involved in fighting cybercrime by tracking and reporting intruders. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's ISP or local police.
- Consumers should be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software. Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organisation are deployed on desktop computers.
- Some security risks can be installed after an end user has accepted the end-user license agreement (EULA), or as a consequence of that acceptance. Consumers should read EULAs carefully and understand all terms before agreeing to them.
- Consumers should be aware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. When users see ads in a program's user interface, they may be looking at a piece of spyware.

Appendix B—Attack Trends Methodology

Attack trends in this report are based on the analysis of data derived from the Symantec Global Intelligence Network, which includes the Symantec DeepSight Threat Management System, Symantec Managed Security Services, and the Symantec Honeypot Network. Symantec combines data derived from these sources for analysis.

Malicious activity by country

To determine the top countries for the "Malicious activity by country" metric, Symantec compiles geographical data on each type of malicious activity to be considered. This includes bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code infections, spam relay hosts, and Internet attacks. The proportion of each activity originating in each country is then determined. The mean of the percentages of each malicious activity that originates in each country is calculated. This average determines the proportion of overall malicious activity that originates from the country in question and is used to rank each country.

Top countries of attack origin

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

Denial of service attacks

Although there are numerous methods for carrying out DoS attacks, Symantec derives this metric by measuring DoS attacks that are carried out by flooding a target with SYN requests. These are often referred to as SYN flood attacks. This type of attack works by overwhelming a target with SYN requests and not completing the initial request, which thus prevents other valid requests from being processed.

In many cases, SYN requests with forged IP addresses are sent to a target, allowing a single attacking computer to initiate multiple connections, resulting in unsolicited traffic, known as backscatter, being sent to other computers on the Internet. This backscatter is used to derive the number of DoS attacks observed throughout the reporting period. Although the values Symantec derives from this metric will not identify all DoS attacks carried out, it will highlight DoS attack trends.

To determine the countries targeted by DoS attacks, Symantec cross-references the target IP addresses of every attack with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

Sectors targeted by DoS attacks were identified using the same methodology as targeted countries. However, in this case, attackers who were considered were those carrying out a set of DoS attacks that were detected by IDS and IPS software.

Bot-infected computers

Symantec identifies bot-infected computers based on coordinated scanning and attack behaviour that is observed in global network traffic. An active bot-infected computer is one that carries out at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall.

For an attacking computer to be considered to be participating in coordinated scanning and attacking, it must fit into that pattern to the exclusion of any other activity. This behavioural matching will not catch every bot-infected computer, and may identify other malicious code or individual attackers behaving in a coordinated way as a botnet. This behavioural matching will, however, identify many of the most coordinated and aggressive bot-infected computers. It will also give insight into the population trends of bot-infected computers, including those that are considered to be actively working in a well coordinated and aggressive fashion at some point in time during the reporting period.

Bot-infected computers by countries and cities

To determine the geolocation of bot-infected computers, Symantec cross-references the IP addresses of every identified bot-infected computer with several third-party subscription-based databases that link the geographic location of systems to IP addresses. While these databases are generally reliable, there is a small margin of error. Only cities that can be determined with a confidence rating of at least four out of five are included for consideration. The data produced is then used to determine the global distribution of bot-infected computers.

Appendix C—Malicious Code Trends Methodology

Malicious code trends are based on statistics from malicious code samples reported to Symantec for analysis. Symantec gathers data from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products in both consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. Observations in this section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from the two databases described below.

Infection database

To help detect and eradicate computer viruses, Symantec developed the Symantec AntiVirus Research Automation (SARA) technology. Symantec uses this technology to analyse, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec Antivirus customers.

On average, SARA receives hundreds of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. Symantec then analyses these suspect files, matching them with virus definitions. An analysis of this aggregate data set provides statistics on infection rates for different types of malicious code.

Malicious code database

In addition to infection data, Symantec Security Response analyses and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, a historical trend analysis was performed on this database to identify, assess, and discuss any possible trends, such as the use of different infection vectors and the frequency of various types of payloads.

In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the *Internet Security Threat Report* to the next.

Geographic location of malicious code instances

Several third-party subscription-based databases that link the geographic locations of systems to IP addresses are used along with proprietary Symantec technology to determine the location of computers reporting malicious code instances. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of malicious code instances.

Appendix D—Phishing Trends Methodology

Phishing attack trends in this report are based on the analysis of data derived from the Symantec Probe Network. Symantec Brightmail AntiSpam data is assessed to gauge the growth in phishing attempts as well as the percentage of Internet mail that is determined to be phishing attempts. Symantec Brightmail AntiSpam field data consists of statistics reported back from customer installations that provide feedback about the detection behaviours of antifraud filters as well as the overall volume of mail being processed.

It should be noted that different monitoring organisations use different methods to track phishing attempts. Some groups may identify and count unique phishing messages based solely on specific content items such as subject headers or URLs. These varied methods can often lead to differences in the number of phishing attempts reported by different organisations.

Top countries hosting phishing Web sites

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

Phishing Web site top-level domains

The data for this section is determined by deriving the top-level domains of each distinct phishing Web site URL. The resulting top-level domains are tabulated and compared proportionately.

Appendix E—Spam Trends Methodology

The Symantec Probe Network is a system of over two million decoy accounts in over 30 countries that attract email messages from around the world. It encompasses more than 600 participating enterprises and attracts email samples that are representative of traffic that would be received by over 250 million mailboxes. The Probe Network includes accounts in countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

Spam trends in this report are based on the analysis of data derived from both the Symantec Probe Network as well as Symantec Brightmail AntiSpam field data. Symantec Brightmail AntiSpam software reports statistics to the Brightmail Logistical Operations Center (BLOC) indicating messages processed, messages filtered, and filter-specific data.

Symantec has classified different filters so that spam statistics and phishing statistics can be determined separately. Symantec Brightmail AntiSpam field data includes data reported back from customer installations providing feedback from antispam filters as well as overall mail volume being processed.

Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not the network layer, where DNS block lists typically operate. This is because SMTP-layer spam filtering is more accurate than network-layer filtering and is able to block spam missed at the network layer. Network-layer filtering takes place before email reaches the enterprise mail server. As a result, data from the SMTP layer is a more accurate reflection of the impact of spam on the mail server itself.

Sample set normalization

Due to the numerous variables influencing a company's spam activity, Symantec focuses on identifying spam activity and growth projections with Symantec Brightmail AntiSpam field data from enterprise customer installations. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

Top countries spam origin

The data for this section is determined by calculating the frequency of originating server IP addresses in email messages that trigger antispam filters in the field. The IP addresses are mapped to their host country of origin and the data is summarised by country based on monthly totals. The percentage of spam per country is calculated from the total spam detected in the field.

It should be noted that the location of the computer from which spam is detected being sent is not necessarily the location of the spammer. Spammers can build networks of compromised computers globally and thereby use computers that are geographically separate from their location.

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

04/08 13585531-2