SYMANTEC ENTERPRISE SECURITY

symantec™

Confidence in a connected world.

Symantec EMEA Internet Security Threat Report

Trends for January–June 07

Volume XII, Published September 2007

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Senior Editor
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Marc Fossi
Analyst
Symantec Security Response

Joseph Blackbird
Analyst
Symantec Security Response

David McKinney
Analyst
Symantec Security Response

Ronald Bowes
Analyst
Symantec Security Response

Nicholas Sullivan
Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Ollie Whitehouse
Security Architect—Advanced Threat Research
Symantec Security Response

Zulfikar Ramzan
Analyst—Advanced Threat Research
Symantec Security Response

Jim Hoagland
Principal Software Engineer
Symantec Security Response

Chris Wee
Manager, Development
Symantec Security Response

Contributors

David Cowings
Sr. Manager of Operations
Symantec Business Intelligence

Dylan Morss
Manager
Symantec Business Intelligence

Shravan Shashikant
Principal Business Intelligence Analyst
Symantec Business Intelligence

Volume XII, Published September 2007

Symantec EMEA Internet Security Threat Report

Contents

EMEA Internet Security Threat Report Overview 4

Attack Trends 6

Malicious Code Trends 19

Phishing Trends 30

Spam Trends 34

Appendix A—Symantec Best Practices 39

Appendix B—Attack Trends Methodology 41

Appendix C—Malicious Code Trends Methodology 43

Appendix D—Phishing Trends Methodology 44

Appendix E—Spam Trends Methodology 45

EMEA Internet Security Threat Report 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 January 1 to June 30, 2007.

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

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

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

The Symantec *EMEA Internet Security Threat Report* is grounded principally on the expert analysis of data provided by all of these sources. By publishing the analysis of Internet security activity in this report, Symantec hopes to provide enterprises and consumers in the EMEA region with the information they need to help effectively secure their systems now and in the future.

Executive Summary

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

Attack Trends Highlights

- The United States was the country of origin of the most attacks against EMEA-based computers, accounting for 35 percent of attacks detected there.
- The United Kingdom was the EMEA country most frequently targeted by denial of service (DoS) attacks, accounting for 46 percent of attacks in the region during this period.

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

- Symantec observed an average of 18,616 active bot-infected computers per day in EMEA, 35 percent of the worldwide daily average of 52,771.
- Germany had the most bot-infected computers in EMEA, accounting for 23 percent of the total, up from 16 percent in the second half of 2006.
- Madrid, Spain had the most bot-infected computers of any EMEA city, as it did in the second half of 2006.
- Germany accounted for 19 percent of malicious activity in EMEA, the most of any country and the same percentage as in the second half of 2006.
- Israel had the most malicious activity per Internet user in EMEA, followed by Poland and Spain.

Malicious Code Highlights

- Trojans were the most common malicious code type in EMEA, accounting for 68 percent of potential malicious code infections in the region.
- The United Kingdom was the top EMEA country for potential infections of back doors and Trojans.
- India was the top EMEA country for potential virus and worm infections.
- The Netsky.P mass-mailing worm was the most frequently reported malicious code sample for the EMEA region.
- The most prevalent new malicious code family reported in the EMEA region was the Metajuan Trojan.
- Threats to confidential information made up 61 percent of potential infections by the top 50 malicious code samples in the EMEA region, less than the worldwide percentage of 65 percent.
- Threats that allow remote access, such as back doors, made up 87 percent of potential infections by confidential information threats.
- Email attachments were the most common propagation mechanism used in EMEA; they were used by 49 percent of propagating malicious code this period.

Phishing Trends Highlights

- Germany was home to the most phishing Web sites in EMEA, with 22 percent of the region’s total.
- Karlsruhe, Germany was the city with the most phishing Web sites in the EMEA region, as it was in the second half of 2006.

Spam Trends Highlights

- Measured by country, the highest source of spam in EMEA originated in the United Kingdom, which accounted for 12 percent of the regional total.
- Germany had more spam zombies than any other EMEA country, with 17 percent of the regional total.
- In the EMEA region, spam made up 67 percent of all monitored email traffic during this reporting period.
- Of the top 20 email-producing countries in the EMEA region, Poland had the highest percentage of email that was spam, with 86 percent.

Attack Trends

This section of the *EMEA Internet Security Threat Report* will provide an analysis of attack activity that Symantec observed in the EMEA region between January 1 and June 30, 2007. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall.

The Symantec Global Intelligence Network monitors attack activity across the entire Internet. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data. Furthermore, Symantec uses proprietary technologies to monitor bot command-and-control servers across the Internet. These resources give Symantec an unparalleled ability to identify, investigate, and respond to emerging threats. This discussion will be based on data provided by all of these sources.

This section of the *EMEA Internet Security Threat Report* will discuss:

- Top countries targeted by denial of service attacks
- Active bot-infected computers
- Bot-infected computers by country
- Bot-infected computers by city
- Malicious activity by country
- Malicious activity by country per Internet user

Over the first six months of 2007, the United States was the country of origin of the most attacks against EMEA-based computers, accounting for 35 percent of all attacks detected by sensors in the region (table 1). This is slightly higher than the worldwide attacks from the United States, which was 25 percent. This indicates that attacks originating in the United States were likely not targeting the EMEA region in particular.

The high rate of attacks is likely due to the United States having the highest number of broadband connections in the world, with 20 percent of all connections.[2] The United States also hosts 18 percent of all worldwide Internet connections.[3] As a result, computers there are more likely to become infected with worm or bot software, which are likely to launch subsequent attacks.

[2] http://www.point-topic.com
[3] http://www.internetworldstats.com

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Attacks	Previous Percentage of Regional Attacks	Percentage of Worldwide Attacks
1	1	United States	35%	33%	25%
2	3	United Kingdom	15%	13%	5%
3	2	China	14%	19%	13%
4	5	Norway	13%	3%	<1%
5	4	Germany	5%	4%	8%
6	6	Italy	3%	3%	3%
7	7	France	2%	3%	6%
8	10	Canada	1%	1%	4%
9	9	Spain	1%	1%	5%
10	11	Poland	1%	1%	2%

Table 1. Top countries of origin of attacks targeting the EMEA region
Source: Symantec Corporation

The United Kingdom was the country of origin of the second highest percentage of attacks detected by sensors in the EMEA region during this period, accounting for 15 percent of the total. This is a small increase from 13 percent during the previous reporting period, when it ranked third place. The regional percentage is significantly larger than the five percent of worldwide attacks that originated in the United Kingdom, which indicates that attack activity originating in the United Kingdom was targeting the EMEA region in particular.

In the previous version of the *EMEA Internet Security Threat Report*, Symantec has noted the tendency for attacks to target computers situated in the region from which they originate.[4] This is likely because organizations have a higher profile in their local area; therefore, they make more attractive targets for attackers from the region. It may also be related to factors such as shared language and living in a proximate time zone.

Further, the United Kingdom has a well established Internet infrastructure. It has the second highest number of broadband connections in EMEA, with 14 percent,[5] and the third highest number of Internet users, with nine percent.[6]

China was the source country of the third highest number of attacks detected by sensors deployed in the EMEA region during the first six months of 2007, accounting for 14 percent of the total. Previously, China was ranked second place with 19 percent of attacks against EMEA. China was the originating country for 13 percent of attack activity, so attacks originating there do not appear to be targeting EMEA in particular.

China’s position here is likely driven by the number of broadband connections in the country. China has the second highest number of broadband connections in the world, with 20 percent of all connections.[7] The high percentage of attacks originating China may also be linked to its high percentage of bots, as 29 percent of bot-infected computers worldwide are located there. Bot-infected computers are often used by attackers to launch attack activity. However, as these computers are often controlled by attackers in other countries, the fact that the attacks originate in China does not necessarily mean that the attackers are located there.

[4] Symantec *EMEA Internet Security Threat Report* (March 2007):
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf : p. 8

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

[6] http://www.internetworldstats.com

[7] http://www.point-topic.com. Although the U.S. and China have the same rounded percentages (20 percent), the United States actually has 20.4 percent of worldwide broadband connections while China has 19.7 percent.

Top countries targeted by denial of service attacks

This metric will assess the geographic location of targets of denial of service (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 organizations in affected countries to take the necessary steps to protect against or minimize the effects of DoS attacks.

DoS attacks are a major threat to Internet-dependent organizations. A successful DoS attack can render Web sites or other network services inaccessible to customers and employees. This could result in the disruption of organizational communications, a significant loss of revenue, and/or damage to the organization's reputation. Furthermore, as Symantec discussed in a previous *Internet Security Threat Report*, criminals have been known to use DoS attacks in extortion schemes.[8]

Over the first six months of 2007, the United Kingdom was the EMEA country most frequently targeted by DoS attacks, accounting for 46 percent of attacks in the region during this period (table 2). This is a decrease from 49 percent during the second half of 2006, when it was also the top-ranked country in EMEA.

In the previous volume of the *EMEA Internet Security Threat Report*, Symantec speculated that some DoS attacks against the United Kingdom may have been conducted to protest a legislation outlawing DoS attacks there.[9] It speculated that groups of so-called hacktivists, attackers that make politically motivated attacks, performed DoS attacks against the United Kingdom in an attempt to protest this new legislation. Another example of this type of Internet-based activism seen during this reporting period took place in Estonia, as is discussed later in this section. The drop in DoS attacks targeting the United Kingdom may indicate that the attackers either feel that they have accomplished their objective or that the targets of the attack have been able to protect themselves against this type of attack.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Attacks	Previous Percentage of Regional Attacks	Percentage of Worldwide Attacks
1	1	United Kingdom	46%	49%	12%
2	2	Germany	10%	11%	2%
3	4	Netherlands	7%	6%	2%
4	3	France	7%	8%	2%
5	5	Italy	4%	4%	1%
6	6	Spain	3%	4%	1%
7	7	Sweden	2%	2%	1%
8	11	Russia	2%	1%	1%
9	9	Ireland	2%	1%	0%
10	14	Poland	2%	1%	0%

Table 2. Top countries targeted by DoS attacks, EMEA region
Source: Symantec Corporation

[8] Symantec *Internet Security Threat Report*, Volume VIII (September 2005): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf : p. 11 and 30

[9] http://news.com.com/2100-7348_3-6134472.html

Germany was targeted by 10 percent of attacks in EMEA during this period, the second highest number in the region. This is a slight decrease from 11 percent in the second half of 2006, when it was also the second ranked country. DoS attacks are generally conducted against Web sites, rather than other organizational resources or individual users. As Germany has the highest number of Web sites in the EMEA region,[10] it is logical that it should be targeted by a high number of DoS attacks.

The Netherlands was targeted by the third highest number of DoS attacks in the EMEA region, accounting for seven percent of attacks during this period. This is up slightly from six percent in the previous period, when the Netherlands was targeted by the fourth highest number of DoS attacks. Although the percentage of attacks against the Netherlands has remained largely unchanged since last period, the percentage of attacks targeting France has fallen, which has resulted in a proportionate increase in the Netherlands.

As was mentioned earlier in this discussion, Estonia appeared to be the target of politically motivated DoS attacks in the first half of 2007. It was targeted by a number of attacks when an unpopular decision made by the Estonian government led to widespread protests both in the physical world and online.[11] The attacks were made against a variety of targets, including government, bank, and newspaper Web sites, although some reports stated that a number of people may have been unable to connect to any Web sites at all.[12] This type of event illustrates the potential impact that DoS attacks can have.

Organizations should ensure that a documented procedure exists for responding to DoS events. One of the best ways to mitigate a DoS attack is to filter upstream of the target. For most organizations, this filtering will involve working in conjunction with their Internet service provider (ISP). Symantec also recommends that organizations perform egress filtering on all outbound traffic. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Active bot-infected computers

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

Bots allow for a wide range of functionality, and most can be updated to assume new functionality by downloading new code and features. They can be used by external attackers to perform DoS attacks against an organization's Web site. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious business and legal consequences.

Bots can also be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft. They can also be used to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications.

[10] Based on the number of unique domain names registered: http://www.webhosting.info/domains/country_stats/
[11] http://www.symantec.com/enterprise/security_response/weblog/2007/06/politics_on_the_wire.html
[12] http://www.nytimes.com/2007/05/19/world/europe/19russia.html?ex=1337227200&en=4817e43658c91382&ei=5088

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. Between January 1 and June 30, 2007, Symantec observed an average of 18,616 active distinct bot-infected computers per day in the EMEA region, down from the 21,707 seen during the previous reporting period (figure 1). The worldwide average for active bots detected on any given day was 52,771, so the EMEA region accounted for about 35 percent of active bots on an average day.

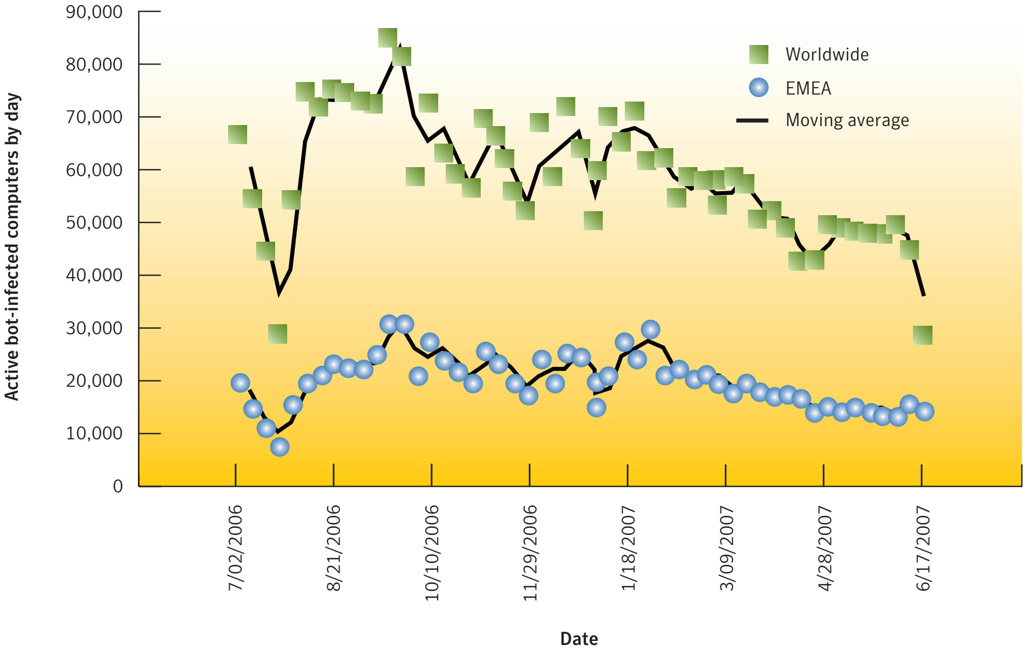

Figure 1. Active bot-infected computers per day, EMEA region
Source: Symantec Corporation

As is evident in figure 1, the number of bot-infected computers by day in EMEA has remained consistent with the worldwide number the past 12 months. This likely indicates that no recent bot infection has specifically propagated in the EMEA region.

One notable exception to this occurred during April of this year, when the worldwide number dropped without a corresponding decrease in bot-infections in the EMEA region. This may be related to the Operation Bot Roast project of the Federal Bureau of Investigation (FBI),[13] which is an ongoing initiative dedicated to detecting, disrupting, and dismantling bot networks in the United States. The FBI announced that it had detected over a million bot-infected computers. Since this project is based in the United States, it is possible that it has had a more noticeable effect on the proportion of bot-infected computers in the United States than in other regions. This could cause a drop in bot-infected computers in the North American region, and therefore worldwide, without a corresponding drop in EMEA.

[13] http://www.fbi.gov/page2/june07/botnet061307.htm

A distinct bot-infected computer is a computer that has been determined to be active at any one point in time (or more) during the period. In the first half of 2007, Symantec identified 2,084,189 distinct bot-infected computers that were considered active in EMEA. This is 41 percent of the 5,029,309 active distinct bots detected worldwide during this period. It is also 10 percent lower than the 2,312,267 active bot-infected computers that Symantec identified in the EMEA region during the second half of 2006.

The decrease in bots observed over the past six months is likely due to a change in bot attack methods. As has been discussed in previous volumes of the Symantec *Internet Security Threat Report*, the exploitation of network-based vulnerabilities to spread bots is likely being slowly abandoned for methods that are more likely to succeed, such as bots that send a mass mailing of themselves.[14] The introduction of default firewalls in popular operating systems such as Microsoft® Windows® XP, as well as a generally increasing awareness of computer security issues among organizations and computer users has made these forms of attack less likely to succeed. As a result, their use has declined.

Furthermore, as an extension of computer security awareness, law enforcement initiatives targeting bot networks may also be having some effect, as is illustrated by the FBI's Operation Bot Roast discussed previously. Since American-based bot networks are likely to make use of bot-infected computers worldwide, Initiatives such as these may result in a reduction in bots in the EMEA region, albeit less than the reduction of bots worldwide. Additionally, as bot networks are dismantled, less bot activity will be observed. Also, bot network owners may also become more careful with their bot networks to avoid detection. This may make them more difficult or impossible to detect.

Symantec also tracks the number of bot command-and-control servers in each region. Bot command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. During the first six months of 2007, 25 percent of worldwide command-and-control servers were located in the EMEA region, compared to the 41 percent of active bots that are located in the region. In the previous reporting period, 27 percent of command-and-control servers were located in the EMEA region, as were 39 percent of active bot-infected computers.

The discrepancy between command-and-control servers and bot-infected computers is important, as it indicates that bots in EMEA are likely being controlled by command-and-control servers that are situated outside the region. This means that some of the attack activity originating in the region is not necessarily being initiated by computers located in the EMEA region. This supports the speculation in the "Top countries of attack origin" section in this report that the prevalence of attack activity originating in the United Kingdom and other EMEA-based countries may be partly due to attack activity controlled by attackers in countries outside the EMEA region.

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[15] 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. 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.

[14] For instance, please see Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 30

[15] Defense-in-depth strategies emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. They should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Bot-infected computers by country

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers both worldwide and across the EMEA region. In order to do this, Symantec calculates the number of computers worldwide that are known to be infected with bots, and assesses which countries within the EMEA region are home to high percentages of these computers. The identification of bot-infected computers is important, as a high percentage of infected machines could mean a greater potential for bot-related attacks. It may also indicate the level of patching and security awareness in the region.

Between January 1 and June 30, 2007, Germany had the highest number of bot-infected computers in the EMEA region, accounting for 23 percent of the total (table 3). This is an increase from 16 percent in the second half of 2006, when Germany was ranked second in EMEA for bot-infected computers. The increase in Germany during this period may be due to a decrease in France, where the percentage of bot-infected computers fell from 16 percent to 11 percent in the first half of 2007.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Bots	Previous Percentage of Regional Bots	Percentage of Worldwide Bots	Average Lifespan (days)	Command-and-Control
1	2	Germany	23%	16%	9%	1	25%
2	3	Spain	15%	14%	6%	2	2%
3	1	France	11%	16%	5%	2	5%
4	6	Italy	9%	6%	4%	3	6%
5	4	United Kingdom	9%	11%	4%	3	11%
6	7	Israel	6%	5%	3%	3	2%
7	5	Poland	6%	8%	3%	3	2%
8	9	Portugal	2%	2%	1%	4	0%
9	8	Turkey	2%	3%	1%	2	5%
10	10	India	2%	2%	1%	4	3%

Table 3. Bot-infected computers by country, EMEA region
Source: Symantec Corporation

Germany’s rank is likely related to its well established, but still expanding, broadband infrastructure. Germany is home to more broadband connections than any other country in EMEA, with 16 percent of the region.[16] It also added more broadband connections between May 2006 and May 2007 than any other country in EMEA.[17]

In Volume XI 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.[18] Frequently, rapidly expanding ISPs will focus their resources on meeting growing broadband demand at the expense of implementing adequate security measures, such as port blocking and ingress and egress filtering. As a result, they may have security infrastructures and practices that are insufficient for their needs. Furthermore, it is also likely that home users and system administrators in countries with a rapidly expanding Internet infrastructure are also struggling to adapt their security practices and policies to deal with broadband Internet.

[16] http://www.point-topic.com
[17] http://www.point-topic.com
[18] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 36

Germany had the shortest lifespan of bot-infected computers of the top ten bot-infected countries in EMEA, with an average of only a single day, a quarter of the worldwide average lifespan of four days. This means that there is very little delay between a German computer becoming infected and then being detected and subsequently disinfected. This likely indicates that German users and ISPs respond to bot infections much more quickly than average users. As such, it is likely that the high proportion of bot infections in Germany are linked more to the sheer number of users than other factors, such as insufficient security measures or awareness.

Spain accounted for 15 percent of bot-infected computers in the EMEA region in the first half of 2007, the second highest total in the region. This is an increase from 14 percent and third place in the second half of 2006. Spain's position in second place is surprising, given that it has only the fifth highest number of broadband connections in the region. This activity may be a result of broadband growth, as Spain had the fifth highest number of broadband connections added between May 2006 and May 2007. As has been stated previously, an ISP focusing on expansion may do so at the expense of security controls. For example, a large Spanish ISP, Telefónica de España, became a stakeholder in one of the largest Italian ISPs, Telecom Italia, in April of 2007.[19]

In Volume XI of the Symantec *EMEA Internet Security Threat Report*, Symantec speculated that the increase in Spain's bot infections was a result of its broadband growth.[20] The report stated that Spain would likely follow the same trend as the United Kingdom; that is, the percentage of bot-infected computers in Spain would increase then, as broadband in Spain became more established, the proportion of infections would plateau and may eventually fall. This occurs because users and ISPs become more experienced and aware of security issues, and begin to put sufficient security controls into place. The percentage of bot-infected computers in Spain appears to have leveled off. As such, Symantec expects the percentage to remain steady or to fall during the upcoming period.

France had the third highest number of bot-infected computers in the EMEA region, with 11 percent of the total, down from 16 percent and first place in the previous period. The decrease in bot-infected computers in France mirrors a decrease in spam zombies there. France now accounts for nine percent of spam zombies in EMEA, down from 14 percent during the previous reporting period. At least one large ISP in France, Orange, has taken steps to block Internet attacks, particularly by providing antivirus and firewall protection,[21] which may account for the falling number of bot infections there.

In the second half of 2005, the United Kingdom had the most bot-infected computers in the region.[22] Since that period, the percentage of bot-infected computers has steadily fallen, with the United Kingdom currently ranking fifth place in EMEA with only nine percent of bot-infected computers in the region. This fall is likely due to the amount of publicity and media attention in the United Kingdom due to the number of bot infections.[23] It is likely that some ISPs in the UK have taken precautions to help prevent bot infections.[24]

[19] http://point-topic.com/content/operatorSource/profiles2/telefonica-de-espana.htm
[20] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf : p. 13
[21] http://assistance.orange.fr/1308.php?dub=2
[22] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 38
[23] http://news.zdnet.co.uk/security/0,1000000189,39192117,00.htm
[24] Some ISPs have recently blocked access to known bot servers: http://seclists.org/fulldisclosure/2007/Jul/0388.html

This decrease may also be driven by changes in bot-distribution methods. Bot-infections often propagate by launching attacks at randomly selected IP addresses on the Internet. These attacks are typically noisy and aggressive, making them easy to detect as bots. Since this method of bot propagation can be easily detected, ISPs and law enforcement can determine that they are occurring much more easily. As a result, attackers may attempt to spread bots more quietly, not attacking aggressively. In that case, they may only be detected as attacks, not as bots, which may allow them to appear to be Internet background noise caused by either worms, misconfigured systems, or ordinary traffic that is detected as malicious.[25]

Many smaller countries, such as Israel, Italy, and Spain, have shown increases in bot-infected computers over the previous reporting period. For instance, Israel reached six percent from five percent, and Italy is up to nine percent from six percent. These countries have not traditionally been targeted by attacks and malicious code, likely because targeting attacking larger countries with more established Internet populations—such as the United Kingdom, France, and Germany—could potentially affect more users. However, the increase seen in these countries may indicate a shift in the focus of attackers, who may be making efforts to target other countries.

Bot-infected computers by city

Madrid, Spain was the EMEA city with the highest number of bot-infected computers during the first six months of 2007 (table 4), which is unchanged from the previous reporting period. Spain had the second most bot-infected computers in the EMEA region during this period, with 15 percent of all bots in the region. The one country with a higher rating, Germany, does not have any cities in the top ten for bot-infections. This is likely due to the fact that bots in Germany are spread out over many different cities, each of which contribute to its overall ranking, while most bots in Spain appear to be concentrated in Madrid.

Regional Rank	Previous Regional Rank	City	Country
1	1	Madrid	Spain
2	9	Petah Tiqwa	Israel
3	7	Rome	Italy
4	5	Milan	Italy
5	2	London	United Kingdom
6	3	Paris	France
7	4	Ankara	Turkey
8	8	Lisbon	Portugal
9	6	Warsaw	Poland
10	12	Haifa	Israel

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

[25] For more information on Internet background noise, see http://www.switch.ch/security/services/IBN/

Petah Tiqwa, Israel had the second highest number of bot-infected computers in the EMEA region, a considerable jump from the previous rank of ninth. This increase may be related to the privatization of a large Israeli ISP. When companies become privatized, their budgets and operating practices may be changed, and focus may be diverted away from activities that don't generate direct revenue streams, such as security. If less attention is focused on security, it is possible that bot-infected computers can operate more easily in Israeli cities.

Furthermore, computer security law enforcement resources in Israel may be insufficient to meet current demands. This prompted a reorganization in 2005 that was intended to create a single information technology authority in the country to deal with computer and Internet crime.[26] As this authority becomes established and takes the necessary measures to prevent bot network activity, bot infections may drop to a level more appropriate for Israel's population of Internet users.

Rome, Italy had the third highest number of bot-infected computers among EMEA cities during this period, a significant increase from the previous period, when it was ranked seventh. Milan, Italy also increased in rank during this period, to fourth from fifth place. As discussed in the "Bot-infected computers by country" section of this report, large Spanish ISP, Telefónica de España, became a stakeholder in one of the largest Italian ISPs, Telecom Italia, in April 2007. The recent rise in bot network activity in Italian cities may be related to the rise in bot network activity in Spanish cities, since the two ISPs may implement similar security controls. Additionally, the expansion may have come at the expense of security infrastructure.

To prevent against bot infection, Symantec recommends that end users practice defense-in-depth strategies, including the deployment of antivirus, firewall, and intrusion detection solutions. Security administrators should also ensure that ingress and egress filtering is in place to block known bot-network traffic and that antivirus definitions are updated regularly.

Malicious activity by country

This metric will assess the countries in which the highest amount of malicious activity takes place or originates. To determine this, Symantec has compiled geographical data on numerous malicious activities that are based in EMEA countries, namely: bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code reports, 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 of 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.

In the first six months of 2007, Germany accounted for 19 percent of malicious activity in the EMEA region, the most of any country (table 5). Germany's rank and percentage of malicious activity have both remained unchanged since the last six months of 2006. Germany's overall high rankings are likely due to its developed broadband infrastructure. Germany has 16 percent of all broadband connections in EMEA, which is more than any other EMEA-based country, thus exposing it to more attacks of opportunity than other countries in the region.

[26] http://www.crime-research.org/news/30.09.2005/1522

During this period, Germany passed strict laws against computer crimes.[27] These laws make it illegal to penetrate a computer system for any reason, including legitimate ones, which makes security research more difficult. For example, performing an authorized penetration test on a company's network may now be considered illegal in Germany. As such, computer systems may be less protected than systems in other countries.[28] Since this law is new, it will likely have a more noticeable effect over the upcoming reporting period.

Germany ranked first for all of the considered activities with the exception of malicious code, for which it ranked third. These rankings likely indicate high levels of bot activity. Some bots can be used to relay spam,[29] and bot-infected computers frequently launch attacks in an attempt to infect more systems.

Overall Rank	Previous Rank	Country	Overall Proportion	Previous Overall Proportion	Malicious Code Rank	Spam Zombies Rank	Command-and-Control Server Rank	Phishing Web sites	Bot Rank	Attack Rank
1	1	Germany	19%	19%	3	1	1	1	1	1
2	3	United Kingdom	11%	10%	1	10	2	2	5	3
3	2	France	9%	11%	5	4	7	5	3	2
4	5	Italy	8%	8%	2	3	3	7	4	5
5	4	Spain	8%	8%	6	6	13	8	2	4
6	6	Poland	5%	5%	9	2	11	6	7	6
7	12	India	4%	2%	4	7	10	14	10	14
8	7	Netherlands	4%	4%	7	17	6	3	12	8
9	8	Turkey	3%	3%	12	5	5	20	9	7
10	10	Russia	3%	3%	25	9	9	4	11	15

Table 5. Malicious activity by country, EMEA region
Source: Symantec Corporation

The United Kingdom had the second highest percentage of malicious activity in the EMEA region during this six-month reporting period, accounting for 11 percent of the regional total. This was a small increase over 10 percent and third place during the last six months of 2006. The United Kingdom ranked first place for malicious code, second for phishing Web sites and command-and-control servers, and third or lower for every other activity.

The numbers of bots and spam zombies detected in the United Kingdom were low this period and have been consistently falling over the previous two periods (the United Kingdom accounted for nine percent of bots detected in EMEA this period, 11 percent in the previous period, and 22 percent in the period before that). This indicates that efforts are likely being made to clean up bot networks and bot network activity there. At least one major broadband provider in the United Kingdom, BT, offers a low-cost package that includes antivirus and firewall software.[30] This type of package may encourage more users to run antivirus software, helping to clean up bot infections.

In the first six months of 2007, France was the third ranked EMEA country for malicious activity, accounting for nine percent of the regional total. This is a small drop from 11 percent and second place in the previous reporting period. France's ranking in the various categories varied a great deal, from being the second highest source of attacks to the seventh highest location of command-and-control servers. France also had a high percentage of bot-infected computers, ranking third place in EMEA.

[27] http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=3194
[28] http://www.infoworld.com/article/07/08/13/German-antihacker-law_1.html
[29] http://news.zdnet.co.uk/security/0,1000000189,39167561,00.htm
[30] http://www.btnetprotect.bt.com/

While France ranked highly for both bot-infected computers and attacks, it has dropped in both since the previous reporting period, after a sharp increase in the period before that. France is a country that has had expanding broadband infrastructure and, in recent periods, has been a target of bot infections. This fall likely indicates that security controls and education have caught up to the broadband growth and penetration. As discussed in the “Bot-infected computers by country” section of this report, users who obtain a new broadband connection may not understand or implement proper Internet security controls, and ISPs that are focusing on expanding may do so at the expense of providing security controls.

Although the United Kingdom and France have switched positions since the previous reporting period, the percentages and, for the most part, positions of the top few countries by malicious activity have remained nearly constant. This supports an assertion made in the “Malicious activity by country” section of the main *Internet Security Threat Report*, which stated that, once malicious activity becomes entrenched within a country, it tends to be difficult to displace unless new security measures are put in place.

Malicious activity by country per Internet user

Having evaluated the top countries in EMEA by malicious activity, Symantec also evaluated the top 15 of these countries according to the number of Internet users located there. This measure is intended to remove the bias of countries with a large population of Internet users from the consideration of the “Malicious activity by country” metric.

In order to determine this, Symantec divided the amount of malicious activity originating in each of the top 15 countries in the EMEA region by the number of Internet users who are located in that country. The proportion assigned to each country in this discussion thus equates to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country. The proportion of malicious activity that would be carried out by each person is the proportion assigned to each country in the discussion below.

During the first six months of 2007, Israel was the most highly ranked country for malicious activity per Internet user. If one person from each of the top 15 countries in EMEA were assessed as a representation of their country’s Internet users, the average user in Israel would carry out 19 percent of the group’s malicious activity (table 6). The ranking has remained unchanged since the previous period.

The prominence of Israel in malicious activity per Internet user is likely influenced by the average hours spent online per user. Israel had the highest hours spent online per unique user in EMEA.[31] Computers that are online more often will allow for more opportunities for attackers to compromise them. It is also possible that the computer security infrastructure implemented by ISPs in Israel is not equipped to handle the load placed upon it.

Furthermore, as was discussed in the “Bot-infected computers by city” section of this report, enforcement efforts in Israel may be insufficient to meet current demands. This prompted a reorganization in 2005 that created a single information technology authority in the country to deal with computer and Internet crime.[32] A regulatory body that is relatively new may not be able to deal with activities such as bot networks as easily. As this authority becomes established and takes the necessary measures to prevent bot network activity, bot infections may drop to a level more appropriate for Israel’s population of Internet users.

[31] http://www.websiteoptimization.com/bw/0703
[32] http://www.crime-research.org/news/30.09.2005/1522

Regional Rank	Previous Regional Rank	Country	Malicious Activity by Internet User
1	1	Israel	19%
2	2	Poland	11%
3	4	Spain	9%
4	8	Germany	8%
5	7	France	7%
6	10	Netherlands	6%
7	5	Switzerland	6%
8	12	United Kingdom	5%
9	9	Belgium	5%
10	11	Italy	5%

Table 6. Malicious activity by country per Internet user
Source: Symantec Corporation

Poland accounted for 11 percent of malicious activity per Internet user, the second highest percentage in the region. Poland's position has also remained constant since the previous reporting period. Poland's rank is largely influenced by high numbers of bot-infected computers as well as a high number of spam zombies, relative to the population. The percentage of bots in Poland has decreased during this period while the number of spam zombies has increased. This might be a sign that spam zombies are able to survive more successfully than bots that are attacking. This could be an indication that little or no spam filtering is done by Polish networks or ISPs.

Spain ranked third, accounting for nine percent of malicious activity per Internet user. Spain's position has increased to third from fourth, filling in Sweden's place; Sweden dropped from 3rd to 12th.

Sweden's previous position was largely related to the number of bot command-and-control servers located there. Sweden now hosts about five percent of command-and-control servers in EMEA, down from 12 percent during the previous reporting period. This may be a sign that bot owners are consolidating their bots, keeping more bots on fewer servers. This is indicative of a broader trend towards the consolidation of bot networks that was discussed in the previous volume of the *Internet Security Threat Report*.[33] Additionally, because it's possible to host a command-and-control server in any country, bot owners using Swedish servers may have moved their bots elsewhere. This may be a sign that police or ISPs have taken additional measures against bots, or are taking enough measures to scare bot owners into keeping them elsewhere.

[33] The Symantec *Internet Security Threat Report*, Volume XI (March 2006):
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 17

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. This discussion is based on malicious code samples causing potential infections reported to Symantec for analysis from the EMEA region between January 1 and June 30, 2007.

The "Malicious Code Trends" section will discuss:

- Malicious code types
- Top country of malicious code infection by type
- Top ten malicious code samples
- Top three new malicious code families
- Threats to confidential information
- Propagation mechanisms

This discussion will include any prevention and mitigation measures that might be relevant to the particular threats being discussed. However, 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 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. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to detect anomalous activity.

End users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. 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.

Malicious code types

During the first six months of 2007, Trojans accounted for 68 percent of the potential malicious code infections in the EMEA region (figure 2). During the same period, they made up 73 percent of the volume of potential malicious code infections worldwide.[34]

[34] It should be noted that several malicious code samples reported in this period are categorized under more than one type, as a result, cumulative percentages included in this discussion may exceed 100 percent.

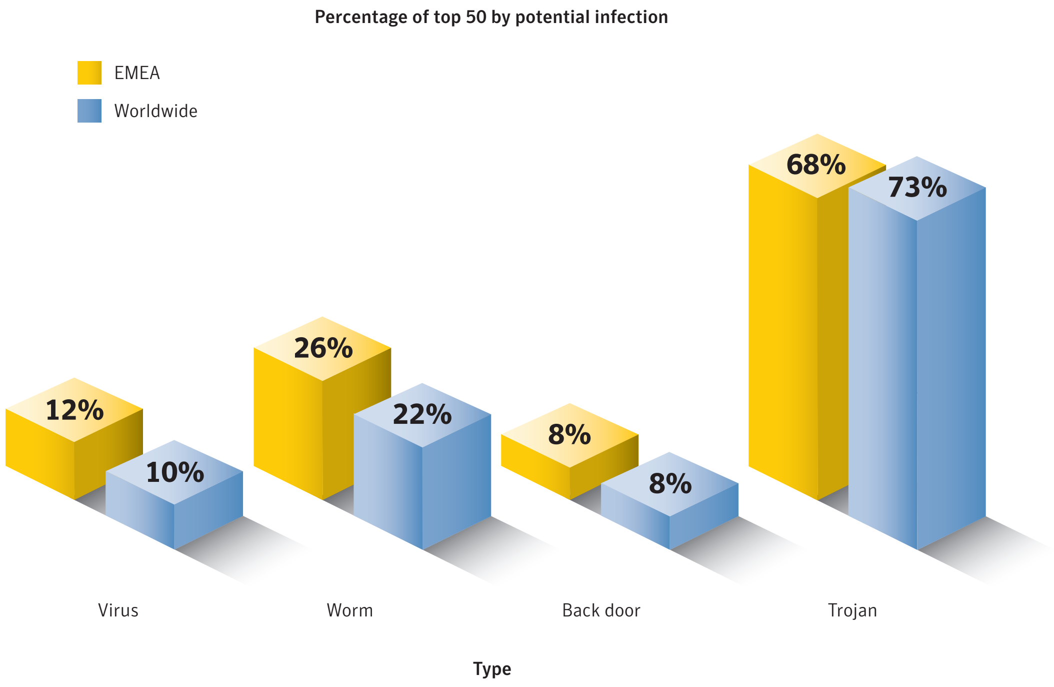

Figure 2. Malicious code types by potential infection
Source: Symantec Corporation

As will be discussed in the “Top ten malicious code samples” section below, three of the top five malicious code samples responsible for potential infections in the region were Trojans. Also, two of the top three new malicious code families in the EMEA region this period—Metajuan and Peacomm—were Trojans.

Trojans are likely gaining prominence because they generate a low volume of traffic compared to network and mass-mailing worms. As a result, they are less likely to draw attention than threats that generate high volumes of email messages or network traffic. The longer a threat remains unnoticed and active on a computer the greater an opportunity it will have to gather more confidential information or cause more damage.

Trojans can expose confidential information, and can be used to install other malicious programs. Furthermore, they can often be used to download subsequent malicious code modules that can be used in subsequent attack activity. These Trojans are referred to as “staged downloaders” and are becoming increasingly common. Staged downloaders are small, specialized 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.

To protect against Trojans, users should avoid executing software that is downloaded from the Internet unless it has been scanned for viruses. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

In the first half of 2007, worms made up 26 percent of the volume of malicious code reports in the EMEA region and 22 percent of the volume worldwide. Many established ISPs in Western Europe are likely implementing a degree of port blocking to prevent the propagation of network worms and email attachment scanning to protect against mass-mailing worms. However, in countries with relatively new ISPs or where demand is extremely high, these measures are most likely not yet in place.

The percentages of viruses and back doors in the EMEA region were in line with worldwide percentages this period, at eight percent both worldwide and in EMEA. Many of the viruses and back doors in the top 50 malicious code causing potential infections were present in both EMEA and worldwide. Since viruses only require a user to execute an infected file to spread, they are not dependent on languages, as is the case with many mass-mailing worms. Similarly, back doors are not dependent upon the language of the victim.

Top country of malicious code infection by type

For the first time, in this edition of the *EMEA Internet Security Threat Report*, Symantec is examining the top countries reporting potential malicious code infections as well as the types of malicious code that are causing potential infections in each country. Because of the different propagation mechanisms used by different malicious code types, and the different effects that each type may have, the geographic distribution of malicious code can indicate where network administrators in different regions can best increase the focus of their security efforts.

The United Kingdom was the top country for potential infections of back doors and Trojans in the first half of 2007 (tables 7 and 8). The top three countries for back doors and Trojans were rounded out by Italy and Germany. This may indicate that ISPs in these countries have begun implementing port blocking and more aggressive email gateway filtering for executable files to reduce mass-mailing and network worms. As a result, attackers targeting users in these countries will likely begin shifting their efforts towards more effective attacks, such as Trojans that are installed when a user visits a Web site exploiting a browser vulnerability. Many of these Trojans will, in turn, download back door server programs onto the compromised computer.

Rank	Top Country
1	United Kingdom
2	Italy
3	Germany

Table 7. Top three countries for back doors, EMEA
Source: Symantec Corporation

Rank	Top Country
1	United Kingdom
2	Italy
3	Germany

Table 8. Top three countries for Trojans, EMEA
Source: Symantec Corporation

India was the EMEA country that reported the highest number of potential infections of both viruses and worms (tables 9 and 10). India is currently experiencing a rapid growth in broadband Internet users.[35] It is likely that this means a number of new users have not adjusted to the always-on nature of broadband Internet connections and the increased security vigilance they require, particularly to protect them from network worms. The growth may also indicate that local ISPs are concentrating their efforts on providing new users with service rather than on security matters such as monitoring worm activity on their networks and blocking ports used by many network worms.

Rank	Top Country
1	India
2	United Kingdom
3	Egypt

Table 9. Top three countries for viruses, EMEA
Source: Symantec Corporation

The high number of viruses causing potential infections in India can also be attributed to broadband growth. If the demand for new broadband connections is higher than the ability of ISPs to fulfill them, some users may share their connections through a router or wireless access point with neighbors awaiting service. If these users share files and folders, this can provide an ideal environment for viruses to propagate. For example, the Sality.U virus was one of the top malicious code samples in the EMEA region this period and caused more potential infections in India than any other country in the region. This virus is able to infect executable files it locates on network shares as well as on local computers.

Rank	Top Country
1	India
2	United Kingdom
3	Spain

Table 10. Top three countries for worms, EMEA
Source: Symantec Corporation

Top ten malicious code samples

The top reported malicious code sample for the EMEA region was the Netsky.P[36] mass-mailing worm (table 11). It was also the second most common malicious code sample in the second half of 2006. This worm was mainly reported to have caused potential infections in Spain and Italy; however it was reported almost four times more in Spain than Italy.

This worm propagates through email and peer-to-peer (P2P) file-sharing networks; however, P2P file sharing has been outlawed in Spain since 2006.[37] This means it is likely that most, if not all, Spanish users affected by Netsky.P receive it through email. This may indicate that Spanish ISPs are not performing adequate email gateway antivirus scanning or that users are susceptible to the social engineering techniques used by the worm's email messages.

[35] http://www.isp-planet.com/cplanet/tech/2007/prime_letter_070628_india_russia.html
[36] http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99
[37] http://www.tmcnet.com/usubmit/2006/06/27/1696993.htm

Regional Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact
1	Netsky.P	Worm, Virus	Spain	Italy	SMTP, P2P	Keystroke logger targets www.e-gold.com
2	Vundo	Trojan	United Kingdom	Netherlands	N/A	Displays advertisements, downloads and installs additional threats
3	Zlob	Trojan	United Kingdom	Germany	N/A	Downloads and installs additional threats
4	Skintrim	Trojan	France	Spain	N/A	Displays advertisements, downloads and installs additional threats
5	Rontokbro	Worm	India	U.A.E.	SMTP	Performs denial of service attacks
6	Sality.U	Virus	India	U.A.E.	CIFS	Injects itself into all processes, consuming system resources
7	Rahack.W	Worm	Germany	Norway	CIFS	Modifies HTML files
8	Alcra.F	Worm	United Kingdom	Netherlands	P2P	Installs Spybot
9	Ecup	Worm	Spain	Italy	P2P	Displays a message
10	Mixor.Q	Worm	Germany	United Kingdom	SMTP	Installs Peacomm

Table 11. Top ten malicious code samples
Source: Symantec Corporation

The Vundo,[38] Zlob,[39] and Skintrim[40] Trojans were the second, third, and fourth most frequently reported malicious code samples in the EMEA region, respectively, in the first half of 2007. These Trojans all download and install additional threats onto the compromised computer, while Vundo and Skintrim also display advertisements.

These staged downloaders are capable of downloading and installing other malicious code onto a compromised computer.[41] They allow an attacker to change the downloadable component to any type of threat that suits his or her objectives. As the attacker's needs change, he or she can change any components that are downloaded by the initial Trojan.[42] The adware components of Vundo and Skintrim also likely provide revenue to the authors of these threats.

These three Trojans were mainly seen in western European countries in the EMEA region. This indicates that they may have been installed through Web sites that are frequently visited by users in these countries that were compromised by attackers. Attackers may also place links to Web sites that install these threats on Web forums frequented by users in these countries. This was observed in Italy during this period when several Web sites were compromised by the MPack kit.[43] It is likely that more Trojans installed by exploiting Web browser vulnerabilities will be observed as ISPs in these countries implement more aggressive email attachment scanning, which will force attackers to find new methods to compromise users.

[38] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[39] http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[40] http://www.symantec.com/security_response/writeup.jsp?docid=2006-121317-1003-99
[41] Staged downloaders, sometimes called modular malicious code, are threats that download and install other malicious code onto a compromised computer.
[42] For an in-depth discussion of staged downloaders, see the "Staged downloaders" section in volume XII of the Symantec *Internet Security Threat Report*.
[43] MPack was one of the notable security threats that emerged in the first half of 2007. It is a commercially available black market attack toolkit. It can launch exploits for browser and client-side vulnerabilities against users who visit a malicious or compromised Web site. For more information on MPack activity in Italy, please see: http://www.symantec.com/enterprise/security_response/weblog/2007/06/italy_under_attack_mpack_gang.html

Some worms use region-specific subject lines and text in their email messages. For example, the Rontokbro worm was the fifth most commonly reported malicious code sample in EMEA during the first six months of 2007.[44] It generated email messages that were composed in Indonesian. This worm was seen in India more than any other country. Similarly, the Sober.AA[45] mass-mailing worm used both German and English for its email messages. It was responsible for a large number of potential infections in EMEA.

Top three new malicious code families

The most prevalent new malicious code family reported in the EMEA region during the first six months of 2007 was the Metajuan Trojan (table 12).[46] Metajuan was also the third most frequently reported new malicious code family worldwide this period. This Trojan may be installed by other malicious code samples or installed by Web pages that are designed to exploit Internet Explorer vulnerabilities. This means that a computer will be compromised by visiting a malicious Web site rather than receiving the Trojan through email.

Trojans that are installed by malicious Web sites are more difficult to detect than those that propagate through email messages. This represents a trend in which attackers are relying upon users to retrieve threats instead of sending the threat to potential victims. Once installed, the Trojan contacts a remote Web site and can download and execute other malicious files on the compromised computer. Metajuan may also display advertisements when the user visits certain Web pages.

Regional Rank	Sample	Type	Propagation Vectors	Impact	Top Reporting Country
1	Metajuan	Trojan	N/A	Downloads other threats and displays ads	United Kingdom
2	Peacomm	Trojan	Spam/ Mixor.Q	Creates an encrypted peer-to-peer network and downloads other threats	United Kingdom
3	Kakavex	Virus	File Sharing	Steals credit card information	United Kingdom

Table 12. Top three new malicious code families
Source: Symantec Corporation

In the first half of 2007, the second most widely reported new malicious code family in the EMEA region was the Peacomm Trojan,[47] also known as the Storm Trojan. This Trojan was spammed in high volumes by the Mixor.Q worm,[48] which prompted Symantec to classify it as a Category 3 threat in January 2007.[49] When Peacomm installs itself on a computer, it attempts to hide itself using rootkit techniques.[50] It also contains a list of other compromised computers that it uses to build an encrypted network of peers, similar to a bot network, although it uses the Overnet peer-to-peer protocol rather than Internet Relay Chat (IRC) in order to make the network more resilient since there is not a single point of failure.[51]

Peacomm listens for commands passed through its peer-to-peer network and downloads and installs other files, such as the Mespam[52] and Abwiz.F Trojans.[53] This can be of particular concern, since a Trojan like Abwiz.F can send confidential information to the remote attacker and relay spam.

[44] http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99
[45] http://www.symantec.com/security_response/writeup.jsp?docid=2007-043010-5416-99&tabid=1
[46] http://www.symantec.com/security_response/writeup.jsp?docid=2007-030112-0714-99
[47] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
[48] http://www.symantec.com/security_response/writeup.jsp?docid=2006-122917-0740-99
[49] A Category 3 threat is a malicious code sample that is considered a moderate threat. It is either currently spreading among computer users but reasonably harmless and easy to contain or has not been released into the wild but is potentially dangerous and difficult to contain.
[50] Rootkit techniques are used by malicious code to hide their presence on a compromised computer.
[51] Overnet is a decentralized peer-to-peer file-sharing protocol. It was taken down due to legal action in September 2006, but due to its decentralized nature, clients are still able to function.
[52] http://www.symantec.com/security_response/writeup.jsp?docid=2007-020915-2914-99
[53] http://www.symantec.com/security_response/writeup.jsp?docid=2006-032311-1146-99

Kakavex was the third most common new malicious code family in the EMEA region during the first six months of 2007.[54] This virus is notable because it may represent the beginning of an interesting trend. Traditionally, most viruses simply infected executable files and may have contained some form of damaging payload. However, in addition to infecting files, the Kakavex virus also attempts to steal credit card information. The virus monitors Internet usage on the infected computer and, under certain circumstances, may display a dialogue box prompting the user for their credit card information. The information is then sent to a remote Web site.

This virus shows that identity thieves appear to be expanding into new territory to steal personal information. In the past they mainly used back doors and Trojans to steal this kind of information; however Kakavex indicates that they are now using viruses to do the same thing, thereby expanding the number of tools available to them for this objective.

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, and/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—this can also severely undermine customer confidence as well as violate local laws.[55] Sensitive corporate information could also be leaked from compromised computers, including financial details, business plans, and proprietary technologies.

In the first six months of 2007, threats to confidential information made up 61 percent of potential infections by the top 50 malicious code samples in the EMEA region. This is somewhat less than the worldwide percentage of 65 percent.

In the EMEA region, threats that allow remote access, such as back doors, made up 87 percent of potential infections by confidential information threats, slightly less than the 88 percent that was reported worldwide during this period (figure 3). Remote access threats tend to be favored by attackers since they are able to perform almost any action on the compromised computer.

[54] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011014-1759-99
[55] Many countries have implemented their own laws in this regard, such as the UK Data Protection Act, which can be found at http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

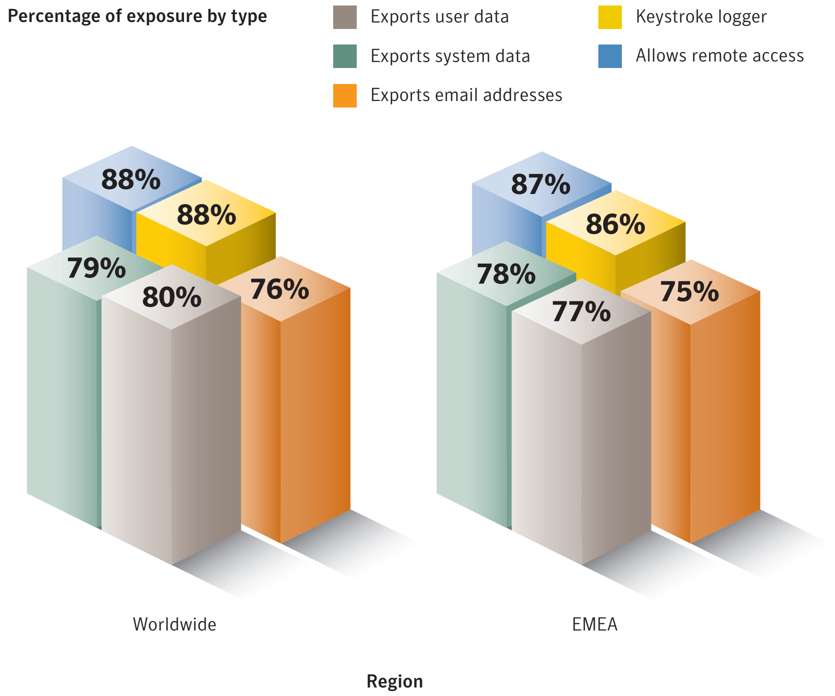

Figure 3. Threats to confidential information by type
Source: Symantec Corporation

Threats that could be used to export user data accounted for 77 percent of potential infections by confidential-information threats in the EMEA region during this reporting period. Across the Internet as a whole, these threats made up 80 percent of potential infections by threats to confidential information during this period.

Seventy eight percent of confidential-information threats in the EMEA region during the first six months of 2007 could be used to export system data, compared to 79 percent of the Internet-wide confidential-information threats. These forms of data leakage can enable an attacker to steal a user’s identity or launch further attacks. If the attacker has access to the user’s personal and system data, he or she can use this to craft a targeted social engineering attack that is highly tailored to that particular user.

Threats that had a keystroke-logging component made up 86 percent of confidential information threats in the EMEA region by potential infection during this six-month period. This is slightly lower than the 88 percent globally. A keystroke logger will record keystrokes on the compromised computer and, in most cases, email the log to the attacker or upload it to a Web site that is under the attacker’s control. This makes it easier for an attacker to gather confidential information from a large number of compromised computers with minimal effort.

Threats that could be used to export email addresses accounted for 75 percent of confidential information threats in the EMEA region, compared to 76 percent worldwide. This form of information harvesting is often used to compile lists of valid email addresses, which are subsequently sold to spammers.

Overall, the percentage of threats to confidential information in the top 50 malicious code samples in the EMEA region is very close to the worldwide percentage. This shows that attackers in EMEA are not using confidential information threats significantly more or less than across the Internet as a whole.

One threat to personal information in EMEA that wasn't commonly seen worldwide was the Bifrose back door.[56] This threat exports documents and system data, sending them to a preconfigured server. Bifrose is a back door program that originated in Sweden. As Symantec has discussed in previous *Internet Security Threat Reports*, attackers are more likely to target their own region than others. This is true for a variety of reasons, including the fact that organizations in the same region likely have a higher profile to local attackers. It may also be related to having a shared language.

Rustock.B[57] was another confidential information threat that was more commonly seen in the EMEA region than worldwide. Once a user is infected with this Trojan, it uses advanced rootkit techniques to hide itself.[58] It then uses the infected computer as a platform to send "pump and dump" stock spam email messages.

Rustock.B is believed to have originated in Russia, so its higher position in EMEA rankings may be explained the same way as Bifrose. Trojans that spread manually will have higher infection rates locally.

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 Simple Mail Transfer Protocol (SMTP), Common Internet File System (CIFS),[59] peer-to-peer services (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 by 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 reported to Symantec 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.

Due to some methodological changes that Symantec made for this reporting period, this volume of the *Internet Security Threat Report* is able to examine propagation mechanisms with increased specificity. For example, where possible, the specific peer-to-peer protocols employed as propagation mechanisms have been identified. This will allow administrators to look at more specific port blocking and protocol filtering based upon the specific propagation mechanisms being discussed. It is also important to note that due to this change, any comparisons to previous reporting periods would not be valid; therefore, they have not been presented here.

Email attachments were used by 49 percent of the propagating malicious code samples detected in the EMEA region during this period, making it the most common propagation mechanism in the region (table 13). It also accounted for 46 percent of the volume of the propagating samples worldwide. Propagation through email attachments is thus very common in both EMEA and worldwide. This is not surprising, as email is one of the most widely employed applications on the Internet and is used by both corporate and home users.

[56] http://www.symantec.com/security_response/writeup.jsp?docid=2004-101214-5358-99
[57] http://www.symantec.com/security_response/writeup.jsp?docid=2006-070513-1305-99
[58] http://www.symantec.com/enterprise/security_response/weblog/2006/06/raising_the_bar_rustocka_advan.html
[59] Common Internet File Sharing (CIFS) is a protocol that defines a standard for remote file access. CIFS allows applications to open and share files across the Internet.

Regional Rank	Propagation Mechanism	Regional Percentage of Threats	Worldwide Percentage of Threats
1	File Transfer/Email Attachment	49%	46%
2	File Sharing/Peer-to-Peer	25%	22%
3	Remotely Exploitable Vulnerability	21%	18%
4	File Sharing/Peer-to-Peer/Kazaa	21%	18%
5	File Sharing/Executables	20%	22%
6	File Transfer/CIFS	18%	24%
7	File Sharing/Peer-to-Peer/Morpheus	17%	15%
8	File Sharing/Peer-to-Peer/eDonkey	17%	15%
9	Back door/Kuang2	3%	3%
10	Back door/SubSeven	3%	3%

Table 13. Propagation mechanisms
Source: Symantec Corporation

Propagation through email attachments accounts for a slightly higher percentage of propagating malicious code in EMEA than it does worldwide. This may be caused by threats targeted specifically towards this region, such as the Sober.AA[60] mass-mailing worm. Sober.AA is present in the top 50 malicious code samples in EMEA, but not worldwide. Emails from Sober.AA are sent in English and German.[61] This has proven an effective propagation technique, particularly as Germany has one of the highest populations of Internet users in EMEA. By tailoring the email messages to specific regions, especially to regions with high populations or to regions where mass-mailing worms are less common, a malicious code author can cause more infections than one who composes emails exclusively in English.

To limit the propagation of these threats, administrators should ensure that all email attachments are scanned at the gateway. Additionally, all executable files originating from external sources, such as email attachments or downloaded from Web sites should be treated as suspicious. All executable files should be checked by antivirus scanners using the most current definitions.

The peer-to-peer propagation vector was used by 25 percent of malicious code threats in the EMEA region to propagate in the first half of 2007, three percent more than the Internet-wide total. The most common P2P protocols used to propagate were Kazaa, at 21 percent, Morpheus, at 17 percent, and eDonkey, also at 17 percent. The higher ranking of P2P propagation in EMEA than worldwide is mostly due to two pieces of malicious code: the Ecup worm[62] and the Fontra virus.[63]

Ecup propagates by copying itself to folders of various file-sharing programs, on both English and Spanish versions of Windows, under a variety of filenames. Because it uses file and folder paths used to install Spanish versions of software in addition to those used in English software, Ecup, like Sober.AA, takes advantage of multiple languages to spread more easily on non-English systems. Because it uses both English and Spanish paths, this worm can be spread by English and Spanish users, thereby increasing the number of potential infections.

[60] http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-043010-5416-99
[61] http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-043010-5416-99
[62] http://www.symantec.com/security_response/writeup.jsp?docid=2006-053111-0818-99
[63] http://www.symantec.com/security_response/writeup.jsp?docid=2006-051116-5811-99

Fontra propagates by infecting files that are already shared by various file-sharing programs. By infecting the files a user already has, Fontra will likely be less auspicious to the eventual targets that download the infected files. Many users' files are likely language-specific. For example, software and movies are typically tailored to a language. As such, this type of virus will initially be limited to infecting people who are downloading programs in that language. For example, a French user will typically download French programs, since that's their native language. Since the majority of Fontra's infections were in EMEA, it is likely that it originated in an EMEA country.

Malicious code that propagates by remotely exploitable vulnerabilities made up 21 percent of malicious code that propagated in the EMEA region in the first half of 2007. By comparison, remotely exploitable vulnerabilities were used by 18 percent of worldwide reports of malicious code that propagates.

Malicious code that spreads through this mechanism will exploit vulnerabilities in remotely accessible services and applications, such as a Web browser, to spread to new computers. The exploitation of remote vulnerabilities was used by two of the top 50 malicious code samples detected in EMEA, the Licum worm[64] and the Spybot worm.[65]

Users and administrators can protect against malicious code that propagates by exploiting vulnerabilities by using a firewall to block incoming connections on any ports that don't require external access. Additionally, the potential for infection by this type of attack can be reduced by keeping software up-to-date or by using an IPS system to block improperly formed traffic at the network boundary.

Propagation by CIFS was used by 18 percent of malicious code in EMEA that propagates, significantly lower than 24 percent of malicious code worldwide. The majority of infections by CIFS occurred in the Asia-Pacific/Japan (APJ) region during this period, inflating the worldwide number significantly. For more discussion on propagation over CIFS in APJ, please see the "Propagation mechanisms" discussion in the *APJ Internet Security Threat Report*.

[64] http://www.symantec.com/security_response/writeup.jsp?docid=2005-071316-2523-99
[65] http://www.symantec.com/security_response/writeup.jsp?docid=2003-053013-5943-99

Phishing Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, 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. This section of the Symantec *EMEA Internet Security Threat Report* will discuss phishing activity that Symantec detected in the EMEA region between January 1 and June 30, 2007.

The data provided in this section is based on statistics derived from the Symantec Probe Network, which consists of over two million decoy email accounts that attract email messages from 20 different countries around the world. The main purpose of the network is to attract spam, phishing, viruses, and other email-borne threats. It encompasses more than 600 participating enterprises around the world, 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 *EMEA Internet Security Threat Report* will discuss:

- Top countries hosting phishing Web sites
- Top cities hosting phishing Web sites
- Phishing—prevention and mitigation

Top countries hosting phishing Web sites

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

This section of the Symantec *EMEA Internet Security Threat Report* will discuss the top countries and cities in which phishing sites are hosted. This data is a snapshot in time and, therefore, does not have insight into changes in the locations of certain phishing sites throughout the period. It should also be noted that because a phishing Web site is hosted in a certain country, this does not mean that the attacker is located in the same country. However, it is likely that a phishing site will be located in the same country as the intended victims of the attack.

During the first six months of 2007, Germany was home to the highest percentage of phishing Web sites in EMEA (table 14) with 22 percent of the region's total. It was the second highest country in the world for phishing Web sites after the United States. The proportion of phishing sites hosted in Germany has declined since the last six months of 2006 when 32 percent of phishing Web sites in the region were located there. This may indicate a shift towards the use of phishing Trojans in Germany.[66] These Trojans are already widely used in Brazil as evidenced by the Bancos[67] and Banpaes[68] information-stealing Trojans. These Trojans steal users' online banking information by presenting fake login pages when the users navigate to their bank's Web site, so there are not any phishing Web sites associated with them.

[66] http://www.bsi.de/english/publications/securitysituation/Lagebericht_2007_englisch.pdf
[67] http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99
[68] http://www.symantec.com/security_response/writeup.jsp?docid=2003-101416-4837-99

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage
1	1	Germany	22%	32%	6%	11%
2	2	United Kingdom	9%	9%	3%	3%
3	4	Netherlands	9%	5%	2%	2%
4	5	Russia	8%	5%	2%	2%
5	3	France	8%	8%	2%	3%
6	8	Poland	4%	3%	1%	1%
7	7	Italy	4%	4%	1%	1%
8	9	Spain	4%	3%	1%	1%
9	13	Czech Republic	3%	2%	1%	1%
10	6	Denmark	3%	4%	1%	1%

Table 14. Top countries hosting phishing Web sites
Source: Symantec Corporation

The United Kingdom had the second highest number of phishing Web sites in the EMEA region in this reporting period. The proportion of phishing sites hosted in the United Kingdom has remained steady since last reporting period. The United Kingdom is an affluent country with a large Internet population and many small Web-hosting companies. Both of these factors make the country a good platform for hosting phishing Web sites.

Between January 1 and June 30, 2007, the Netherlands had the third highest number of phishing Web sites in the EMEA region, with nine percent of the total. This is a significant increase from the five percent of phishing sites hosted there in the previous period. The Netherlands was not in the top ten countries in EMEA for bot-infected computers during this period, suggesting that most of the phishing sites are hosted through Web-hosting companies.

There are several major ISPs in the Netherlands that allow the hosting of Web sites. There are also over a thousand Web-hosting companies in the Netherlands that could be used to illicitly host phishing Web sites.[69] If a phishing Web site is hosted on a large provider, it may take days for the provider to discover the illegal site and shut the site down.

Top cities hosting phishing Web sites

Karlsruhe, Germany was the city with the most phishing Web sites in the EMEA region in the first six months of 2007 (table 15). This is unchanged from last period. Karlsruhe is referred to as the “Internet capital of Germany,”[70] as there are a number of Internet companies located there, and it is home to some of the largest Web-hosting providers in Germany.[71] As Germany hosted the highest number of phishing Web sites in the region during this reporting period, it is logical that Karlsruhe—and the various Internet providers in the city—should host a significant number of them.

[69] http://www.webhosting.info/webhosts/globalstats/
[70] http://www.technologieregion-karlsruhe.de/WirtschaftsRegion/kommunikation.en
[71] http://www.webhosting.info/webhosts/tophosts/Country/DE

Regional Rank	Previous Regional Rank	City	Country
1	1	Karlsruhe	Germany
2	4	Moscow	Russia
3	3	London	United Kingdom
4	2	Paris	France
5	7	Amsterdam	Netherlands
6	13	Bucharest	Romania
7	5	Munich	Germany
8	12	Copenhagen	Denmark
9	19	Prague	Czech Republic
10	6	Roubaix	France

Table 15. Top cities by phishing Web sites
Source: Symantec Corporation

Moscow hosted the second most phishing Web sites in the EMEA region during this reporting period. This is a jump from last period when Moscow was ranked fourth in EMEA in this category. Russia has recently seen a large increase in broadband usage, posting a 55 percent increase from the first quarter of 2006 to the first quarter of 2007.[72]

London was host to the third most phishing Web sites in the EMEA region. London is home to many small Web-hosting companies and is the third highest bot-infected city in EMEA. Bot-infected computers are frequently used to host phishing Web sites by downloading other threats. This means that phishing Web sites are probably hosted on both compromised machines and with small Web-hosting companies in London.

Using a small Web-hosting company to host a phishing site can be advantageous for an attacker. These companies may not have the same amount of security resources as larger Web-hosting companies. As a result, they may not have adequate security measures in place to prevent, detect, or remove the illicit hosting of phishing Web sites.

Phishing—prevention and mitigation

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

DNS block lists also offer protection against potential phishing emails.[73] Organizations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.[74]

To protect against potential phishing activity, administrators should always follow Symantec best practices as outlined in Appendix A of this report. Symantec also recommends that organizations educate their end users about phishing.[75] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, as well as provide a means to report suspected phishing sites.[76]

[72] http://point-topic.com
[73] 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.
[74] 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.
[75] 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
[76] A good resource for information on the latest phishing threats can be found at: http://www.antiphishing.org

Organizations 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 using the legitimate Web site to create an illegitimate Web site that could be used for phishing.

Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[77] So-called typo domains and homographic domains should also be monitored.[78] This can be done with the help of companies that specialize in domain monitoring; some registrars also provide this service.

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

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.[79] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[77] The term cousin domain refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com" cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.

[78] Typo domains are domain names that use common misspellings of a legitimate domain name, for example the domain "symatnec.com" would be a typo domain for "symantec.com". A homographic domain name uses numbers that look similar to letters in the domain name, for example the character for the number "1" can look like the letter "l".

[79] 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 January 1 and June 30, 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 optimized 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.

This section of the Symantec *EMEA Internet Security Threat Report* will explore the following:

- Top ten countries of spam origin
- Top spam zombie countries and cities
- Spam as a percentage of all email by country

Top ten countries of spam origin

This section will discuss the top ten countries of spam origin in the EMEA region. 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 summarized. Each IP address is mapped to a specific country and charted over time.

The highest source of spam in EMEA this period was a collection of undetermined European countries (table 16). Symantec determines the country of origin of spam by identifying the owner of the IP address from which the spam was sent and then determining the country in which that owner—typically an ISP—operates. However, some ISPs in the EU operate in more than one country. As a result, the country of origin cannot be definitively determined.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage	Percent of Email That is Spam	Previous Percent of Email That is Spam
1	1	Undetermined European Countries	21%	20%	7%	7%	83%	81%
2	2	United Kingdom	12%	10%	4%	3%	43%	42%
3	5	Poland	8%	8%	3%	3%	86%	87%
4	6	Germany	7%	7%	2%	2%	64%	66%
5	9	Switzerland	6%	4%	2%	1%	66%	56%
6	3	France	5%	9%	2%	3%	60%	67%
7	8	Italy	5%	4%	2%	1%	75%	74%
8	7	Belgium	5%	6%	2%	2%	60%	61%
9	10	Russia	5%	3%	2%	1%	81%	68%
10	4	Spain	4%	8%	1%	3%	82%	84%

Table 16. Top ten countries of spam origin, EMEA region
Source: Symantec Corporation

The second highest volume of spam detected being sent from the EMEA region during this period originated in the United Kingdom, which accounted for 12 percent of the total. This is an increase over last period when the United Kingdom was still the top country but contributed only 10 percent of the spam coming from EMEA.

Spam can be sent using a compromised computer by either using it as a spam server, which is known as a spam zombie, or by using it to send mail through legitimate mail servers hosted by ISPs or other organizations using the computer user's email account. When a country has numerous legitimate mail servers, it is likely that many of them are used to surreptitiously send spam. This is especially true if any of the servers are misconfigured and can be used as open relays. Since the United Kingdom had only the eighth most spam zombies in the EMEA region during this period, it is likely that a large amount of the spam from the United Kingdom is sent through compromised legitimate mail servers.

English is by far the most popular language used in spam. Sixty percent of all spam detected worldwide during this period was composed in English, down from 65 percent in the previous reporting period. Finely tuned spam filters in English-speaking countries are sensitive to both the country of origin of a spam message and its language. Because of this, an English language spam directed at an English-speaking country is less likely to be detected as spam if it is coming from another English-speaking country than if it comes from a place that is less likely to send English-language mail.

Poland had the third highest volume of spam in the EMEA region in the first six months of 2007, accounting for eight percent of the region's total. Poland produced the same level of spam as last period but moved into third place in the region because of sharply reduced levels of spam from France and Spain.

Poland experienced a 46 percent increase in broadband connectivity from the first quarter of 2006 to the first quarter of 2007.[80] This likely created the opportunity for many compromised computers that could be used as spam zombies, particularly as Poland was ranked second in this region for this category. A large Internet service provider has been identified as the source of many of the spam messages originating from Poland.

France and Spain both experienced significant drops in their levels of spam over the previous six months. During this period, spam zombies in both countries dropped by a comparable amount, which likely contributed to the declining levels of spam.

Top spam zombie countries and cities

A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed. Between January 1 and June 30, 2007, Germany had more spam zombies than any other EMEA country, with 17 percent of the regional total (table 17). This is similar to the last six months of 2006, when Germany hosted 16 percent of spam zombies in EMEA and was also the top-ranked EMEA country. The only country with more spam zombies in the world during this period was the United States.

Germany likely ranks high on the list because it has the highest number of broadband-connected computers in the region.[81] Broadband-connected computers make ideal spam zombies because they are always connected to the Internet and have enough bandwidth to send many spam messages at once. Germany is also home to the second most bot-infected computers in the region, many of which are probably used to send spam.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage
1	1	Germany	17%	16%	9%	8%
2	4	Poland	11%	9%	6%	5%
3	5	Italy	10%	8%	5%	4%
4	2	France	9%	14%	5%	7%
5	6	Turkey	6%	6%	3%	3%
6	3	Spain	6%	13%	3%	7%
7	10	India	6%	4%	3%	2%
8	7	Israel	6%	5%	3%	3%
9	9	Russia	5%	4%	3%	2%
10	8	United Kingdom	4%	5%	2%	3%

Table 17. Top spam zombie countries
Source: Symantec Corporation

Poland accounted for the second most spam zombies in the EMEA region with 11 percent. This is an increase from the last six months of 2006, when Poland accounted for nine percent of the region's spam zombies and was the fourth-ranked country in the region.

[80] http://www.point-topic.com
[81] http://www.point-topic.com

This increase is likely due to the rapid growth of broadband connectivity in Poland. As mentioned above, broadband-connected computers make ideal spam zombies because, often, they are always connected to the Internet and have enough bandwidth to send many spam messages at once. Further, in countries in which rapid expansion of connectivity is taking place, many users who connected to the Internet are not well informed about computer security practices. These users' computers are more likely to be infected by a bot or other malicious code and thus used as spam zombies. Further, once infected, these machines are likely to remain undetected for extended periods of time.

Italy had the third highest number of spam zombies in the EMEA region during the first half of 2007, with 10 percent of the region's total. This is an increase from last period when Italy only accounted for eight percent of the region's spam zombies. This increase is likely related to the June 2007 MPack attack in Italy, which was previously discussed in the "Top ten malicious code samples" section of this report. There is a high likelihood that many computers that were lured to MPack servers in this attack had Trojans installed on them that relay spam.

Madrid had the highest number of spam zombies of any city in the EMEA region (table 18). This city has maintained its position at the top of this list despite dropping numbers of spam zombies in Spain. Most Spanish users are connected to the Internet through the country's dominant ISP, which is located in Madrid. This means that many of the actual spam zombie computers may be in other cities close to Madrid, but the centralized location of the ISP makes it appear as though they are located within that city.

Regional Rank	Previous Regional Rank	City	Country
1	1	Madrid	Spain
2	4	Petah Tiqwa	Israel
3	8	Milan	Italy
4	6	Moscow	Russia
5	N/A	Istanbul	Turkey
6	3	Ankara	Turkey
7	13	Budapest	Hungary
8	10	Warsaw	Poland
9	15	Katowice	Poland
10	21	Poznan	Poland

Table 18. Top spam zombie cities
Source: Symantec Corporation

Petah Tiqwa had the second highest number of spam zombies in the EMEA region. Despite its small population, Petah Tiqwa is home to a number of large ISPs that serve the surrounding areas. Just like in Madrid, many of the actual spam zombie computers may be in other cities close to Petah Tiqwa, but the location of the ISP makes it appear as though they are located within that city. As was discussed in the "Bot-infected computers by city" section of this report, Petah Tiqwa had the second highest number of bot-infected computers in the EMEA region during this period. Many of these bots were likely used as spam zombies.

Milan had the third highest number of spam zombies of EMEA cities during this period. Milan was fourth in the region for bots, indicating that many of the bots located in Milan are used for sending spam rather than for attacks. The increase in Milan's ranking may indicate that many of the spam-sending Trojans detected in Italy in this period could be located there.

Spam as a percentage of all email by country

Symantec calculates the percentage of email that is spam by dividing the total number of emails that are identified as spam by Symantec Brightmail AntiSpam filters by the total of the inbound email messages received by the sample customer base.[82] Between January 1 and June 30, 2007, spam made up 61 percent of all monitored email traffic across the Internet as a whole. In the EMEA region alone, spam made up 67 percent of all monitored email traffic during this reporting period.

Of the top 20 email-producing countries in the EMEA region, the top five countries according to the percent of spam by volume are listed in table 19. It is important to note that these percentages are not related to the total volume of spam produced by these countries, but are instead a representation of the percentage of all email originating from each country that Symantec has identified as spam.

Country	Percent	Previous Percent
Poland	86%	87%
Spain	82%	84%
Hungary	82%	81%
Russia	81%	68%
Italy	75%	74%

Table 19. Top five EMEA countries by percentage of spam
Source: Symantec Corporation

Of the top 20 email-producing countries in the EMEA region, Poland produced the highest percentage of spam, with 86 percent. Poland has a history of high percentages of spam. It was the second highest country in EMEA in the previous six-month when 87 percent of email was spam. Since that time, no noteworthy changes have been made to address the issue. New Polish antispam regulations could have an effect on this percentage but they did not come into effect until July 3, 2007, at which time this report was already in production.[83]

Spain had the second highest percentage of spam; 82 percent of all mail originating there was classified as spam. Hungary also had a spam percentage of 82 percent, making it the third highest spam-producing country in the EMEA region.

[82] Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not at 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.

[83] http://www.mt.gov.pl/article/english/press_releases/article.php/id_art/9d754fd47e6dc6f7490ade74c1aeefcf

Appendix A—Symantec Best Practices

Enterprise Best Practices

1. Employ defense-in-depth strategies, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated antivirus, firewalls, intrusion detection, and intrusion protection systems on client systems.
2. Turn off and remove services that are not needed.
3. 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.
4. 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.
5. Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
6. Enforce an effective password policy.
7. 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.
8. Isolate infected computers quickly to prevent the risk of further infection within the organization. Perform a forensic analysis and restore the computers using trusted media.
9. 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.
10. 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.
11. Educate management on security budgeting needs.
12. Test security to ensure that adequate controls are in place.
13. Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software. Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organization are deployed on desktop computers.

Consumer Best Practices

1. 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.
2. Consumers should ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.
3. 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.
4. Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
5. 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.
6. Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
7. 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.
8. 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.
9. 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 organization are deployed on desktop computers.
10. 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.
11. Consumers should beware 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.

Attack definitions

In order to avoid ambiguity with the findings presented in this discussion, Symantec's methodology for identifying various forms of attack activity is outlined clearly below. This methodology is applied consistently throughout our monitoring and analysis. The first step in analyzing attack activity is to define precisely what an attack is. Attacks are individual instances of malicious network activity. Attacks consist of one IDS or firewall alert that is indicative of a single attack action.

Explanation of research inquiries

This section will provide more detail on specific methodologies used to gather and analyze the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warranted additional detail.

Denial of service attacks

Although there are numerous methods for carrying out denial of service (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 bots based on coordinated scanning and attack behavior observed in network traffic. For an attacking computer to be considered to be participating in this coordinated scanning and attacking, it must fit into that pattern to the exclusion of any other activity. This behavioral matching will not catch every bot network computer, and may identify other malicious code or individual attackers behaving in a similarly coordinated way as a bot network. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers and will give insight into the population trends of bot network 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.

This metric explores the number of active bot-infected computers that the Symantec Global Intelligence Network has detected and identified during the first six months of 2007. Identification is carried out on an individual basis by analyzing attack and scanning patterns. Computers generating attack patterns that show a high degree of coordination are considered to be bot-infected computers.

As a consequence of this, Symantec does not identify all bot-infected computers, but only those that are actively working in a well coordinated and aggressive fashion. Given Symantec's extensive and globally distributed sensor base, it is reasonable to assume that the bot activities discussed here are representative of worldwide bot trends, and can thus provide an understanding of current bot activity across the Internet as a whole.

Bot-infected computers by countries and cities

This metric is based on the same data as the "Bot-infected computers" discussion of the "Attacks Trends" section of the report. 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.

Lifespan of bot-infected computers

Using previously identified bot-infected computers, Symantec determined the life span of these infections by measuring the time between their first and last detected activity. However, to ensure that the lifespan reflects a continuous bot infection, if the identified computer was inactive for 30 days or longer it was considered to be disinfected. As such, any further bot-like activity would be considered a new infection.

Top originating countries

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.

Appendix C—Malicious Code Trends Methodology

The trends in the “Malicious Code Trends” section 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 the “Malicious Code Trends” section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from 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 analyze, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec AntiVirus customers.

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

Malicious code database

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

In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the *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 behaviors of antifraud filters as well as the overall volume of mail being processed.

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

Phishing attempt definition

The Symantec Probe Network is a system of over two million decoy accounts that attract email messages from 20 different countries 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 covers countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

The Symantec Probe Network data is used to track the growth in new phishing activity. A phishing attempt is a group of email messages with similar properties, such as headers and content, that are sent to unique users. The messages attempt to gain confidential and personal information from online users.

Symantec Brightmail AntiSpam software reports statistics to Symantec Security Response that indicate 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 is used to identify general trends in phishing email messages.

Top countries and cities 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. 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.

Appendix E—Spam Trends Methodology

The Symantec Probe Network is a system of over two million decoy accounts that attract email messages from 20 different countries 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 having more than 1,000 total messages per day. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

Explanation of research inquiries

This section will provide more detail on specific methodologies used to produce the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warranted additional detail.

Top countries and cities of 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 summarized 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.

Top countries and cities by spam zombies

The data in this section is determined by examining the logical connecting IP addresses in spam messages received by the Symantec Probe Network. IP addresses that meet a certain volume requirement are processed through a set of heuristics to determine if they are behaving like zombie servers. If an IP address meets some or all of the heuristic requirements it will be listed as a zombie IP address. Symantec then cross-references the addresses with several third-party subscription-based databases that link the geographic locations of systems to IP addresses. 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 spam zombies.

Spam as a percentage of email scanned

The data for this section is determined by dividing the number of email messages that trigger antispam filters in the field by the total number of email messages scanned. These filters are distributed across the Symantec Brightmail AntiSpam customer base. The data for this section is based on monthly totals.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

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

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

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