



Confidence in a connected world.

Symantec EMEA Internet Security Threat Report

Trends for 2008

Volume XIV, Published April 2009

Marc Fossi

Executive Editor
Manager, Development
Security Technology and Response

Eric Johnson

Editor
Security Technology and Response

Trevor Mack

Associate Editor
Security Technology and Response

Dean Turner

Director, Global Intelligence Network
Security Technology and Response

Joseph Blackbird

Threat Analyst
Symantec Security Response

Mo King Low

Threat Analyst
Security Technology and Response

Teo Adams

Threat Analyst
Security Technology and Response

David McKinney

Threat Analyst
Security Technology and Response

Stephen Entwisle

Threat Analyst
Security Technology and Response

Marika Pauls Laucht

Threat Analyst
Security Technology and Response

Candid Wueest

Threat Analyst
Security Technology and Response

Greg Ahmad

Threat Analyst
Security Technology and Response

Darren Kemp

Threat Analyst
Security Technology and Response

Ashif Samnani

Threat Analyst
Security Technology and Response

Symantec EMEA Internet Security Threat Report

Contents

Introduction	4
Highlights	5
Threat Activity Trends	7
Malicious Code Trends	24
Phishing and Spam Trends	36
Appendix A—Symantec Best Practices	42
Appendix B—Threat Activity Trends Methodology	44
Appendix C—Malicious Code Trends Methodology	46
Appendix D—Phishing and Spam Trends Methodology	47

Introduction

The Symantec *EMEA Internet Security Threat Report* provides an annual overview and analysis of Internet threat activity, a review of known vulnerabilities, and highlights of malicious code in the Europe, Middle East, and Africa (EMEA) region. Trends in phishing and spam are also assessed. Previously presented every six months, this volume of the Symantec *EMEA Internet Security Threat Report* will alert readers to current trends and impending threats that Symantec has observed in the region for all of 2008.

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 32,000 recorded vulnerabilities (spanning more than two decades), affecting more than 72,000 technologies from more than 11,000 vendors. Symantec also facilitates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 50,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

Spam data is captured through the Symantec Probe Network, a system of more than 2.5 million decoy accounts, MessageLabs Intelligence, and other Symantec technologies in more than 86 countries from around the globe. Over eight billion email messages, as well as over one billion Web requests, are scanned per day across 16 data centres. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

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

Highlights

The following section will offer a brief summary of the security trends that Symantec observed in the EMEA region in 2008. This includes highlights of the metrics that are discussed in the Symantec *EMEA Internet Security Threat Report*.

Threat Activity Trends Highlights

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

Malicious Code Trends Highlights

- Trojans were the most common type of malicious code identified in EMEA in 2008, accounting for 66 percent of the top 50 potential infections in the region—a minor increase from 64 percent in 2007.
- The United Kingdom was the top ranked country for back doors and Trojans in EMEA in 2008; Egypt was the top ranked country for viruses; and Saudi Arabia was the top ranked country for worms.
- The Vundo Trojan was the top malicious code sample by potential infection identified in EMEA in 2008, unchanged from 2007; it was also the top ranked sample globally.
- The Brisv Trojan was the top new malicious code family reported in 2008 in the EMEA region, as well as globally.
- In EMEA during 2008, 87 percent of confidential information threats had remote access capabilities, compared to 94 percent in the previous year.

Symantec EMEA Internet Security Threat Report

- The most common propagation method for malicious code was through shared executable files, accounting for 65 percent of potential infections in EMEA, which is a substantial increase from 37 percent in 2007.
- In 2008, 1 percent of the volume of the top 50 samples in EMEA had the capability to modify Web pages, unchanged from 2007.

Phishing and Spam Trends Highlights

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

Threat Activity Trends

This section of the Symantec *EMEA Internet Security Threat Report* will provide an analysis of threat activity that Symantec observed in EMEA in 2008. The malicious activity discussed in this section not only includes attack activity, but also phishing websites hosted, malicious code, spam zombies, bot-infected computers, and command-and-control server activity. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activity can be found in their respective sections of this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious activity by country
- Top countries of attack origin
- Bot-infected computers
- Bot-infected computers by country
- Bot command-and-control servers
- Bot command-and-control servers by country
- Top Web-based attacks
- Web-based attacks by country
- Threat activity—protection and mitigation

Malicious activity by country

This metric will assess the countries in which the most malicious activity took place or originated in EMEA in 2008. To determine this, Symantec compiled regional data on numerous malicious activities, including: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Germany ranked first for overall malicious activity in EMEA during 2008, with 14 percent of the total, a drop from 18 percent in 2007 (table 1). Within the specific categories, Germany remained top-ranked for spam zombies and phishing hosts, but dropped from second to sixth for malicious code. It also dropped from first to second for bot activity and attack origin.

Symantec EMEA Internet Security Threat Report

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	Germany	14%	18%	6	1	1	2	2
2	2	United Kingdom	11%	11%	1	7	2	6	1
3	4	Spain	9%	8%	4	5	7	1	4
4	5	Italy	8%	8%	5	3	8	3	5
5	3	France	7%	9%	2	8	5	7	3
6	6	Poland	6%	6%	12	6	4	4	8
7	7	Turkey	6%	4%	7	2	13	5	6
8	8	Russia	6%	4%	9	4	3	10	7
9	9	Netherlands	3%	3%	8	20	6	15	10
10	10	Israel	3%	3%	23	9	9	9	11

Table 1. Malicious activity by country, EMEA

Source: Symantec Corporation

Germany's drop from second to sixth in malicious code for 2008 is likely due to slight shifts in the percentages of the other countries in EMEA, rather than from a significant drop in the number of instances of malicious code in Germany. There was less than a 1 percent difference between second-ranked France and Germany in this category. Thus, the drop of Germany from second to sixth is simply a slight reshuffling of the percentages of these four countries.

Germany's drop in bot activity from first in 2007 to second in 2008 equals a percentage drop from 21 percent to 14 percent. This drop is more likely due to an increase in bot activity in Turkey than from a decrease in actual activity in Germany. Bot activity in Turkey more than doubled from 2007 to 2008, from 4 percent to 9 percent.

Another factor influencing Germany's top rank in overall malicious activity is that it has the largest broadband market in EMEA (and the fourth largest market globally), with 22.5 million subscribers. Malicious activity usually affects computers connected to high-speed broadband Internet. These connections are attractive targets for attackers because they provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and a typically more stable connection.

The second ranked country in EMEA for overall malicious activity in 2008 was the United Kingdom, with 11 percent of the total, unchanged from 2007. Within this, the only specific category in which the United Kingdom ranked first was for malicious code activity, the same ranking it had in 2007. This ranking is likely due to the United Kingdom again being the top country in 2008 for some of the most common types of malicious code in EMEA, including Trojans and back doors, as is discussed in the ["Malicious Code Trends"](#) section, of this report.

The rankings and percentages for the United Kingdom in malicious activity have remained fairly constant from 2007 to 2008. This trend correlates with the premise that the proportion of malicious activity that originates within any country with a well-established broadband Internet infrastructure remains relatively static unless new methods are taken to reduce the amount of originating malicious activity.¹

¹ http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 18

One area of change for the United Kingdom that will be important to watch is the planned deployment of fibre-to-the-home (FTTH).² In anticipation of the 2012 London Olympic Games, British Telecom is rolling out FTTH trials in neighbourhoods in London and Cardiff, and intends to expand this service further if the trials are successful.³

FTTH is based on an infrastructure of fibre-optic lines, which provide higher bandwidth capacities than traditional DSL or cable lines. Fibre-optic infrastructure is expanding both within EMEA and globally, though the level of deployment varies among countries. Symantec expects trials or deployment of FTTH services in larger centres to affect bot activity since botnet operators are likely to target such connections; this is because, if compromised, they offer the greatest bandwidth capacity for carrying out attacks.

Spain ranked third for overall malicious activity in EMEA in 2008, with 9 percent of the regional total, an increase from 8 percent in 2007 when it ranked fourth. The only specific category in which Spain ranked first in 2008 was for bot activity, up from second in 2007. Spain's rank in all categories increased with the exception of attack origin, which remained unchanged from 2007. However, the rise in rankings is modest and attributable more to a drop in malicious activity in other countries rather than to an increase in Spain.

Of the remaining countries in this category, malicious activity in Turkey is worth noting because it is the only country ranked in the top 10 for which malicious activity increased in every category. In particular, the percentage of recorded bot activity more than doubled, and spam activity increased by 1,200 percent from 2007. These increases are discussed in greater detail in [“Bot-infected computers by country”](#) and [“Top countries of spam origin”](#)

Top countries of attack origin

The top countries of attack origin have been identified through analysis of data collected through the Symantec Global Intelligence Network. The analysis includes intrusions, attempted intrusions, and reconnaissance activity. This activity is initiated by attackers targeting specific individuals or organisations, as well as automated attack activities—such as bots and other types of malicious code—that may not be targeting specific Internet addresses.

In 2008, 28 percent of attacks targeting the EMEA region originated in the United States, an increase from 22 percent in 2007 (table 2). This increase may simply be due to the combination of the volume of traffic originating in the United States and that malicious activity usually coincides with high-speed broadband connectivity. The United States has one of the most established broadband infrastructures in the world, with over 92 percent of its Internet users on high-speed broadband connections.⁴ This equates to 78.7 million broadband subscribers and a growth of 20 percent from 2007.⁵

² Also known as FTTP (Fibre-to-the-premise)

³ See <http://www.zdnetasia.com/news/communications/0,39044192,62044419,00.htm> and <http://news.bbc.co.uk/2/hi/technology/7667761.stm>

⁴ <http://www.websiteoptimization.com/bw/0812/>

⁵ <http://point-topic.com>

Symantec EMEA Internet Security Threat Report

2008 EMEA Rank	2007 EMEA Rank	Country	2008 EMEA Percentage	2007 EMEA Percentage	2008 Global Percentage
1	1	United States	28%	22%	25%
2	2	China	14%	16%	13%
3	3	United Kingdom	10%	11%	6%
4	8	France	4%	3%	4%
5	7	Italy	4%	3%	3%
6	6	Germany	3%	4%	6%
7	14	Russia	3%	1%	2%
8	10	Canada	3%	2%	3%
9	15	Netherlands	2%	1%	1%
10	43	United Arab Emirates	2%	<1%	<1%

Table 2. Top countries of attack origin, EMEA

Source: Symantec

The increase in attacks from the United States targeting EMEA during this reporting period may have been due to the operations of two ISPs based in the United States that were alleged to have been providing Internet services to botnet operators and spammers.⁶ The subsequent shutdown of these ISPs resulted in an immediate and significant drop in spam and bot levels in EMEA (as well as worldwide).

However, following the shutdown, spam and bot numbers in EMEA increased again. Indications are that the botnet operators found alternative hosting services in EMEA soon after the shutdown.⁷ The interim hosting apparently allowed the botnets controllers to relocate at least a portion of their bot command-and-control (C&C) servers.⁸ Also in 2008, the bot C&C servers associated with the Srizbi⁹ botnet were relocated to Estonia, with the domain names being registered in Russia.¹⁰ These shifts from the use of hosting services in the United States to services located in EMEA would account for the rise in malicious activity targeting EMEA that originated in the United States.

China ranked second for originating attacks on EMEA this period, with 14 percent of the total, down from 16 percent in 2007. This figure correlates with China's 15 percent total for global attacks in 2008, indicating that attacks originating in China are not especially targeting EMEA and that its ranking here is simply due to the amount of malicious activity originating there in general, which is attributable to China having the greatest number of broadband subscribers globally.¹¹

The United Kingdom ranked third for originating attacks on EMEA in 2008, with 10 percent of the total, a decrease from 11 percent in 2007. This 10 percent share for EMEA is nearly double the United Kingdom's global percentage, which indicates that a substantial amount of the attack volume originating in the United Kingdom is targeting the EMEA region. Symantec has noted a tendency for attacks to often target computers in geographical proximity.¹² One reason for this is that organisations are likely to have higher profiles in their local area and, therefore, make more attractive targets for regional attackers. Other factors include shared language and similar cultural and social interests—which would lead, for example, to regionally focused phishing attacks.

⁶ Cf. http://www.message-labs.com/mlireport/MLIRReport_Annual_2008_FINAL.pdf : p. 25, and http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 3

⁷ http://www.message-labs.com/mlireport/MLIRReport_Annual_2008_FINAL.pdf : p. 26

⁸ <http://news.softpedia.com/news/Cybercriminals-Move-Fast-as-McColo-Takes-a-Short-Breath-of-Air-98033.shtml>

⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99

¹⁰ http://www.pcworld.com/businesscenter/article/154554/spammers_regaining_control_over_srizbi_botnet.html

¹¹ <http://www.point-topic.com>

¹² http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_emea_09_2007.en-us.pdf : p. 7

One final change in ranking worth noting here is the rise of the United Arab Emirates (U.A.E.), from forty-third in 2007 to tenth in 2008. This increase may simply be due to significant broadband expansions that have occurred there recently. Broadband subscriptions in the U.A.E. have risen by nearly 900 percent in the last four years. As noted previously, the growth in broadband availability in a country often results in a corresponding growth in malicious activity. It should also be noted that, although the U.A.E. made a substantial jump in the rankings for this measurement in 2008, after a certain ranking, even small changes in activity are often enough to substantially shift a country's position in the rankings.

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), peer-to-peer (P2P), or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a bot network (botnet), which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organisation's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers (which can be used in identity theft) all of which can have serious financial and legal consequences. Bots are also inexpensive and relatively easy to propagate. In 2008, Symantec observed advertisements for bot-infected computers in the underground economy for as little as \$0.04 per bot.¹³ This is much cheaper than in 2007, when \$1 was the cheapest price advertised for bots. For botnets, attackers favour decentralised command-and-control models because they are difficult to disable and, most importantly, can be lucrative for their controllers. In one example, a botnet owner arrested in New Zealand admitted to earning \$21,500 over a two-year span from his activities.¹⁴

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; rather, a single such computer can be active on a number of different days. In 2008, Symantec observed an average of 32,188 active bots per day in the EMEA region (figure 1); this is a 47 percent increase from 2007, when 21,864 active bots were detected. In 2008, active bots in the EMEA region accounted for 51 percent of active bot activity globally.

¹³ All figures are provided in U.S. dollars

¹⁴ <http://www.itworld.com/security/58670/botnet-master-sees-himself-next-bill-gates>

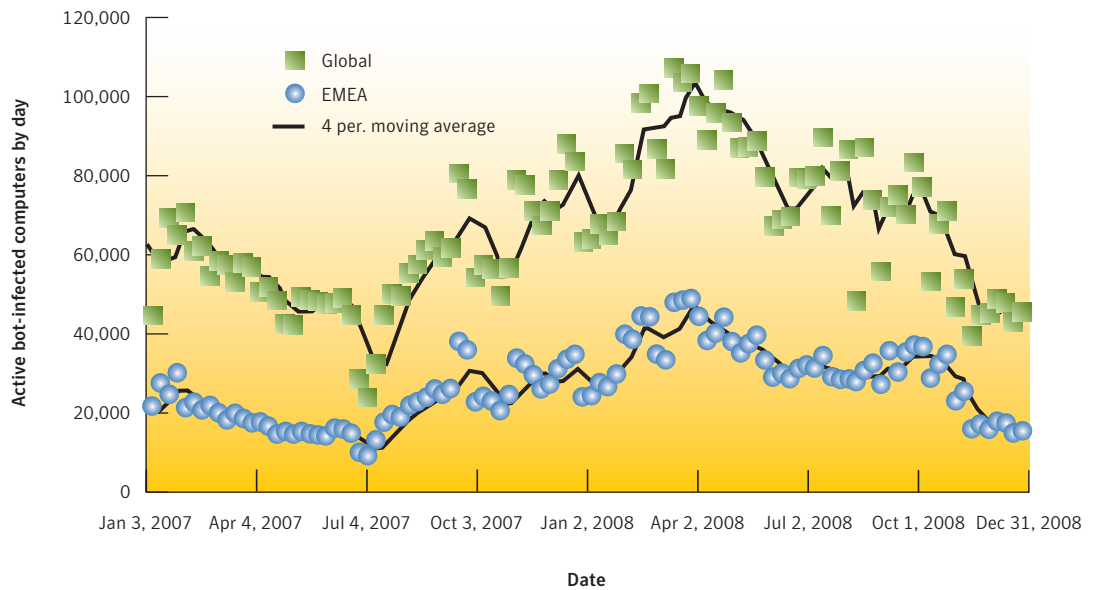


Figure 1. Active bot-infected computers, EMEA and global
Source: Symantec

Symantec also measures distinct bot-infected computers, which are computers that were active at least once during the reporting period. There were 4,776,967 distinct bot-infected computers recorded in the EMEA region in 2008. This is 9 percent more than the 4,378,892 observed in EMEA in the previous reporting period. The increase in both overall active and distinct bot-infected computers observed in 2008 may be due to their popularity among attackers, and because platforms such as HTTP increase their effectiveness.

It is worth noting that bot activity in EMEA in 2008 very closely mirrors global bot activity during the same period. Symantec has observed a growing trend toward the globalisation of malicious activity in which attackers are not restricted by geography. Many botnets are globally dispersed, allowing for much more flexibility in their activities.¹⁵ Bots in a certain area can be used to launch an attack and then remain offline for a specific period of time in order to make it harder to predict the location of the next attack. This tactic would take pressure off of bots in highly monitored areas such as the United States.¹⁶ It may also be more difficult to disable a botnet that has components in many different countries because this would require a significant coordination of law enforcement efforts across a number of regions in order to successfully disable the botnet.

Bot-infected computers by country

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

¹⁵ <http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=208804851>
¹⁶ <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39160885,00.htm>

Symantec EMEA Internet Security Threat Report

Spain ranked first for bot-infected computers in EMEA in 2008, up from second in 2007 (table 3). Its regional share was unchanged at 15 percent for both years. Given that its regional share remained unchanged, Spain's rise to first in 2008 is likely due to a drop in bot activity in second-ranked Germany rather than an increase in Spain.

In a previous volume of the Symantec *EMEA Internet Security Threat Report*, it was speculated that bot activity in Spain would likely follow the same trend as has been observed in the United Kingdom; that is, the percentage of bot-infected computers would increase as broadband penetration increased and then would eventually level off as the broadband infrastructure became more established.¹⁷ This trend occurs as users and ISPs become more aware of security issues and more adept at instigating protective measures from infection. This is proving to be true in Spain since, with broadband growth slowing significantly over 2008, there has also been a correlating plateau in bot activity.¹⁸

2008 EMEA Rank	2007 EMEA Rank	Country	2008 EMEA Percentage	2007 EMEA Percentage	2008 Global Percentage
1	2	Spain	15%	15%	8%
2	1	Germany	14%	21%	7%
3	4	Italy	11%	10%	5%
4	6	Poland	10%	8%	5%
5	8	Turkey	9%	4%	4%
6	5	United Kingdom	8%	8%	4%
7	3	France	6%	10%	3%
8	9	Portugal	4%	3%	2%
9	7	Israel	3%	5%	2%
10	10	Russia	3%	2%	2%

Table 3. Bot-infected computers by country, EMEA

Source: Symantec

Germany ranked second for bot-infected computers in 2008, accounting for 14 percent of the region—a decrease from 21 percent in 2007. One reason for the drop in the proportion of activity in Germany is the proportional increase in activity recorded in Turkey (discussed below). The drop in activity in Germany may also be due to efforts taken to evenly distribute traffic during peak periods, which may have impeded the ability of attackers to send out large volumes of traffic.¹⁹

Italy ranked third for bot activity in EMEA this period, with 11 percent of the regional total. By comparison, Italy ranked fourth in 2007, accounting for 10 percent of the bot activity in the EMEA region. As with Spain, because Italy's proportion of activity remained relatively unchanged, its increase in ranking is likely due to the drop in Germany's proportion of activity, as well as a drop in activity in France, which ranked third in 2007.

France's decrease from ranking third in 2007 to seventh in 2008 may be due to a government initiative to develop a system to allow Internet users to report spam directly to their ISPs.²⁰ Users can install a toolbar in their email client that allows them to forward offending messages to the ISP from which they originated. The ISP collects these emails in a database and ultimately decides whether or not to suspend the account of the sender.

¹⁷ http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf : p. 13

¹⁸ http://www.typicallyspanish.com/news/publish/article_19664.shtml

¹⁹ http://www.focus.de/digital/internet/kabel-deutschland_aid_264070.html

²⁰ <http://pcworld.about.com/od/spam/France-kicks-off-nationwide-sp.htm>

Another new piece of legislation under consideration in France is intended to curb illegal file sharing by blocking Internet access for those caught either uploading or downloading copyrighted material.²¹ If this regulation is enacted, users that are caught illegally sharing files will have three chances to cease their activities before their Internet privileges are suspended for a year.²² It remains to be seen whether or not such legislative efforts will affect botnet infection trends, as there is often a correlation between botnet infections and illegal file sharing.

Worth noting is Turkey's share of bot-infected computers in EMEA for 2008, which more than doubled to 9 percent from 4 percent in 2007. Some of the bot activity found in Turkey can be attributed to the relocation of bots that compose a botnet associated with the Peacomm Trojan, which first appeared in January 2007.²³ After a significant drop in size in April 2008, and inactivity after September 2008, Peacomm reappeared as the Waledac²⁴ botnet at the end of 2008. After the botnet was disabled, the botnet operators are believed to have found new computers to infect, many of which were in Turkey.²⁵

Bot command-and-control servers

Bot C&C servers are computers that botnet owners use to relay commands to bot-infected computers on their networks. Symantec tracks the number of bot C&C servers worldwide, as well as regionally. For the first time, in this volume of the *Symantec EMEA Internet Security Threat Report*, bot C&C servers controlled over HTTP are included in this analysis alongside traditional IRC bot C&C servers.²⁶ This change in measurement was made due to the trend of botnet owners shifting away from traditional IRC bot C&C communication frameworks and toward managing their botnets through HTTP bot C&C servers, which is reflected in the percentages for this reporting period. In 2008, Symantec identified 5,147 distinct new bot C&C servers in EMEA (figure 2), of which 40 percent were through IRC channels and 60 percent were over HTTP.

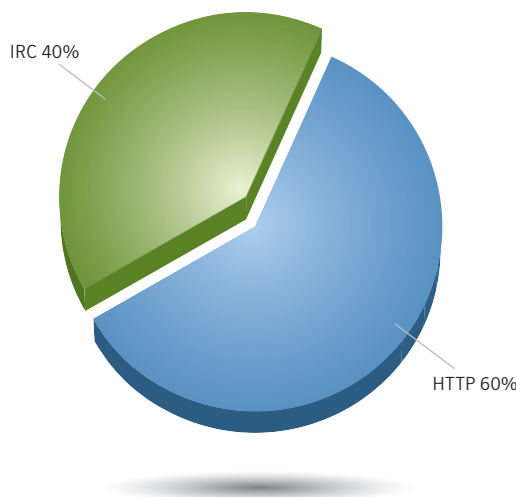


Figure 2. Bot command-and-control servers by type, EMEA

Source: Symantec

²¹ <http://news.bbc.co.uk/2/hi/technology/7706014.stm>

²² <http://euobserver.com/871/27026>

²³ http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99

²⁴ http://www.symantec.com/en/th/enterprise/security_response/writeup.jsp?docid=2008-122308-1429-99

²⁵ <http://www.scmagazineus.com/Botnet-storms-on-the-horizon/article/119586/>

²⁶ Not included in this measurement are bot C&C servers over P2P protocols; also, because this is the first report in which HTTP bot C&C servers are included in this analysis, 2007 comparisons are unavailable.

Botnet owners are moving away from traditional IRC-based botnets since they are easier to detect, track, filter, and block than botnets based on HTTP traffic. This is because malicious botnet traffic can be hidden within legitimate traffic over HTTP. (Most HTTP bot transmissions are encrypted to avoid detection.) To filter the traffic, organisations would have to inspect the encrypted HTTP traffic and identify and remove bot-related traffic, while still allowing legitimate traffic to pass through. Because of this, it is very difficult to pinpoint and disable a bot C&C structure. It is also unreasonable to block all HTTP traffic because that would restrict all access to the Web. Botnet owners have also been switching away from using P2P for bot C&C server communications because such traffic is more easily detected due to the “noise” it creates in transmission. Moreover, many enterprises and other organisations also block P2P ports to prevent such high-bandwidth traffic from entering their networks.

Symantec observed an average of 14 new active bot C&C servers per day in 2008, of which six were IRC-based and eight were controlled over HTTP, on average (figure 3). Because most of the major botnets—such as Srizbi, Rustock, and Pandex²⁷—have HTTP bot C&C architectures, fluctuations in their activity contribute to the variations in new bot C&C servers. These fluctuations are thought to be due, in part, to owners testing their botnets on HTTP channels for encryption, covertness, and so on.

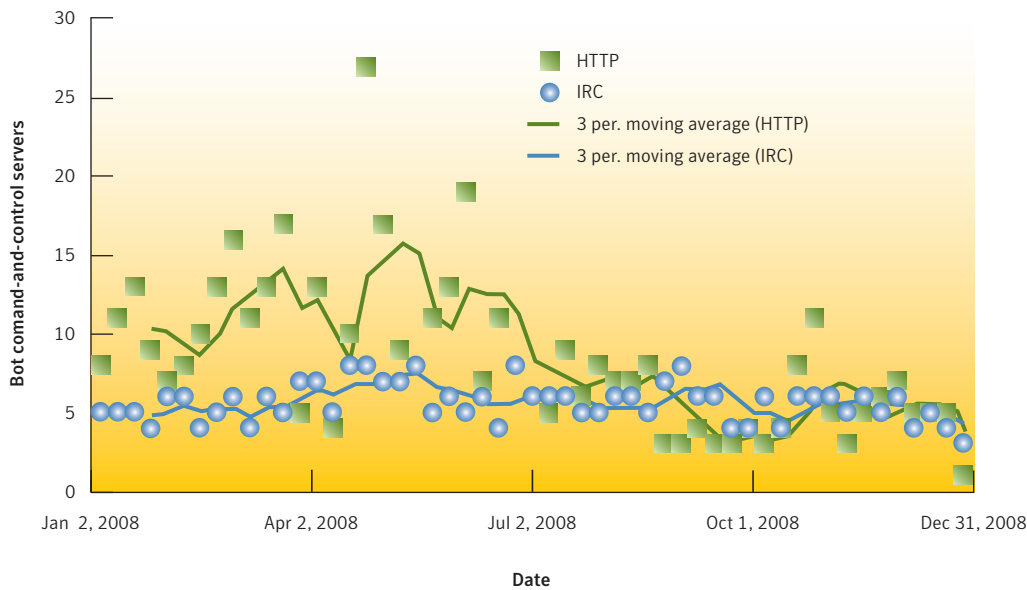


Figure 3. Bot command-and-control servers by day, EMEA
 Source: Symantec

Bot C&C server activity also exemplifies the trend toward the globalisation of malicious activity, as is demonstrated by the way that activity in EMEA closely follows global patterns. While there is a difference in scale because EMEA hosts fewer servers overall, there is a close correlation in activity between averages in EMEA and globally. Thus, fluctuations in the number of servers active at a given time in EMEA are probably due to fluctuations in global activity, rather than from specific changes within EMEA.

²⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2007-042001-1448-99

Bot command-and-control servers by country

Recognising the ongoing threat posed by bot C&C servers, Symantec tracks their distribution both worldwide and regionally. For regions, Symantec calculates the number of bot C&C servers worldwide and then assesses which countries within a region are home to high percentages of these computers. Because bot owners seek hosting services with stable Internet connections, high bandwidth, and whose security measures may not be properly developed or rigidly enforced, comparing countries with high proportions of bot C&C servers may indicate the level of end-user education and implementation of security practices in those countries. It may also demonstrate the potential for the infrastructures to withstand penetration by bot-infected computers. Note that bot C&C servers may not be located in the same place as the person controlling the botnet or even the bot-infected computer itself.

Additionally, it is worth noting that “normal” bot-infected computers can often become bot C&C servers. Botnet owners commonly use a fast-flux domain name service scheme, where the control of a botnet is decentralised, using a number of computers throughout the network.²⁸ Because there is no centralised bot C&C server, the botnet can be broken up into smaller pieces, therefore making its activities more difficult to detect and disable. In this way, bot C&C server distribution can sometimes mirror bot distribution.

Russia ranked first for bot C&C servers in the EMEA region in 2008, with 20 percent of the regional total (table 4). Of the bot C&C servers found in Russia, only 7 percent were IRC-based, while the remaining 93 percent used the HTTP protocol for communication. Russia’s top ranking is likely due to many bot C&C servers being moved there after the shutdown of a major ISP in the United States.²⁹ As discussed in [“Top countries of attack origin,”](#) this ISP was responsible for hosting bot C&C servers for three of the world’s largest botnets. Given the size and potential to generate profit of these three botnets, it is not surprising that new locations were quickly found to host these servers soon after they were disabled by the shutdown. Also contributing to the high ranking of Russia may be the continued role of the Russian Business Network (RBN) in the hosting and distribution of malicious content, including purported DoS attacks on many Georgian institutions in 2008.³⁰

C&C Rank	Country	C&C Percentage
1	Russia	20%
2	Germany	15%
3	Israel	9%
4	United Kingdom	7%
5	Netherlands	6%
6	Ukraine	5%
7	France	4%
8	Romania	4%
9	Turkey	3%
10	Italy	2%

Table 4. Bot command-and-control servers by country, EMEA

Source: Symantec

²⁸ http://news.zdnet.com/2100-1009_22-180416.html

²⁹ http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/

³⁰ Cf. http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf : p. 5, 8, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112201>, or <http://news.zdnet.co.uk/security/0,1000000189,39459928,00.htm>

Germany ranked second for bot C&C servers, with 15 percent of the total. Forty percent of bot C&C servers identified in Germany functioned over IRC, while 60 percent used HTTP. Germany's high ranking is likely due in part to its large and well-established broadband infrastructure; with such a large and mature market, it meets many of the requirements for supporting bot C&C servers. The top countries worldwide in 2008 for bot C&C servers were the United States, China, Russia, and Germany, in that order. Other than Russia, the top countries for bot C&C servers were also those with the most broadband subscribers and the most malicious activity worldwide.

Israel ranked third for bot C&C servers in EMEA in 2008, accounting for 9 percent of activity. Twenty-one percent of the servers in Israel were IRC-based, while the remaining 79 percent used HTTP. The rapid growth of broadband in Israel may be contributing to the rate of malicious activity found there.

It is also worth noting that, of the bot C&C servers in the top three countries, the majority of servers in each country are HTTP-based. As noted in the [“Bot command-and-control servers”](#) discussion, the shift away from IRC-based servers toward HTTP-based servers seems to be growing, with this shift more pronounced in EMEA than in other regions.

Top Web-based attacks

The widespread deployment of Web applications, along with the ubiquity of easy-to-exploit Web application security vulnerabilities, has resulted in the prevalence of Web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise or break into specific networks to gain access to those computers. Instead they are now focused on attacking and compromising websites in order to use them to mount additional, client-side attacks.

These attack types can be found globally and Symantec identifies each by an associated distinct detection signature. Most attack types target specific vulnerabilities or weaknesses in Web browsers or other client-side applications that process content originating from the Web. This metric will assess the top distinct Web-based attacks originating from compromised legitimate sites as well as malicious sites that have been created to intentionally target Web users in the EMEA region.

The attacks discussed can involve social engineering to entice a victim to view a malicious website, but most attacks exploit trusted high-traffic websites. When the user visits a compromised website, a number of attack methods are used. Malicious content from the website can directly exploit a vulnerability in the browser, a browser plug-in, or a desktop application. An attack such as this may require nothing more than the user visiting the site from which the attack originates. In the case of a drive-by download, the attack will occur without any interaction required from the user.³¹

Attackers also use malicious websites for compromises, such as misleading the user to indirectly authorize a specific technology that then downloads malicious code, or prompting the user to click on a pop-up or banner ad. Attackers can also redirect all traffic from a legitimate website to a malicious website from which the user's computer will then be attacked. In all of these types of Web-based attacks, the user is unaware of the compromise.

³¹ A drive-by download is any download that occurs without a user's prior knowledge or authorization and does not require user interaction. Typically this is an executable file.

Symantec EMEA Internet Security Threat Report

Once an attacker has compromised a website and injected malicious content, he or she can passively attack visitors of the compromised site. This type of attack is very efficient for attackers because they only have to compromise one Web page in order to affect multiple users. When a user visits a compromised Web page, the attack is carried out through the user's browser. The attack will either target vulnerabilities in the browser itself or third-party applications that are activated by the browser.

All Web-based attack traffic goes through HTTP or HTTPS protocols. The benefit of this for attackers is that it is unreasonable to block these protocols because legitimate organisations depend on them for their day-to-day business. In addition, filtering a large volume of HTTP traffic would significantly slow throughput traffic. HTTP traffic is also difficult to filter with intrusion detection/intrusion prevention systems (IDS/IPS) because it is difficult to distinguish malicious traffic from legitimate traffic, and HTTP traffic can be encrypted, thus enabling attacks to be obfuscated within legitimate traffic.

Attackers are not only employing manual methods to exploit these issues, but they are also using automated tools, such as Neosploit,³² to exploit client-side vulnerabilities. Such toolkits are widely available and prepackaged so that people with minimal technical knowledge are able to use them effectively. Once a computer is compromised, the attacker can then gain access to any connected networks and steal private information and/or system resources.

Another attraction of the Web for exploitation is the profusion of dynamic sites that use Web-based applications, such as forums, photo-sharing galleries, blogs, and online shopping applications. Dynamic sites are prime targets for attackers using bot-infected computers to propagate and host malicious content because Web application and site-specific vulnerabilities can put these types of site at risk.

Attackers are also especially drawn to large, popular websites with trusted reputations. This is not only because a successful compromise can reach a greater number of people (who tend to have an inherent trust for legitimate websites and are thus more susceptible to attack), but, as mentioned, it may be difficult to block attacks to these sites using security tools without disrupting legitimate traffic.

These developments and trends indicate that Web-based threats have not only become widespread, but that they also have increased in sophistication and severity. In particular, Symantec has noticed that botnets (such as Asprox,³³ which was initially used for phishing scams) are being redesigned to specifically exploit cross-site scripting vulnerabilities and inject malicious code into compromised websites.³⁴

Many Web-based attacks exploit vulnerabilities that are considered medium severity. This means that they can compromise the account of the user who is currently logged in. This typically means that the user does not require administrative privileges to run the affected applications. While the danger of client-side vulnerabilities may be limited by best practices, such as restricting Web applications to the administrative level, such measures are often impractical given how integral Web applications are to the delivery of content for many businesses. Medium-severity vulnerabilities affecting client or desktop applications are often sufficient for an attacker to engage in revenue-generating malicious activities and the further propagation of attacks and malicious code.

In 2008, the most common Web-based attack targeting the EMEA region exploited the Adobe Flash® Player Multimedia File Remote Buffer Overflow Vulnerability,³⁵ accounting for 22 percent of the regional total (table 5). This exploit also ranked first in the APJ region, and fourth globally in 2008. The vulnerability

³² <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=1>

³³ http://www.symantec.com/security_response/writeup.jsp?docid=2007-060812-4603-99

³⁴ http://www.message-labs.com/mlireport/MLIRReport_Annual_2008_FINAL.pdf : p. 33

³⁵ See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=22964 and <http://www.securityfocus.com/bid/28695>

Symantec EMEA Internet Security Threat Report

exploited in this attack was published on April 8, 2008, and fixes have also been available since then. The vulnerability is also exploited by the Swif.C Trojan to install additional malicious code onto compromised computers.³⁶

Rank	Attack	Percentage
1	Adobe SWF Remote Code Executable	22%
2	Adobe Acrobat PDF Suspicious File Download	8%
3	ANI File Header Size Buffer Overflow	7%
4	SnapShot Viewer ActiveX File Download	3%
5	AOL SuperBuddy ActiveX Code Executable	1%
6	Microsoft Internet Explorer COM Object Memory Corruption	1%
7	QuickTime RTSP URI Buffer Overflow	1%
8	Microsoft Internet Explorer msdds.dll Code Executable	1%
9	Microsoft Internet Explorer Malformed XML Buffer Overflow	1%
10	Microsoft Internet Explorer VML RecolorInfo Code Executable	<1%

Table 5. Top Web-based attacks, EMEA

Source: Symantec

The Adobe Flash Player is a popular multimedia technology with a substantial install base, and many websites now commonly employ Shockwave Flash (SWF) files to present content, especially streaming video.³⁷ Launching successful attacks may be quite simple once a successful exploit is developed because the attacker just has to compromise a high-traffic website with a specially crafted SWF. Since this technology is very common, users typically do not suspect it for malicious content. Moreover, if the user already has the player installed, there is no further interaction involved for the attack to be successful.

The second most common Web-based attack in EMEA is related to malicious Adobe Acrobat® PDF activity.³⁸ This attack accounted for 8 percent of Web-based attacks in EMEA during 2008. Specifically, attempts to download suspicious PDF documents were observed. This may indicate attempts by attackers to distribute malicious PDF content to victims via the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious file would be designed to exploit an arbitrary vulnerability in the application that processes it, typically Adobe Acrobat Reader.® A successful attack could ultimately compromise the integrity and security of an affected computer. This attack is assumed to be popular due to the common use and distribution of PDF documents on the Web. Also, browsers can be configured to automatically render a PDF document by default. Specific exploit activity related to malicious PDF files was observed in 2008.³⁹

The percentage of plug-in vulnerabilities affecting Adobe Acrobat in comparison to the total number of browser plug-in vulnerabilities increased to 4 percent in 2008 from 1 percent in 2007. This demonstrates that attackers are increasingly targeting Adobe Acrobat. In addition, the reappearance of the Neosploit toolkit in 2008 may have contributed to the popularity of this type of attack because that toolkit is designed to exploit vulnerabilities in PDF documents.⁴⁰

³⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2008-052714-3021-99

³⁷ http://www.adobe.com/products/player_census/flashplayer/

³⁸ http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153

³⁹ <https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Pidief-the-Word-for-Exploits/ba-p/305564#A141>

⁴⁰ <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=2>

In 2008, the third most common Web-based attack in EMEA exploited the Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability.⁴¹ This attack accounted for 7 percent of Web-based attacks in EMEA in 2008. The ANI (animated cursor file) handler is a default component of the Microsoft® Windows® operating system and is used by a significant number of widely used Microsoft applications, as well as the Windows shell. If successfully exploited, the vulnerability allows an attacker to execute arbitrary code embedded in a malformed ANI file originating from the Web or other sources. This vulnerability was published on Jan. 11, 2005, and fixes have been available since that time. Exploit code was publicly available the following day. As with the Microsoft Internet Explorer® ADODB.Stream Object File Installation Weakness, the prominence of this type of attack indicates that computers in the region are likely not being sufficiently patched and updated.

Vulnerabilities such as those discussed here continue to generate a large amount of observed attack activity because they can be reliably exploited. This makes these vulnerabilities prime candidates for automation. Despite the fact that fixes are available, as mentioned, it is likely that there are still enough unpatched systems in existence that these attacks continue to enjoy success. When attacks prove successful, they are often adopted by a large number of malicious code variants and attack toolkits. This can cumulatively create a large amount of attack activity. It is also likely that older malicious code variants continue to attempt to automatically exploit these vulnerabilities as a means of propagation.

Top countries of origin for Web-based attacks

This metric will assess the top countries of origin for Web-based attacks against users in EMEA by determining the location of computers from which the attack occurred. Note that the server hosting the exploit may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects his or her browser to a malicious server in another country.

Once an attacker has compromised a legitimate website, users who visit the website may be attacked by several additional means. One way is through a drive-by download, which can include installation of malicious code without the user's knowledge, or which will mislead the user to indirectly authorize a malicious download via a fake client-side application authorization request. Another way is to redirect the user to another website that is used to host malicious code. Sites and servers hosting a variety of malicious exploits can be found worldwide. Multiple domains can be associated with one compromised site, which is used to exploit one or more security vulnerabilities in affected client browsers.

In 2008, Ukraine ranked as the top country of origin for Web-based attacks in EMEA, accounting for 31 percent of the regional total (table 6). The prominence of Ukraine in this metric is likely due to the compromise of a U.S.-based electronic bill payment processing company's website. The attackers were able to obtain account credentials to the company's domain using a phishing attack.⁴² From there, they were able to gain access to the company's website. Customers, thinking they were visiting the legitimate website, were redirected to a malicious website hosted on servers in Ukraine, where they were attacked and infected with a Trojan.⁴³ In addition to this compromise, there were at least 71 domains that were redirected to the malicious Ukrainian server during this time, indicating that it was likely that a group of attackers were responsible for these wide-scale attacks.⁴⁴

⁴¹ Cf. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=21719 or <http://www.securityfocus.com/bid/12233>

⁴² <http://www.networkworld.com/news/2008/120508-network-solutions-phishing-came-before.html>

⁴³ http://www.csoonline.com/article/474365/CheckFree_Warns_Million_Customers_After_Hack

⁴⁴ <http://blog.kievukraine.info/2008/12/digging-deeper-into-checkfree-attack.html>

2008 EMEA Rank	2008 Global Rank	Country	2008 EMEA Percentage	2008 Global Percentage
1	3	Ukraine	31%	12%
2	4	Netherlands	19%	8%
3	5	Russia	13%	5%
4	6	United Kingdom	11%	5%
5	9	Latvia	4%	1%
6	10	France	3%	1%
7	11	Estonia	3%	1%
8	12	Germany	3%	1%
9	13	Austria	2%	1%
10	14	Sweden	2%	1%

Table 6. Top countries of origin for Web-based attacks, EMEA

Source: Symantec

In 2008, the Netherlands was the second-ranked country of origin for Web-based attacks in EMEA, with 19 percent of the regional total. The high ranking of the Netherlands is likely due to an attack conducted via servers and computers hosted from there in 2008. The attack exploited a multiple arbitrary remote code-execution and security vulnerability in Adobe Acrobat through both browsers and email.⁴⁵ As noted in the “[Top Web-based attacks](#)” discussion, the popularity of Adobe Acrobat PDF documents is likely a factor for attackers favouring this type of attack. The attack used banner advertisements to install a Trojan from a website based in the Netherlands.⁴⁶ Once installed on a user’s computer, the Trojan disables antivirus software and modifies files on the computer. It backs up critical files and renames itself in an attempt to avoid detection and, as well, it allows for remote access of the infected system.⁴⁷

Russia was the third-ranked country of origin for Web-based attacks in EMEA in 2008, with 13 percent of the total. This ranking may be due to the prevalence of more than half a million websites that were compromised in May with malicious code that was hosted in Russia and the United States. Web forums hosted by PHP-based bulletin board applications were exploited to inject malicious JavaScript into forum content. These forums would then infect visitors with variants of the Zlob Trojan⁴⁸ disguised as a video codec installer. The exploit changes browser and DNS settings on the infected computer and enables additional attacks, including turning the infected computer into a zombie.⁴⁹ This attack follows the trend of attackers inserting malicious code into legitimate high-traffic websites where users are likely to be more trusting of the content, rather than attempting to lure users to visit specially designed malicious sites.

In addition, the website of the U.S. Consulate in Russia was compromised in September 2008, with a majority of the compromised pages being hosted in Russia; the website attempted to install Trojans and other malicious code onto the computers of visitors to the site.⁵⁰ Hackers also compromised an online news website in September with an SQL-injection attack; visitors to the site were redirected to a malicious website on a Russian domain, which then attempted to further attack the computers and install malicious code.⁵¹

⁴⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2008-020915-1008-99

⁴⁶ <http://www.vnunet.com/vnunet/news/2209318/attacks-target-pdf-flaw>

⁴⁷ Cf. <https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Pidief-the-Word-for-Exploits/ba-p/305564#A141> or <http://www.adobe.com/support/security/bulletins/apsb08-13.html>

⁴⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99

⁴⁹ http://www.channelregister.co.uk/2008/05/13/zlob_trojan_forum_compromise_attack/

⁵⁰ <http://www.govtech.com/gt/143431?topic=117671>

⁵¹ http://news.cnet.com/8301-1009_3-10041743-83.html

Of note, six of the top 10 countries for Web-based attacks in EMEA were also in the top 10 countries of origin for Web-based attacks globally, and countries in the EMEA region accounted for 41 percent of the worldwide total, more than any other region. Exploit packs may be one reason for the prominence of the EMEA region in this measurement. Many of these exploit packs—including MPack,⁵² IcePack,⁵³ and Neosploit⁵⁴—originated in Russia and it is likely that the developers of these attack kits are responsible for much of their continued propagation. These attackers could possibly be compromising websites around the world and redirecting visitors to computers in EMEA that host the exploit code being used to target client-side vulnerabilities in Web browsers.

Also contributing to the prominence of the EMEA region during this period were a number of other high-profile Web-based attacks that occurred there. One example was in January, when another embassy website in Russia was compromised, this time that of the Netherlands. As in the attack above, visitors to the site were misled into installing malicious code.⁵⁵ Another example occurred in August, when several hundred domains in the Netherlands were compromised and defaced.⁵⁶ A third case occurred when more than a thousand UK websites were compromised and users visiting these sites risked being infected with the Asprox Trojan.⁵⁷ The success of these attacks on government sites can be attributed, in part, to the inherent trust that visitors to such sites will have, making these visitors more liable to accept prompts to download files if requested.

Web-based attacks are a major threat to computer networks for both enterprises and end users. Attacks such as drive-by downloads are covert and very difficult to mitigate because most users are unaware that they are being attacked. Organisations are thus confronted with the complicated task of having to detect and filter attack traffic from legitimate traffic. Since many organisations rely on Web-based tools and applications to conduct business, it is likely that the Web will continue to be the primary conduit for attack activity favoured by malicious code developers.

Threat Activity—protection and mitigation

There are a number of measures that enterprises, administrators, and end users can employ to protect against malicious activity. Organisations should monitor all network-connected computers for signs of malicious activity, including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organisations should employ defence-in-depth strategies, including the deployment of antivirus software and a firewall.⁵⁸ Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

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

⁵² https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/vulnerabilities_exploits/article-id/93#M93

⁵³ <https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Honor-Among-Thieves/ba-p/306084#A193>

⁵⁴ <http://blogs.zdnet.com/security/?p=1593>

⁵⁵ http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/

⁵⁶ <http://blogs.zdnet.com/security/?p=1788>

⁵⁷ http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4381034.ece

⁵⁸ Defence-in-depth emphasises multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology.

Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. By creating and enforcing policies that identify and restrict applications that can access the network, organisations can minimise the effect of malicious activity, and hence, minimise the effect on day-to-day operations. Also, administrators should limit privileges on systems for users who do not require such access and they should also restrict unauthorised devices, such as external portable hard-drives and other removable media.

To reduce the likelihood of identity theft, organisations that store personal information should take the necessary steps to protect data transmitted over the Internet or stored on their computers. This should include the development, implementation, and enforcement of a secure policy requiring that all sensitive data is encrypted. Organisations should implement a data loss protection (DLP) solution that not only prevents data breaches, but also mitigates potential data leaks from within an organisation. Access to sensitive information should be restricted and organisations should also enforce compliance to information storage and transmission standards such as the PCI standard.⁵⁹

Policies that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorised individuals should be put in place and enforced. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen. This step should be part of a broader security policy that organisations should develop and implement in order to ensure that any sensitive data is protected from unauthorised access. This would ensure that even if the computer or medium on which the data were lost or stolen, the data would not be accessible. This step should be part of a broader security policy that organisations should develop and implement in order to ensure that any sensitive data is protected from unauthorised access.

⁵⁹ <https://www.pcisecuritystandards.org/>

Malicious Code Trends

Symantec gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Underpinning these products are the Symantec Digital Immune System and Symantec Scan and Deliver technologies, as well as Norton Community Watch, which allow customers to automate the process of reporting viruses and other malicious code threats.

This discussion is based on malicious code samples detected by Symantec in 2008 in the EMEA region, with the following trends being analysed:

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

Malicious code types

Analysing the prevalence of malicious code types provides insight into the general diversity in the threat landscape and, combined with the data of other metrics, helps Symantec more accurately determine emerging trends in malicious code. There were very few variations between the proportions of malicious code types detected in EMEA and those detected globally during 2008. The proportion of Trojans made up 66 percent of the volume of the top 50 potential infections in EMEA, only 2 percent lower than the global proportion at 68 percent (figure 4). This was a minor increase from 2007, when Trojans accounted for 64 percent of the volume of the top 50 potential infections in EMEA.

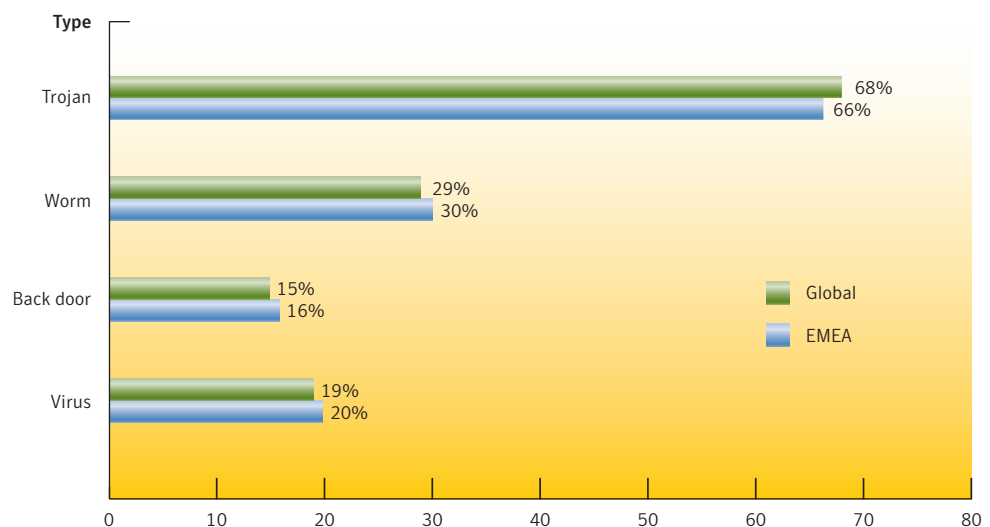


Figure 4. Potential infections by type, EMEA
Source: Symantec

Symantec EMEA Internet Security Threat Report

The previous volume of the Symantec *EMEA Internet Security Threat Report*, discussed the increasing use of Trojans that perform staged attacks, and this trend has continued in 2008.⁶⁰ These types of attacks typically involve an initial compromise, followed by the installation of another piece of malicious code, such as another Trojan that downloads and installs adware.

The proportion of Trojans in EMEA remained relatively static in 2008 and supports the argument that attackers are gravitating toward the use of a smaller number of more successful Trojans.⁶¹ This means that once a Trojan has had a moderate degree of success, minor variations of it are created and used in new attacks. Malicious code developers can use this approach to increase productivity, thereby bolstering the supply of goods for sale in the underground economy.

The rapid deployment of variant threats derived from existing Trojans may additionally benefit developers and attackers by increasing the pressure on security implementations and services. For example, analysing and securing against a significant increase in threats requires increased time and resources on the part of security organisations and enterprises. For this reason, Trojans may have reached a saturation point, insofar as the usefulness of newly developed Trojans is being offset by already well-established and effective Trojans.

Worms were the second most common type of malicious code in EMEA during 2008, accounting for 30 percent of the volume of the top 50 potential infections, which is a small increase from 28 percent in 2007. This percentage was only slightly higher than the 29 percent global proportion of worms. The relatively stable proportion of worms indicates that the declining trend for worms, noted in the previous volume of the Symantec *Global Internet Threat Security Report*, has subsided.⁶² This is partly due to the continued relevance of prominent mass-mailing worms that bolstered worm numbers, and also because of the relatively prolific emergence of the Mabezat worm,⁶³ discussed below.

The percentage of worms may also increase due to the recent and growing success of attacks by the Downadup worm, which propagates by exploiting the Microsoft Windows Server® Service RPC Handling Remote Code Execution Vulnerability.⁶⁴ First identified toward the end of 2008, Downadup continues to attract a lot of attention because of its sophistication and aggressive infection routine.

In 2008, the proportion of back door samples in the volume of the top 50 malicious code samples for EMEA declined to 16 percent—a fairly significant drop from 24 percent in 2007. Similar to the year-over-year decline in back doors globally, this indicates that back doors are not being incorporated into new frontline threats. This is attributed to the trend toward multistage attacks in which back door threats are being employed in the later stages of attacks. Furthermore, one tactic employed in first-stage attacks is to disable or reduce the software capabilities on affected computers, meaning that threats installed during later stages may go undetected. Because of this there may be less need for new unique back doors or Trojans.

Viruses accounted for 20 percent of the volume of the top 50 malicious code samples in EMEA during 2008, slightly higher than the global proportion of 19 percent. This was an increase from 17 percent in 2007. The primary factor of this growth was due to increases in new or existing malicious code that included a virus component, such as the Gammima worm,⁶⁵ which is engineered to steal online gaming credentials. Another notable contributor in this manner is the Mabezat worm, mentioned above, that infects executable files.

⁶⁰ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ga_rpt_istr13_emea_04-2008-13585531-1.en-us.pdf : p. 20

⁶¹ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 49

⁶² http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ga_rpt_istr13_emea_04-2008-13585531-1.en-us.pdf : p. 20

⁶³ http://www.symantec.com/security_response/writeup.jsp?docid=2007-120113-2635-99

⁶⁴ http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99&tabid=3

⁶⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2007-032206-2043-99

Geolocation by type of malicious code

This metric examines the top countries for potential malicious code infections in EMEA by malicious code type. Because of the different propagation mechanisms used by different malicious code types, and the different effects that each malicious code type may have, information about the geographic distribution of malicious code can help network administrators improve their security efforts. Table 7 shows the top three countries in EMEA in 2008 for each of the main malicious code categories.

Rank	Top Countries			
	Back Doors	Trojans	Viruses	Worms
1	United Kingdom	United Kingdom	Egypt	Saudi Arabia
2	Spain	France	Turkey	United Kingdom
3	France	Germany	United Kingdom	Spain

Table 7. Geolocation by type of malicious code, EMEA

Source: Symantec

Back doors

For back doors in 2008, the top three countries were the United Kingdom, Spain, and France, in that order. The most notable change from 2007 is the rise of Spain from fifth to third, bumping Germany to fourth place. These rankings are the result of minor variations in the levels of potential back door infections in each country. The United Kingdom, Spain, and France remain leaders in EMEA for the number of broadband connections.⁶⁶ While Spain and France surpassed Germany in 2008 for the number of potential back door infections, the difference in numbers between the two was low and does not suggest any abnormal back door activity. This indicates that back door activity is proportionally static throughout the EMEA region.

Trojans

In 2008, the United Kingdom ranked first among countries in EMEA for the number of potential Trojan infections, followed by France and then Germany. These countries also ranked in the top three in 2007, when Germany ranked second and France ranked third. These countries also accounted for the highest number of potential infections in EMEA by the four Trojans in the top 10 malicious code samples recorded in 2008. As with back doors, the distribution of Trojans remained largely unchanged during 2008 and is considered to be primarily a reflection of a well-established broadband infrastructure in the region.

Viruses

The top three countries for potential virus infections during this period were Egypt, Turkey, and United Kingdom, in that order. Both Egypt and the United Kingdom were in the top three countries in 2007, although the United Kingdom ranked second in 2007 instead of third. At that time, Symantec speculated that virus activity in Egypt was likely due to the high growth in the number of broadband users combined with a possible lack of security awareness in a relatively inexperienced Internet community.⁶⁷ The same appears to be true in 2008, when prominent viruses, or worms with virus components—such as Sality,⁶⁸

⁶⁶ <http://www.point-topic.com>

⁶⁷ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ga_rpt_istr13_emea_04-2008-13585531-1.en-us.pdf : p. 22

⁶⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2007-011223-3919-99

Pagipef,⁶⁹ and Almanah—⁷⁰ were the most prevalent threats in Egypt by a significant margin. However, the gap between the numbers for the top two countries is significant, with worms being twice as common in Egypt than in second-ranked Turkey.

The reasons for Egypt's prominence in this measurement may be that many Egyptians still primarily use Internet cafés or other publicly accessible shared computers to access the Internet.⁷¹ As noted, public computers used by large numbers of people for a wide variety of purposes have an increased window of exposure to attack. These patterns likely increase the exposure of Egyptians to malicious attacks, including from worms.

Turkey made a substantial jump in rank for potential virus infections, moving from eighth in 2007 up to second in 2008. The reasons for this are similar to those of Egypt. Several prominent viruses and worms with virus components—including Almanah, Gammima, and Pinfi⁷²—dominated the number of potential virus infections in Turkey. The top five threats affecting Egypt and Turkey propagate by copying to removable media or network shares, indicating that there may also be a surge in the use of these technologies in those countries. Turkey is also experiencing high growth in broadband connectivity,⁷³ which would result in a correlating growth in malicious code threats, as is typical of countries with a rapidly growing broadband infrastructure.

Worms

In 2008, Saudi Arabia had the highest number of potential worm infections in EMEA. This is a significant change from 2007, when Saudi Arabia was ranked thirteenth for potential worm infections. This change is attributable to a large increase in potential infections by the Mabezat worm, which is the third most common malicious code family in EMEA in 2008. The United Kingdom and Spain ranked second and third, respectively, for potential worm infections in 2008. These two countries also ranked in the top three for 2007.

The primary explanation for the large number of potential infections in Saudi Arabia is that the outbreak of the Mabezat worm is believed to have originated there. Because Mabezat propagates through removable drives and network shares (along with email), the initial outbreak is likely to have primarily affected computers in relatively close proximity to each other. The initial success of propagation in a concentrated area increases the potential to spread to computers in a similar environment, industry, region, or country before eventually achieving a more balanced distribution.

Top malicious code samples

The top malicious code sample in EMEA during 2008 was the Vundo Trojan,⁷⁴ which is unchanged from 2007 (table 8). Vundo is a prominent threat that was also the top-ranked malicious code sample globally during 2007 and 2008. Additionally, this Trojan was the second most prominent staged downloader globally in 2008. Once this Trojan is installed on a computer, it attempts to contact certain IP addresses in order to download and install its secondary components. One of the files it attempts to install is an adware program that will periodically display pop-up advertisements. In EMEA, the United Kingdom accounted for the most potential infections by Vundo during 2008, followed by France.

⁶⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2007-112909-3431-99

⁷⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99

⁷¹ <http://opennet.net/research/profiles/egypt>

⁷² http://www.symantec.com/security_response/writeup.jsp?docid=2003-011708-2030-99

⁷³ <http://www.point-topic.com>

⁷⁴ http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99

Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact
1	Vundo	Trojan/back door	United Kingdom	France	N/A	Display advertisements, and downloads and installs additional threats
2	Wimad	Trojan	United Kingdom	France	N/A	Exploits DRM technology to download additional threats
3	Gampass	Trojan	United Kingdom	France	N/A	Steals online game account credentials
4	SillyFDC	Worm	Spain	Russia	Mapped and removable drives	Downloads and installs additional threats
5	Mabezat	Worm/virus	Saudi Arabia	United Arab Emirates	SMTP, CIFS, removable drives	Encrypts and infects files
6	Zlob	Trojan/back door	United Kingdom	Germany	N/A	Downloads and installs additional threats
7	Brisv	Trojan	Poland	United Kingdom	N/A	Modifies multimedia files, causing multimedia players to open malicious URLs
8	Gammima	Worm/virus	Turkey	Saudi Arabia	Removable drives	Steals online game account credentials
9	Sality	Worm/virus	Egypt	Russia	Executables	Removes security applications and services
10	Rontokbro	Worm	United Arab Emirates	France	SMTP	Performs DoS attacks

Table 8. Top malicious code samples, EMEA

Source: Symantec

The second most common sample in EMEA during 2008 was the Wimad Trojan.⁷⁵ As with Vundo, the United Kingdom had the highest number of potential Wimad infections, followed by France. Wimad was also the most prevalent downloader component globally during 2008. This Trojan arrives on computers as a licence-protected multimedia file. When the file is opened, the Wimad Trojan exploits the intended functionality of digital rights management (DRM) technology in order to open a browser window and access an attacker-controlled URL. DRM technology normally attempts to open a legitimate DRM-related URL to check a user's access privileges when opening a multimedia file; however, in this case, Wimad changes the URL data to redirect DRM traffic to an attacker-controlled website. When the attacker's Web page is processed, a deceptive social-engineering message is displayed, attempting to entice the user to click a button. If the button is clicked, the Trojan can then download other malicious threats, including adware and spyware.

The third most common malicious code sample in EMEA during 2008 was the Gampass Trojan.⁷⁶ Gampass was the most common malicious code sample in the Asia-Pacific/Japan region (APJ) during 2007 and 2008, and has been steadily gaining prevalence worldwide, as it ranked second globally in 2008. The Trojan steals credentials for online gaming accounts. A significant factor in the growing infection rate of Gampass is that it was the most downloaded component in staged attacks globally during 2008, as discussed in the concurrent Symantec *Global Internet Security Threat Report*. The highest number of potential Gampass infections in 2008 was in the United Kingdom, followed by France.

⁷⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2005-011213-2709-99

⁷⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99&tabid=1

The emergence of the Mabezat worm in EMEA during 2008 is noteworthy. Because this worm was discovered in December 2007, it was not considered in the “Top new malicious code families” metric for 2008; however, the rise of this worm to the fifth highest-ranked malicious code sample in EMEA in 2008 is a testament to its rapid success. Mabezat propagates using SMTP and by copying itself to network shares and removable media. The worm also incorporates a virus component that encrypts and infects a variety of file types, rendering them unusable. The prominence of this worm demonstrates the trend in the resurgence of malicious code that propagates through removable media. Successful threats of this nature are the primary contributors to the increasing popularity of the shared executables as a propagation method, as discussed below in [“Propagation mechanisms.”](#)

Top new malicious code families

The rankings for the top new malicious code families in EMEA in 2008 closely resemble the rankings for the top new malicious code families globally. The Brisv Trojan⁷⁷ was the most common new malicious code family in EMEA in 2008 (table 9); it was also the top new malicious code family globally during this time. In the EMEA region, Poland had the highest number of potential infections by this Trojan, followed by the United Kingdom.

Brisv scans computers for multimedia files including .asf, .mp2, .mp3, .wma and .wmv. The Trojan then modifies a data marker in the files with a malicious URL. Although other applications appear to be unaffected, when the files are opened using Microsoft Windows Media® Player, the marker is automatically processed, causing the application to open a browser window and access the malicious URL, which may in turn expose the victim to additional threats. The effectiveness of this Trojan is heightened by the possibility that unknowing victims will share the malicious multimedia files with other users. As a result, the tainted files can potentially affect users whose computers did not interact with the Trojan itself.

Interestingly, when Brisv scans for multimedia files, it converts all .mp2 and .mp3 files in encounters into the .wma format prior to injecting the malicious code, even while preserving the original file extensions of the (now) converted files. The reason for converting files into the .wma format is so that Windows Media Player will process the injected marker data properly. This is an example of increased sophistication in malicious code development.

⁷⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2008-071823-1655-99

Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact
1	Brisv	Trojan	Poland	United Kingdom	N/A	Modifies multimedia files, causing multimedia players to open malicious URLs
2	Tidserv	Trojan/ back door	United Kingdom	Germany	N/A	Allows remote access, installs additional threats, and displays advertisements
3	Auraax	Worm	Netherlands	Germany	CIFS	Downloads additional threats
4	Blusod	Trojan	United Kingdom	France	N/A	Displays fake antivirus alerts and downloads additional threats
5	Spakrab	Trojan/ back door	United Kingdom	Spain	N/A	Allows remote access and sends spam email
6	Ircbrute	Worm/ back door	United Arab Emirates	Russia	Removable drives	Allows remote access and performs DoS attacks
7	Mebroot	Trojan/ back door	Italy	Spain	N/A	Overwrites the Master Boot Record (MBR) and allows remote access
8	Brojack	Trojan	United Kingdom	Germany	N/A	Modifies Internet settings and removes browser plug-ins
9	Hatihati	Trojan	Egypt	Saudi Arabia	N/A	Installs a pirated version of anti-theft software and sends SMS messages to the attacker
10	Koobface	Worm	United Kingdom	Israel	Social networking sites	Modifies social networking settings to add malicious URLs to user profiles

Table 9. Top new malicious code families, EMEA

Source: Symantec

The Tidserv⁷⁸ Trojan was the second most common new malicious code family in EMEA during 2008, and it ranked fourth globally. The United Kingdom and Germany accounted for the first and second highest number of potential infections by Tidserv, respectively. The Tidserv Trojan first installs a rootkit in order to obfuscate its presence on a computer, and then opens a back door.⁷⁹ Additionally, Tidserv displays advertisements and downloads additional malicious threats, which indicates that there may be financial motivation behind the distribution of the Trojan. These ads are hosted remotely and, much like legitimate Internet advertising, the attacker can rotate the ads as desired.

The Auraax⁸⁰ worm was the third most common new malicious code family in EMEA during this reporting period. Auraax also ranked third globally. The Netherlands and Germany had the first and second highest number of potential Auraax infections. This worm propagates by copying itself to all removable drives and network shares that it can locate. An autorun instruction file is also created in these drives or shares that automatically executes Auraax whenever the drives or shares are accessed.⁸¹ The worm obfuscates itself by overwriting certain kernel drivers with a rootkit to avoid detection. This worm also downloads additional malicious code onto compromised computers.

⁷⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2008-091809-0911-99&tabid=1

⁷⁹ A collection of tools (programs) that enable administrator-level access to a computer or network.

⁸⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2008-092409-4704-99&tabid=2

⁸¹ Autorun is a function of the Windows operating system that launches newly detected processes or applications (e.g., the insertion of a CD-ROM or USB drive). Windows searches the root directory of the drive for an autorun information file that contains instructions for what process or application to launch.

Auraax protects itself on affected computers by modifying the “hosts” file to prevent users from accessing a variety of computer security websites.⁸² The URLs of these sites are added to the hosts file and configured so that access to the URLs is redirected to the local address. Interestingly, Auraax also adds several advertising websites to the hosts file and makes them inaccessible. This is somewhat peculiar behaviour because malicious code is sometimes used to distribute advertisements and increase hits to advertising Web pages, rather than to hide them. This could be because some of the additional threats downloaded by Auraax attempt to target and replace legitimate advertisements. By making the destination websites inaccessible, the worm may be attempting to increase the chances that URLs in the illegitimate advertisements are accessed instead of the legitimate advertisements. This could be particularly deceiving for users because the maliciously placed advertisements may appear in the same locations and styles as those of the legitimate advertisements.

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats may expose sensitive data such as system information, confidential files and documents, or logon credentials. Some malicious code threats, such as back doors, can give a remote attacker complete control over a compromised computer. Threats to confidential information are a particular concern because of their potential for use in fraudulent 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 an enterprise, the exposure of confidential information can lead to significant data leakage. If it involves customer-related data such as credit card information, customer confidence in the enterprise can be severely undermined. Moreover, it can also violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies, could also be leaked from compromised computers.

Eighty-seven percent of the threats to confidential information identified in EMEA during 2008 were classified as allowing remote access (figure 5), a decrease from 94 percent in 2007. This was 4 percent higher than the global percentage of 83 percent. This decrease is mainly attributable to the previously discussed decrease in the percentage of potential infections from back doors. The underlying reason may also be that attackers are less interested in administering individually compromised computers than they are in harvesting the compromised assets, which can be accomplished without installing a back door. For example, keystroke-logging applications can be automated so that there is little interaction required by the attacker after the initial attack. Back doors, on the other hand, frequently require an added degree of interaction after they are successfully established on a compromised computer.

⁸² The “hosts” file contains a list of hostnames mapped to IP addresses. This information is used by computers, in conjunction with or in lieu of DNS (domain name system), to locate nodes on the network.

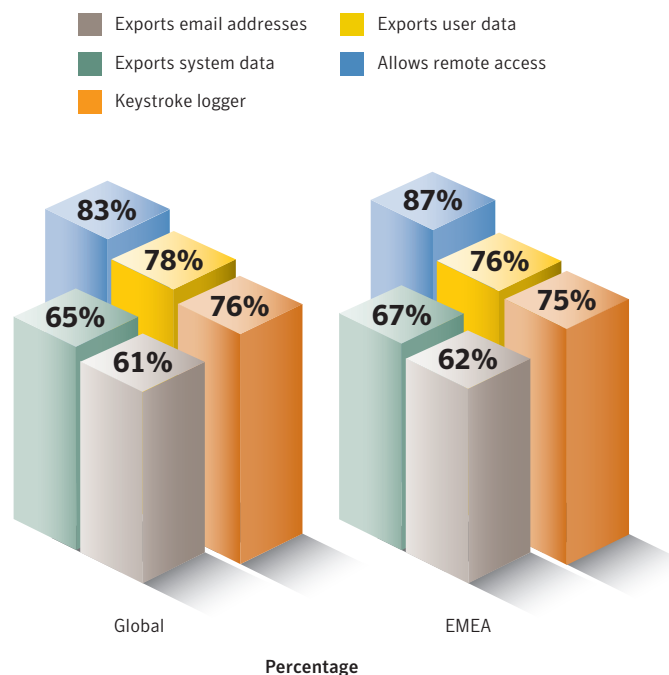


Figure 5. Threats to confidential information, EMEA and global
 Source: Symantec

In 2008, 76 percent of threats to confidential information in EMEA were classified as threats that export user data; this is similar to 2007 when 75 percent of malicious code infections were thus classified, and only slightly less than the global classification in 2008 of 78 percent. Threats that are capable of this type of information exposure are favourable to criminals because leaked data can be used to steal a user’s identity or aid in further attacks. Increases in this type of exposure are not surprising considering the potential value of harvested information. For example, the sale of bank account credentials ranges between \$10 and \$1,000 in the underground economy, and credit card numbers with CVV2 numbers can be sold for as high as \$30 each.⁸³

The third most prevalent threat to confidential information of the top 50 malicious code samples in EMEA in 2008 was keystroke loggers, with 75 percent of malicious code infections having this capability; this is an increase from 67 percent in 2007 and was similar to the 2008 global percentage of 76 percent. Successfully installed keystroke loggers record keystrokes on compromised computers and then return the data to the attacker. This can be achieved by emailing it to the attacker or by uploading the data to an attacker-controlled website. The attacker can process the keystroke data to extract user account credentials such as those for online banking websites, stock-trading websites, or online game accounts. Additional data, such as information typed in email messages or other documents, could also be exposed. This information can then be sold in the underground economy or used to launch further attacks.

⁸³ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 77

Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These means are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), Simple Mail transfer protocol (SMTP), Common Internet File System (CIFS), P2P, and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised via a back door server and using it to upload and install itself. This metric will discuss the most popular propagation mechanisms that were detected being used by malicious code samples in EMEA in 2008.⁸⁴

Malicious code that propagated as shared executable files accounted for 65 percent of potential infections in EMEA, compared to the global proportion of 66 percent (table 10). Shared executable files are a propagation vector used by viruses as well as worms to copy themselves to removable media. The popularity and increased use of USB-based media, such as removable drives or media players, have resulted in a resurgence of malicious code that propagates using shared executable files. The relatively large capacity available on many current portable USB devices may result in malicious code going largely unnoticed. Furthermore, the autorun functionality on these devices is an attractive mechanism for attackers because it can allow malicious code to be launched without direct user interaction. Many high-profile worms use this mechanism, including four of the top malicious code samples in the EMEA region—Mabezat, SillyFDC,⁸⁵ Sality, and Gammima. It is interesting to note that, as previously discussed, the Mabezat worm uses this mechanism to propagate along with email and network sharing—all of which account for the top three propagation mechanisms in 2008.

EMEA Rank	Propagation Mechanism	EMEA Percentage	Global Percentage
1	File sharing executables	65%	66%
2	File transfer/email attachment	34%	31%
3	File transfer/CIFS	33%	30%
4	Remotely exploitable vulnerability	11%	12%
5	File sharing/P2P	8%	10%
6	SQL	3%	3%
7	Back door/Kuang2	3%	3%
8	Back door/SubSeven	3%	3%
9	File transfer/Embedded HTTP URI/instant messenger	2%	4%
10	File transfer/instant messenger	2%	2%

Table 10. Top propagation vectors, EMEA

Source: Symantec

⁸⁴ 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.

⁸⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

To limit the propagation of threats that propagate through removable drives, administrators should ensure that all such devices are scanned for viruses when they are connected to a computer. If removable drives are not needed within the enterprise, endpoint security and policy can prevent computers from recognising these drives when they are attached. Additionally, policies and user education policies should be implemented to prevent users from attaching unauthorised devices to computers within the enterprise. Disabling autorun, or similar functionality, can also deny attempted attacks.⁸⁶

In 2008, 34 percent of malicious code in the EMEA region propagated via email attachments, slightly more than the 31 percent measured globally. This remains relatively consistent with the percentage from 2007, which was 35 percent. Two of the top malicious code samples in EMEA—Mabezat and Rontokbro⁸⁷—propagate using this mechanism. This indicates that this mechanism continues to remain a common and reliable means of propagation in the region.

In 2008, 33 percent of the top 50 malicious code samples in EMEA used the Common Internet File Sharing (CIFS) protocol to propagate, slightly higher than the 30 percent recorded globally. This is also an increase from the 25 percent recorded in 2007 and is primarily attributable to the prominence of the Mabezat worm on top of other threats such as Fujacks,⁸⁸ Almanah, and Pinfi, which have all ranked in the top 50 malicious threats in EMEA during previous years.

To protect against threats that use the CIFS protocol to propagate, all shared directories or files should be protected with strong passwords, and only users who require the resources should be given access to them. If other users do not need to write to a shared directory or file, they should only be given “read” permissions. This will prevent malicious code from copying itself to the shared directory or modifying shared files. Finally, CIFS shares should not be exposed to the Internet. Blocking TCP port 445 at the network boundary will help to protect against threats that propagate using CIFS.

Malicious code—protection and mitigation

It is critical that end users and enterprises maintain the most current antivirus definitions to protect against the high quantity of new malicious code threats. IDS, IPS, and other behaviour-blocking technologies should also be employed to prevent compromise by new threats. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.

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

⁸⁶ https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/grab_bag/article-id/109

⁸⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2008-021916-0751-99

⁸⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111415-0546-99

To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of IPS technologies can prevent exploitation of browser and plug-in vulnerabilities through signatures and behaviour-based detection, in addition to address space layout randomization (ASLR).⁸⁹ End users should employ defence-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

⁸⁹ ASLR is a security mechanism that randomises data in memory to prevent the success of attacks that leverage memory corruption vulnerabilities, such as buffer overflows.

Phishing and Spam Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organisation by mimicking (or spoofing) a specific brand, usually one that is well known, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Phishing generally requires an end user to enter his or her credentials into an online data entry field. This is one of the characteristics that distinguishes phishing from spam-based scams (such as the widely disseminated 419 scam and other social engineering scams).⁹⁰ The data that end users enter can then be used for fraudulent purposes.

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 because it can be used to deliver Trojans, viruses, and phishing attempts.⁹¹ Spam can also be used to deliver drive-by downloaders, which require no other end-user interaction than navigation to the URLs contained in the spam messages. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email gateways.

The results used in this analysis are based on data returned from the Symantec Probe Network, as well as 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 Symantec 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, this network is continuously optimised in order to attract new varieties of spam attacks.

In addition to the Symantec Probe Network, phishing information is also gathered through the Symantec Phish Report Network, which is an extensive antifraud community of organisations and end users.⁹² Members of the Symantec Phish Report Network contribute and receive fraudulent website addresses for alerting and filtering across a broad range of solutions.

This section will discuss the following trends that Symantec identified in the EMEA region in 2008:

- Top countries hosting phishing websites and top targeted sectors
- Top countries of spam origin

Top countries hosting phishing websites and top targeted sectors

This metric will assess the EMEA countries in which the most phishing websites were hosted, and the most popular sector targeted within each country. This data is a snapshot in time, and does not offer insight into the changes in the locations of certain phishing sites since the data was analysed. It should also be noted that the fact that a phishing website is hosted in a certain country does not necessarily mean that the attacker is located in that country.

⁹⁰ http://nortontoday.symantec.com/features/security_at_30.php

⁹¹ <http://news.bbc.co.uk/2/hi/technology/6676819.stm>

⁹² <http://www.phishreport.net/>

Poland hosted the highest percentage of phishing websites in EMEA in 2008, with 18 percent of the regional total (table 11). This is a significant change from 2007, when Poland was the site of only 4 percent of phishing websites and the eighth-ranked country in this category. As it was for all countries in the top ten, the top sector most frequently spoofed by phishing websites based in Poland in 2008 was the financial sector, which accounted for 90 percent of the total. This is not surprising, as financial service organisations were spoofed by 76 percent of all detected lures worldwide in 2008.

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	2008 Top Targeted Sector	Percentage of Lures in Country Targeting Top Sector
1	8	Poland	18%	4%	Financial	90%
2	4	France	11%	10%	Financial	74%
3	5	Russia	10%	8%	Financial	54%
4	1	Germany	9%	15%	Financial	70%
5	2	United Kingdom	9%	13%	Financial	77%
6	6	Italy	6%	8%	Financial	57%
7	3	Netherlands	6%	11%	Financial	57%
8	7	Israel	5%	6%	Financial	63%
9	9	Spain	5%	3%	Financial	71%
10	11	Turkey	3%	2%	Financial	81%

Table 11: Top countries hosting phishing websites and top targeted sectors

Source: Symantec

France had the second highest percent of EMEA-based phishing websites in 2008, with 11 percent of the total. This is a slight increase from 2007, when France hosted 10 percent of phishing websites, fourth most in EMEA for that period. The percentage of lures targeting the financial sector for France in 2008 was 74 percent.

Russia had the third highest number of phishing websites in EMEA in 2008, with 10 percent. This is an increase over 2007, when it was the fifth ranked country with 8 percent of phishing websites. Russia had the eighth highest percentage of malicious activity in EMEA in 2008, with 6 percent of the regional total. This is the same rank as 2007 but an increase in the percentage of lures, which was 4 percent in that year. The percentage of lures targeting the financial sector for Russia in 2008 was 54 percent.

Phishing lures predominantly targeting the financial sector demonstrates how focused phishers are on financial gain. Brands and activities associated with the financial sector are most likely to yield data that could be used in financially motivated attacks, such as bank account credentials. As a result, it is not surprising that the majority of phishing activity targets the financial sector.

Many phishing attacks that spoof financial services brands will prompt users to enter credit card information or banking credentials into fraudulent sites. If this is done, the phishers can then capture and sell such information in the underground economy. This has been made easier for phishers because of the increasingly widespread acceptance of online banking. For example, 44 percent of Internet users in the United States perform some degree of online banking, as do 64 percent of users in Canada and 46 percent of those in France.⁹³ Because of this, end users may be more easily fooled into entering their information into fraudulent websites that mimic the brand of their financial services provider.

Top countries of spam origin

This section will discuss the top 10 countries of spam origin in EMEA in 2008. 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 compared. Each IP address is mapped to a specific country and charted over time. The nature of spam and its distribution on the Internet presents challenges in identifying the location of people who are sending it because many spammers try to redirect attention away from their actual geographic locations. In an attempt to bypass DNS block lists, they use Trojans that relay email, which allows them to send spam from sites distinct from their physical location. In doing so, they tend to focus on compromised computers in those regions with the largest bandwidth capabilities. As such, the region in which the spam originates may not correspond to the region in which the spammers are located.

The highest percentage of spam detected in EMEA in 2008 originated in Russia, with 14 percent of the total (table 12). This is an increase from 2007, when 10 percent of spam originated from Russia and it was the third highest country of origin. Worldwide, Russia accounted for 6 percent of all originating spam. While it accounted for a relatively small percentage of worldwide spam, the amount of spam originating in Russia increased significantly—by 445 percent over the course of 2008.

⁹³ <http://www.comscore.com/press/release.asp?press=2524>

2008 EMEA Rank	2007 EMEA Rank	2008 Global Rank	Country	2008 EMEA Percentage	2007 EMEA Percentage
1	3	2	Russia	14%	10%
2	8	3	Turkey	13%	4%
3	1	6	United Kingdom	7%	15%
4	4	7	Germany	6%	9%
5	5	8	Italy	6%	6%
6	2	9	Poland	6%	10%
7	6	10	Spain	5%	6%
8	7	13	France	5%	6%
9	20	19	Romania	3%	1%
10	10	20	Netherlands	3%	1%

Table 12. Spam country of origin, EMEA

Source: Symantec

As was discussed in the [“Bot command-and-control servers by country”](#) discussion, Russia had the most bot C&C servers in EMEA in 2008, with 20 percent of the total, and was third-ranked in the world. Russia had the fourth highest volume of spam zombies in EMEA in 2008.

The increase in spam activity originating in Russia is likely due to two factors. First, broadband connectivity in Russia is increasing more rapidly than in almost any other country.⁹⁴ Second, many observers believe that organized crime activity in Russia includes a significant degree of online fraud.⁹⁵ By way of illustration, 13 percent of malicious websites that were detected by Symantec in 2008 were located in Russia, as noted in the [“Top countries of origin for Web-based attacks”](#) discussion in this report. This could mean that legitimate Web-hosting space has been compromised for malicious use. Since many Web-hosting accounts also include access to email accounts, the attackers could also use the compromised account to relay spam through the host’s mail servers.

Turkey had the second highest volume of spam detected in EMEA in 2008, with 13 percent of the total. This is a significant increase from 2007, when 4 percent of spam detected in EMEA originated in Turkey and it was the eighth-ranked country. Worldwide, Turkey had the third highest volume of spam in 2008, with 5 percent of all detected spam. This is a significant increase from 2007 when Turkey had the fifteenth highest volume of spam, with just 1 percent. Not only is this a considerable jump in rankings, but the volume of spam originating in Turkey increased by nearly 1,200 percent.

Turkey also had 9 percent of the bot-infected computers in EMEA in 2008, the fifth highest total in the region. This is a significant increase from 2007 when only 4 percent of bots in EMEA were located in Turkey. Bots are often used to disseminate spam, so the high number of bots in Turkey contributed to the high volume of spam originating there.

The volume of spam originating in Turkey in 2008 was not steady, but rather increased from August until the end of the year. During that time, Turkey was the second-ranked country of origin, with the volume of spam varying from six to 8 percent of the global total.⁹⁶ This may be related to the migration of bot C&C servers following the shutdown of a number of ISPs during the same period. Analysts believe that these ISPs were being used by spammers to distribute their attacks.⁹⁷ Therefore, spammers would have been forced to

⁹⁴ MessageLabs Intelligence: 2008 Annual Security Report http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 29

⁹⁵ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 78

⁹⁶ http://www.symantec.com/business/theme.jsp?themeid=state_of_spam#

⁹⁷ Cf. http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html, http://www.crn.com/security/212002220_or http://www.messagelabs.com/mlireport/MLIReport_2008.09_Sep_Final.pdf

procure new service providers following the shutdown of their preferred ISPs. A noticeable increase in spam activity originating in Turkey suggests that a sizeable proportion of spammers relocated their spam servers to bot-infected computers in that country.

The United Kingdom was the country of origin for the third highest volume of EMEA-based spam, with 7 percent of the regional total. This is a considerable drop-off from 2007, when it was the top-ranked country, accounting for 15 percent of spam originating in the region. Because this discussion is assessed on a percentage basis, it is likely that the drop in the percentage of spam originating in the United Kingdom is due more to an increase in activity originating in Russia and Turkey rather than a decrease in the absolute volume originating in the United Kingdom.

Phishing and spam—protection and mitigation

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

DNS block lists also offer protection against potential phishing emails.⁹⁸ Organisations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.⁹⁹

To protect against potential phishing activity, administrators should always follow Symantec best practices, as outlined in Appendix A of this report. Symantec also recommends that organisations educate their end users about phishing.¹⁰⁰ They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, and provide a means to report suspected phishing sites.¹⁰¹

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

Organisations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.¹⁰² So-called typo domains and homographic domains should also be monitored.¹⁰³ This can be done with the help of companies that specialise in domain monitoring; some registrars also provide this service.

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

End users should follow best security practices, as outlined in Appendix A of this report. They should use an antiphishing solution. As some phishing attacks may use spyware and/or keystroke-logging applications, Symantec advises end users to use antivirus software, antispam software, firewalls, toolbar blockers, and

⁹⁸ 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.

⁹⁹ 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.

¹⁰⁰ Cf. <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm> for a guide on how to avoid phishing

¹⁰¹ Cf. <http://www.antiphishing.org> for information on the latest phishing threats

¹⁰² "Cousin domains" refers to domain names that include some of the key words of an organisation's domain or brand name; for example, for the corporate domain "bigbank.com", cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.

¹⁰³ Typo domains are domain names that use common misspellings of a legitimate domain name, for example the domain "symantec.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".

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.¹⁰⁴ Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

Consumers could also take more security precautions to ensure that their information will not be compromised. When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not public ones. Further, they should not store passwords or bank card numbers. They should also avoid following links from within messages (whether in email, instant messages, online forums, etc.) as these may be links to spoofed websites; instead, they should manually type in the URL of the website. Also, consumers should be aware of the amount of personal information that they post on the Internet, as criminals may take advantage of this public information in malicious activities such as phishing scams.

¹⁰⁴ <http://www.fbi.gov/majcases/fraud/internetschemes.htm>

Appendix A—Symantec Best Practices

Enterprise best practices

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

Consumer best practices

- Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Keep virus definitions updated regularly. By deploying the latest virus definitions, you can protect your computer against the latest viruses known to be spreading in the wild.
- Routinely check to see if your operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- Deploy an antiphishing solution. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
- Get involved by tracking and reporting attack attempts. 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.
- 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.
- Avoid clicking on links and/or attachments in email or IM messages, as these may also expose computers to unnecessary risks.
- Read end-user licence agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or as a consequence of that acceptance.
- Be aware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. These ads may be spyware.

Appendix B—Threat Activity Trends Methodology

Threat activity 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, the Symantec Honeypot network, and proprietary Symantec technologies. Symantec combines data derived from these sources for analysis.

Malicious activity by country

To determine the top countries for the “Malicious activity by country” metric, Symantec compiles geographical data on each type of malicious activity to be considered, namely: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The proportion of each activity originating in each country is then determined. The mean of the percentages of each malicious activity that originates in each country is calculated. This average determines the proportion of overall malicious activity that originates from the country in question and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Bot-infected computers

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

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

Bot command-and-control servers

Symantec tracks the number of new bot C&C servers detected worldwide. Only IRC and HTTP bot C&C server trends will be evaluated in the methods botnet owners are using to communicate with their bot-infected computers.

Top Web-based attacks

To evaluate this metric, Symantec identifies each distinct attack delivered via the Web, hereafter referred to as Web-based attack, hosted on malicious websites that are detected by intrusion prevention technology. A Web-based attack is any attack that is carried out against a client-side application originating from the Web. Symantec determines the top Web-based attacks by determining the most common attacks carried out against users. Due to the nature of Web-based attacks, the total number of attacks carried out is a good measure of the success and popularity of the attack.

Each attack discussed targets a specific vulnerability or weakness in Web browsers or other client-side applications that process content originating from the Web. These attacks can vary in their delivery methods; some rely on misleading a user into downloading a malicious file, while others occur without any knowledge or interaction by the user.

Top countries/regions of origin for Web-based attacks

Web-based attacks can be found globally and Symantec identifies each by an associated distinct detection signature. Most attack types target specific vulnerabilities or weaknesses in Web browsers or other client-side applications that process content originating from the Web. Note that the server hosting the exploit may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects his or her Web browser to a malicious server in another country or region.

Appendix C—Malicious Code Trends Methodology

Malicious code trends are based on statistics from malicious code samples reported to Symantec for analysis. The data is gathered from over 130 million client, server, and gateway systems that have deployed Symantec's antivirus products in both consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. Observations in this section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from the two databases described below.

Infection database

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

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

Malicious code database

In addition to infection data, Symantec Security Response analyses and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, a historical trend analysis was performed on this database to identify, assess, and discuss any possible trends, such as the use of different infection vectors and the frequency of various types of payloads. In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the *Symantec 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 and Spam Methodology

Phishing and spam attack trends in this report are based on the analysis of data captured through the Symantec Probe Network, a system of more than 2.5 million decoy accounts, MessageLabs Intelligence, and other Symantec technologies in more than 86 countries around the globe. Over eight billion email messages, as well as over one billion Web requests, are scanned per day across 16 data centres. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

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

Symantec Brightmail AntiSpam data is also used to gauge the growth in phishing attempts as well as the percentage of Internet mail determined to be phishing attempts. Data returned includes 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 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.

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.

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 warrant additional detail.

Top countries hosting phishing websites

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

Top countries 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 summarised by country based on monthly totals. The percentage of spam per country is calculated from the total spam detected in the field.

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

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 providing security, storage, and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

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

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

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
04/09 20016964