SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Internet Security Threat Report

April 2010

Regional Data Sheet—Europe, Middle East, and Africa

An important note about these statistics

The statistics discussed in this document are based on attacks against an extensive sample of Symantec customers. The attack activity was detected by the Symantec™ Global Intelligence Network, which includes Symantec Managed Security Services and Symantec DeepSight™ Threat Management System, both of which use automated systems to map the IP address of the attacking system to identify the country in which it is located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker.

Introduction

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 and territories 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 133 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.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 5 million decoy accounts; MessageLabs Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries. Over 8 billion email messages, as well as over 1 billion Web requests, are processed 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 *Internet Security Threat Report*, which gives enterprises and consumers the essential information to effectively secure their systems now and into the future.

In addition to gathering Internet-wide attack data for the Symantec *Global Internet Security Threat Report*, Symantec also gathers and analyses attack data that is detected by sensors deployed in specific regions. This regional data sheet will discuss notable aspects of malicious activity Symantec has observed in the Europe, Middle East, and Africa (EMEA) region in 2009.

Highlights

Threat Activity Trends Highlights

- Germany was the source of the highest percentage of malicious activity observed by Symantec in the EMEA region in 2009, accounting for 12 percent of the total, a decrease from 14 percent in 2008. Globally, Germany ranked fourth for malicious activity by country in 2009, with 5 percent of the total.
- The United States was the top country of origin for attacks detected by EMEA-based sensors in 2009, accounting for 36 percent of all detected attacks; this is an increase from 28 percent in 2008, when it also ranked first in EMEA. The United States was also the top country of origin for attacks detected against targets globally in 2009, with 23 percent of the worldwide total.
- In 2009, the most common Web-based attack targeting the EMEA region was related to malicious PDF activity, which accounted for 56 percent of the regional total. This was also the top Web-based attack observed globally in 2009, accounting for 49 percent of the worldwide total.
- In 2009, the United Kingdom was the top country of origin for Web-based attacks that targeted the EMEA region, with 12 percent of the total. Ukraine was the top country of origin for Web-based attacks targeting EMEA in 2008, with 31 percent of the total at that time.
- In 2009, Symantec observed an average of 19,500 active bots per day in the EMEA region; this is a 39 percent decrease from 2008, when Symantec observed an average of 32,188 active bots per day in the EMEA region.
- Germany was the top country for bot-infected computers in the EMEA region for 2009, with 14 percent of the total. In 2008, Spain was the top-ranked country in EMEA for bot-infected computers with 15 percent of the total. Globally in 2009, Germany ranked fifth with 7 percent of the total for bot-infected computers.
- Lisbon was again the top city in EMEA for bot infections in 2009, with 8 percent of the total—up from 5 percent in 2008.
- In 2009, Symantec identified 12,362 distinct bot command-and-control servers in EMEA, of which 47 percent were controlled through IRC channels and 53 percent through HTTP. In 2008, Symantec identified 5,147 distinct bot command-and-control servers in EMEA, of which 40 percent operated through IRC channels and 60 percent through HTTP.
- In 2009, Germany was the top country for bot command-and-control servers in EMEA, with 24 percent of the regional total. In 2008, Russia was the top country for bot command-and-control servers in EMEA, with 20 percent of the regional total during that period. Germany ranked second in this measurement globally in 2009, with 11 percent of the worldwide total.

Malicious Code Trends Highlights

- The Sality.AE virus was the top malicious code sample by potential infection in the EMEA region in 2008, replacing the Vundo Trojan from the year previous. Sality.AE was also the top malicious code sample causing potential infection globally in 2009.
- The Induc virus was the top new malicious code family reported in the EMEA region in 2009, as it was globally.
- In 2009, 49 percent of the volume of the top 50 potential infections in the EMEA region were classified as worms—an increase from 30 percent in 2008.
- In the EMEA region in 2009, the United Kingdom was the top-ranked country for potential infections by back doors and Trojans, Egypt was the top-ranked country for viruses, and Saudi Arabia was the top-ranked country for worms.
- In the EMEA region in 2009, 85 percent of confidential information threats had remote access capabilities, a slight decrease from 87 percent in the previous reporting period.
- The most common propagation method for malicious code in EMEA in 2009 was through shared executable files, accounting for 77 percent of potential infections—an increase from 65 percent in 2008.

Phishing and Spam Trends Highlights

- In 2009, Spain hosted the highest percentage of phishing URLs in the EMEA region, with 11 percent of the total. Eighty-eight percent of the phishing URLs in Spain in 2009 targeted the financial services sector.
- In 2009, 24 percent of all spam detected by Symantec worldwide originated in EMEA. On a per-country basis, 10 percent of all spam detected in EMEA originated in Poland. In 2008, Russia was the top-ranked country for originating spam in EMEA, with 13 percent of the total at that time. Poland ranked fifth globally in 2009, with 4 percent of spam detected worldwide.

Threat Activity Trends

This section will discuss the following metrics:

- Malicious activity by country
- Attack origin by country
- Web-based attacks by type
- Web-based attacks by country
- Bot-infected computers
- Bot-infected computers by country

Malicious activity by country

This metric will assess the countries in the EMEA region in which the highest amount of malicious activity took place or originated in 2009. To determine this, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing hosts, bot-infected computers, and attack origins. The rankings are determined by calculating the average of the proportion of these malicious activities that originated in each country.

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections make attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, an increased probability of constantly connected systems, and typically more stable connections. Symantec has also noted in the past that malicious activity in a country tends to increase in relation to growth in broadband infrastructure. One particular reason for this is that new users may be unaccustomed to, or unaware of, the increased risk of exposure to malicious attacks from such robust connections.

Germany was the top-ranked country for malicious activity in EMEA in 2009, with 12 percent of the regional total (table 1). This is a decrease from 14 percent in 2008, when Germany also ranked first in EMEA. Globally in 2009, Germany ranked fourth in this measurement, accounting for 5 percent of the worldwide total—a decrease from third rank and 6 percent in 2008. Germany has a well-established broadband infrastructure, with the highest number of broadband users in the EMEA region.[1] Germany ranked first in EMEA in phishing hosts, bot-infected computers, and attack origin. Globally, Germany ranked second in phishing hosts, fifth in bot-infected computers, and third in attack origin by country.

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

EMEA Rank 2009	EMEA Rank 2008	Country	Percentage 2009	Percentage 2008	2009 Activity Rank: Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	Germany	12%	14%	10	4	1	1	1
2	2	United Kingdom	9%	11%	1	8	4	8	2
3	8	Russia	8%	6%	5	1	3	11	6
4	6	Poland	7%	6%	11	2	5	4	8
5	3	Spain	7%	9%	6	6	7	3	5
6	4	Italy	7%	8%	8	5	10	2	4
7	7	Turkey	6%	6%	4	3	11	5	7
8	5	France	6%	7%	9	14	6	6	3
9	14	Romania	4%	2%	14	9	2	31	11
10	18	Hungary	2%	1%	38	16	9	9	16

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

The United Kingdom ranked second for malicious activity in the EMEA region in 2009, with 9 percent of the regional total. This is a decrease from 11 percent in 2008, when it also ranked second. Globally, the United Kingdom ranked sixth for malicious activity, down from fourth in 2008. The United Kingdom's high ranking in this metric is primarily due to its high volume of malicious code activity, for which it ranked first in EMEA in 2009. The United Kingdom also ranked second for originating attacks in 2009 in EMEA. Notably, the United Kingdom has the second-highest number of broadband users in the EMEA region.[2]

Russia ranked third for malicious activity in the EMEA region in 2009, accounting for 8 percent of the total. In 2008, Russia ranked eighth in this metric, with 6 percent of the total. Globally in 2009, Russia accounted for 3 percent of all malicious activity, the seventh-highest percentage observed. In specific activity measurements in 2009, Russia ranked first in EMEA for phishing hosts.

Attack origin by country

This discussion measures the top countries of originating attacks targeting the EMEA region in 2009. An attack is generally considered to be any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS), intrusion prevention system (IPS), or firewall.

In 2009, the United States was the top country of origin for attacks against EMEA targets, accounting for 36 percent of all attacks detected by Symantec sensors in the region (table 2). This result is likely due to the high level of attack activity originating in the United States generally, as it was also the top country for originating attacks globally, with 23 percent of the total worldwide. It also ranked first for overall global malicious activity, with 19 percent of that total.

[2] Ibid

EMEA Rank 2009	EMEA Rank 2008	Country	Percentage 2009 EMEA	Percentage 2008 EMEA	Percentage 2009 Global
1	1	United States	36%	28%	23%
2	3	United Kingdom	14%	10%	6%
3	4	France	6%	4%	4%
4	2	China	5%	14%	12%
5	17	Singapore	3%	1%	<1%
6	9	Netherlands	3%	2%	1%
7	6	Germany	3%	3%	9%
8	7	Russia	2%	3%	2%
9	16	Australia	2%	1%	2%
10	8	Canada	2%	3%	2%

Table 2. Top countries of attack origin targeting EMEA
Source: Symantec

As noted above, malicious activity is most often associated with computers that are connected to high-speed broadband Internet. The United States ranks second worldwide for broadband subscribers, behind only China (which ranked fourth for originating attacks targeting EMEA in 2009, with 5 percent of the total).[3] Furthermore, the United States had the highest number of bot-infected computers globally in 2009, and much of the attack activity targeting EMEA countries would have been conducted through these bot networks.

The United Kingdom and France ranked second and third, respectively, for attacks targeting the region in 2009. The United Kingdom accounted for 14 percent of all EMEA-directed attacks, while France accounted for 6 percent of the total. The regional percentages of originating attacks for the United Kingdom and France were higher than their global percentages, indicating that attacks originating in of these two countries may have been targeting the EMEA region specifically.

Previous editions of the Symantec *Internet Security Threat Report* have noted that attacks often target the region in which they originate due to proximity, shared language, or similar social and cultural interests.[4] It is also likely that targets within the region are of more interest to attackers based there than are external targets. Of the top 10 countries of origin for attacks targeting EMEA, five are located in the region itself.

Web-based attacks by type

This metric will assess the top distinct Web-based attacks in the EMEA region in 2009. This includes those originating from legitimate sites that have been compromised as well as from websites that are specifically developed for malicious purposes that targeted Web users. During this reporting period, the most common Web-based attack targeting the EMEA region was related to malicious PDF activity, which accounted for 56 percent of the regional total (table 3).[5] This attack also ranked first globally, while ranking third in the Asia-Pacific/Japan (APJ) region in 2009.

[3] http://www.websiteoptimization.com/bw/0812/
[4] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_v.pdf : p. 11
[5] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153

Specifically, this attack consists of attempts by attackers to distribute malicious PDF content to victims through the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious PDF file would be designed to exploit arbitrary vulnerabilities in applications that are able to process this type of file.

Rank	Attack	Percentage
1	PDF Suspicious File Download	56%
2	MSIE ADODB.Stream Object File Installation Weakness	14%
3	HTTP MSIE WPAD Spoofing Vulnerability	9%
4	HTTP MSIE Malformed XML Buffer Overflow	3%
5	HTTP Adobe® SWF Remote Code Execution	3%
6	HTTP MSIE7 Uninitialized Memory Code Execution	2%
7	HTTP MS MPEG2TuneRequestControl ActiveX Instantiation	2%
8	MSIE DHTML CreateControlRange Code Execution	1%
9	HTTP MSIE COM Object Memory Corruption	1%
10	MSIE Popup Window Address Bar Spoofing Weakness	1%

Table 3. Top Web-based attacks, EMEA
Source: Symantec

The second most common Web-based attack observed in EMEA in 2009 was related to the Microsoft® Internet Explorer® ADODB.Stream Object File Installation Weakness vulnerability.[6] This vulnerability accounted for 14 percent of Web-based attacks in the region during this reporting period. This vulnerability allows attackers to install malicious files on a vulnerable computer when a user visits a website hosting an exploit. This issue was published on August 23, 2003, and fixes have been available since July 2, 2004.

In 2009, the third most common Web-based attack in EMEA exploited the Microsoft Internet Explorer WPAD Spoofing Vulnerability.[7] This attack accounted for 9 percent of Web-based attacks in EMEA in 2009. This vulnerability allows attackers to trick the application's automatic proxy configuration feature to use a non-authorised server as a proxy server. This would allow an attacker on a different network to read Web traffic from the application. This issue was published on December 2, 1999, and fixes have been available since that time. The fact that this vulnerability is still highly ranked 10 years after it was discovered indicates that a great number of computers in the region remain unpatched against it.

[6] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or http://www.securityfocus.com/bid/10514
[7] Please see http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=22689 or http://www.securityfocus.com/bid/846

Web-based attacks by country

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.

In 2009, the United Kingdom ranked as the top country of origin for Web-based attacks in EMEA, accounting for 12 percent of the regional total (table 4). Globally in 2009, the United Kingdom ranked fourth, with 4 percent of the total.

Overall Rank		Country	Percentage	
EMEA	Global		EMEA	Global
1	4	United Kingdom	12%	4%
2	5	Russia	12%	4%
3	6	Germany	12%	4%
4	8	Italy	7%	2%
5	9	Netherlands	7%	2%
6	10	France	7%	2%
7	11	Romania	7%	2%
8	14	Spain	5%	2%
9	18	Poland	4%	1%
10	22	Ukraine	2%	1%

Table 4. Top countries of origin for Web-based attacks, EMEA
Source: Symantec

In 2009, Russia was the second-ranked country of origin for Web-based attacks in EMEA, followed by Germany. As with the top-ranked United Kingdom, these countries each accounted for 12 percent of the regional total (the difference in rank is due to rounding of numbers). The top three EMEA countries each accounted for 4 percent of Web-based attacks globally. There were no related events that were significant enough to affect the amount of Web-based attacks originating in these countries, and the rankings of the top countries of origin for Web-based attacks in EMEA are similar to rankings for malicious activity by country, suggesting that the number Web-based attacks originating in these countries is a reflection of the overall malicious activity occurring there.

Bot-infected computers

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 2009, Symantec observed an average of 19,500 active bots per day in the EMEA region (figure 1), which is a 39 percent decrease from 2008, when 32,188 active bots were detected. In 2009, active bots in the EMEA region accounted for 48 percent of all active bots observed globally.

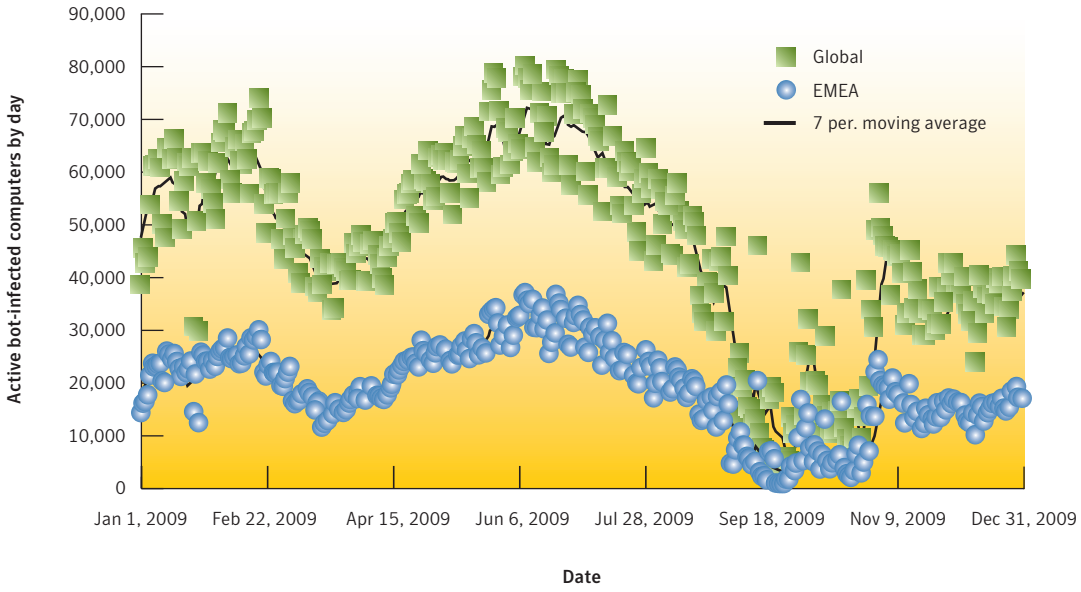

Figure 1. Active bot-infected computers, EMEA and global
Source: Symantec

Symantec also measures distinct bot-infected computers, which are computers that were active at least once during the reporting period. There were 3,249,704 distinct bot-infected computers recorded in the EMEA region in 2009. This is 32 percent less than the 4,776,967 observed in EMEA in 2008. It is worth noting that bot activity in EMEA in 2009 again closely mirrored global bot activity, as was the case in 2008, except for the substantial drop in global activity in 2009 from September to November. This dip is discussed in detail in the concurrent volume of the Symantec *Global Internet Security Threat Report* and is mainly attributed to the shutdown of several botnets at this time, as well as changing propagation patterns.[8]

[8] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf : p. 32

Bot-infected computers by country

In 2009, the EMEA region accounted for 48 percent of all bot-infected computers detected globally. Within the region, Germany had the highest percentage of bot-infected computers, with 14 percent of the regional total (table 5). This is the same percentage as 2008, when Germany ranked second in this category. Globally in 2009, Germany ranked fifth with 7 percent of the worldwide total.

EMEA Rank		Country	Percentage		
2009	2008		2009 EMEA	2008 EMEA	2009 Global
1	2	Germany	14%	14%	7%
2	3	Italy	12%	11%	6%
3	1	Spain	12%	15%	6%
4	4	Poland	12%	10%	6%
5	5	Turkey	7%	9%	3%
6	7	France	7%	6%	3%
7	8	Portugal	5%	4%	2%
8	6	United Kingdom	5%	8%	2%
9	13	Hungary	4%	1%	2%
10	9	Israel	3%	3%	1%

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

Italy had the second-highest number of bot-infected computers in EMEA in 2009, with 12 percent of the total. Italy accounted for 6 percent of the worldwide total in 2009, which made it the sixth-ranked country globally.

Spain ranked third for bot-infected computers in the EMEA region in 2009, with 12 percent of the total. It ranked seventh for bot-infected computers globally in 2009, accounting for 6 percent of the worldwide total.

Bot-infected computers are often used to send high volumes of spam; however, of the three top bot-infected countries in EMEA in 2009, none were in the top three for originating spam. This may indicate that some command-and-control bots have been disabled in the region, but also that high numbers of the bots that made up their networks still reside on computers in those countries.

Malicious Code Trends

This discussion is based on malicious code samples detected by Symantec in the EMEA region in 2009, with the following trends being analysed:

- Malicious code types
- Geolocation by type of malicious code
- Malicious code samples
- New malicious code families
- Threats to confidential information
- Propagation mechanisms

Malicious code types

In 2009, worms made up 49 percent of the volume of the top 50 potential infections in EMEA, more than the 43 percent that was recorded globally in 2009 (figure 2). The regional percentage of 49 percent is a significant increase from 2008, when worms accounted for 30 percent of the volume of the top 50 potential infections in EMEA. One of the primary contributors to this increase was the Downadup (a.k.a., Conficker) worm.[9] In addition, seven of the top 10 malicious code samples in EMEA in 2009 were classified as worms, up from five in 2008. There was also a marked increase in the proportion of viruses. Notably, in the top 10 malicious code samples in EMEA in 2009, five of the worms and one Trojan incorporated a virus component. It is likely that the surge in worm and virus activity is closely related. With the increasing professionalism that Symantec has observed in malicious code development over the past several reporting periods, it has become apparent that threats are now being developed with multiple attack vectors to enhance propagation; the more advanced a threat is, the more computers it can potentially compromise.

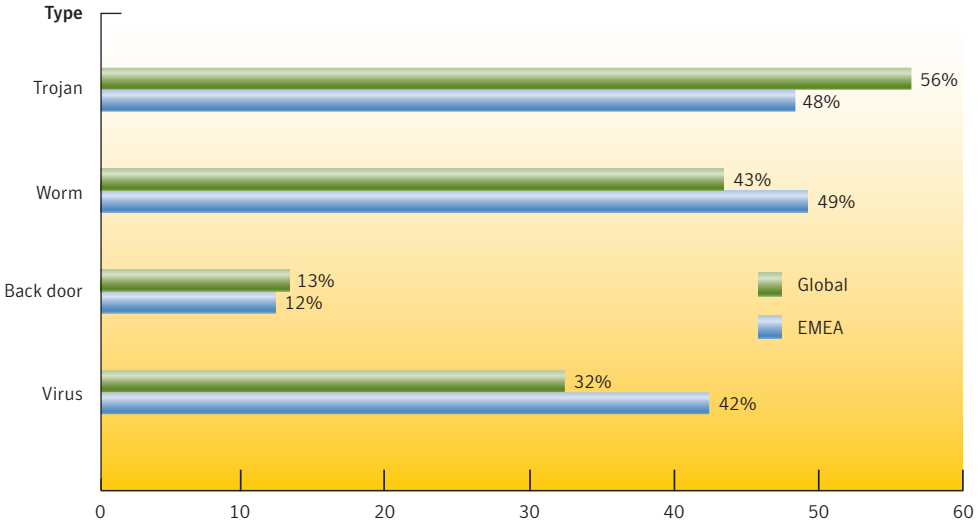

Figure 2. Potential infections by type, EMEA
Source: Symantec

[9] See http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed1.pdf and http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99

Trojans were the second most common type of malicious code in EMEA in 2009, accounting for 48 percent of the volume of the top 50 potential infections—a sizable drop from 66 percent in 2008. This percentage was lower than the global proportion of Trojans of 56 percent in 2009. Because this discussion is based on a proportional analysis, this large drop can be attributed to the surge in worm activity in the region during this reporting period.

In 2009, viruses accounted for a substantially larger proportion of the volume of the top 50 malicious code samples than in the previous reporting period, with 42 percent of the total in 2009, compared to 19 percent in 2008. This was also higher than the global proportion of viruses in 2009, which was 32 percent. As mentioned, five of the top 10 malicious code samples in EMEA in 2009 were classified both as worms and viruses, including the top three ranked samples (table 7), which would explain the correlation in the increases in worm and virus activity in the region. In 2008, only three of the top 10 malicious code samples had a virus component, and the highest-ranked sample of those three was only ranked fifth.

Geolocation by type of malicious code

Symantec examines the types of malicious code causing potential infections in each region. The increasing regionalisation of threats can cause differences between the types of malicious code being observed from one area to the next, such as when threats employ certain languages or localised events as part of their social engineering techniques. Table 6 shows the top three countries in EMEA in 2009 for each of the main malicious code types.

	Country by Type			
Rank	Back doors	Trojans	Viruses	Worms
1	United Kingdom	United Kingdom	Egypt	Saudi Arabia
2	Spain	Russia	Turkey	United Arab Emirates
3	Germany	Spain	Saudi Arabia	Egypt

Table 6. Geolocation by type of malicious code, EMEA
Source: Symantec

Back doors

For back doors in 2009, the top three ranked countries were the United Kingdom, Spain, and Germany, in that order. The only change from 2008 is France dropping in rank from third to sixth, which resulted in Germany rising up into third rank. This shift is the reversal of the shift observed from 2007 to 2008. This suggests that France's ranking in 2008 was due to an aberration of activity that has since returned to previous levels.

Trojans

The United Kingdom ranked first among countries in EMEA for number of potential Trojan infections in 2009, followed by Russia and Spain. Russia rose to second rank from ninth in 2008, while Spain rose to third rank from fifth in 2008. The rank of the United Kingdom for Trojans is likely influenced by it also ranking first for back doors in EMEA in 2009. This is because Trojans are a favourite vehicle for attackers attempting to distribute back doors. For example, 75 percent of Trojans identified in the volume of the top 50 potential infections in EMEA in 2009 included a back door component. As for the increases in rank for Russia and Spain in 2009, their changes in percentage compared to the countries ranked lower in the top 10 countries during this reporting period were minimal, which indicates that the shifts in rank were due to typical variances, rather than from any anomalous change in malicious Trojan activity.

Viruses

The top three ranked countries for potential virus infections during this period were Egypt, Turkey, and Saudi Arabia, in that order. Egypt and Turkey retained their ranks from 2008, while Saudi Arabia rose to third rank from 11th in 2008 due to a significant increase in virus activity. As mentioned previously, there was a notable relation between worm and virus activity in EMEA in 2009. The surge in virus activity may be directly related to the high level of worm activity that also occurred in the country in 2009.

Worms

In 2009, Saudi Arabia had the highest number of potential worm infections in EMEA, unchanged from 2008. The United Arab Emirates and Egypt ranked second and third for potential worm infections in 2009, respectively. These two countries ranked fourth and fifth in 2008, respectively, and their increase in rank for 2009 is attributed to the drop in rank of the United Kingdom and Spain, from second and third in 2008 to sixth and eighth in 2009, respectively. The rise of worm activity in the United Arab Emirates and Egypt can be attributed to the previously mentioned connection between worm and virus activity in the region, as both of these countries ranked in the top five for viruses.

Malicious code samples

In 2009, Symantec created 2,895,802 new malicious code signatures. This is a 71 percent increase over 2008, when 1,691,323 new malicious code signatures were added. Although the percentage increase in signatures added is less than the 139 percent increase from 2007 to 2008, the overall number of malicious code signatures by the end of 2009 grew to 5,724,106. This means that of all the malicious code signatures created by Symantec, 51 percent of that total was created in 2009.

The most common malicious code sample by potential infections in EMEA in 2009 was the Sality.AE virus (table 7).[10] Sality.AE was also the top sample worldwide in 2009. Sality.AE is designed to download and install additional malicious software on a victim's computer, as well as to prevent access to various security-related domains, stop security-related services, and delete security-related files in the process. The virus also infects .exe and .scr files on a compromised local (C) drive as well as on any writable networked resource. Sality.AE also copies itself to attached removable drives.

[10] http://www.symantec.com/security_response/writeup.jsp?docid=2008-042106-1847-99

Rank	Sample	Type	Infection Vectors	Top-Ranked Country	Second-Ranked Country	Impact
1	Sality.AE	Virus, worm	Executables	Egypt	Turkey	Removes security applications and services
2	Mabezat.B	Worm, virus	SMTP, CIFS, removable drives	Saudi Arabia	South Africa	Encrypts and infects files
3	Brisv.A	Trojan, virus	Multimedia files	United Kingdom	France	Modifies multimedia files, causing multimedia players to open malicious URLs
4	SillyFDC	Worm	Mapped and removable drives	Russia	Turkey	Downloads and installs additional threats
5	Downadup	Worm, back door	P2P, CIFS, remote vulnerabilities	Italy	Russia	Downloads and installs additional threats
6	Gammima	Worm, virus	Removable drives	Turkey	Spain	Steals online game account credentials
7	Gampass	Trojan	N/A	Turkey	Spain	Steals online game account credentials
8	Almanahe	Worm, virus	CIFS	Turkey	Egypt	Downloads and installs additional threats
9	Chir	Worm, virus	SMTP and executables	Pakistan	Spain	Infects files and exposes user information
10	Fakeavalert	Trojan	N/A	United Kingdom	Netherlands	Displays false antivirus alerts and lowers security settings

Table 7. Top malicious code samples, EMEA
Source: Symantec

The second most common malicious code sample causing potential infections in EMEA in 2009 was the Mabezat.B worm.[11] Mabezat spreads through email, removable drives, and network shares protected by weak passwords. It also infects executable files and encrypts data files.

The third most frequently reported malicious code sample causing potential infections in EMEA during this period was the Brisv.A Trojan.[12] Brisv.A was the second-ranked sample causing potential infection globally in 2009. This Trojan scans computers for a wide range of multimedia files and, upon discovery, it then modifies a data marker in the files with a malicious URL.[13] The marker is a part of the Windows Media® Audio (WMA) format. Although other applications appear to be unaffected, when the files are opened using Windows Media Player, the marker is automatically processed, causing the application to open a Web browser window and access the malicious URL. Accessing the malicious URL may expose the user to additional threats.

The effectiveness of Brisv.A is heightened by the possibility that unknowing victims may share the compromised multimedia files with others through peer-to-peer (P2P), email, or other means of propagation. As a result, the compromised files can potentially affect users whose computers were not exposed to the Trojan itself. This Trojan was initially discovered in July 2008. Its prominence in the EMEA region in 2009 may indicate that a significant number of users and administrators have not updated their software or antivirus programs to mitigate this threat.

[11] http://www.symantec.com/security_response/writeup.jsp?docid=2007-120113-2635-99
[12] http://www.symantec.com/security_response/writeup.jsp?docid=2008-071823-1655-99
[13] This includes ASF, MP2, MP3, WMA and WMV extensions.

New malicious code families

In 2009, the Induc virus was the most common malicious code sample by potential infections both in EMEA and globally (table 8).[14] Induc infects the Delphi compilation process so that all files compiled with Delphi will also be infected. The virus propagates as the infected applications are distributed. In EMEA, Russia was responsible for the most potential infections of Induc in 2009, followed by Germany.

Rank	Sample	Type	Infection Vectors	Top-Ranked Country	Second-Ranked Country	Impact
1	Induc	Virus	Delphi-compiled applications	Russia	Germany	Infects the Delphi compilation process
2	Changeup	Worm	Mapped and removable drives	Portugal	Nigeria	Contacts external URLs
3	Bredolab	Trojan	N/A	United Kingdom	Germany	Downloads additional files
4	Ergrun	Trojan	N/A	United Kingdom	Spain	Downloads additional files
5	Pilleuz	Worm, back door	P2P, IM, removable drives	Russia	Ukraine	Opens a back door, copies itself to shared folders, and sends IM messages with links to itself
6	Swifi	Trojan	N/A	United Kingdom	Germany	Exploits a vulnerability in Adobe Flash Player
7	Palevo	Worm, back door	Remote vulnerabilities	Germany	Netherlands	Lowers security settings and checks for further commands
8	Interrupdate	Trojan	N/A	United Kingdom	Sweden	Prevents security updates
9	Sopiclick	Trojan	N/A	United Kingdom	Netherlands	Increases certain website statistics and downloads additional files
10	Fostrem	Trojan	N/A	United Kingdom	Turkey	Exploits an ActiveX vulnerability and downloads additional files

Table 8. Top new malicious code families, EMEA
Source: Symantec

The second most common new malicious code family in both EMEA and globally during 2009 was the Changeup worm.[15] This worm propagates by copying itself to removable and mapped drives. Changeup also connects to websites via a TCP port and downloads additional threats. In the EMEA region in 2009, the highest number of Changeup distributions originated in Portugal, followed by instances distributed from Nigeria.

The Bredolab Trojan[16] was the third most common new malicious code family both in EMEA and globally in 2009. Bredolab is primarily distributed through spam and drive-by-download attacks. When this Trojan is executed, it copies itself to the computer and creates a registry entry to ensure that it is run every time the computer starts. Bredolab has been observed downloading random other malicious threats, including password stealers, rootkits, back doors, and misleading applications.[17] The United Kingdom was the highest ranked country for Bredolab infections in EMEA in 2009, followed by Germany.

[14] http://www.symantec.com/security_response/writeup.jsp?docid=2009-081816-3934-99
[15] http://www.symantec.com/security_response/writeup.jsp?docid=2009-081806-2906-99
[16] http://www.symantec.com/security_response/writeup.jsp?docid=2009-052907-2436-99
[17] http://www.symantec.com/connect/blogs/taking-closer-look-trojanbredolab

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.

Of the threats to confidential information from the volume of top 50 malicious code samples in EMEA in 2009, 85 percent were classified as allowing remote access, a slight decrease from 87 percent in 2008 (figure 3). This was 13 percentage points lower than the global percentage of 98 percent. The lower prevalence of threats to confidential information in EMEA compared to global rankings can be partially attributed to the lower rank of the Downadup worm, because it ranked fifth globally in 2009, but sixth in EMEA. This worm is the highest-ranking threat to confidential information both globally and in EMEA, so a proportional change in ranking would have a noticeable effect.

The threats that were ranked higher than Downadup in EMEA accounted for 82 percent of the top 10 by volume, but globally the threats that ranked higher than Downadup account for only 74 percent of the top 10 by volume. This alone accounts for approximately 8 percent of the difference. Overall, the number of threats to confidential information decreased in 2009, but the proportions and types of threats remained nearly unchanged from 2008.

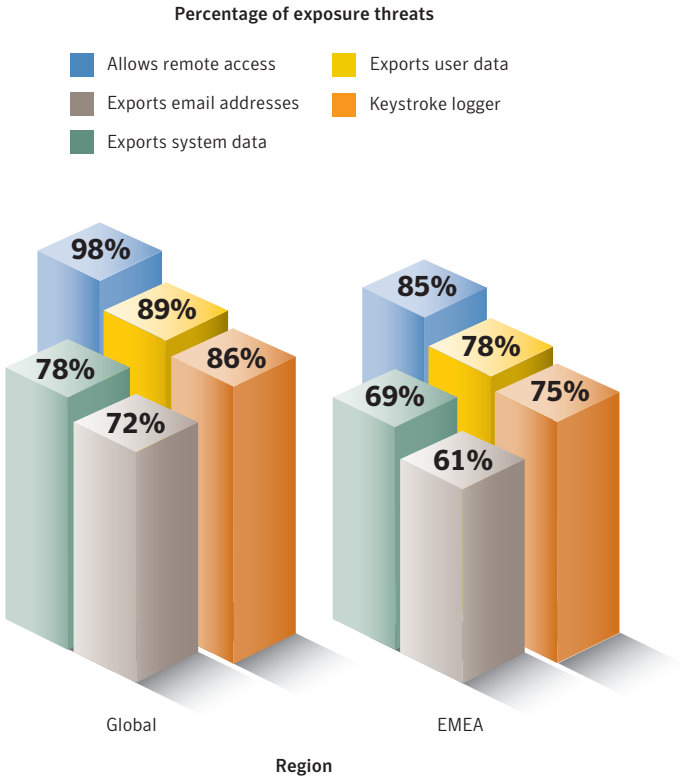

Figure 3. Threats to confidential information, EMEA and global
Source: Symantec

In 2009, 78 percent of threats to confidential information in EMEA were classified as threats that export user data, which is similar to 2008, when 76 percent of malicious code infections were thus classified, but somewhat less than the global classification in 2009 of 89 percent. Threats that are capable of this type of information exposure are favoured by attackers 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 observed by Symantec in the underground economy in 2009 ranged between $15 and $850, while credit card information was being sold for as high as $30 per sample.[18]

The third most prevalent threat to confidential information of the volume of the top 50 malicious code samples in EMEA in 2009 was keystroke loggers, with 75 percent of malicious code infections having this capability; this is unchanged from 2008. Successfully installed keystroke loggers record keystrokes on compromised computers and then return the data to the attacker, who can then process the results to extract any worthwhile, saleable information, such as user account credentials for online banking, stock-trading websites, or online game accounts.

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),[19] 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 through a back door server and using it to upload and install itself. The samples discussed here are assessed by percentage of potential infections.[20]

In 2009 in EMEA, 77 percent of the volume of potential infections could propagate through file-sharing executables, compared to a global proportion of 72 percent (table 9). This is an increase from 65 percent in EMEA in 2008. File-sharing executables are the propagation mechanisms used by many viruses and some worms to copy themselves onto removable media. The continued resurgence in this vector over the past few years coincides with the increased use of removable drives and other portable devices, as has been discussed in previous volumes of the Symantec *Global Internet Security Threat Report*.[21]

[18] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf : p. 73 : all currency in U.S. dollars
[19] CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.
[20] 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.
[21] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 68

Rank	Propagation Mechanism	Percentage	
		EMEA	Global
1	File-sharing executables	77%	72%
2	File transfer, CIFS	40%	42%
3	File transfer, email attachment	29%	25%
4	Remotely exploitable vulnerability	15%	24%
5	File sharing, P2P	3%	5%
6	SQL	2%	2%
7	Back door, Kuang2	2%	2%
8	Back door, SubSeven	2%	2%
9	File transfer, embedded HTTP URI, instant messenger	2%	4%
10	File transfer, instant messenger	2%	1%

Table 9. Top propagation vectors, EMEA
Source: Symantec

In 2009, 40 percent of the volume of the top 50 malicious code samples in EMEA used the CIFS protocol to propagate, nearly the same as the 42 percent measured globally. This is an increase from 33 percent in 2008 in EMEA. Propagation through the CIFS protocol overtook propagation through email in 2009, both globally and in EMEA. A single computer that becomes infected with malicious code through CIFS can spread the malicious code to internal, protected file servers and trigger the rapid spread of infection throughout an entire networked organisation.

In 2009, malicious code in EMEA that propagated in email attachments accounted for 29 percent of the total for propagation vectors, compared to 25 percent measured globally for this method. The regional percentage is a decrease from 34 percent observed in 2008. This decrease could be attributable to malicious code authors having less success with attacks using email attachments over the past few years due to increased user awareness and increased vigilance and accuracy for email protection mechanisms.

Phishing and Spam Trends

This section will discuss the following metrics:

- Phishing URLs by country and top targeted sectors
- Countries of spam origin

Phishing URLs by country and top targeted sectors

This metric will assess the EMEA countries in which the most phishing URLs were hosted, as well as the most popular sector targeted within each country. It should be noted that the fact that a phishing URL is hosted in a certain country does not necessarily mean that the attacker is located in that country.

Spain hosted the highest percentage of phishing URLs observed in EMEA in 2009, with 11 percent of observed URLs in the region (table 10). This is an increase from 2008, when Spain ranked ninth with 5 percent of phishing URLs in EMEA. Spain was the third-ranked country in EMEA for bot-infected computers in 2009, with 12 percent of the total and only 2 percentage points behind first-ranked Germany. It is likely that many of these bots were used to disseminate spam that included links to phishing URLs. The sector most frequently spoofed by phishing URLs based in Spain in 2009 was the financial sector, which accounted for 88 percent of the total for phishing URLs identified there.

EMEA Rank			Percentage		2009 Top Sector	Percentage of URLs
2009	2008	Country	2009	2008	Targeted in Country	Targeting Sector
1	9	Spain	11%	5%	Financial services	88%
2	1	Poland	11%	18%	Financial services	89%
3	18	Romania	10%	1%	Financial services	89%
4	3	Russia	9%	10%	Financial services	73%
5	5	United Kingdom	9%	9%	Financial services	86%
6	4	Germany	8%	9%	Financial services	76%
7	2	France	6%	11%	Financial services	74%
8	6	Italy	5%	6%	Financial services	75%
9	13	Hungary	5%	1%	Financial services	90%
10	7	Netherlands	4%	6%	Financial services	87%

Table 10. Top countries hosting phishing URLs and top targeted sectors
Source: Symantec

Poland ranked second in EMEA in 2009 for phishing URLs, with 11 percent of the total. This is a decrease from 2008 when Poland hosted 18 percent of phishing URLs and was the top-ranked country in EMEA for this metric.

Romania had the third-highest number of phishing websites in the region in 2009, with 10 percent of the total. This is an increase over 2008, when it ranked 18th with 1 percent of phishing URLs. One explanation for this rise is that Romania jumped from 14th rank in 2008 to ninth in 2009 for malicious activity in EMEA. Specifically, Romania ranked second for phishing hosts. These hosts were likely used to disseminate the high volume of phishing URLs seen in the region.

The top sector targeted by phishing URLs in each of the top 10 countries during 2009 was the financial services sector. The percentage of URLs spoofing the financial services sector in a number of the top EMEA countries in 2009 was higher than the global average of 76 percent. This indicates that the financial services sector is being especially targeted in EMEA, likely due to the concentration of financial institutions in the region. The primary motive behind most phishing activity is financial gain. Phishers typically exploit brands associated with the financial sector because data garnered from phished financial websites is most likely to yield online banking account and login details.

Countries of spam origin

In 2009, 24 percent of all spam detected by Symantec worldwide originated in EMEA. On a per-country basis, 10 percent of all spam detected in EMEA originated in Poland (table 11). Poland ranked fifth globally in 2009, with 4 percent of spam detected worldwide

A recent report shows that, although in its emergent stage, Poland's fixed broadband market is one of the largest in Eastern Europe.[22] It may be that broadband-connected computers in Poland could be susceptible to compromise and, therefore, it is possible that a higher percentage of computers are serving as spam servers. Despite the fact that it ranked first for spam in EMEA, Poland was only ranked second for spam zombies. This may indicate that spam originating from Poland might have been sent via botnets, such as those established by numerous malicious code samples.

Overall Rank		Country	Percentage	
EMEA	Global		EMEA	Global
1	5	Poland	10%	4%
2	7	Turkey	9%	3%
3	8	Russia	9%	3%
4	12	Romania	6%	2%
5	13	Germany	5%	2%
6	14	Spain	5%	2%
7	15	Ukraine	5%	2%
8	16	United Kingdom	5%	2%
9	17	Italy	5%	2%
10	21	Czech Republic	4%	1%

Table 11. Top countries of spam origin, EMEA
Source: Symantec

Turkey ranked second for spam origination in the EMEA region in 2009, with 9 percent of the regional total. It ranked seventh for originating spam globally during this reporting period, with 3 percent of the worldwide total. Turkey's prominence in this measurement may be due to it having the third-most spam zombies in 2009.

Russia was the third-ranked country of spam origin in 2009, accounting for 9 percent of the regional total. Globally in 2009, it ranked eighth with 3 percent of worldwide spam. Russia had the highest number of spam zombies in EMEA in 2009.

[22] http://www.budde.com.au/Research/Poland-Telecoms-Mobile-Broadband-and-Forecasts.html

Appendix A—Symantec Best Practices

Symantec encourages all users and administrators to adhere to the following basic security 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. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.
- Administrators should limit privileges on systems for users that do not require such access and they should restrict unauthorised devices, such as external portable hard-drives and other removable media.
- Turn off and remove services that are not needed for normal company network operations.
- Test security regularly to ensure that adequate controls are in place.
- Educate management on security budgeting needs.
- 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.
- Administrators should update antivirus definitions regularly to protect against the high quantity of new malicious code threats and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. IDS, IPS, and other behaviour-blocking technologies should also be employed to prevent compromise by new threats.
- Always 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.
- As compromised computers can be a threat to other systems, Symantec recommends that affected enterprises notify their ISPs of any potentially malicious activity.
- 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. Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorised communications are not taking place.
- Mail servers should be configured to block email that appears to come from within the company, but that actually originates from external sources.
- Consider using domain-level or email authentication in order to verify the actual origin of an email message to protect against phishers who are spoofing email domains.
- 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.

- Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organisation are deployed on desktop computers.
- Isolate infected computers quickly to prevent the risk of further infection within the organisation.
- 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.
- Perform a forensic analysis and restore the computers using trusted media.
- 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.
- 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.
- Employ Web-server log monitoring to track if and when complete downloads of company websites, logos, and images are occurring, as this may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing.
- Network administrators should review Web proxy logs to determine if any users have visited known blacklisted sites.

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. A free security scan is available through the Symantec Security Check at www.symantec.com/securitycheck.
- 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.
- Deploy an antiphishing solution, such as an antiphishing toolbar for Web browsers. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

- 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 bankcard numbers.
- Review bank, credit card, and credit information frequently to monitor any irregular activities. For further information, the Internet Crime Complaint Center (IC3) has also released a set of guidelines on how to avoid Internet-related scams. See http://www.ic3.gov/default.aspx for more information.
- 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 license 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 because 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.

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
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

04/10 20959304