[Symantec Corporation](http://www.symantec.com/index.jsp)

Internet Security Threat Report - 2010

**Custom Report**

**Threat Activity Trends**

During this reporting period, the United States had the most overall malicious activity, with 19 percent of the total—down slightly from 20 percent in 2009, when it also ranked first.   
  
The United States was the top country for originating network attacks in 2010, with 22 percent—down from 24 percent in 2009.   
  
The average daily volume of Web-based attacks observed in 2010 was 93 percent higher than in 2009.   
  
Attacks related to the Phoenix toolkit were the most prominent of the Web-based attack activities observed in 2010, with 39 percent of the top 10 activities observed.   
  
Of the search terms that resulted in visits to malicious websites, 49 percent were in the adult entertainment category.   
  
In 2010, the healthcare sector had the highest percentage of data breaches that could lead to identity theft, with 27 percent—an increase from 15 percent in 2009.   
  
The financial sector was the top sector in 2010 for identities exposed in data breaches, with 23 percent—a decrease from 60 percent in 2009.   
  
The leading cause of data breaches that could lead to identity theft in 2010 was the theft or loss of a computer or other data-storage device, with 36 percent of the total; this is nearly unchanged from its 37 percent total in 2009.   
  
Hacking was the leading source of reported identities exposed in 2010 with 42 percent of the total—down from 60 percent in 2009.   
  
The most exposed type of data in deliberate breaches (hacking, insider breaches, or fraud) was customer-related information, accounting for 59 percent of the total. Customer data also accounted for 85 percent of identities exposed in deliberate breaches.   
  
Of malicious URLs observed on social networking sites during a three-month period in 2010, 66 percent made use of a URL shortening service; of these, 88 percent were clicked at least once.   
  
The United States had the most bot-infected computers in 2010, accounting for 14 percent of the total—an increase from 11 percent in 2009.   
  
Taipei was the city with the most bot-infected computers in 2010, accounting for 4 percent of the total; it also ranked first in 2009, with 5 percent.   
  
In 2010, Symantec identified 40,103 distinct new bot command-and-control servers; of these, 10 percent were active on IRC channels and 60 percent on HTTP.   
  
The United States was the location for the most bot command-and-control servers, with 37 percent of the total.   
  
The United States was the most targeted county by denial-of-service attacks, with 65 percent of the total.

**Vulnerability Trends**

The total number of vulnerabilities for 2010 was 6253—a 30 percent increase over 4814 vulnerabilities documented in 2009 and the most of any year recorded by Symantec.   
  
The number of new vendors affected by vulnerabilities increased to 1914 in 2010 from 734 in 2009—a 161 percent increase.   
  
Among the new vendors affected by vulnerabilities in 2010, 76 vulnerabilities were rated as being high severity—a 591 percent increase over the 11 such vulnerabilities in 2009.   
  
There were 191 vulnerabilities documented in Chrome in 2010, versus 41 in 2009.  
  
Internet Explorer had the longest average window of exposure to vulnerabilities in 2010, with an average of four days in 2010 (based on a sample set of 47 vulnerabilities).  
  
In 2010, 346 vulnerabilities affecting browser plug-ins were documented by Symantec, compared to 302 vulnerabilities affecting browser plug-ins in 2009.   
  
The highest number of plug-in vulnerabilities affected ActiveX controls, with 117 of the total; this is a decrease from 134 in 2009.   
  
Symantec identified 14 zero-day vulnerabilities in 2010, an increase from 12 in 2009. Eight of these affected Web browsers and browser plug-ins.  
  
In 2010, there were 15 public SCADA vulnerabilities identified; in 2009, the total was 14.

**Malicious Code Trends**

The top three malicious code families in 2010 were Sality, Downadup, and Mabezat, all of which had a worm component.   
  
The top 10 malicious code families detected in 2010 consisted of five families with worm and virus components, one worm with a backdoor component, two worms, one virus with a backdoor component, and one Trojan.   
  
The top three new malicious code families detected in 2010 were the Ramnit worm, the Sasfis Trojan, and the Stuxnet worm.  
  
In 2010, 56 percent of the volume of the top 50 malicious code samples reported were classified as Trojans—the same percentage as in 2009.   
  
In 2010, Sality.AE was the most prevalent potential malicious code infection in every region except for North America, where Ramnit was the most prevalent.   
  
The percentage of threats to confidential information that incorporate remote access capabilities increased to 92 percent in 2010 from 85 percent in 2009.  
  
In 2010, 79 percent of threats to confidential information exported user data and 76 percent had a keystroke-logging component; these are increases from 77 percent and 74 percent, respectively, in 2009.  
  
In 2010, propagation through executable file sharing accounted for 74 percent of malicious code that propagates—up from 72 percent in 2009.  
  
In December 2010, approximately 8.3 million malicious files were reported using reputation-based detection.  
  
The percentage of documented malicious code samples that exploit vulnerabilities decreased to 1 percent in 2010 from 6 percent in 2009.

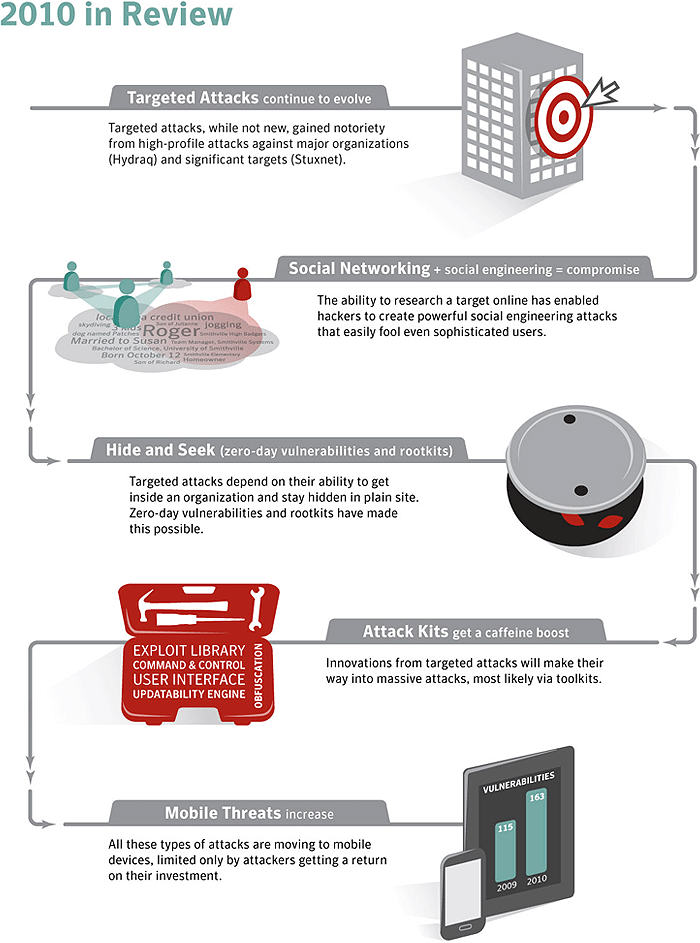
**Fraud Actvity Trends**

The most frequently spoofed organization was banks, which accounted for 56 percent of phishing attacks blocked in 2010.   
  
Credit cards were the most commonly advertised item for sale on underground servers known to Symantec, accounting for 22 percent of all goods and services advertised—an increase from 19 percent in 2009.  
  
The United States was the top country advertised for credit cards on known underground servers, accounting for 65 percent of the total; this is a decrease from 67 percent in 2009.   
  
The top three spam botnets that delivered the highest volume of spam in 2010 were Rustock, Grum, and Cutwail.  
  
India was the leading source of botnet spam in 2010, with 8 percent of the worldwide total.   
  
Approximately three quarters of all spam in 2010 was related to pharmaceutical products.

**About This Report**

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify and analyze, to deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.   
  
More than 240,000 sensors in more than 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 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 that provide valuable insight into attacker methods.   
  
In addition, Symantec maintains one of the world’s most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 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 24,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.   
  
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; as well as other Symantec technologies. Data is collected in more than 86 countries from around the globe. Over 8 billion email messages, as well as over 1 billion Web requests are processed per day across 16 data centers. 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, analyze, 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 secure their systems effectively now and into the future.

**Executive Summary**



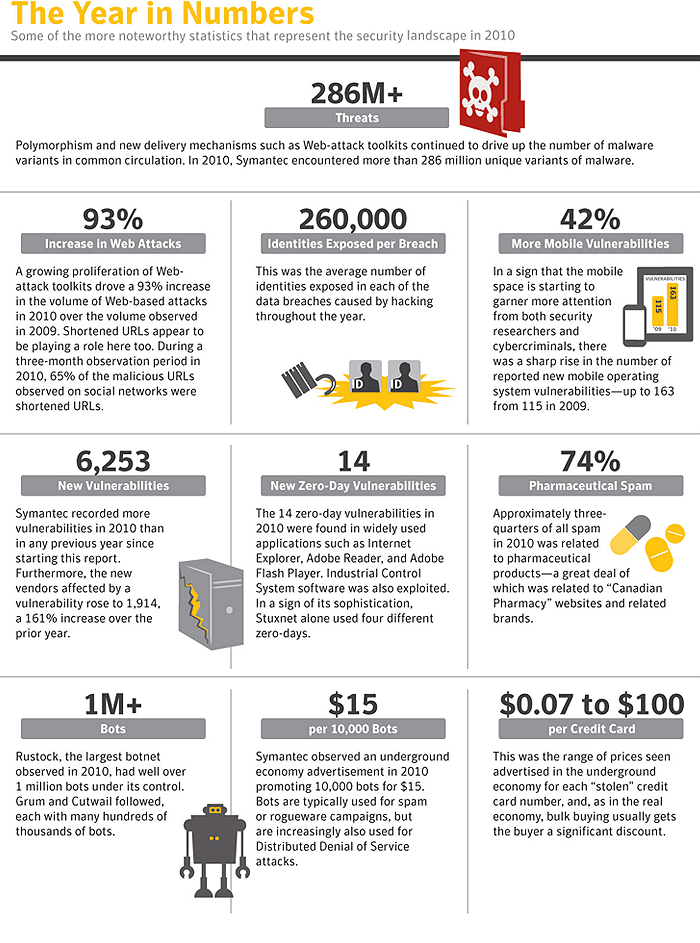
**Source: Symantec Corporation**

Symantec recorded over 3 billion malware attacks in 2010 and yet one stands out more than the rest—Stuxnet. This attack captured the attention of many and led to wild speculation on the target of the attacks and who was behind them. This is not surprising in an attack as complex and with such significant consequences as Stuxnet. In a look back at 2010, we saw five recurring themes:   
  
**1. Targeted attacks.** Almost forgotten in the wake of Stuxnet was Hydraq. Hydraq’s intentions were old-fashioned compared to the cyber-sabotage of Stuxnet—it attempted to steal. What made Hydraq stand out was what and from whom it attempted to steal—intellectual property from major corporations. Targeted attacks did not start in 2010, and will not end there. In addition, while Hydraq was quickly forgotten and, in time, Stuxnet may be forgotten as well, their influence will be felt in malware attacks to come. Stuxnet and Hydraq teach future attackers that the easiest vulnerability to exploit is our trust of friends and colleagues. Stuxnet could not have breached its target without someone being given trusted access with a USB key. Meanwhile, Hydraq would not have been successful without convincing users that the links and attachments they received in an email were from a trusted source.   
  
**2. Social networks.** Whether the attacker is targeting a CEO or a member of the QA staff, the Internet and social networks provide rich research for tailoring an attack. By sneaking in among our friends, hackers can learn our interests, gain our trust, and convincingly masquerade as friends. Long gone are the days of strange email addresses, bad grammar and obviously malicious links. A well-executed social engineering attack has become almost impossible to spot.   
  
**3. Zero-day vulnerabilities and rootkits.** Once inside an organization, a targeted attack attempts to avoid detection until its objective is met. Exploiting zero-day vulnerabilities is one part of keeping an attack stealthy since these enable attackers to get malicious applications installed on a computer without the user’s knowledge. In 2010, 14 such vulnerabilities were discovered. Rootkits also play a role. While rootkits are not a new concept, techniques continue to be refined and redeveloped as attackers strive to stay ahead of detection tools. Many of these rootkits are developed for use in stealthy attacks. There were also reports in 2010 of targeted attacks using common hacker tools. These are similar to building products – in this case attack tools – with “off the shelf” parts in order to save money and get to market faster. However, innovation runs in both directions, and attacks such as Stuxnet will certainly provide an example of how targeted attacks are studied and their techniques copied and adapted for massive attacks.   
  
**4. Attack kits.** What brings these techniques to the common cybercriminal are attack kits. Zero-day vulnerabilities become everyday vulnerabilities via attack kits; inevitably, some of the vulnerabilities used on Stuxnet as well as the other 6,253 new vulnerabilities discovered in 2010 will find their way into attack kits sold in the underground economy. These tools—easily available to cybercriminals—also played a role in the creation of the more than 286 million new malware variants Symantec detected in 2010.   
  
**5. Mobile threats.** As toolkits make clear, cybercrime is a business. Moreover, as with a legitimate business, cybercrime is driven by a return on investment. Symantec believes that this explains the current state of cybercrime on mobile threats. All of the requirements for an active threat landscape existed in 2010. The installed base of smart phones and other mobile devices had grown to an attractive size. The devices ran sophisticated operating systems that come with the inevitable vulnerabilities—163 in 2010. In addition, Trojans hiding in legitimate applications sold on app stores provided a simple and effective propagation method. What was missing was the ability to turn all this into a profit center equivalent to that offered by personal computers. But, that was 2010; 2011 will be a new year.   
  
This report discusses these trends, impending threats, and the continuing evolution of the Internet threat landscape in 2010. Supporting the commentary are four appendices of data collected over the course of the year covering the following categories:

* Threat activity
* Vulnerabilities
* Malicious code
* Fraud activity

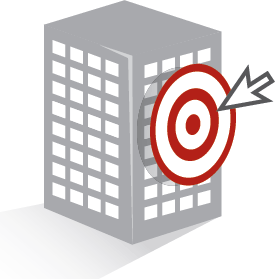
Along with this analysis, Symantec provides a comprehensive guide to best practices for both enterprises and consumers to adhere to in order to reduce their risk from the dangers of the current Internet security threat landscape.

**Notable Statistics**

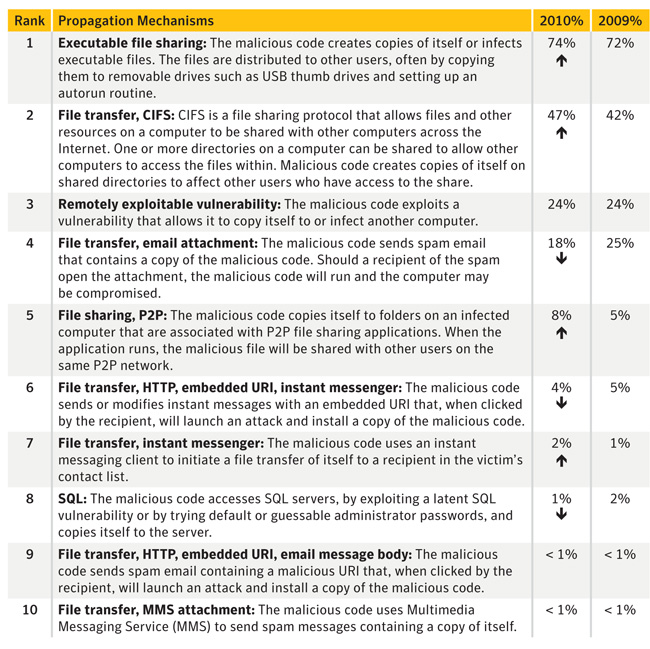


Source: Symantec Corporation

**Threat Landscape**



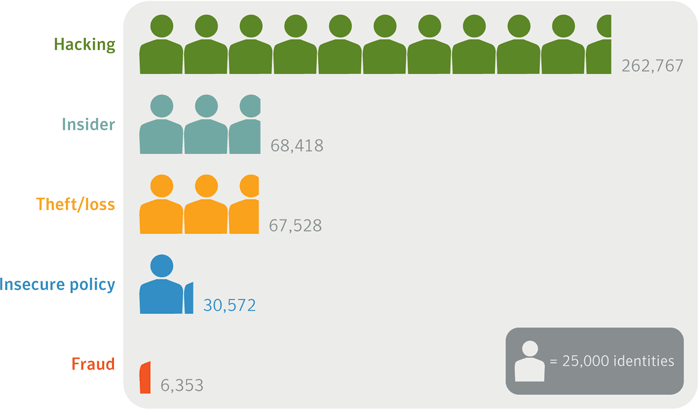
**Targeted attacks continue to evolve**

The year was book-ended by two significant targeted attacks: Hydraq (a.k.a. Aurora) rang in the New Year, while Stuxnet, though discovered in the summer, garnered significant attention through to the end of the year as information around this threat was uncovered. Although these threats have been analyzed in-depth, there are lessons to be learned from these targeted attacks.   
  
There were large differences in some of the most publicized targeted attacks in 2010. The scale of attacks ranged from publicly traded, multinational corporations and governmental organizations to smaller companies. In addition, the motivations and backgrounds of the alleged attackers varied widely. Some attacks were also much more effective—and dangerous—than others. All the victims had one thing in common, though—they were specifically targeted and compromised.   
[The Trojan.Hydraq Incident](http://www.symantec.com/connect/blogs/trojanhydraq-incident)   
[Read about the Stuxnet worm](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)   
  
Many organizations have implemented robust security measures such as isolated networks to protect sensitive computers against worms and other network intrusions. The Stuxnet worm, though, proved that these “air-gapped” networks can be compromised and that they still require additional layers of security. While Stuxnet is a very complex threat, not all malicious code requires this level of complexity to breach an isolated network. Because an increasing amount of malicious code incorporates mechanisms to propagate through removable media such as USB drives, isolated networks require some of the same policies and protection as user networks to prevent compromise. Endpoint protection that blocks access to external ports, such as a device control policy can help defend against these threats.   
  


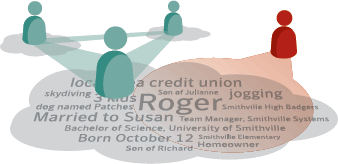
**Propagation mechanisms**  
Source: Symantec Corporation

While many targeted attacks are directed at large enterprises and governmental organizations, they can also target SMBs and individuals. Similarly, senior executives are not the only employees being targeted. In most cases, a successful compromise only requires victimizing a user with access to even just limited network or administrative resources. A single negligent user or unpatched computer is enough to give attackers a beachhead into an organization from which to mount additional attacks on the enterprise from within, often using the credentials of the compromised user.   
  
While Stuxnet included exploit code for an unprecedented number of zero-day vulnerabilities, such code is not a requirement for targeted attacks by any means. More commonly, research and reconnaissance are used to mount effective social engineering attacks. Attackers can construct plausible deceptions using publicly available information from company websites, social networks, and other sources. Malicious files or links to malicious websites can then be attached to or embedded in email messages directed at certain employees using information gathered through this research to make them seem legitimate. This tactic is commonly called spear phishing.

* [Stuxnet Using Three Additional Zero-Day Vulnerabilities](http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities)

Spear-phishing attacks can target anyone. While the high profile, targeted attacks that received a high degree of media attention such as Stuxnet and Hydraq attempted to steal intellectual property or cause physical damage, many of these attacks simply prey on individuals for their personal information. In 2010, for example, data breaches caused by hacking resulted in an average of over 260,000 identities exposed per breach—far more than any other cause. Breaches such as these can be especially damaging for enterprises because they may contain sensitive data on customers as well as employees that even an average attacker can sell on the underground economy.   
  


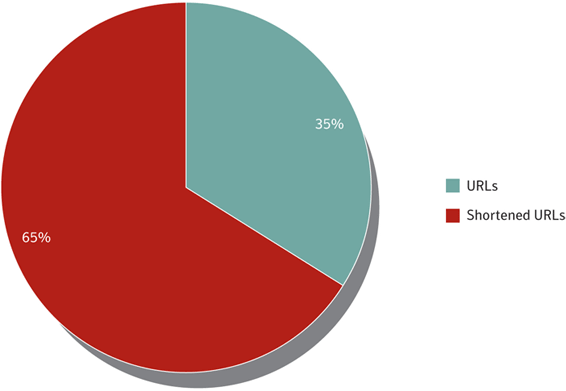
**Average number of identities exposed per data breach by cause**  
Source: Based on data provided by OSF DataLoss DB

While much of the attention focused on targeted attacks is fueled by the sophisticated methods attackers use to breach their targets, the analysis often overlooks prevention and mitigation. In many cases, implementing best practices, sufficient policies, and a program of user education can prevent or expose a targeted attack. For example, restricting the usage of USB devices limits exposure to threats designed to propagate through removable media. Educating users not to open email attachments and not to click on links in email or instant messages can also help prevent breaches.   
  
If a breach occurs, strong password policies that require the use of different passwords across multiple systems can prevent the attack from expanding further into the network. Limiting user privileges can help to reduce the number of network resources that can be accessed from a compromised computer.   
  
Since one of the primary goals of targeted attacks is information theft, whether the attackers seek customer records or intellectual property, proper egress filtering should be performed and data loss prevention solutions employed. This can alert network operations personnel to confidential information leaving the organization.   
  
While Stuxnet is a very sophisticated threat, not all targeted attacks need to employ such a high degree of complexity in order to succeed. Ignoring best practices enables less sophisticated attacks to be successful. However, it is almost certain that we will continue to see targeted attacks and that the tactics used will evolve and change. Stuxnet may have provided less sophisticated attackers with a blueprint to construct new threats. At the very least administrators responsible for supervisory control and data acquisition (SCADA) systems should review security measures and policies to protect against possible future threats.   
  


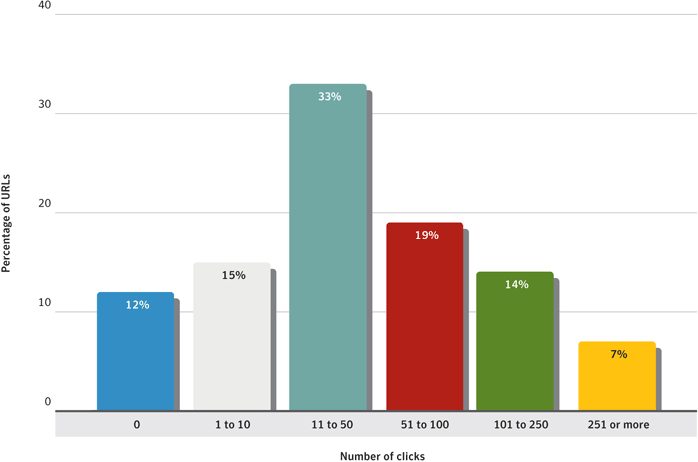
**Social networking + social engineering = compromise**

Social networks continue to be a security concern for organizations. Companies and government agencies are trying to make the most of the advantages of social networking and keep employees happy while, at the same time, limiting the dangers posed by the increased exposure of potentially sensitive and exploitable information. Additionally, malicious code that uses social networking sites to propagate remains a significant concern.   
  
Attackers exploit the profile information available on social networking sites to mount targeted attacks. For example, many people list employment details in their profiles, such as the company they work for, the department they work in, other colleagues with profiles, and so on. While this information might seem harmless enough to divulge, it is often a simple task for an attacker to discover a company’s email address protocol (e.g., firstname.lastname@company.com) and, armed with this information along with any other personal information exposed on the victim’s profile, create a convincing ruse to dupe the victim. For example, by finding other members of the victim’s social network who also work for the same organization, the attacker can spoof a message from that person to lend an air of additional credibility. This might be presented as an email message from a coworker who is also a friend that contains a link purporting to have pictures from a recent vacation (the details of which would have been gathered from the social networking site). With a tantalizing enough subject line, the ruse can be difficult for most people to resist because the point of social networking sites is to share this type of information.   
  
Attackers can also gather other information from social networking sites that can indirectly be used in attacks on an enterprise. For example, an employee may post details about changes to the company’s internal software or hardware profile that may give an attacker insight into which technologies to target in an attack.   
  
While increased privacy settings can reduce the likelihood of a profile being spoofed, a user can still be exploited if an attacker successfully compromises one of the user’s friends. Because of this, organizations should educate their employees about the dangers of posting sensitive information. Clearly defined and enforced security policies should also be employed.   
  
Malicious code that uses social networking sites to infect users in a concerted attack is also a threat. For example, current variants of the Koobface worm can not only send direct messages from an infected user’s account on a site to all of that user’s friends in the network, but also are capable of updating status messages or adding text to profile pages. Moreover, in addition to possibly giving attackers access to an infected user’s social networking site account, some threats can also infect the user’s computer. In the case of Koobface, the worm attempts to download fake antivirus applications onto compromised computers. These threats should be a concern for network administrators because many users access their social networks from work computers.

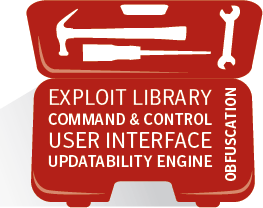
* [The Risks of Social Networking](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf)
* [Symantec Report on Rogue Security Software](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf)

A favorite method used to distribute an attack from a compromised profile is to post links to malicious websites from that profile so that the links appear in the news feeds of the victim’s friends. Moreover, attackers are increasingly using shortened URLs for this because the actual destination of the link is obscured from the user.1 During a three-month period in 2010, nearly two-thirds of malicious links in news feeds observed by Symantec used shortened URLs.   
  


**Malicious URLs targeting social networking users**  
Source: Symantec

An indication of the success of using shortened URLs that lead to malicious websites is the measure of how often these links are clicked. Of the shortened URLs leading to malicious websites that Symantec observed on social networking sites over the three-month period in 2010, 73 percent were clicked 11 times or more, with 33 percent receiving between 11 and 50 clicks. Only 12 percent of the links were never clicked. Currently, most malicious URLs on social networking sites lead to websites hosting attack toolkits.   
  


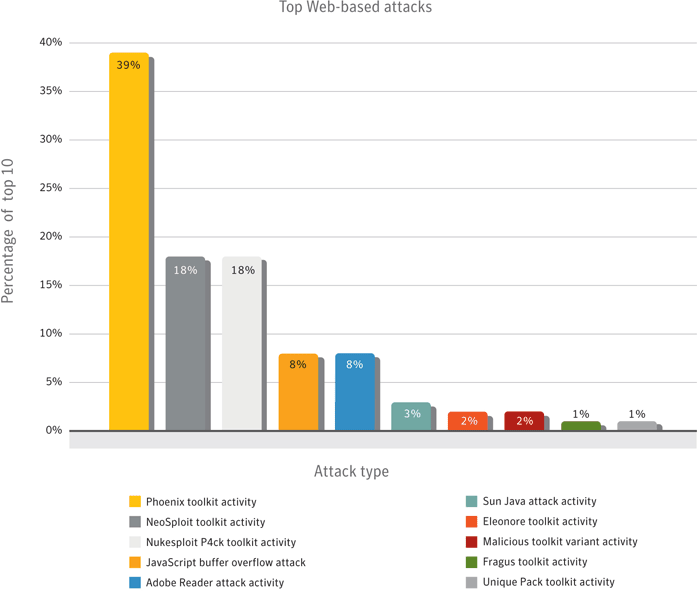
**Clicks per malicious shortened URL during three-month period in 2010**  
Source: Symantec

Other applications on social networking sites that appear to be innocuous may have a more malicious motive. Many surveys and quizzes ask questions designed to get the user to reveal a great deal of personal information. While such questions often focus on generic details (shopping tastes etc.), they may also ask the user to provide details such as his or her elementary school name, pets’ names, mother’s maiden name, and other questions that, not coincidentally, are frequently used by many applications as forgotten password reminders.   
  
As more people join social networking sites and the sophistication of these sites grows, it is likely that increasingly complex attacks will be perpetrated through them. Users should ensure that they monitor the security settings of their profiles on these sites as often as possible, especially because many settings are automatically set to share a lot of potentially exploitable information and it is up to users to restrict access themselves.   
  


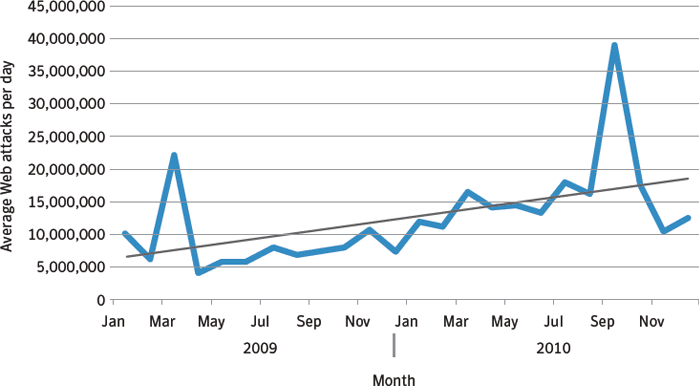
**Attack kits get a caffeine boost**

While targeted attacks are focused on compromising specific organizations or individuals, attack toolkits are the opposite side of the coin, using broadcast, blanket attacks that attempt to exploit anyone unfortunate enough to visit a compromised website. The previous edition of the Symantec *Internet Security Threat Report* discussed the growing prevalence of Web-based attacks and the increased use of attack toolkits. In 2010, these kits continued to see widespread use with the addition of new tactics.   
  
The Phoenix toolkit was responsible for the largest amount of Web-based attack activity in 2010. This kit, as well as many others, also incorporates exploits for Java vulnerabilities. The sixth highest ranked Web-based attack during the reporting period was also an attempt to exploit Java technology. One of the appeals of Java to attackers is that it is a cross-browser, multi-platform technology. This means that it runs on almost every Web browser and operating system available—a claim few other technologies can make. As such, Java can present an appealing target to attackers.

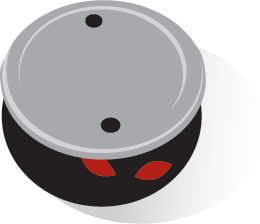
* [Symantec *Internet Security Threat Report*, Volume 15](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf)
* [Symantec *Report on Attack Kits and Malicious Websites*](http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf)



**Web-based attack activity, 2010**  
Source: Symantec

The volume of Web-based attacks per day increased by 93 percent in 2010 compared to 2009. Because two-thirds of all Web-based threat activity observed by Symantec is directly attributable to attack kits, these kits are likely responsible for a large part of this increase. The increased volume of Web-based attack activity in 2010 is not a sudden change. Although the average number of attacks per day often fluctuates substantially from month to month, depending on current events and other factors, Web-based attacks have risen steadily since Symantec began tracking this data from the beginning of 2009 through to the end of 2010. Along with other indications of increased Web-based attack usage, such as the rise in attack toolkit development and deployment, Symantec expects this trend to continue through 2011 and beyond.   
  


**Average Web attacks per day, by month, 2009-2010**  
Courtesy: Symantec

Because users are more likely to be protected against older vulnerabilities, attack toolkit developers advertise their toolkits based on the rate of success of the vulnerabilities that are included and the newness of the exploits. To remain competitive and successful, attack kit developers must update their toolkits to exploit new vulnerabilities as they emerge on the threat landscape. Because of this, the kit developers either discontinue the use of less successful exploits in favor of newer ones with higher success rates, or incorporate new exploits that the kits are programmed to try first. Thus, in the future, Java exploits may be dropped or marginalized in favor of other technologies that developers consider more vulnerable. To protect against all Web-based attacks, users should employ intrusion protection systems and avoid visiting unknown websites.   
  


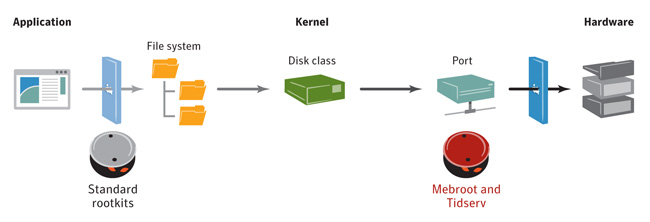
**Hide and seek**

A rootkit is a collection of tools that allows an attacker to hide traces of a computer compromise from the operating system and, by extension, the user. They use hooks into the operating system to prevent files and processes from being displayed and prevent events from being logged. Rootkits have been around for some time—the Brain virus was the first identified rootkit to employ these techniques on the PC platform in 1986—and they have increased in sophistication and complexity since then.   
  
The primary goal of malicious code that employs rootkit techniques is to evade detection. This allows the threat to remain running on a compromised computer longer and consequently increases the potential harm it can do. If a Trojan or backdoor is detected on a computer, the victim may take steps to limit the damage such as changing online banking passwords and cancelling credit cards. However, if the threat goes undetected for an extended period, this not only increases the possibility of theft of confidential information, but also gives the attacker more time to capitalize on this information.

* [Morris and the Brain](http://www.symantec.com/connect/blogs/morris-and-brain)

The current frontrunners in the rootkit arena are Tidserv, Mebratix, and Mebroot. These samples all modify the master boot record (MBR) on Windows computers in order to gain control of the computer before the operating system is loaded. While rootkits themselves are not new, this technique is a more recent development. This makes these threats even more difficult to detect by security software.

* [Read about Tidserve](http://www.symantec.com/security_response/writeup.jsp?docid=2008-091809-0911-99)
* [Trojan.Mebratix.B – the Ghost in MBR](http://www.symantec.com/connect/blogs/trojanmebratixb-ghost-mbr)
* [Learn about Mebroot](http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-010718-3448-99)



**Tidserv and Mebroot infection process**  
Source: Symantec Corporation

Many Tidserv infections were discovered by chance in February 2010 when they were uncovered by a patch issued by Microsoft for an unrelated security issue in Windows. The malicious code made some changes to the Windows kernel that caused infected computers to “blue screen” every time they rebooted after the patch was applied. Because the file infected by Tidserv is critical to Windows startup, the computers would not even start properly in Safe Mode, forcing users to replace the infected driver files with known good copies from a Windows installation CD.

* [Tidserv and MS10-015](http://www.symantec.com/connect/blogs/tidserv-and-ms10-015)
* [Microsoft Security Bulletin MS10-015 - Important](http://www.microsoft.com/technet/security/Bulletin/MS10-015.mspx)

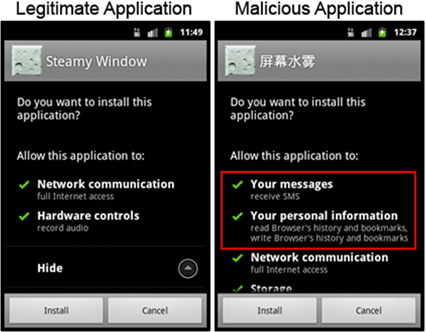
Tidserv also made news in 2010 when a version was discovered that was capable of injecting itself into 64-bit driver processes on 64-bit versions of Windows. This shows that Tidserv developers are not only still active, but they are seeking out new techniques to allow their creation to infect the most computers possible. Since the primary purpose of Tidserv is to generate revenue, this comes as no surprise.

* [Tidserv 64-bit Goes Into Hiding](http://www.symantec.com/connect/blogs/tidserv-64-bit-goes-hiding)

Computers infected with Tidserv have search queries redirected to sites hosting fake antivirus applications. By hijacking the search results, Tidserv exploits the user’s trust in the search engine they are using. Since the search terms are intercepted by the threat, the subsequently hijacked results can also be tailored to mirror the original search terms to lend a sense of credibility and potentially increase the likelihood of users falling prey to the ruse.   
  
To date, many Trojans seen in targeted attacks have not been very advanced in features or capabilities, with their primary purpose being to steal as much information as quickly as possible before discovery. However, the longer a targeted attack remains undetected, the more likely it is that information will be compromised. Considering the media attention given to recent high-profile targeted attacks such as Hydraq and Stuxnet, many network security professionals are likely operating with increased vigilance for these threats. As such, to circumvent the increased attention, attackers will likely modify their attacks and employ techniques such as rootkit exploits. Symantec expects any advancement in rootkits to eventually make their way into targeted attacks.   
  


**Mobile threats**

Since the first smartphone arrived in the hands of consumers, speculation about threats targeting these devices has abounded. While threats targeted early “smart” devices such as Symbian and Palm in the past, none of these threats ever became widespread and many remained proof-of-concept. Recently, with the growing uptake in smartphones and tablets, and their increasing connectivity and capability, there has been a corresponding increase in attention, both from threat developers and security researchers.   
  
While the number of immediate threats to mobile devices remains relatively low in comparison to threats targeting PCs, there have been new developments in the field. As more users download and install third-party applications for these devices, the chances of installing malicious applications also increases. In addition, because most malicious code now is designed to generate revenue, there are likely to be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking.   
  
As with desktop computers, the exploitation of a vulnerability can be a way for malicious code to be installed on a mobile device. In 2010, there were a significant number of vulnerabilities reported that affect mobile devices. Symantec documented 163 vulnerabilities in mobile device operating systems in 2010, compared to 115 in 2009. While it may be difficult to exploit many of these vulnerabilities successfully, there were two vulnerabilities that affected Apple’s iPhone iOS operating platform that allowed users to “jailbreak” their devices. The process of jailbreaking a device through exploits is not very different from using exploits to install malicious code. In this case, though, users would have been exploiting their own devices.

  
**Pjapps installation screen**  
Source: Symantec

Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile app marketplaces in the hopes that users will download and install them. In March 2011, Google reported that it had removed several malicious Android applications from the Android Market and even deleted them from users’ phones remotely. Attackers also take a popular legitimate application and add additional code to it, as happened in the case of the Pjapps Trojan for Android devices. Astute users were able to spot that something was amiss when the application was requesting more permission than should have been necessary.   
  
Until recently, most Trojans for mobile devices simply dialed or texted premium rate numbers from the phone. While Pjapps also contains this capability, it also attempts to create a bot network out of compromised Android devices. While the command-and-control servers that Pjapps is programmed to contact no longer appear to be active, the attempt to create a botnet out of mobile devices demonstrates that attackers are actively researching mobile devices as a platform for cybercrime.

* [An Update on Android Market Security](http://googlemobile.blogspot.com/2011/03/update-on-android-market-security.html)
* [ComputerWorld article: Google throws 'kill switch' on Android phones](http://www.computerworld.com/s/article/9213641/Google_throws_kill_switch_on_Android_phones)
* [Android Threats Getting Steamy](http://www.symantec.com/connect/blogs/android-threats-getting-steamy)

Over the last several years, most malicious online activity has focused on generating revenue. While mobile device Trojans have made attempts at revenue generation through premium-rate services, this is still not as profitable as credit card fraud and the theft of online banking credentials. Some of the first threats of this kind to arrive will likely be either phishing attacks or Trojans that steal data from mobile devices. Because the blueprints for such threats are already well established on personal computers, adapting them to mobile devices should be relatively easy. For example, as mobile devices introduce new features such as wireless payments it is likely that attackers will seek ways to profit from them the way they have with personal computers. Attackers are constantly looking for new avenues to exploit and profit from unsuspecting users, but until there is adequate return on investment to be found from exploiting new devices, they will continue to use tried and true methods.

* [PCMag.com article: Apple Hires Near-Field Communications Manager](http://www.pcmag.com/article2/0,2817,2367840,00.asp)

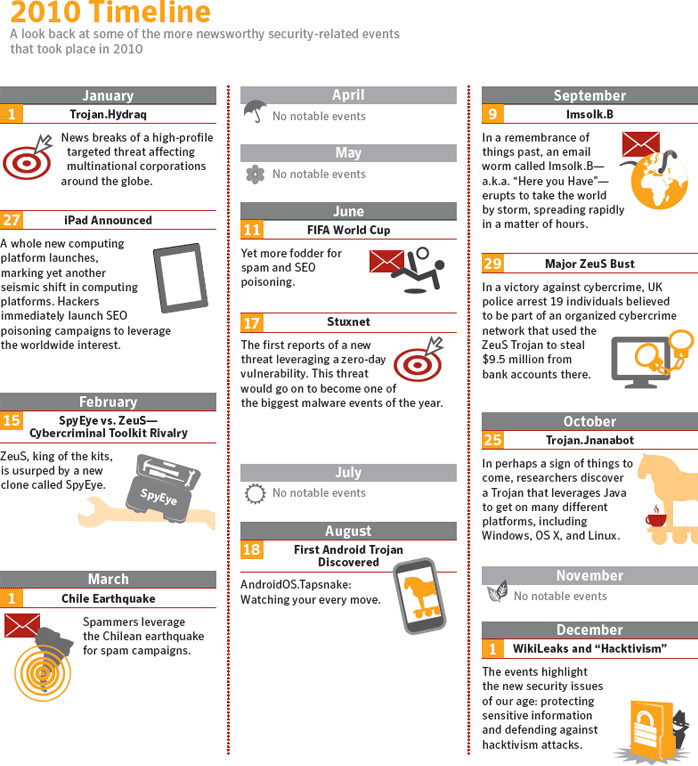
**Conclusion**

The volume and sophistication of malicious activity increased substantially in 2010. The Stuxnet worm became the first piece of malicious code able to affect physical devices while simultaneously attempting exploits for an unprecedented number of zero-day vulnerabilities. While it is highly unlikely that threats such as Stuxnet will become commonplace because of the immense resources required to create it, it does show what a skilled group of highly organized attackers can accomplish. Targeted attacks of this nature, along with Hydraq and others, have shown that determined attackers have the ability to infiltrate targets with research and social engineering tactics alone. This matters because recent studies have shown that the average cost per incident of a data breach in the United States was $7.2 million USD, with the largest breach costing one organization $35.3 million USD to resolve. With stakes so high, organizations need to focus their security efforts to prevent breaches.

* [2010 Annual Study: U.S. Cost of a Data Breach](http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf)

Social networking sites provide companies with a mechanism to market themselves online, but can also have serious consequences. Information posted by employees on social networking sites can be used in social engineering tactics as part of targeted attacks. Additionally, these sites also serve as a vector for malicious code infection. Organizations need to create specific policies for sensitive information, which may inadvertently be posted by employees, while at the same time be aware that users visiting these sites from work computers may introduce an avenue of infection into the enterprise network. Home users also need to be aware of these dangers because they are at equal risk from following malicious links on these sites.   
  
Attack toolkits continue to lead Web-based attack activity. Their ease of use combined with advanced capabilities make them an attractive investment for attackers. Since exploits for some vulnerabilities will eventually cease to be effective, toolkit authors must incorporate new vulnerabilities to stay competitive in the marketplace. Currently, attackers are targeting certain exploits, such as those for Java vulnerabilities. However, this could change if their effectiveness diminishes. Toolkit authors are constantly adapting in order to maximize the value of their kits.   
  
While the purpose of most malicious code has not changed over the past few years as attackers seek ways to profit from unsuspecting users, the sophistication of these threats has increased as attackers employ more features to evade detection. These features allow malicious code to remain resident on infected computers longer, thus allowing attackers to steal more information and giving them more time to use the stolen information before the infections are discovered. As more users become aware of these threats and competition among attackers increases, it is likely that more threats will incorporate rootkit techniques to thwart security software.   
  
Currently, mobile threats have been very limited in the number of devices they affect as well as their impact. While these threats are not likely to make significant inroads right away, their impact is likely to increase in the near future. To avoid the threats that currently exist, users should only download applications from regulated marketplaces. Checking the comments for applications can also indicate if other users have already noticed suspicious activity from installed applications.  
  
1URL shortening services allow people to submit a URL and receive a specially-coded shortened URL that redirects to the submitted URL

**2010 Timeline**



**Source: Symantec Corporation**

**Threat Activity Trends Introduction**

The following section of the Symantec *Internet Security Threat Report* provides an analysis of threat activity, as well as other malicious activity, and data breaches that Symantec observed in 2010. The malicious activity discussed in this section not only includes threat activity, but also phishing, malicious code, spam zombies, bot-infected computers, and attack origins. 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 activities can be found in their respective sections within this report.  
  
This section discusses the following metrics, providing analysis and discussion of the following trends:

* Malicious activity by source
* Web-based attack prevalence
* Web-based attack activity
* Malicious websites by search term
* Data breaches that could lead to identity theft
  + By sector
  + By cause
  + Type of information exposed in deliberate breaches
* Malicious shortened URLs on social networking sites
* Bot-infected computers

**Malicious Activity by Source**

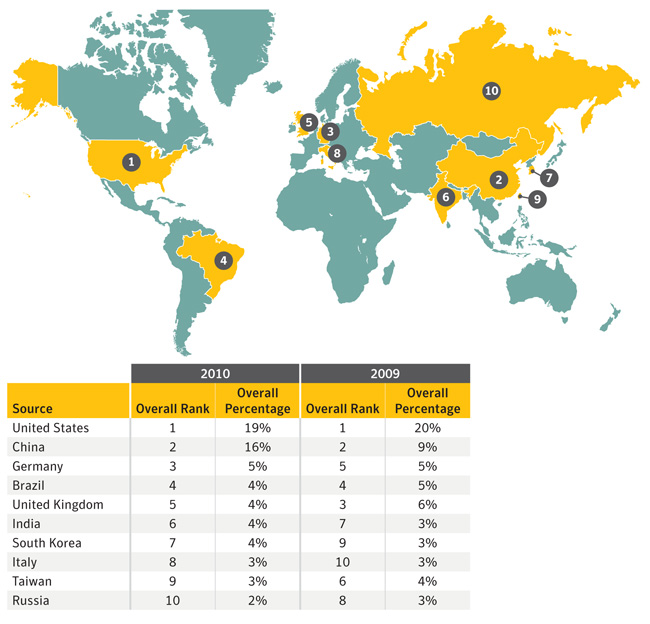
**Background**

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically a more stable connection. Symantec categorizes malicious activities as follows:   
  
**Malicious code:** This includes viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, or compromising the security or integrity of a victim’s computer data.  
  
**Spam zombies:** These are compromised systems that are remotely controlled and used to send large volumes of junk or unsolicited emails. These emails can be used to deliver malicious code and phishing attempts.  
  
**Phishing hosts:** A phishing host is a computer that provides website services for the purpose of attempting to illegally gather sensitive, personal and financial information while pretending that the request is from a trusted, well-known organization. These websites are designed to mimic the sites of legitimate businesses.  
  
**Bot-infected computers:** These are compromised computers that are being controlled remotely by attackers. Typically, the remote attacker controls a large number of compromised computers over a single, reliable channel in a bot network (botnet), which is then used to launch coordinated attacks.  
  
**Network attack origins:** This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.

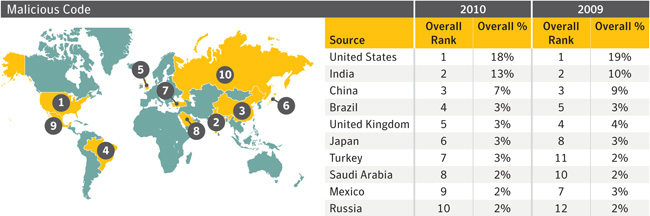
**Methodology**

This metric assesses the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing hosts, bot-infected computers, and network attack origin.   
  
The proportion of each activity originating in each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

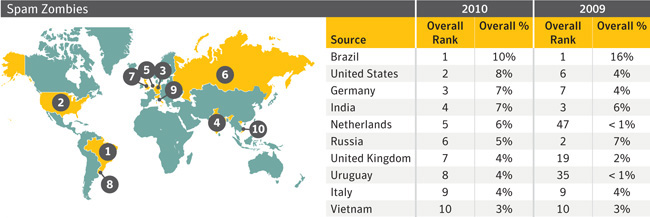
**Data**



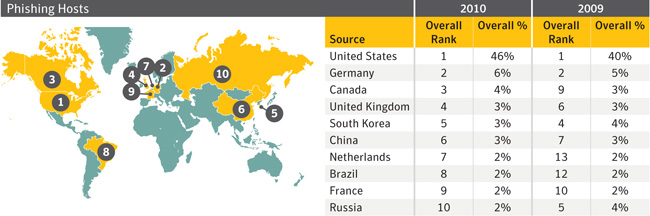
**Table 1. Malicious activity by source: overall rankings, 2009–2010**  
Source: Symantec Corporation



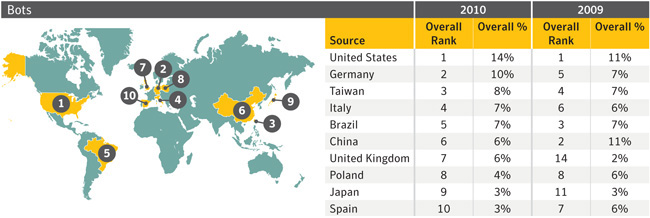
**Table 2. Malicious activity by source: malicious code, 2009–2010**  
Source: Symantec Corporation



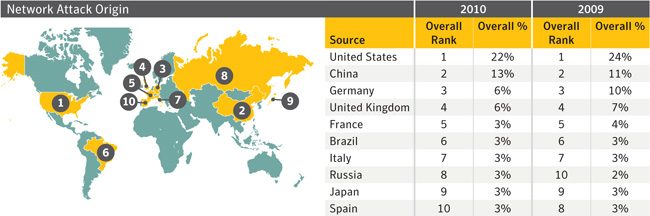
**Table 3. Malicious activity by source: spam zombies, 2009–2010**  
Source: Symantec Corporation



**Table 4. Malicious activity by source: phishing hosts, 2009–2010**  
Source: Symantec Corporation



**Table 5. Malicious activity by source: bots, 2009–2010**  
Source: Symantec Corporation



**Table 6. Malicious activity by source: network attack origins, 2009–2010**  
Source: Symantec Corporation

**Commentary**

**Frontrunners continue to pull away from the pack:** In 2010, the United States and China were once again the top sources for overall malicious activity. The United States saw an increase in spam zombies, phishing hosts, and bot-infected computers during this reporting period, which are all related to botnet activity. The United States is the main source of bot-infected computers for Rustock, one of the largest and most dominant botnets in 2010, and for the botnet associated with the Tidserv Trojan. At the end of 2010, Rustock was estimated to have 1.1 million to 1.7 million bots and accounted for 48 percent of all botnet spam sent out during the year. The Tidserv Trojan uses an advanced rootkit to hide itself on a computer, and over half of all infected computers that were part of this botnet were located in the United States in 2010. As such, these factors would have contributed to the increases in spam zombie and bot-infection percentages for the United States. China's rise as a source of malicious activity is related to a spike in Web-based attacks originating from compromised computers and Web servers based there. Much of this activity was linked to ZeuS activity. Symantec will monitor this activity and provide more detail in future reports if the activity continues.

* [Learn about the Rustock Trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99)
* [Read about the Tidserve trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2008-091809-0911-99)
* [MessageLabs Intelligence: 2010 Annual Security Report](http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf)

**Jockeying for position after the frontrunners:** The bottom eight of the top 10 sources continue to be separated by a narrow margin. Beyond the United States and China, there was only a 4 percent difference (after rounding) for overall malicious activity between the remaining eight sources of the top 10 during this reporting period. The same limited percentage difference was also the case in 2009. This suggests that it would only take a small shift in the overall malicious activity landscape to affect the rankings. As such, it may be likely that the rankings of the countries in this bottom eight group for malicious activity will vary for the next reporting period without any dramatic shifts in malicious activity occurring.  
  
**Spam zombies drop significantly in China:** China’s rank in spam zombies dropped from eighth in 2009 to 23rd in 2010. This drop in spam zombie activity may be related to the drop in spam originating from China in 2010, which, in turn, may be due to increased regulations governing domain registration there. Potential registrants can no longer register a .cn domain name anonymously and are required to provide paper application forms, official business seals, and an identity card. The amount of spam originating from .cn domains has decreased from over 40 percent of all spam detected in December 2009 to less than 10 percent by March 2010. The decrease in spam originating from China may also be due to new regulations issued by China’s Ministry of Information Industry (MII) in March 2010. These regulations require all ISPs to register the IP addresses of their email servers with Chinese authorities and to maintain logs of all email traffic for at least 60 days.

* [A Drop in .cn Spam](http://www.symantec.com/connect/blogs/drop-cn-spam)
* [State of Spam and Phishing Report, February 2010](http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_and_phishing_report_02-2010.en-us.pdf)
* [Global Times article: China no longer a top spam mail sender](http://www.globaltimes.cn/www/english/sci-edu/china/2010-05/529639.html)

**Spam zombies dominant in Brazil:** Brazil has ranked first in spam zombies for the past three reporting periods. Factors that influence this high ranking may include the prominence of large, dominant botnets in Brazil. Brazil is a strong source of bot-infected computers for major botnets that send out spam email messages, including Rustock, Maazben, and Ozdok (Mega-D).

* [MessageLabs Intelligence: 2010 Annual Security Report](http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf)
* [Evaluating Botnet Capacity](http://www.symantec.com/connect/blogs/evaluating-botnet-capacity)
* [Read about the Ozdok (Mega-D) trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99)

**Web-Based Attack Prevalence**

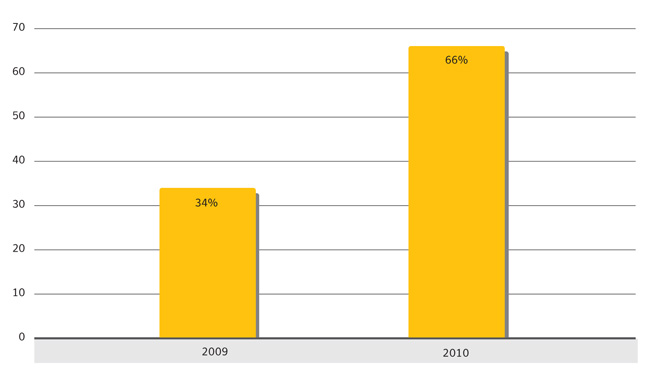
**Background**

The circumstances and implications of Web-based attacks vary widely. They may target specific businesses or organizations, or they may be widespread attacks of opportunity that exploit current events, zero-day vulnerabilities, or recently patched and publicized vulnerabilities against which some users are not yet protected. While some major attacks garner significant attention when they occur, examining overall Web-based attacks provides insight into the threat landscape and how attack patterns may be shifting. Moreover, analysis of the underlying trend can provide insight into potential shifts in Web-based attack usage and can assist in determining the likelihood of Web-based attacks increasing in the future.

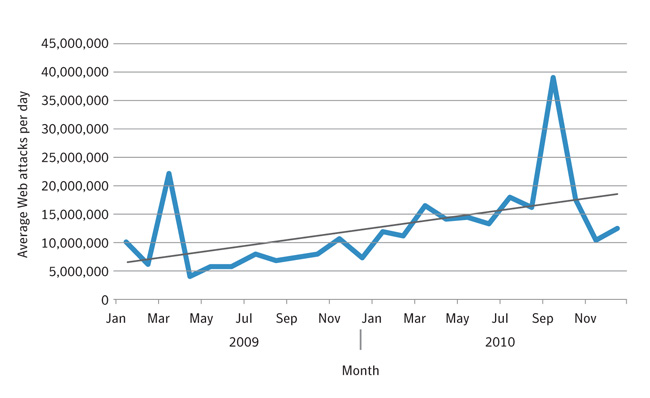
**Methodology**

This metric assesses changes to the prevalence of Web-based attack activity by comparing the overall volume of activity and the average number of attacks per day in each month during the current and previous reporting periods. These monthly averages are based on telemetry data of opt-in participants and, therefore, may not be directly synonymous with overall activity levels or fluctuations that occurred as a whole. However, underlying trends observed in the sample data provide a reasonable representation of overall activity trends.

**Data**



**Figure 1. Web-based attack activity, 2009–2010**  
Source: Symantec Corporation



**Figure 2. Average Web attacks per day, by month, 2009–2010**  
Source: Symantec Corporation

**Commentary**

**Web-based attacks nearly double:** The number of daily Web-based attacks observed was 93 percent higher in 2010 than in 2009. This may not be surprising given the pervasiveness of Web-based attacks fueled by growing cybercriminal activity, as discussed in reports such as the Symantec *Report on Attack Kits and Malicious Websites*; however, the substantial difference in yearly proportions suggests that these attacks will continue to increase in the future.

* [Symantec *Report on Attack Kits and Malicious Websites*](http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf)

**Consistent upward trend:** The increased volume of Web-based attacks in 2010 was not a sudden change. Although the average number of attacks per day often fluctuates substantially from month to month, depending on current events and other factors, Web-based attacks have risen steadily since Symantec began tracking this data from the beginning of 2009 through 2010. Given the other indications of increased Web-based attack usage, such as the rise in attack toolkit development and deployment, Symantec expects this trend to continue.   
  
**About the anomalous activity fluctuations:** There are two spikes in attack-related activity worth mentioning—in March 2009 and September 2010. While these fluctuations stand out as significant, they are anomalous to the overall activity observed and are not likely to have a substantial or long term affect on underlying trends.

* The spike in March is mainly due to fluctuations from reports of several generic attacks. This may have been the result of abnormally widespread attack campaigns that capitalized on compromised high-traffic websites or successful black hat SEO campaigns that targeted significantly popular search terms during the month.
* The spike in September may be due to the high volume of activity related to the Tidserv Trojan. This may have been the result of attackers ramping up attacks in an attempt to increase the number of computers they affect and deploying new Tidserv variants to change or add functionality. For example, the Tidserv.L variation was discovered August 25, 2010. Attackers may also have been sending out large volumes of communications to Tidserv compromised computers to provide them with updated configuration and attack information.
* [Learn about the Tidserve Trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2008-091809-0911-99)
* [Read about the Tidserve.L Trojan variation](http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-082514-3812-99)

**Web-Based Attack Activity**

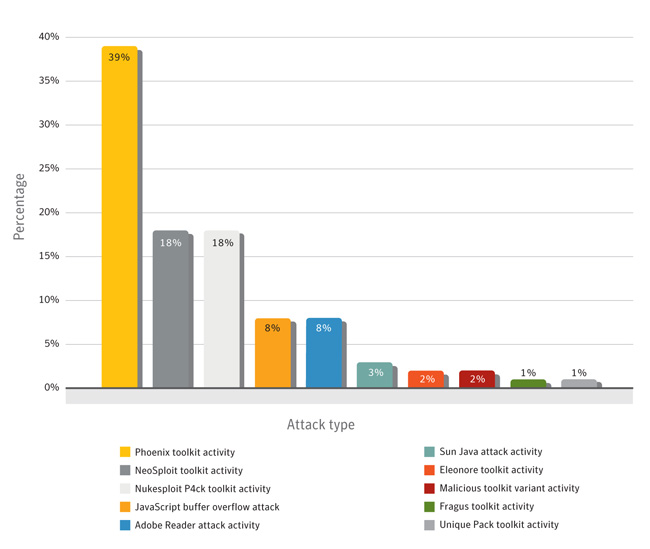
**Background**

The increasing pervasiveness of Web browser applications—along with increasingly common, easily exploited Web browser application security vulnerabilities—has resulted in the widespread growth of Web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers. Symantec analyzes attack activity to determine which types of attacks and attack toolkits are being used by attackers. This can provide insight into emerging Web attack trends and may indicate the types of attacks with which attackers are having the most success.

**Methodology**

This metric assesses the top Web-based attack activity originating from compromised legitimate sites and intentionally malicious sites set up to target Web users in 2010. To determine this, Symantec ranks attack activity by the volume of associated reports observed during the reporting period. The top 10 Web-based attack activities are analyzed for this metric.

**Data**



**Figure 3. Web-based attack activity**  
Source: Symantec Corporation

**Commentary**

**Phoenix is rising:** The most prominent volume of Web-based attack activity observed in 2010 was related to the Phoenix toolkit. Security researchers first observed this toolkit in 2009, although it is rumored to have been first released in 2007. This activity refers to the attempts to download and execute exploit code that is specific to the Phoenix toolkit. Some versions of Phoenix exploit as many as 16 vulnerabilities that affect multiple technologies. These include Sun Java SE, Microsoft Windows Media Player, Microsoft Internet Explorer, Adobe Flash Player, and Adobe Reader. Successful attacks may install a specific rogue security software application (PC Defender Antivirus) onto compromised computers.

* [PCDefender](http://www.symantec.com/security_response/writeup.jsp?docid=2010-021812-5220-99)
* [Microsoft Windows Media Player Plugin Buffer Overflow Vulnerability](http://www.securityfocus.com/bid/16644)
* [Microsoft Active Template Library Header Data Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/35558)
* [Adobe Flash Player Multimedia File Remote Buffer Overflow Vulnerability](http://www.securityfocus.com/bid/28695)
* [Adobe Acrobat and Reader CVE-2010-0188 Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/38195)

**Java is being targeted:**

* **Java presents an attractive point of attack for attackers:** As evidenced by activity related to the Phoenix attack kit, as well as numerous other kits that successful employ Java exploits, Java presents an attractive point of attack for attackers. Furthermore, the sixth ranked Sun Java attack activity refers to Java attacks that are not directly relatable to a specific attack toolkit. In some cases, the exploit code used in these attacks may be the same across multiple kits if the authors acquired the code from the same source.
* **Attackers may begin favoring Java exploits:** Detecting Java attacks can be challenging because the technology relies on a runtime environment that adds additional layers of processing that need to be analyzed. While Java attacks that occurred in 2010 gained a significant amount of attention, they may not have been launched as frequently as attacks that exploited other technologies. One reason for this may be that attack toolkits often launch attacks in a sequence, trying one exploit after another until an exploit succeeds, all options are exhausted, or the source of the attacks is blocked by the victim. This could result in blocked or successful attacks occurring prior to the Java exploits being launched. Over time, attackers may begin weighting the sequence of attack attempts in favor of those that exploit Java vulnerabilities in order to increase their chances of success.
* **Symantec expects the volume of Java-related attacks to increase:** The authors of newly released kits such as Dragon Pack and Bleeding Life have been touting the success of included Java exploits. As a result, Symantec expects the volume of Java-related attacks to increase.
* [“Perfect” Client-Side Vulnerabilities](http://www.symantec.com/connect/blogs/perfect-client-side-vulnerabilities)
* [Microsoft: ‘Unprecedented Wave of Java Exploitation’](http://krebsonsecurity.com/2010/10/microsoft-a-tidal-wave-of-java-exploitation/)
* [Exploit Packs Run on Java Juice](http://krebsonsecurity.com/2011/01/exploit-packs-run-on-java-juice/)

**Malicious Websites by Search Term**

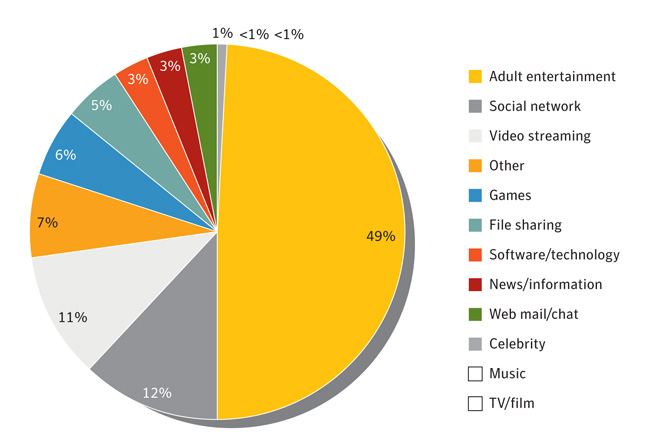
**Background**

This section discusses search terms used to lure potential victims to malicious websites. Broad website categories can be determined by categorizing common search terms that result in malicious websites being visited. This may provide insight into what sort of legitimate websites attackers try to compromise the most. This may also indicate the categories of Web pages and search terms that attackers try to exploit the most when performing black hat search engine optimization (SEO). Black hat SEO is the technique of trying to get a URL ranked higher by a search engine than it would be without interference.

**Methodology**

The data for this metric consists of a collection of unique terms used in searches that resulted in malicious websites being visited, and the number of malicious website hits that subsequently occurred. When the use of a search term results in a malicious website being visited, the incident is counted as a malicious website hit. The rank of each unique search term is then determined based on the volume of malicious website hits that have occurred. This metric analyzes the top 100 search terms based on the Latin alphabet and with logical meaning. Note that, while Symantec has categorized terms wherever possible, the “other” category consists of generic terms where no straightforward categorization was logically feasible.

**Data**



**Figure 4. Malicious websites by search term type**  
Source: Symantec Corporation

**Commentary**

**Most searches are for specific domain names:** Of the volume of the top 100 search terms analyzed, 81 percent of the searches were for specific sites by domain name. This reinforces indications that attackers are attempting to capitalize on legitimate websites to target potential victims. Of this percentage, 5 percent were misspelled domain names, and all of these were in the video streaming category. This indicates that attackers were using typosquatting methods. Typosquatting is when attackers register a domain name that closely resembles a legitimate website (e.g., synantec.com) and then present a mock (and maliciously coded) replica website at that address in the hope that users making the typo do not realize their error. In addition, if they can get the mock site ranked high by search engines, users may think the site is valid and click on the listing without looking too closely at the actual URL.   
  
**Attacks play on base emotions:** The prominence of adult entertainment search terms in this metric is not surprising given the popularity of online adult entertainment.

* According to one estimate, 12 percent of all websites are pornographic and over 28,000 people are viewing these sites every second.
* One reason why attackers target adult websites is that many of these sites act as Web portals that aggregate the content of numerous other sites without any direct association with them. Given this, visitors to such portals may be more accepting of content from unknown or unfamiliar sources.
* Another reason may be due to the widespread use of multimedia on these sites. Many adult sites use leading browser multimedia applications, which visitors would require in order to view content. (It should be noted that many of the search terms that Symantec categorized in adult entertainment are primarily adult video streaming websites and, thus, were not included in the video streaming category to negate duplicated results).
* [cnet article: Sunday is most popular day for online porn](http://news.cnet.com/8301-17852_3-20006703-71.html#ixzz1HYXYHw78)

**Attackers are targeting social networks:** Social networks are being used to deliver an increasing range of multimedia content. As noted with adult sites, this presents a broader selection of potential vulnerabilities for the attacker to exploit. Moreover, because social network users believe they are among friends, they may be more willing to open links or download unknown files if they trust the source. A successful attack that dupes victims in this manner can then spread further via the web of friendships, thus increasing the likelihood of successful attacks on subsequent victims.   
  
**The case of the missing plug-in:** One reason for the high ranking of video streaming in this metric is due to a common ploy with video files online. To get victims to download malicious payloads, attackers present pop-ups or other prompts that tell the visitor that he or she requires additional components to view or open certain files. While this ploy is used across many Internet technologies, video codecs are especially exploited in this manner because there is a wide range of different platforms available for viewing video. Users would possibly accept these prompts because of this. These “missing codecs” are often laden with malicious payloads.  
  
**Yet more multimedia:** As with adult and social networking terms, the percentage of search terms observed in the video streaming category is not surprising considering the current popularity of streaming video websites. By using these sites to initiate attacks, attackers are capitalizing on a very large traffic base of users. As with adult video entertainment, in order to view content, users of general audience video streaming websites must ensure that their browsers are equipped with the necessary plug-ins. Therefore, attackers using toolkits that exploit vulnerabilities in these plug-ins may have an increased chance of success if they launch attacks from these sites.   
  
**The importance of caution:** The results of this data analysis underscore how Web users should exercise caution, regardless of the websites they visit on a regular basis or those that they may visit on a one-off search for something out of the ordinary. Additionally, Web users should ensure that domain names are correctly spelled when browsing directly to a website or searching for a specific domain.

**Data Breaches That Could Lead to Identity Theft**

**Background**

Identity theft continues to be a high-profile security issue, particularly for organizations that store and manage large amounts of personal information. Not only can compromises that result in the loss of personal data undermine customer and institutional confidence, they can result in damage to an organization’s reputation and can be costly for individuals recovering from the resulting identity theft. In 2010, the average cost per incident of a data breach in the United States was $7.2 million, an increase of 7 percent from 2009 (all figures in USD). The most expensive data breach to resolve cost one organization $35.3 million.

* [2010 Annual Study: U.S. Cost of a Data Breach](http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf)

Many countries have existing data breach notification legislation that regulates the responsibilities of organizations conducting business within the particular government after a data breach has occurred. For example, in the United States, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have all enacted legislation requiring notification of security breaches involving personal information.

* [State Security Breach Notification Laws](http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx)

**Methodology**

Using publicly available data provided by the Open Security Foundation (OSF) Dataloss DB, Symantec determines the sectors that were most often affected by these breaches, as well as the most common causes of data loss. The OSF records data breaches that have been reported by legitimate media sources and have exposed personal information, including name, address, Social Security number, credit card number, or medical history. The sector that experienced the loss along with the cause of loss that occurred is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

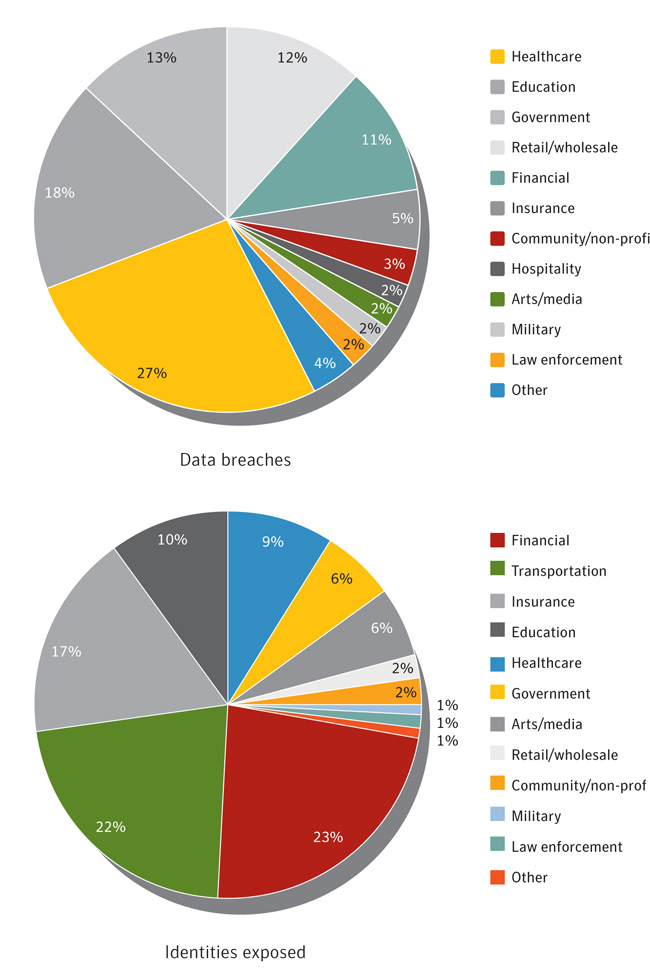
* [Open Security Foundation](http://datalossdb.org/)

This discussion also explores the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data. An identity is considered exposed if personal or financial data related to the identity is made available through the data breach. A data breach is considered deliberate when the cause of the breach is due to hacking, insider intervention, or fraud. A data breach is considered to be caused by hacking if data related to identity theft was exposed by attackers external to an organization gaining unauthorized access to computers or networks. A data breach is considered to be caused by insecure policy if it can be attributed to a failure to develop, implement, and/or comply with adequate security policy.  
  
It should be noted that some sectors may need to comply with more stringent reporting requirements for data breaches than others do. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports. (For one example of this, please see the Fair and Accurate Credit Transactions Act of California.) Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are not required or encouraged to report data breaches may be under-represented in this data set.

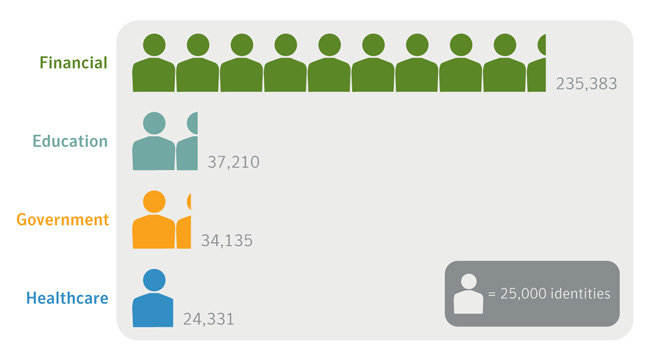
* [Facts on FACTA, the Fair and Accurate Credit Transactions Act](http://www.privacyrights.org/fs/fs6a-facta.htm)

**Data Breaches That Could Lead to Identity Theft, by Sector**

**Data**



**Figure 7. Data breaches that could lead to identity theft and identities exposed, by sector**  
Source: Based on data provided by OSF DataLossDB (due to rounding, percentages may not total 100 percent)



**Figure 8. Average number of identities exposed per data breach, by notable sector**  
Source: Based on data provided by OSF DataLossDB

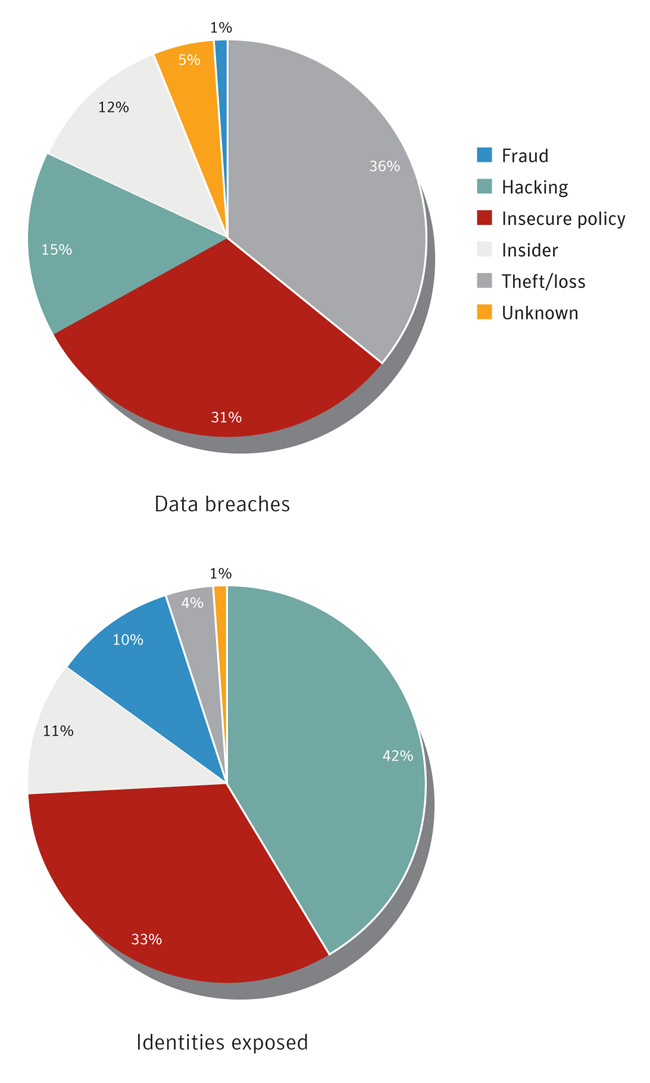
**Commentary**

**A high number of data breaches does not necessarily equate to identities exposed:** The top three sectors reporting data breaches in 2010 (healthcare, education, and government) accounted for only a quarter of all identities exposed during the reporting period. This is due to the small number of identities exposed in each of the data breaches in these sectors. In 2010, the average number of identities exposed per data breach for each of these sectors was less than 38,000, whereas the average number of identities exposed per breach for the financial sector was 236,000.   
  
**Large-scale breaches are likely to result in more identities exposed:** The top sector for identities exposed in 2010, the financial sector (at 23 percent) also had the highest average number of identities exposed per incident (235,383). Much of this is due to a breach in March 2010 when a financial sector organization exposed sensitive information on 3.3 million customers, including government-issued identification numbers.

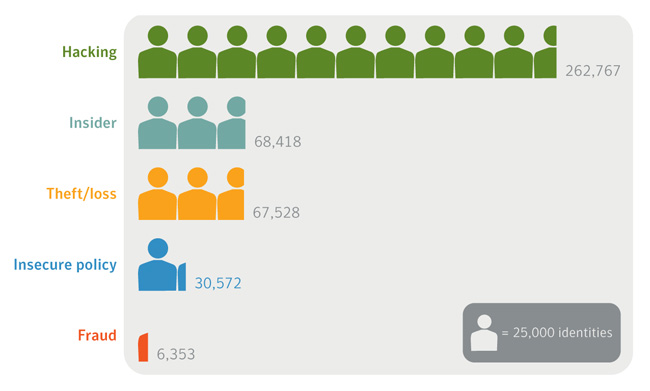
* [The Wall Street Journal article: Data Theft at Loan Firm Hits Borrowers](http://online.wsj.com/article/SB10001424052748704100604575146360834054370.html)

**Breaches That Could Lead to Identity Theft, by Cause**

**Data**



**Figure 9. Data breaches that could lead to identity theft and identities exposed, by cause**  
Source: Based on data provided by OSF DataLossDB (due to rounding, percentages may not total 100 percent)



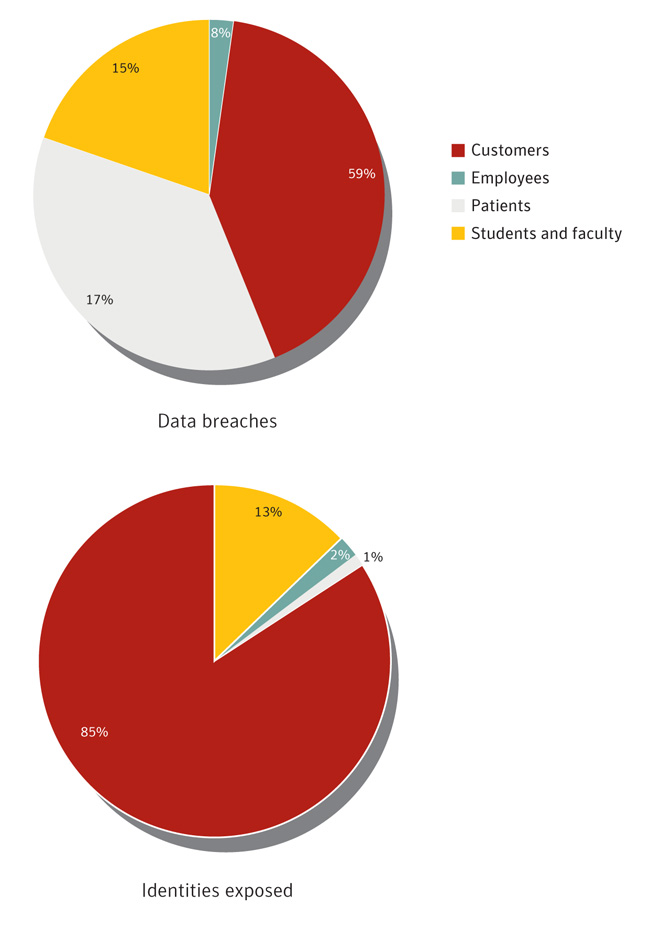
**Figure 10. Average number of identities exposed per data breach, by cause**  
Source: Based on data provided by OSF DataLossDB

**Commentary**

**Data breaches are costly and many are easily preventable:** The average cost to resolve a data breach in 2010 was $7.2 million. Of the various causes of data breaches, those due to insecure policy are readily preventable. Insecure policy was the second most common cause of data breaches across all sectors that could lead to identity theft in 2010, responsible for nearly one third of the total. Many data breaches due to insecure policy can be prevented with measures such as the development of stronger security policies and ensuring that all users are educated in company security and data management policies.   
  
**Hacking continues to be the leading cause for identities exposed:** Although hacking was only the third most common cause of data breaches that could lead to identity theft in 2010, it was the top cause for reported identities exposed, with 42 percent of the total. In 2009, hacking was responsible for 60 percent of identities exposed. The average number of identities exposed per data breach was 262,767, with the three largest reported breaches accounting for 7.4 million identities exposed.

**Type of information exposed in deliberate breaches**

**Data**



**Figure 11. Type of information exposed in deliberate breaches**  
Source: Based on data provided by OSF DataLossDB (due to rounding, percentages may not total 100 percent)

**Customers are the favorite target:** Customer-related information was the most exposed type of data in 2010, both for deliberate breaches and the identities exposed in those breaches. Customer-related data may be more attractive because it typically contains financial information such as credit card numbers and bank account numbers that can be used for lucrative fraud schemes and large financial payouts. For example, in one insider-driven data breach, an employee stole customer information and used it to commit fraud to the amount of $150,000. In another case, employees used stolen customer credentials to file fraudulent tax claims. Upon discovery, the alleged culprits had $290,000 spread across 17 bank accounts.

**Malicious Shortened URLS on Social Networking Sites**

**Background**

Shortened URLs have become popular in recent years as a means of conserving space in character-limited text fields, such as those used for microblogging. Some URLs consist of a substantial number of characters that can eat up character limits, break the flow of text, or cause distortions in how Web pages are rendered for users. URL shortening services allow people to submit a URL and receive a specially-coded, shortened URL that redirects to the original URL. When a user clicks on the shortened URL, the service will redirect the person to the submitted Web page.  
  


**Figure 12. Example of a shortened URL**  
Source: Symantec Corporation

These services can be very convenient when referring people to Web pages that have very long URLs. However, attackers capitalize on these services because potential victims are usually unable to determine where the URL will send them. An example of this involves attackers mimicking popular posts, but replacing legitimate URLs with shortened ones in the hopes that users will be less likely to notice that the URL has been changed.  
  
Social networking sites provide an effective platform from which to launch this sort of attack. Users who see a link posted by a friend may be more likely to trust the integrity of the link and may click on it with little fear of danger. Therefore, an attacker who compromises a social networking account can post URLs linking to malicious websites and prey on the trust of the social network connected to that account in order to launch attacks. One example of how attackers can perform these attacks is the Koobface worm, which spreads through social networks by posting URLs to videos.

* [Turning Good News into Bad News](http://www.symantec.com/connect/blogs/turning-good-news-bad-news)
* [Read about the Koobface worm](http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99)

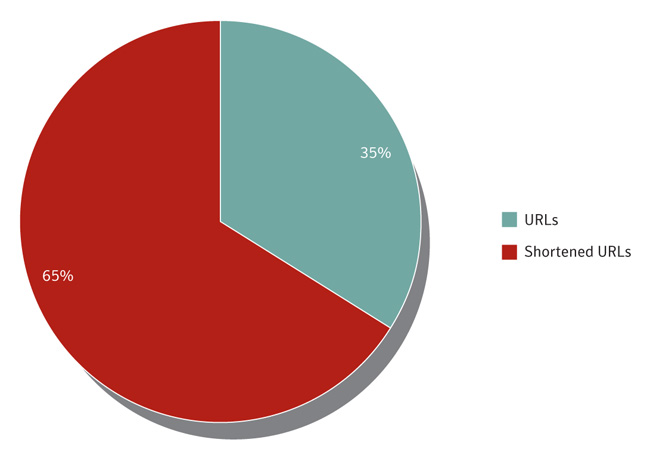
The concept of a malicious URL shortening service has even been proposed. The idea of the conceptual malicious service is that it would perform two tasks. First, it would secretly use a victim’s browser to perform a denial-of-service attack on a website, as defined by the attacker. Second, it would refer victims to a website, which may or may not be legitimate. In this way, attackers could perform attacks using shortened URLs as described above while also using the computer resources of victims to attack other targets.

* [Spare Clock Cycles article: The Evil URL Shortener](http://spareclockcycles.org/2010/12/19/d0z-me-the-evil-url-shortener/)

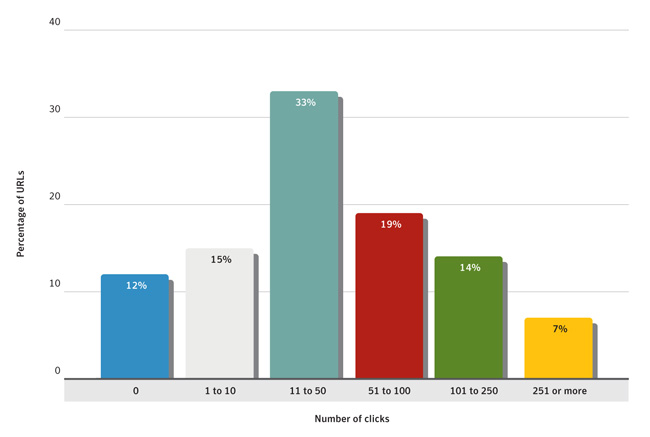
**Methodology**

This metric analyzes malicious URLs that Symantec observed on social networking sites during a three-month period in 2010. The number of malicious URLs observed is compared to the number of shortened URLs observed to determine the prevalence of URL shortening services in these attacks. The number of times each shortened URL was clicked is examined to determine the number of potentially successful attacks associated with each URL. This may provide insight into the overall effectiveness of this type of attack.

**Data**



**Figure 13. Malicious URLs targeting social networking users**  
Source: Symantec Corporation



**Figure 14. Clicks per malicious shortened URL**  
Source: Symantec Corporation

**Commentary**

**Shortened malicious URLS observed more often:** During the three-month observation period in 2010, 65 percent of the malicious URLs observed on social networks were shortened URLs. Because shortened URLs were clearly more prominent during this time, it is difficult to say if this suggests an overall preference by attackers. Changes to this percentage in coming years may indicate the differing levels of overall success that attackers are experiencing between long and shortened URLs.  
  
**Majority of shortened malicious URLs lure potential victims:** Of the shortened URLs observed, 88 percent were clicked at least once, suggesting that this is an effective method for attackers to launch attacks on unsuspecting users. This indicates that shortened URLs are a reliable means for attackers to launch attacks on social networking sites.  
  
**Shortened URL click volumes:** In measuring the click-through rate, 33 percent of shortened malicious URLs were clicked between 11 and 50 times. It is difficult to determine why the number of shortened URLs that received more than 50 or less than 11 clicks was so low in comparison. One possible reason is the speed at which information moves through social networks. Users who receive posts from a large pool of people may not have time to read every post they receive, let alone click on every posted link. Another possibility is that some of these URLs were posted on user accounts that had fewer than 100 friends associated with the account and therefore would have a relatively limited exposure. Reaction to and removal of some of the malicious URLs by the administrators of the social networks may also have limited the amount of clicks they received.

**Bot-Infected Computers**

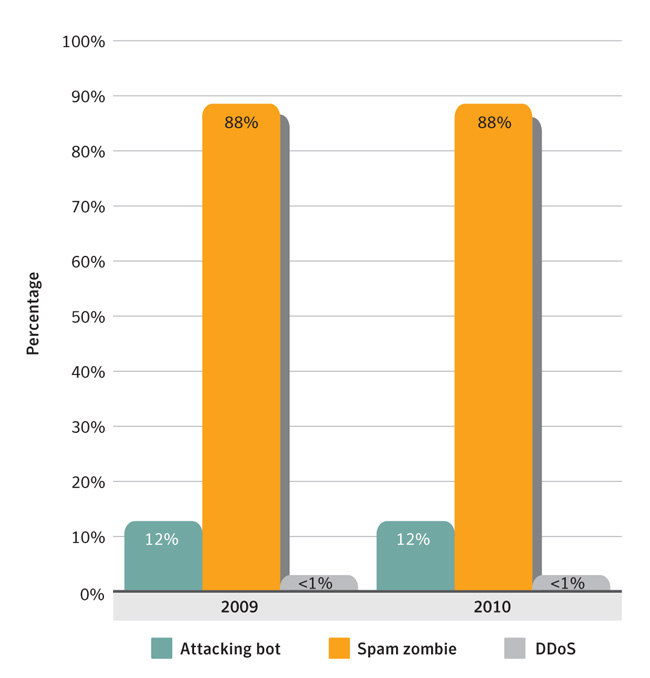
**Background**

Bot-infected computers, or bots, are programs that are covertly installed on a user’s machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet relay chat (IRC), P2P, or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a 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 organization’s website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information that may be used in identity theft from compromised computers—all of which can lead to serious financial and legal consequences.   
  
Attackers favor bot-infected computers with a decentralized command-and-control (C&C) model because they are difficult to disable and allow the attackers to hide in plain sight among the massive amounts of unrelated traffic occurring over the same communication channels, such as P2P. Most importantly, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate. For example, Symantec observed an advertisement on an underground forum in 2010 promoting a botnet of 10,000 bots for $15. (The advertisement did not stipulate whether the cost was for purchase or rental).

**Methodology**

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. A distinct bot-infected computer is a distinct computer that was active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they can be classified as actively attacking bots, bots that send out spam (i.e., spam zombies), or bots that are used for DoS campaigns.   
  
DoS campaigns may not always be indicative of bot-infected computer activity and can be accomplished without having to use bots. For example, systems that participated in the high-profile DoS “Operation Payback” attacks conducted against companies that denied services to WikiLeaks—forcing their websites to go offline—primarily used an open-source network stress-testing tool called Low-Orbit Ion Cannon (LOIC). This utility is widely available and can be readily downloaded from the Web.

**Data**



**Figure 15. Bot-infected computers**  
Source: Symantec Corporation

**Commentary**

**Spam zombie proportions appear to be rising.** Although the proportions for each year appear to be the same, due to rounding there was, in reality, a one percent increase in spam zombies in 2010 from 2009. This slight increase in the proportion of spam zombies of the total bot-infected computers is the result of bots sending out larger volumes of spam instead of attacking or propagating. Botnets are responsible for a significant amount of spam, accounting for 88 percent of all spam distributed in 2010, as discussed in the Fraud section of this report.   
  
**The economic viability of spam zombies.** Using bots to send out spam emails can be more economically viable than using them to mount attacks because, ostensibly, the costs to operate the bots are borne by the owner of the compromised computers and, thus, botnet controllers absorb very little of these costs. As such, despite a very small positive response (click-through conversion) rate of one response per 12.5 million spam email messages, some botnets can send out billions of spam messages per day and, thus, still generate potentially large profits.

* [Spamalytics: An Empirical Analysis of Spam Marketing Conversion](http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf)

**Vulnerability Trends Introduction**

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security. Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities being identified in the threat landscape because early detection and patching will minimize the chances of being exploited. This section discusses selected vulnerability trends, providing analysis and discussion of the trends indicated by the data. The following metrics are included:

* Total number of vulnerabilities
* Web browser vulnerabilities
* Window of exposure for Web browsers
* Web browser plug-in vulnerabilities
* Zero-day vulnerabilities
* SCADA vulnerabilities

**Total Number of Vulnerabilities**

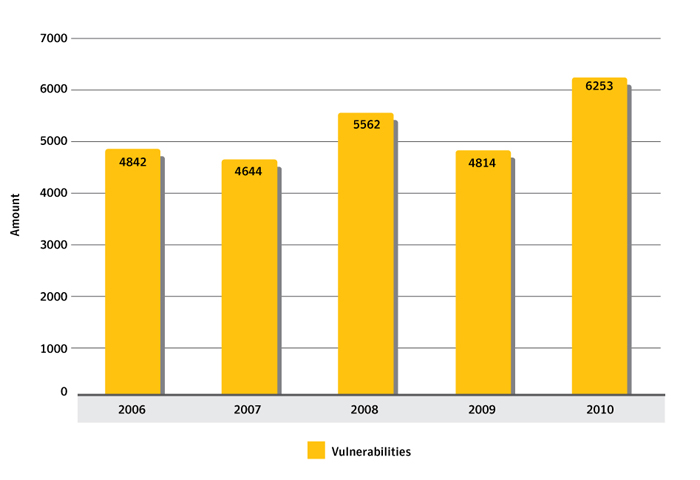
**Background**

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security. Vulnerabilities can affect both software and hardware. The total number of vulnerabilities for 2010 is based on research from independent security experts and vendors of affected products. The yearly total also includes zero-day vulnerabilities that attackers uncovered and were subsequently identified post-exploitation. Calculating the total number of vulnerabilities provides insight into vulnerability research being conducted in the threat landscape. There are many motivations for conducting vulnerability research, including security, academic, promotional, software quality assurance, and, of course, the malicious motivations that drive attackers. Symantec gathers information on all of these vulnerabilities as part of its DeepSight vulnerability database and alerting services. Examining these trends also provides further insight into other topics discussed in this report.  
  
Discovering vulnerabilities can be advantageous to both sides of the security equation: legitimate researchers may learn how better to defend against attacks by analyzing the work of attackers who uncover vulnerabilities; conversely, cybercriminals can capitalize on the published work of legitimate researchers to advance their attack capabilities. As noted in the recently published Symantec *Report on Attack Kits and Malicious Websites*, the vast majority of vulnerabilities that are exploited by attack toolkits are publicly known by the time they are exploited.1

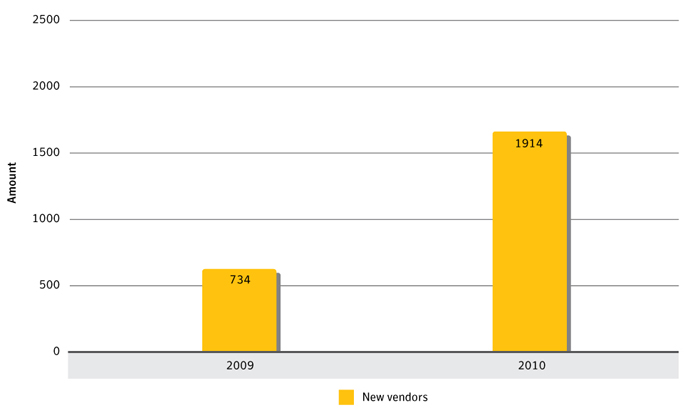
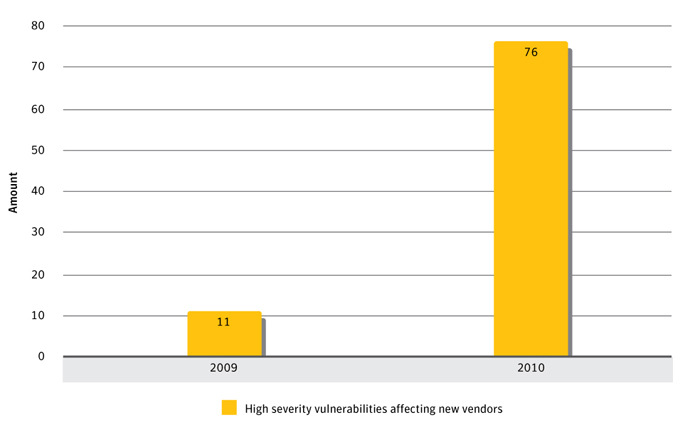
**Methodology**

Information about vulnerabilities is made public through a number of sources. These include mailing lists, vendor advisories, and detection in the wild. Symantec gathers this information and analyzes various characteristics of the vulnerabilities (including technical information and ratings) in order to determine the severity and impact of the vulnerabilities. This information is stored in the DeepSight vulnerability database, which houses over 42,000 distinct vulnerabilities spanning a period of over 20 years. As part of the data gathering process, Symantec scores the vulnerabilities according to version 2.0 of the community-based CVSS (Common Vulnerability Scoring System).2 Symantec adopted version 2.0 of the scoring system in 2008. The total number of vulnerabilities is determined by counting all of the vulnerabilities published during the reporting period. All vulnerabilities are included, regardless of severity or whether or not the vendor who produced the vulnerable product confirmed them.

**Data**



**Total vulnerabilities identified, 2006-2010**   
Source: Symantec Corporation

**New vendors reporting vulnerabilities and high severity vulnerabilities, 2009 & 2010**  
Source: Symantec Corporation

**Observations**

**The total number of vulnerabilities is on the rise:** While there have been some fluctuations, the general trend over the past five years is an increase in the number of vulnerabilities. The total number of vulnerabilities for 2010 was 6253—an increase from 4814 vulnerabilities documented in 2009. This is a 30 percent increase over 2009. There were more vulnerabilities in 2010 than in any previous year recorded by Symantec. (While the greater majority of these are classified as medium severity—95 percent, with the remaining five percent evenly split between severe and mild—it is important to note that the exploitation of medium severity vulnerabilities can be as potentially damaging to a user’s computer as the dangers posed by high severity vulnerabilities). There are a number of likely reasons for the rise in identified vulnerabilities:  
  
**More vendors affected results in more vulnerabilities:** The number of new vendors affected by vulnerabilities in 2010 increased to 1914 from 734 new vendors who were affected by vulnerabilities in 2009—a 161 percent increase. The new vendors for 2010 comprise a mix of vendors who have recently started releasing products as well as established vendors with no previous record of public vulnerabilities. This reflects a wider range of interest from security researchers, but may also be an indicator that more vendors are becoming security conscious and releasing security notifications for their software. This correlates to the increase in vulnerabilities as a result of the increase in research and published advisories in relation to the products maintained by these vendors.  
  
**More sources reporting vulnerabilities:** The increase in vulnerabilities may be due to the increase in the number of sources reporting vulnerabilities in 2010 (including security researchers and vendors). While there is an increase in the number of new vendors affected by vulnerabilities, there are also more security researchers in the field. It makes sense that, if there are more individuals and organizations performing security research, the number of vulnerabilities documented would also increase.  
  
**This vuln for hire:** Interest by security researchers into “vulnerability for sale programs” influences the increase of vulnerabilities in 2010. The commercialization of vulnerabilities (through programs that purchase vulnerabilities) may also be a factor in the increase in the total number of vulnerabilities. Vendors that buy third-party vulnerability research collectively published 338 advisories in 2010, nearly twice the 180 advisories published in 2009. These vendors purchase vulnerability information from security researchers in exchange for money. The rise in the number of advisories published by these vendors indicates that more security research is being driven by financial incentives. This influences the increase in the overall number of vulnerabilities published during the year.  
  
**Severity of vulnerabilities increases:** Among the new vendors affected by vulnerabilities in 2010, 76 vulnerabilities were rated as being high severity, which is a 591 percent increase over the 11 high severity vulnerabilities affecting new vendors in 2009. This indicates that security researchers are seeking out high severity vulnerabilities in products produced by vendors that previously had no record of public vulnerabilities. In the case of new software, it may be less mature from a security standpoint than older software. This is also true for software with a shorter history of vulnerabilities, as it may not have been exposed to the same level of auditing as software with a longer history of vulnerabilities.

**Web Browser Vulnerabilities**

**Background**

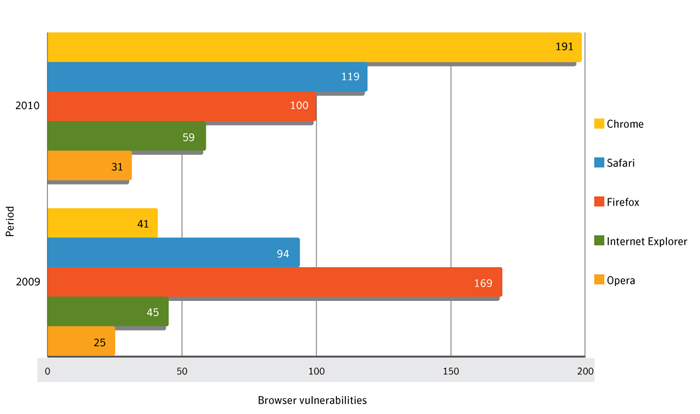
Web browsers are now ubiquitous components for computing for both enterprise and individual users. Moreover, one study estimates that users typically spend more than 60 hours a month online, with most of that interaction occurring via a browser.1 Web browser vulnerabilities are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and adware. In addition, Web browsers are exposed to a greater amount of potentially untrusted or hostile content than most other applications and are particularly targeted by multi-exploit attack kits.2  
  
Web-based attacks can originate from malicious websites as well as from legitimate websites that have been compromised to serve malicious content. Some content, such as media files, documents, or presentation formats, are often presented in browsers via browser plug-in technologies. While browser functionality is often extended by the inclusion of various plug-ins, the addition of plug-in component also results in a wider potential attack surface for client-side attacks. For more on vulnerabilities specific to plug-ins, see the “Web Browser Plug-in Vulnerabilities” discussion in this report.

**Methodology**

Browser vulnerabilities are a sub-set of the total number of vulnerabilities cataloged by Symantec throughout the year. To determine the number of vulnerabilities affecting browsers, Symantec considers all vulnerabilities that have been publicly reported, regardless of whether they have been confirmed by the vendor. While vendors do confirm the majority of browser vulnerabilities that are published, not all vulnerabilities may have been confirmed at the time of writing. Vulnerabilities that are not confirmed by a vendor may still pose a threat to browser users and are therefore included in this study. This metric examines the total number of vulnerabilities affecting the following Web browsers:

* Apple Safari
* Google Chrome
* Microsoft Internet Explorer
* Mozilla Firefox3
* Opera

**Data**



**Browser vulnerabilities, 2009-2010**  
Source: Symantec Corporation

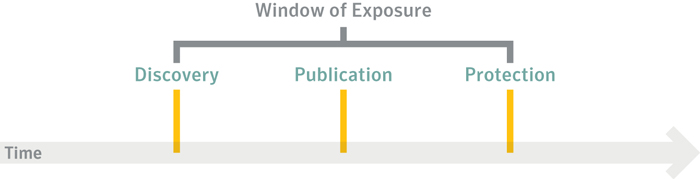
**Commentary**

**Chrome vulnerabilities rise significantly:** During 2010, there were 150 more vulnerabilities documented in Chrome than in 2009. One reason for this is that 2010 was a year of rapid development for Chrome, with nearly 20 stable versions of the browser released.4 Many security researchers (both internal to Google and external) have contributed to this development. This is, in part, due to Google’s bug bounty program, in which researchers receive cash payments for responsibly disclosing security vulnerabilities.5 This follows the same approach used by Mozilla, which first began offering a bug bounty in 2004 to encourage security research into its browser engine.   
  
**Safari totals driven up by Google’s bug bounty:** Safari was affected by 119 vulnerabilities in 2010—up from 94 in 2009. Safari may have indirectly been affected by the Google bug bounty program because the underlying browser engine, WebKit, is used by both Chrome and Safari. Apple released nine versions of the Safari browser with security-related updates in 2010, an increase from four in 2009.   
  
**Firefox vulnerabilities drop off dramatically:** There were 100 vulnerabilities documented in Firefox in 2010—a decrease from 169 in 2009. While Mozilla offers bounties to researchers for responsibly disclosed vulnerabilities, it appears as though Firefox has not been subject to the same scrutiny from researchers as in previous years. Symantec believes that this is due in part to the relative maturity and stability of the Mozilla engine and, as a result, that researchers may be focusing their efforts on easier-to-find vulnerabilities elsewhere.

* 1<http://www.visualeconomics.com/how-the-world-spends-its-time-online_2010-06-16>
* 2<http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf>: p.53:
* 3As of ISTR 15, Symantec limits the Mozilla browsers studied to only Firefox because the Mozilla Foundation no longer supports the Mozilla suite.
* 4<https://sites.google.com/a/chromium.org/dev/getting-involved/dev-channel>
* 5<http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html>

**Window of Exposure for Web Browsers**

**Background**

The window of exposure for Web browsers is the difference in days between the time when exploit code affecting a vulnerability is made public and the time when the affected vendor makes a patch publicly available for that vulnerability. During this time, the computer or system on which the affected application is deployed may be susceptible to attack. Measuring the time that it takes for vendors to release patches for vulnerabilities may provide insight into overall vendor security responsiveness.  
  


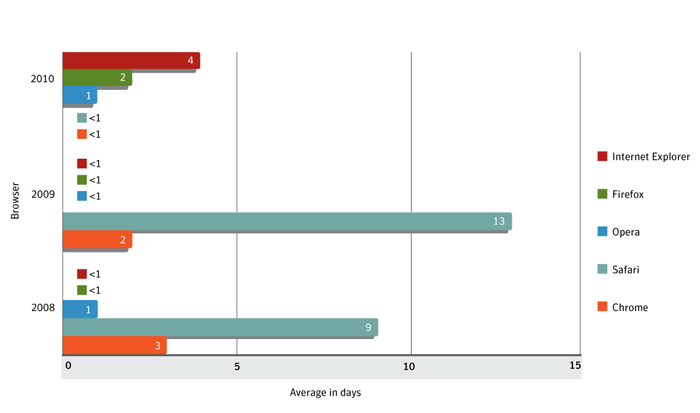
**Depiction of possible window of exposure**  
Source: Symantec Corporation

Patch release times may be influenced by a number of factors, including the number of vulnerabilities during the time period and the amount of importance the vendor attaches to the vulnerability. Vulnerabilities that are being actively exploited may be patched quickly to reduce the risk to users. It may also be more or less trivial to patch some vulnerabilities in comparison to others. Vendors must evaluate these factors when patching vulnerabilities. In addition, some vulnerabilities examined were patched by the vendor at the time they were announced. This may be due to an internal security audit by the vendor, which may have revealed the vulnerability, or it may have been because security researchers discovered the vulnerability and responsibly disclosed it to the vendor. Other vulnerabilities are independently reported by security researchers prior to the release of a patch, indicating that security researchers may not have coordinated with the vendor to disclose the vulnerability—meaning that the vulnerability was published before the vendor could release a patch. It is also possible that the researcher attempted to report the vulnerability but the vendor was unresponsive. Public exploits for browser vulnerabilities are often incorporated into attack toolkits, which pose a serious risk to Web users if they are unaware or unprotected against the threats.

**Methodology**

This metric is derived from the average amount of time it takes to release a patch in comparison to the average amount of time it takes for exploit code to be made publicly available. This metric also includes maximum patch times, which is the maximum amount of time required to release a patch for all of the patched vulnerabilities in the data set.

**Data**



**Window of exposure for Web browsers, 2008-2010**  
Source: Symantec Corporation

**Commentary**

**The longest window of exposure was held by Internet Explorer:** Internet Explorer had an average window of exposure of four days in 2010 based on a sample set of 47 vulnerabilities. In 2009, the average window of exposure for Internet Explorer was less than one day based on a sample set of 28 patched vulnerabilities. The maximum amount of time required to patch a vulnerability in Internet Explorer was 125 days in 2010, a significant increase over a maximum patch time of 18 days in 2009.  
  
**Firefox’s window of exposure increased in 2010:** The average window of exposure for Firefox in 2010 was two days based on a sample set of 99 patched vulnerabilities. This is an increase over the average window of exposure of less than one day in 2009 based on a sample set of 175 vulnerabilities. The maximum amount of time required to patch a vulnerability in 2010 was 53 days, which is a decrease from a maximum patch time of 75 days in 2009.  
  
**The window of exposure for Safari saw the largest change over previous years:** In 2010, the average window of exposure for Safari was less than one day based on a sample set of 110 patched vulnerabilities. This is a decrease from 13 days in 2009 based on a sample set of 78 patched vulnerabilities. The maximum time to patch a vulnerability in 2010 was 283 days. The maximum time for Apple to patch a Safari vulnerability in 2009 was 145 days. The decrease may be related to WebKit, because Google Chrome also uses the component. With two organizations backing the component, in addition to the bug bounty policy initiated by Google and community collaboration, both Safari and Google Chrome had low window of exposures in 2010, despite being the browsers affected by the greatest number of vulnerabilities.  
  
**Chrome’s window of exposure increased by a small amount, despite a substantial increase in the number of patched vulnerabilities:** Chrome had an average window of exposure of less than one day in 2010, based on a sample set of 191 patched vulnerabilities. In 2009, the average window of exposure was two days based on a sample set of 29 patched vulnerabilities. The maximum amount of time to patch a vulnerability was seven days in 2010, a decrease from a maximum patch time of 16 days in 2009.  
  
**Opera’s window of exposure remains low, ranging from less than one day to one day:** The average window of exposure for Opera in 2010 was one day based on a sample set of 27 vulnerabilities. In 2009, the average window of exposure for Opera was less than one day. In 2010, the maximum amount of time to patch a vulnerability affecting Opera was 20 days, compared to a maximum patch time of three days in 2009.  
  
**Internet Explorer is affected by zero-day vulnerabilities:** There were three zero-day vulnerabilities in Internet Explorer in 2010 that were patched by Microsoft. Two of the three zero-day vulnerabilities affected versions 6 through 8 of Internet Explorer, while the third affected versions 6 and 7. It should be noted that these zero-day vulnerabilities may have been exploited for an undetermined amount of time prior to becoming public knowledge and may have been a factor in the overall increase in the window of exposure for Internet Explorer.

* The first vulnerability was exploited to install Trojan.Hydraq during targeted attacks and was patched seven days after becoming public knowledge.1
* The second zero-day vulnerability was exploited in targeted attacks to install Backdoor.Sykipot on vulnerable computers.2 Microsoft released a patch for this vulnerability 21 days after it became publicly known. This is noteworthy because the initial exploit was designed to target users of Internet Explorer 6, although the vulnerability also affected Internet Explorer 7. Exploits were later released that targeted Internet Explorer 7 as well. This vulnerability did not affect Internet Explorer 8.
* The third zero-day vulnerability was also exploited in targeted attacks to install the Pirpi backdoor.3 Microsoft released a patch for this vulnerability 41 days after it was publicly identified.
* The window of exposure for each of the three zero-day vulnerabilities in Internet Explorer was longer than the average window of exposure for the other vulnerabilities identified in Internet Explorer in 2010, meaning that users of the browser were more exposed to these zero-day vulnerabilities than to other vulnerabilities affecting Internet Explorer in 2010. Of the vulnerabilities affecting Internet Explorer in 2010, 81 percent were patched in less than one day after becoming public knowledge. The remaining 19 percent were patched after one day or longer.
* [Learn about the Hydraq trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99)
* [Read about Sykipot](http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-031015-0224-99)
* 1<http://www.securityfocus.com/bid/37815>
* 2<http://www.symantec.com/connect/blogs/zero-day-attack-ie6-jssykipot-doesn-t-spare-retired-software>
* 3Please see <http://www.symantec.com/security_response/writeup.jsp?docid=2010-110314-3703-99>, <http://www.securityfocus.com/bid/44536> and <http://www.securityfocus.com/bid/44536>

**Web Browser Plug-in Vulnerabilities**

**Background**

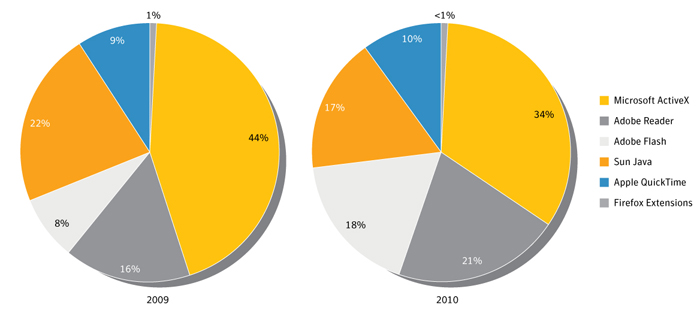
This metric examines the number of vulnerabilities affecting plug-ins for Web browsers. Browser plug-ins are technologies that run inside the Web browser and extend its features, such as allowing additional multimedia content from Web pages to be rendered. This often requires execution environments to be enabled so that the applications can be run inside the browser. Many browsers now include various plug-ins in their default installation and, as well, provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of Web browsers and are often required in order to use many commercial sites. Vulnerabilities affecting these plug-ins are an increasingly favored vector for a range of client-side attacks, and the exploits targeting these vulnerabilities are commonly included in attack kits. Some plug-in technologies include automatic update mechanisms that aid in keeping software up to date, which may aid in limiting exposure to certain vulnerabilities. Alternatively, plug-ins without automatic update notifications may result in users being exposed to increased chances of being exploited.

**Methodology**

Web browser plug-in vulnerabilities comprise a sub-set of the total number of vulnerabilities cataloged by Symantec over the reporting period. The vulnerabilities in this section cover the entire range of possible severity ratings and include vulnerabilities that are both unconfirmed and confirmed by the vendor of the affected product. Confirmed vulnerabilities consist of security issues that the vendor has publicly acknowledged, by either releasing an advisory or otherwise making a public statement to concur that the vulnerability exists. Unconfirmed vulnerabilities are vulnerabilities that are reported by third parties, usually security researchers, which have not been publicly confirmed by the vendor. That a vulnerability is unconfirmed does not mean that the vulnerability report is not legitimate, only that the vendor has not released a public statement to confirm the existence of the vulnerability. Symantec analyzed the following plug-in technologies:

* Adobe Reader1
* Adobe Flash Player
* Apple QuickTime
* Microsoft ActiveX
* Mozilla Firefox extensions
* Oracle Sun Java platform Standard Edition (Java SE)

**Data**



**Browser plug-in vulnerabilities, 2009 & 2010**  
Source: Symantec Corporation

**Commentary**

**Plug-in vulnerabilities continue to rise:** In 2010, 346 vulnerabilities affecting browser plug-ins were documented by Symantec, compared to 302 vulnerabilities affecting browser plug-ins in 2009.   
  
**ActiveX vulnerabilities decline:** Although the highest number of vulnerabilities was in ActiveX controls, with 117 of the total, this is down from 2009, when 134 vulnerabilities identified affected ActiveX controls. Vulnerabilities in ActiveX have been declining in recent years. One reason for the decline may be that ActiveX is a plug-in technology specifically for Internet Explorer, which has been steadily losing market share for several years.2 It may also be due to the increased use of Internet Explorer 8 over earlier versions because Internet Explorer 8 has substantially enhanced security features surrounding ActiveX plug-ins.3  
  
**Adobe was increasingly targeted:** Vulnerabilities in Adobe plug-ins have again increased in 2010. Adobe technologies, such as Reader and Flash Player, have been increasingly used by attackers as a vector to distribute malicious software to both unsuspecting random users and specifically chosen targets. For example, all four of the zero-day vulnerabilities affecting browser plug-ins in 2010 were against cross-platform Adobe products (as noted in the “Zero-Day Vulnerabilities” discussion).   
  
**The impact of sandboxing:** The identification of vulnerabilities is likely also affected by some browser plug-in vendors deploying sandboxing techniques in their products to limit attacks in the wild. Sandboxing can provide a mechanism to isolate potentially malicious code from system resources that may be targeted by attackers.

* 1Note that Symantec analyzed only major plug-ins for this report; other PDF reader applications are prone to similar vulnerabilities.
* 2<http://www.conceivablytech.com/5438/business/the-third-double-digit-browser-chrome-blasts-past-10/>
* 3Please see [and](http://w3schools.com/browsers/browsers_stats.asp) <http://blogs.msdn.com/b/ie/archive/2008/05/07/ie8-security-part-ii-activex-improvements.aspx>

**Zero-Day Vulnerabilities**

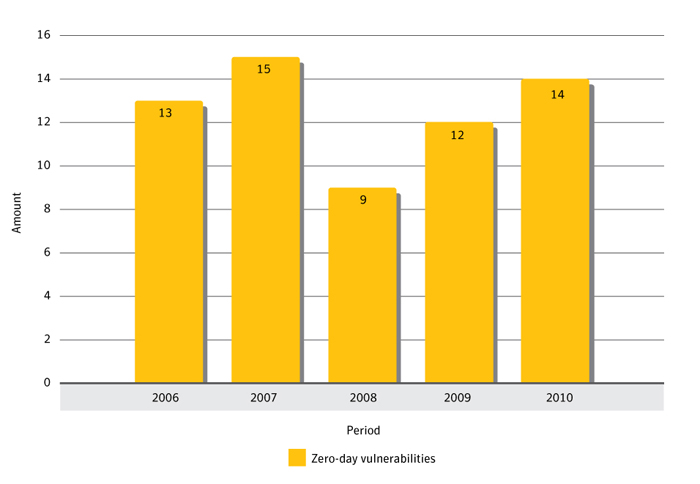
**Background**

Zero-day vulnerabilities are vulnerabilities against which no vendor has released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases these threats can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

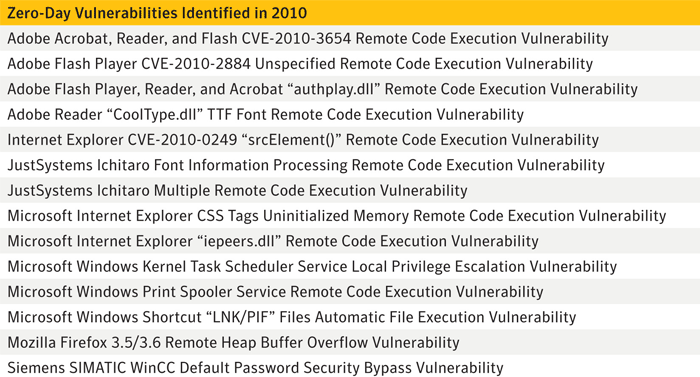
**Methodology**

Zero-day vulnerabilities are a sub-set of the total number of vulnerabilities documented over the reporting period. A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the affected vendor prior to exploitation and, at the time of the exploit activity, the vendor had not released a patch. The data for this section consists of the vulnerabilities that Symantec has identified that meet the above criteria.

**Data**



**Zero-day vulnerabilities, 2006-2010**  
Source: Symantec Corporation



**Zero-day vulnerabilities by name, 2010**  
Source: Symantec Corporation

**Commentary**

**Zero-day vulnerabilities used in high-profile attacks:** The zero-day vulnerabilities identified in 2010 were used in very high-profile attacks that affected widely used applications. For example, the Stuxnet worm combined four zero-day vulnerabilities to target industrial control systems: a zero-day vulnerability that affected SCADA software was exploited in conjunction with three zero-day vulnerabilities in Microsoft Windows.1 The Stuxnet worm is the first known malicious attack to target industrial control systems. Stuxnet was deployed by attackers to target nuclear power facilities, mostly in Iran.  
  
**Stuxnet components being used in other attacks:** One of the vulnerabilities used in the Stuxnet worm was also used in the W32.Changeup.C worm. This vulnerability affected Windows shortcuts. It is interesting that this particular vulnerability was recycled from the Stuxnet attacks to be used in another unrelated worm.

* [Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability](http://www.securityfocus.com/bid/41732)

**Browsers targeted by zero-day vulnerabilities:** Of the 14 zero-day vulnerabilities identified in 2010, four affected Web browsers. These vulnerabilities were exploited to execute malicious code:

* In January 2010, attackers exploited a zero-day vulnerability in Internet Explorer to target several high-profile companies.2 This attack is known as “Aurora,” and it used the Hydraq Trojan to install malicious code onto target computers, successful installations of which would have allowed attackers to steal sensitive data. The attacks prompted Microsoft to release an out-of-band advisory and patch-set on January 21, 2010.
* Multiple versions of Firefox were targeted with the Belmoo backdoor, which exploited a previously unknown use-after-free memory corruption error documented by the “Mozilla Firefox 3.5/3.6 Remote Heap Buffer Overflow Vulnerability.” Mozilla patched this vulnerability one day after it became public knowledge.
* In March 2010, Microsoft disclosed the “iepeers.dll Remote Code Execution Vulnerability,” a zero-day vulnerability that affected versions 6 and 7 of Internet Explorer. It was exploited in the wild using the JS.Sykipot Trojan.3
* The “Microsoft Internet Explorer CSS Tags Uninitialized Memory Remote Code Execution Vulnerability” affected multiple versions of Internet Explorer. The vulnerability became known after a series of attacks in the wild using Backdoor.Pirpi.
* [Mozilla Foundation Security Advisory 2010-73](http://www.mozilla.org/security/announce/2010/mfsa2010-73.html)
* [Microsoft Internet Explorer 'iepeers.dll' Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/38615)
* [Microsoft Internet Explorer CSS Tags Uninitialized Memory Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/44536)
* [Learn about the Pirpi Trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2010-110314-3703-99)

**Browser plug-ins targeted by zero-day vulnerabilities:** Of the 14 zero-day vulnerabilities identified in 2010, four affected Web browser plug-ins, all of which affected Adobe products:

* Adobe Reader was affected by an exploitable heap-memory corruption vulnerability, “Adobe Reader 'CoolType.dll' TTF Font Remote Code Execution Vulnerability.” This vulnerability was exploited to install Bloodhound.exploit.357 via targeted email-based attacks.4
* Adobe Reader and Flash Player were exposed to the “Adobe Acrobat, Reader, and Flash CVE-2010-3654 Remote Code Execution Vulnerability,” which was exploited in limited attacks using Trojan.Pidief. Exploit code was publicly available via the Metasploit Project three days before the vendor released patches.
* In September 2010, Adobe Reader and Flash Player were exposed to the zero-day “Adobe Flash Player CVE-2010-2884 Unspecified Remote Code Execution Vulnerability.”
* Adobe Reader and Flash Player were affected by the zero-day vulnerability, “Adobe Flash Player, Reader, and Acrobat 'authplay.dll' Remote Code Execution Vulnerability,” which was exploited using the Pidief Trojan. Exploit code was publicly available one day before Adobe released a patch for the vulnerability.
* [Adobe Reader 'CoolType.dll' TTF Font Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/43057)
* [Read about Bloodhound.Exploit.357](http://www.symantec.com/security_response/writeup.jsp?docid=2010-090901-2159-99)
* [Adobe Acrobat, Reader, and Flash CVE-2010-3654 Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/44504)
* [Adobe Flash Player CVE-2010-2884 Unspecified Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/43205)
* [Adobe Flash Player, Reader, and Acrobat 'authplay.dll' Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/40586)
* 1<http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>
* 2Please see <http://www.securityfocus.com/bid/37815> and <http://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit>
* 3Please see <http://www.symantec.com/security_response/writeup.jsp?docid=2010-031014-2034-99> and <http://www.symantec.com/connect/blogs/zero-day-attack-ie6-jssykipot-doesn-t-spare-retired-software>
* 4<http://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back>

**SCADA vulnerabilities**

**Background**

This metric will examine the SCADA (Supervisory Control and Data Acquisition) security threat landscape. SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes—but is not limited to—power generation, manufacturing, oil and gas, water treatment, and waste management. Therefore, the security of SCADA technologies and protocols is a concern related to national security because the disruption of related services can result in the failure of infrastructure and potential loss of life—among other consequences.

**Methodology**

This discussion is based on data surrounding publicly known vulnerabilities affecting SCADA technologies. The purpose of the metric is to provide insight into the state of security research in relation to SCADA systems. To a lesser degree, this may provide insight into the overall state of SCADA security. Vulnerabilities affecting SCADA systems may present a threat to critical infrastructure that relies on these systems. Due to the potential for disruption of critical services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks. This is a concern for governments and/or enterprises that are involved in the critical infrastructure sector. While this metric provides insight into public SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure there is likely private security research conducted by SCADA technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

**Data**

**The number of SCADA vulnerabilities rose in 2010:** In 2010, there were 15 public SCADA vulnerabilities, an increase over the 14 vulnerabilities in 2009.

**Commentary**

**The Stuxnet worm exploited zero-day vulnerabilities to target industrial control systems:** The worm exploited three zero-day vulnerabilities in Microsoft Windows and a vulnerability in SCADA automation software.. Symantec discovered that the worm hijacks the behavior of PLCs (Programmable Logic Controllers) to sabotage operations performed by the industrial control systems managed by the affected software.1 Stuxnet included rootkit functionality to hide itself on infected computers, including the first documented rootkit for a PLC.2 The worm is also capable of stealing code and design documents so that the attackers can reverse-engineer connected industrial control systems that the worm has discovered and develop specific payloads targeting those systems.   
  
**Majority of infected Stuxnet hosts are in Iran:** Symantec posed the possibility that Stuxnet was designed to target gas lines or powerplants in Iran.3 Other sources have speculated that Stuxnet was responsible for disrupting uranium enrichment programs in the country.4 The president of Iran later claimed that the worm had created problems affecting centrifuges responsible for producing enriched uranium.5 While it is currently unknown who was responsible for creating the threats, Symantec believes that due to the amount of sophistication and resources required to create Stuxnet, it was likely beyond the capabilities of a typical gang of cybercriminals. Stuxnet underlines the possibility of sophisticated attacks against critical infrastructure such as industrial control systems.

* 1<http://www.symantec.com/connect/blogs/stuxnet-breakthrough>
* 2<http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>
* 3<http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>, p. 6
* 4<http://www.theglobeandmail.com/news/technology/iran-uranium-enrichment-program-targeted-by-stuxnet-worm-study-confirms/article1800982/>
* 5<http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8169381/Iran-confirms-Stuxnet-worm-halted-centrifuges.html>
* 6<http://news.cnet.com/8301-27080_3-20023124-245.html>

**Malicious Code Trends Introduction**

Symantec collects malicious code information from its large global customer base through a series of opt in anonymous telemetry programs, including Norton Community Watch, Symantec Digital Immune System and Symantec Scan and Deliver technologies. Well over 100 million clients, servers and gateway systems actively contribute to these programs. New malicious code samples, as well as detection incidents from known malicious code types, are reported back to Symantec. These resources give Symantec’s analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in malicious code activity in the threat landscape. Reported incidents are considered potential infections if an infection could have occurred in the absence of security software to detect and eliminate the threat.   
  
Malicious code threats are classified into four main types—backdoors, viruses, worms, and Trojans:

* **Backdoors** allow an attacker to remotely access compromised computers.
* **Trojans** are malicious code that users unwittingly install onto their computers, most commonly through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.
* **Viruses** propagate by infecting existing files on affected computers with malicious code.
* **Worms** are malicious code threats that can replicate on infected computers or in a manner that facilitates them being copied to another computer (such as via USB storage devices).

Many malicious code threats have multiple features. For example, a backdoor is always categorized in conjunction with another malicious code feature. Typically, backdoors are also Trojans, however many worms and viruses also incorporate backdoor functionality. In addition, many malicious code samples can be classified as both worm and virus due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.   
  
This discussion is based on malicious code samples detected by Symantec in 2010, with the following trends being analyzed:

* Top malicious code families
* Prevalence of malicious code features
* Top malicious code samples by region
* Threats to confidential information
* Propagation mechanisms

**Top Malicious Code Families**

**Background**

Symantec analyzes new and existing malicious code families to determine which threats types and attack vectors are being employed in the most prevalent threats. This information also allows administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

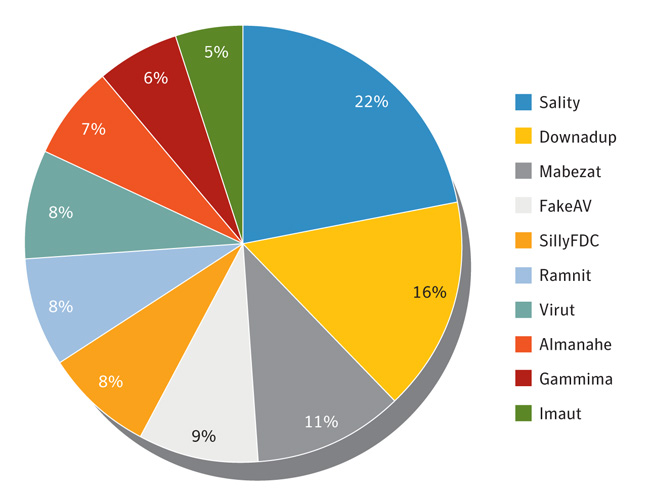
**Methodology**

A malicious code family is initially composed of a distinct malicious code sample. As variants to the sample are released, the family can grow to include multiple variants. Symantec determines the most prevalent malicious code families by collating and analyzing anonymous telemetry data gathered for the reporting period. In 2010, over 1.5 billion malicious code detections were made using this method. Malicious code is classified into families based on variants in the signatures assigned by Symantec when the code is identified. Variants appear when attackers modify or improve existing malicious code to add or change functionality. These changes alter existing code enough that antivirus sensors may not detect the threat as an existing signature.

**Data**



**Table 7. Top malicious code families, 2010**  
Source: Symantec Corporation



**Figure 16. Relative volume of reports of top 10 malicious code families in 2010, by percentage**  
Source: Symantec Corporation

**Commentary**

**Sality is again the top malicious code family:** The top malicious code family by volume of potential infections in 2010 was Sality. Samples in the Sality family were responsible for significantly more potential infections than the second ranked malicious code family in 2010, Downadup. This is primarily the result of activity by Sality.AE. Discovered in 2008, Sality.AE has been a prominent part of the threat landscape since then, including being the top malicious code sample identified by Symantec in 2009.1 Sality may be particularly attractive to attackers because it uses polymorphic code that can hamper detection. Sality is also capable of disabling security services on affected computers. These two factors may lead to a higher rate of successful installations for attackers. Sality propagates by infecting executable files and copying itself to removable drives such as USB devices. The virus then relies on Microsoft Windows AutoRun functionality to execute when those drives are accessed. This can occur when an infected USB device is attached to a computer. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Sality.AE (as well as SillyFDC and others) effective vehicles for installing additional malicious code on computers. This effectiveness is borne out by Sality.AE being the top ranked staged downloader in 2010. (Please see the discussion on staged downloaders for more.)

* [Read about Sality](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99)
* [Learn about the Downadup worm](http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99)
* [Learn more about Sality.AE](http://www.symantec.com/security_response/writeup.jsp?docid=2008-042106-1847-99)
* [Read about SillyFDC](http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99)

**Downadup is still going strong:** Downadup (a.k.a. Conficker) was the second ranked malicious code family by volume of potential infections in 2010—up from being fifth ranked potential infection in 2009. This is primarily due to activity by the Downadup.B variant. This worm was initially discovered in December 2008 and garnered a significant amount of attention during 2009 because of its sophisticated attributes and effectiveness. Downadup propagates by exploiting vulnerabilities in order to copy itself to network shares. Despite the release of a patch for the vulnerability on October 23, 2008 (i.e., before Downadup was even active), the worm was estimated still to be on more than 6 million PCs worldwide at the end of 2009.2 Although this number decreased during 2010, estimations are that it was still on possibly as many as 5 million PCs by the end of the year.  
  
**The Stuxnet worm in 2010:** Despite being developed for a very specific type of target, the number of reports of potential Stuxnet infections observed by Symantec in 2010 placed the worm at rank 29 among malicious code families. This may be a testament to the effectiveness of its ability to propagate on computers used to control system capacity in industrial sectors. The Stuxnet worm generated a significant amount of attention in 2010 because it was the first malicious code designed specifically to attack Programmable Logic Controller (PLC) industry control systems.3 Additionally, the worm also propagated using exploits for four zero-day vulnerabilities—a record for a piece of malicious code. Two of these were remote code execution vulnerabilities and two were local privilege escalation vulnerabilities. (Privilege escalation occurs when administrative abilities are enabled on a computer beyond what is allowed for the user.) Not only did Stuxnet exploit what were, at the time, zero-day vulnerabilities, it also exploits a variety of other vulnerabilities, which indicates the extraordinary sophistication, thought, and planning that went into making this threat. This worm is important because the possibility of such an attack had been discussed in the past but never observed outside of lab environments. Notably, Stuxnet is the first malicious code family that can have directly affect the physical world and proves the feasibility for malicious code to cause potentially dramatic physical destruction.

* [Read about Stuxnet](http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99)

**The Hydraq Trojan:** Although Hydraq accounted for a very small number of reported potential infections in 2010, it is noteworthy because it was used in a high profile targeted attack with alleged political motivations. The attack was an attempt to access a corporate network and steal confidential information. Also known as Aurora, Hydraq was first discovered on January 11, 2010. It propagates via email attachments or by being downloaded by other threats. Once executed, it then installs a backdoor and attempts to contact a remote command-and-control server to receive updates and further instructions.

* [Learn more about the Hydraq Trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99)

**The Ramnit virus:** It is worth noting the sixth-ranked malicious code family, Ramnit. This virus propagates by infecting executable files and copying itself to removable drives. This family is interesting because it managed to account for enough reported potential infections to rank among the top malicious code families this reporting period without drawing a significant amount of attention, despite being discovered early in 2010.

* [Read about the Ramnit virus](http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99)
* 1<http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf>; p.51
* 2See <http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker> and <http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx>
* 3See <http://www.symantec.com/connect/blogs/stuxnet-breakthrough> and <http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/>

**Prevalence of Malicious Code Features**

**Background**

As noted in the introduction to this section of the report, Symantec categorizes malicious code features into four basic categories—backdoors, Trojans, viruses, and worms:

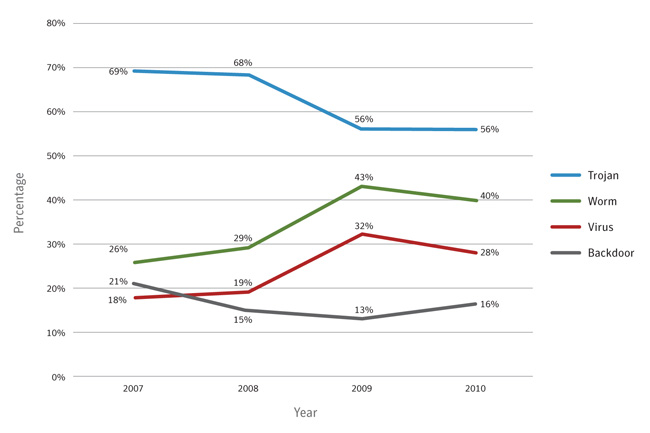
* **Backdoors** allow an attacker to remotely access compromised computers.
* **Trojans** are malicious code that users unwittingly install onto their computers, through either opening email attachments or downloading from the Internet. Trojans are often downloaded an installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.
* **Viruses** propagate by infecting existing files on affected computers with malicious code.
* **Worms** are malicious code that can replicate on infected computers or in a manner that facilitates it being copied to another computer (such as via USB storage devices).

Many malicious code threats have multiple features. For example, a backdoor is always categorized in conjunction with another malicious code feature. Typically, backdoors are also Trojans, however many worms and viruses also incorporate backdoor functionality. In addition, many malicious code samples can be classified as both worm and virus due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.   
  
Analyzing the prevalence of each malicious feature provides insight into the general diversity of the threat landscape. Combined with the data from other metrics, this helps Symantec more accurately determine emerging trends in malicious code.

**Methodology**

This analysis focuses on the top 50 most prevalent malicious code samples of 2010. Each code sample is analyzed and its features categorized into one of the four basic categories. The sum of this feature is measured by its volume proportional to the prevalence of each code sample in which it is found.   
  
As previously noted, malicious code samples are often characterized by more than one category; therefore, the volume of potential infections associated with each sample may apply to the proportions of multiple types. The proportions of the top 50 potential infections of the current period are compared to those of the top 50 potential infections of the previous period in order to observe shifting malicious code activity in the threat landscape. Since these are proportional figures, it should be noted that a change in proportion does not represent a year-over-year increase or decrease in potential infections.

**Data**



**Figure 17. Prevalence of malicious code types by potential infections, 2007–2010**  
Source: Symantec Corporation

**Commentary**

**Financial motivations keep Trojans on top:** Trojans made up the highest percentage of the top 50 potential malicious code infections for 2010, as has been the case in previous years. Trojans continue to be a prominent malicious code threat because the majority of malicious activity is now financially motivated; many Trojans are designed to steal information and are a primary means for attackers to harvest sensitive information, such as credit card information or banking credentials, which can be used to generate revenue. In 2010, the percentage of potential infections by Trojans was 56 percent—the same percentage as 2009. Another significant contributing factor in the proportional stability of Trojans was the Sasfis Trojan, which was the tenth ranked malicious code sample of 2010, despite having been active for only one year.

* [Read about the Sasfis trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2010-020210-5440-99)

**Trojans are effective in social engineering attacks:** The effectiveness of social engineering attacks also contributed to the continued prominence of Trojans. A victim who is convinced through social engineering tactics to willingly download and execute malicious code can have his or her computer compromised regardless of certain computer-based security measures. This is a very efficient means of distributing Trojans and has been use effectively for many years. For example, the Zlob Trojan is disguised as a video codec installer and potential victims are enticed to download and install it by being told that it is required to view a particular video.

* [Read about the Zlob trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99)

**Worms and viruses usually trend together:** The decrease in potential worm infections, from 43 percent in 2009 to 40 percent in 2010, may be closely related to the similar decrease in viruses (from 32 percent to 28 percent in that time). This corresponding decrease is because prominent malicious code samples of these types often include both worm and virus components (in order to increase their chances of successful propagation). This connection is further indicated by the top 10 malicious code families of 2010, of which five have both virus and worm attributes. Therefore, subtle proportional shifts to either malicious code type are likely to mirror each other.

**Top Malicious Code Samples by Region**

**Background**

Symantec examines the types of malicious code causing potential infection in each region. Attackers are increasingly focusing their attacks on specific targets and on specific regions. The regionalization 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 localized events as part of their social engineering techniques. For example, Downadup was particularly successful in Brazil when it was first released, because it is able to specifically target certain regions based on the identification of the language setting of a computer, one of which was “Portuguese (Brazilian).”¹ Because of the varying propagation mechanisms used by different malicious code types, and the diverse effects that each malicious code type may have, information about the geographic distribution of malicious code can help network administrators improve their security efforts. It should be noted that the numbers below represent proportional geographic percentages and that proportional percentage fluctuations over time may not indicate an actual change to the raw number of reports from a specific region.

**Methodology**

This metric assesses the location of malicious code samples causing potential infections. To determine this, Symantec measures the volume of potential malicious code infections that were reported in the following geographical regions: North America (NAM), Europe, the Middle East, and Africa (EMEA), Asia, Pacific, and Japan (APJ), and Latin America (LAM). The top malicious code samples are ranked for each region. Reported incidents are considered potential infections if an infection could have occurred in the absence of security software to detect and eliminate the threat.

**Data**



**Table 8. Top malicious code samples, by region, 2010**  
Source: Symantec Corporation

**Commentary**

**Trojans rank highest in NAM:** While notable Trojans and backdoors—such as FakeAV, Sasfis, and Tidserv—accounted for a significant number of reports in all regions, they were overshadowed by worms and virus reports from all regions except NAM.   
  
**Sality.AE rules the viruses:** The most prominent virus reported in 2010 was Sality.AE. Although the volume of potential Sality.AE infections was proportionally lower in 2010, this virus continued to be the most prominent virus reported in APJ, EMEA, and LAM by a substantial margin. For example, Virut was the second most prominent virus in APJ and EMEA but Sality.AE accounted for nearly four times as many reports.

**Threats to Confidential Information**

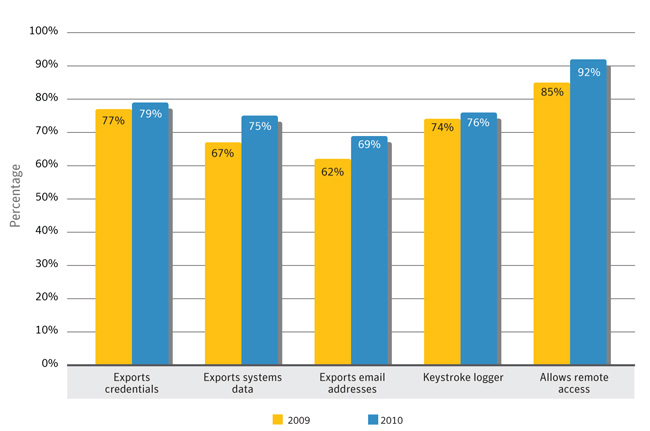
**Background**

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 backdoors, can give a remote attacker complete control over a compromised computer.   
  
Threats to confidential information are a particular concern because of their potential for use in criminal activities. Operators in the underground economy use these malicious threats to gain access to banking and credit card information and online credentials, and to target specific enterprises. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.  
  
Within the enterprise, the exposure of confidential information can lead to significant data loss. 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 form compromised computers.

**Methodology**

This metric assesses the prominence of different types of threats to confidential information in 2010. To determine this, Symantec analyzes the top 50 malicious code samples (as ranked by the volume of potential infections reported during the year). Each sample is analyzed for its ability to expose confidential information and these findings are then measured as a percentage of threats to confidential information.

**Data**



**Figure 18. Threats to confidential information, by type**  
Source: Symantec Corporation

**Commentary**

**Threats to confidential information that allow remote access:** Malicious code that allows remote access accounted for 92 percent of threats to confidential information in 2010, up from 85 percent in 2009. Remote access has been the most prominent threat to confidential information for some time, likely because of the convenience and versatility it provides attackers. Remotely accessing compromised computers allows attackers to perform a wide variety of additional actions that need not be hardcoded in the malicious code that establishes the backdoor.  
  
**Threats to confidential information that export user data and log keystrokes:** In 2010, 79 percent of threats to confidential information export user data, and 76 percent were keystroke loggers, up from 77 percent and 74 percent in 2009, respectively. Both of these threats are effective means for attackers to harvest sensitive financial information, online banking or other account credentials, and other confidential information.  
  
**Growth of threats to confidential information:** As observed in previous years of the Symantec *Internet Security Threat Report*, each category of threats to confidential information is slowly growing, a trend that continued in this reporting period. In 2010, 64 percent of potential infections by the top 50 malicious code samples were threats to confidential information, an increase from 58 percent in 2009. The importance of these threats to the financial considerations of attackers is the primary driver behind this; the exposure of information that can be used or sold for monetary gain is an integral aspect of cybercrime that uses malicious code.

**Propagation Mechanisms**

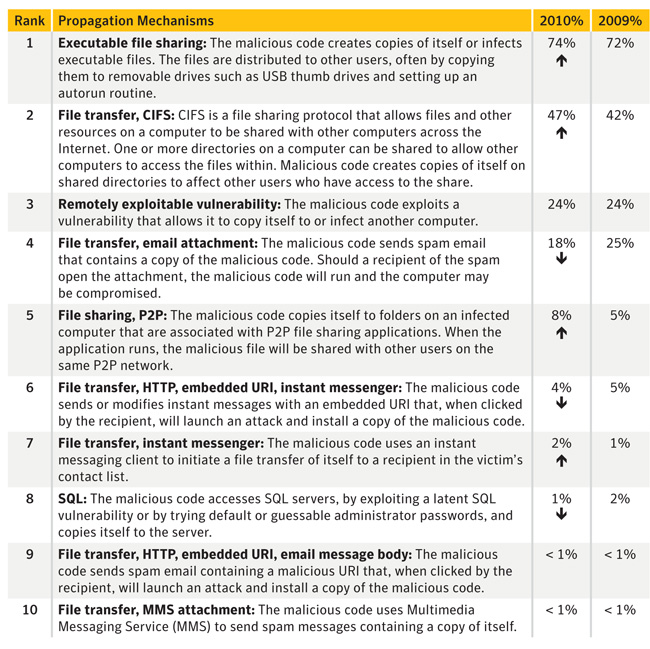
**Background**

Worms and viruses use various means to spread 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), peer-to-peer file transfers (P2P), and remotely exploitable vulnerabilities.1 Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a backdoor server and using the existing backdoor to upload and install itself.

**Methodology**

This metric assesses the prominence of propagation mechanisms used by malicious code. To determine this, Symantec analyzes the malicious code samples that propagate and then ranks associated propagation mechanisms according to the related volumes of potential infections observed during the reporting period.2

**Data**



**Table 9. Propagation mechanisms**  
Source: Symantec Corporation

**Commentary**

**Reliability of propagation mechanisms:** There were very few changes to propagation mechanism percentages from 2009 to 2010. This suggests that attackers are seeing relatively stable success rates with the mechanisms they employ. When a propagation mechanism becomes less reliable, due to patching or other mitigations, attackers will incorporate other mechanisms and a new trend will emerge.  
  
**SillyFDC, Sality.AE and Stuxnet lead the way in executable file sharing:** In 2010, 74 percent of malicious code propagated as executables, an increase from 72 percent in 2009. This propagation mechanism is typically employed by viruses and some worms to infect files on removable media. For example, the SillyFDC worm and Sality.AE virus use this mechanism and were both significant contributing factors in this metric for 2010, as they were among the top three ranked malicious code samples for the year. The Stuxnet worm also propagates using this mechanism. Despite being designed for a very specific target, this worm has affected a very large number of systems in multiple countries. This highlights the effectiveness of this propagation mechanism, especially in industrial sectors. However, Stuxnet also makes use of several other mechanisms, so some of its success is likely due to the number of different propagation mechanisms it could use. As malicious code continues to become more sophisticated, more threats may employ multiple mechanisms. That said, the dominance of this propagation mechanism may decline significantly in the future. This is because, in February 2011, Microsoft announced an update to its AutoPlay functionality that restricts autorun functionality to CD and DVD media. As adoption of this update increases, attackers who have been relying on this mechanism for their malicious code to propagate may turn instead to other mechanisms.  
  
**Remotely exploitable vulnerabilities steady thanks, in part, to Downadup:** The percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2010 was identical to that of 2009—at 24 percent. This follows a significant increase observed in 2009. The previous volume of the Symantec *Internet Security Threat Report* discussed that the emergence of the Downadup worm in 2009 was a significant contributor to the increase of this propagation type. It is likely that the continued prevalence of Downadup and the emergence of the Stuxnet worm in 2010 are significant factors in the consistent percentage observed in this reporting period for propagation through remotely exploitable vulnerabilities.  
  
**File sharing via email attachments continues to decline:** It is worth noting the continued decline in the percentage of malicious code that propagated through email attachments for the fourth year running. While this propagation mechanism is still effective (there remains a substantial difference in percentage between this mechanism and the next-ranked propagation via P2P), Symantec anticipates that this downward trend will continue into the near future.  
  
**“Here You Have”:** Despite the decline of propagation using email attachments, Imsolk.B is a testament to how malicious code can still be propagated via email. Commonly known as the “Here you Have” email virus, the Imsolk.B mass-mailing worm was discovered in early September 2010. This is the first mass-mailer worm of this magnitude since the LoveBug worm in 2000. Imsolk.B propagates by enticing email recipients to open a misleading attachment that would then install the worm. The worm garnered significant attention because it affected the computers of several large corporations. The attention that this generated may have lead to rapid and widespread adoption of specific protections against the worm because it accounted for a relatively small number of reported potential infections for the remainder of the year.

* 1CIFS 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.
* 2Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

**Fraud Activity Trends Introduction**

Fraud activity discusses trends in phishing, spam. It also discusses activities observed on underground economy servers, because this is where much of the profit is made from phishing and spam attacks.   
  
Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they can then use to commit fraudulent acts. Phishing generally requires victims to provide their credentials, often by duping them into filling out an online form. 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).

* [419 – The Oldest Trick in the Book and Yet Another Scam](http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam)

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. Spam can also include URLs that often link to malicious sites that, without the user being aware of it, attack a user’s system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email gateways.

* [BBC News article: Spammers plunder Plusnet e-mail](http://news.bbc.co.uk/2/hi/technology/6676819.stm)

Underground economy servers are black market forums for advertising and trading stolen information and services. This discussion assesses underground economy servers according to the different types of goods and services advertised. It should be noted that this discussion might not necessarily be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec monitored during this period.  
  
This section discusses the following metrics:

* Phishing scams using current events
* Underground economy servers—goods and services available for sale
* Spam delivered by botnets
* Originating sources of botnet spam
* Significant spam tactics
* Spam by category

**Phishing Scams Using Current Events**

**Background**

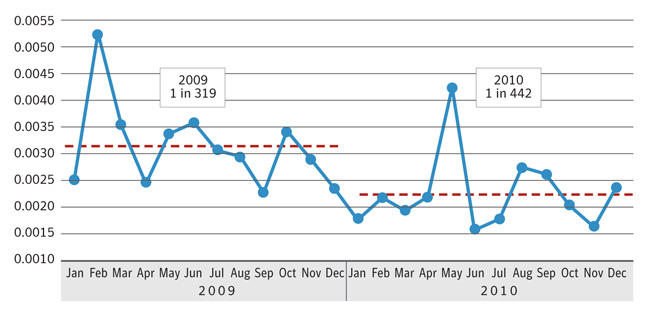
This section discusses the proportion of unwanted email traffic that is identified as phishing attacks and looks more closely at the emerging trends, particularly social engineering techniques and how attackers can automate the use of RSS news feeds to incorporate news and current affairs stories into their scams.

**Methodology**

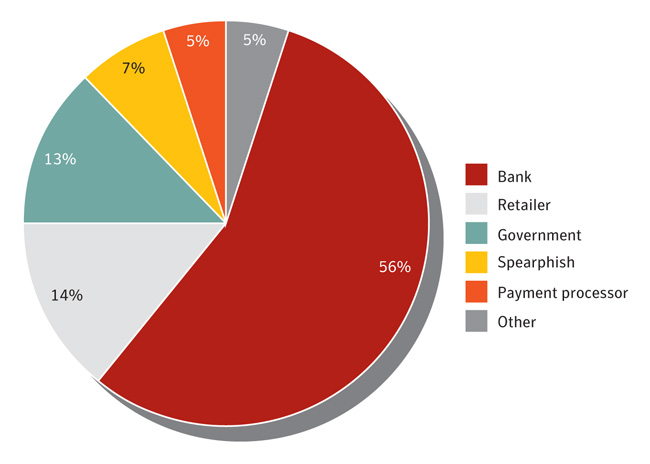
The data for this section is based on the analysis of email traffic collected from MessageLabs Intelligence global honeypots and from the analysis of malicious and unwanted email traffic data collected from the company’s clients worldwide. The analysis of phishing trends is based on emails processed by MessageLabs Intelligence’s Skeptic™ technology, and recorded after perimeter traffic shaping and botnet connection mitigation techniques are applied. This means that the measurements from clients’ traffic are from phishing emails not sent from a previously known botnet (these would be blocked by perimeter traffic controls). Botnet spam accounted for 88 percent of all spam in 2010, but does vary by client, so this analysis is based on the remaining 15-20 percent of email traffic not throttled at the perimeter. In other words, the spam that reaches this stage has evaded signatures and other traditional countermeasures. The honeypots are not affected in this way and collected approximately 30-50 million spam emails each day during 2010.

* [Skeptic technology - a higher level of confidence](http://www.messagelabs.com/aboutus/tech/skeptic_technology)

**Data**

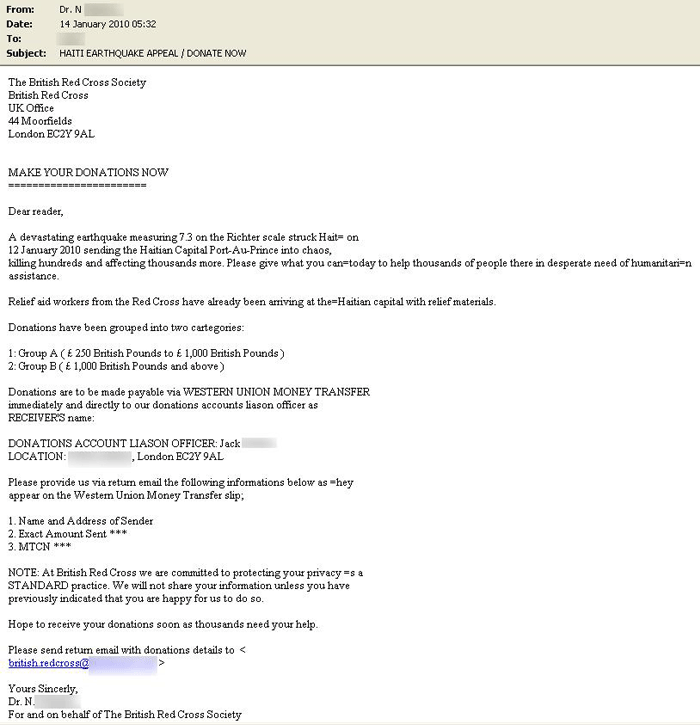


**Figure 19. Phishing rates, 2009–2010**  
Source: MessageLabs Intelligence

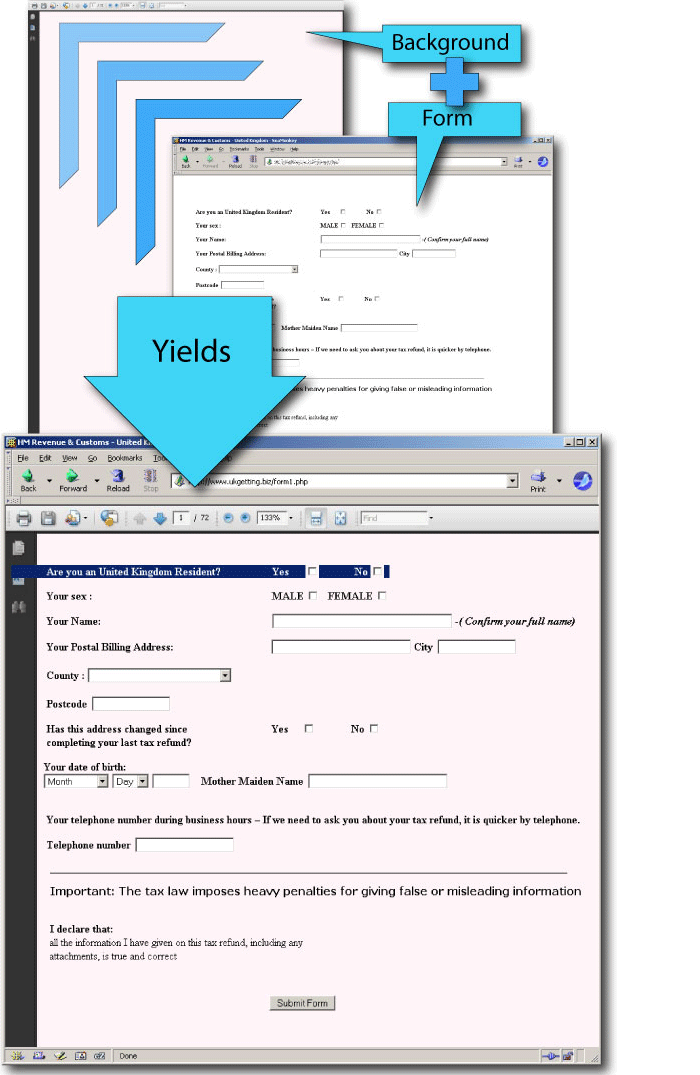


**Figure 20. Phishing category types, top 200 organizations, 2010**  
Source: MessageLabs Intelligence

**Commentary**

**Banking information most sought after in phishing URLs:** Of the top 200 organizations observed, the most frequently spoofed were banks, which accounted for 56 percent of phishing attacks blocked in 2010. It is not surprising that banks are spoofed by phishing URLs more than any other category. Phishing URLs spoofing banks attempt to steal a wide variety of information that can be used for identity theft and fraud. Attackers seek information such as names, government-issued identification numbers, bank account information, and credit card numbers. Cybercriminals are more focused on stealing financial information that can make them large amounts of money quickly versus goods that require a larger time investment, such as scams.  
  
**Phishing schemes continue to use major events to entice recipients:** Many email-based fraud attempts referred to major events in 2010. Examples include:  
  
**Haiti earthquake:** One observed example played on people’s sympathies for the victims of the major earthquake in Haiti in January 2010. Aid was quickly offered by many countries and many charities sought donations to provide support. Cybercriminals exploited the outpouring of support by sending 419 scam emails in which they spoofed a charity using legitimate credentials, but used a payment processor that would deposit any “donations” into accounts that they controlled.  
  


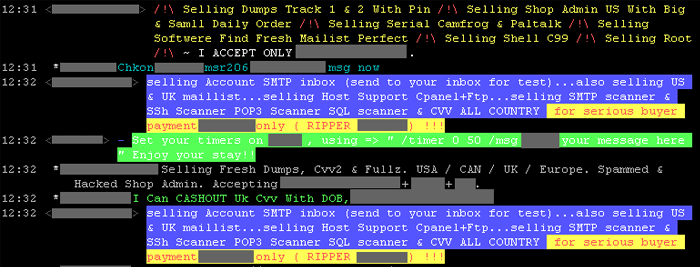
**Figure 21. Phishing email for Haiti earthquake scam**  
Source: MessageLabs Intelligence

**FIFA World Cup:** Major sporting events, such as the FIFA World Cup, are usually exploited by cybercriminals. MessageLabs Intelligence identified a wide variety of different threats relating to the FIFA World Cup before, during, and after the latest tournament, which took place in South Africa in June 2010, including spam, scams, and malicious code attacks. Examples of fraudulent 419 scam emails include offers for game tickets and fake hotel rooms. Some of the scams were a little more unusual, such as one that sought companies to provide additional electricity and power for the World Cup event itself. Ultimately, all of these scams were designed to obtain the recipient’s personal details and money by means of deception and fraud.  
  
**Tax rebate scams in the United Kingdom:** In 2010, the United Kingdom’s tax collecting agency, HMRC, announced that approximately 6 million people in the country had paid the wrong amount of tax and stated that it would start sending letters to the affected people. Depending on their circumstances, people people were invited to claim back overpaid tax, or submit a demand for payment of unpaid tax. Emails soon appeared that exploited the confusion caused by the announcement. In 2010, phishing attacks spoofing HMRC accounted for nearly 11 percent of all phishing emails blocked globally. Comparatively, phishing attacks spoofing the U.S. Internal Revenue Service accounted for less than 1 percent of the total.   
  
**“Picture-in-picture” scam:** One particularly interesting phishing scam identified in 2010 used a novel “picture-in-picture” (PiP) technique to disguise the message as a PDF file. Although the scam does not directly refer to the HMRC announcement about incorrect tax payments, mentioned above, it still attempted to trick recipients into revealing confidential information about themselves in the hope of receiving a windfall. Opening the attachment revealed an HTML page designed to look like a PDF document. The phishing email claimed that the recipient was entitled to a refund, and included an HTML attachment, which when opened, used HTML frames to load a fake website hosted on a compromised Web server. The website was noteworthy because it used a PiP attack to disguise the page to appear as though it was a PDF document being displayed within a Web browser using a plug-in. A PiP attack involves a combination of images and screenshots that are used to mimic the on-screen controls and appearance of an application such as a PDF reader or, in some cases, an entire Windows desktop. This phishing site included a background image, shown in the example above, which was designed to appear like a popular PDF viewer application.  
  


**Figure 22. Phishing email using PiP scam**  
Source: MessageLabs Intelligence

**Underground Economy Servers—Goods and Services Available for Sale**

**Background**

This discussion focuses on the most frequently advertised items for sale on underground economy servers observed by Symantec. Underground economy servers are black market forums used for the promotion and trade of stolen information and to provide services to facilitate these illegal activities. They are typically chat servers on which stolen data is bought and sold. Information observed for sale includes government-issued identification (such as Social Security numbers), credit card numbers, bank account and debit card information, user accounts, and email address lists—basically, any bits of personal and sensitive information for which thieves can find a buyer. Services include cashiers, scam page hosting, and job advertisements such as for scam developers or phishing partners.1 Advertisers use specially written messages to pitch their wares or to offer services. Typical advertisements contain the available items, prices, and other details such as payment options, contact information, and qualifiers to describe the goods such as “100% successful,” “fast,” or “legit.”  
  


**Figure 23. Sample screenshot of advertisements on an underground economy server**  
Source: Symantec Corporation

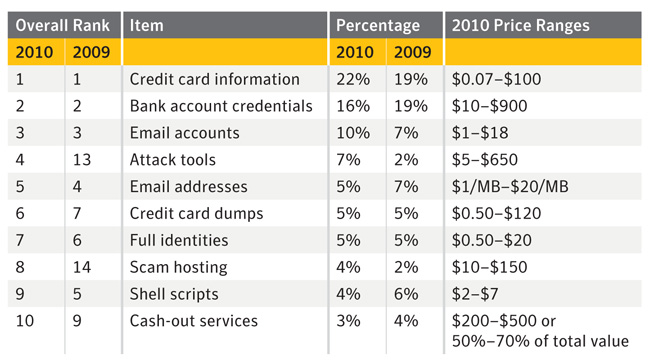
Much of the underground economy commerce occurs within channels on Internet Relay Chat (IRC) servers. IRC is an Internet communications protocol that is attractive to cybercriminals for a number of reasons: it offers real-time group communications, requires very little bandwidth, and the IRC client software is freely available across all operating systems. For an in-depth analysis of how the underground Internet economy functions, please see the Symantec *Report on the Underground Economy*, published November 2008.

* [Symantec *Report on the Underground Economy*](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf)

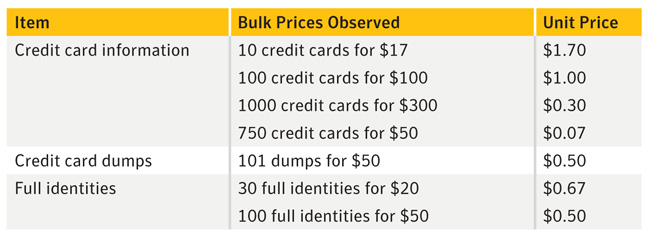
**Methodology**

This metric is based on data that is gathered by proprietary Symantec technologies that observe activity on underground economy servers and collect data. Each server is monitored by recording communications that take place on them. This data is used to derive the data presented in this metric. It should be noted that this discussion is not necessarily representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec observed during this period.  
  
The measure of goods and services available for sale is by distinct messages, which are considered as single advertisements for a good or service, though the same advertisement may appear thousands of times. To qualify as a new message, there must be variations such as price changes or other substantive alterations in the message. (All figures in USD.)

**Data**



**Table 11. Goods and services available for sale on underground economy servers, 2009–2010**  
Source: Symantec Corporation



**Table 12. Goods and services available for sale on underground economy servers, 2010**  
Source: Symantec Corporation

**Commentary**

**Cybercriminals are after the quick money:** In 2010, as in previous years, credit card information and bank account credentials continue to be the top two advertised items by a large margin. Credit card information and bank account credentials have consistently ranked first and second, respectively, in this metric since Symantec began to observe underground economy servers in 2007. This continuing distribution of goods and services on underground economy servers shows that advertisers continue to concentrate on financial information because criminals are more focused on purchasing goods that can make them large amounts of money quickly versus goods that require more time and resources, such as scams or bot-infected computers.  
  
**Credit card theft can happen anywhere:** One reason for the continued top ranking of credit card information may be because there are many ways credit card information can be obtained for fraud. This includes phishing schemes, monitoring merchant card authorizations, the use of magnetic stripe skimmers, or breaking into databases and other data breaches that expose sensitive information. The sizeable number of credit card transactions each year and frequency of usage gives thieves many opportunities to capture and steal this information to sell on the underground economy. For example, there were over 23.9 billion credit card transactions in the United States in 2008. This amounts to an average of 79 credit card transactions per resident, annually.

* [CPSS – Red Book statistical update](http://bis.org/publ/cpss93p2.pdf)

**Like a smash and grab, only online:** The promise of quick payouts makes bank account credentials popular. Bank account credentials remain popular on the underground economy because the ability to withdraw currency directly from a bank account is advantageous and attractive to criminals. They can realize a more immediate payout than with online credit card purchases, which need to be sold to realize a purely financial reward. Criminals also use bank accounts as intermediary channels for money laundering or to fund other online currency accounts that only accept bank transfers for payments.  
  
**Quality vs. quantity:** Prices for credit card information continued to range widely: The prices of credit card information advertised in 2010 ranged from $0.07 to $100 per card. The wide range in prices may be a reflection of simple supply and demand, where higher bulk availability results in lower prices and rarer cards are advertised at higher prices.

* **Main factors that influence prices** include the amount of information included with the card, the quality or validity of the card, type of card, and bulk purchase sizes. Higher-priced credit cards purportedly include enough information to make the data usable for the criminal. This includes personal information such as SSNs, addresses, phone numbers, email addresses, card-specific information such as CVV2 numbers, PINs, and online verification service passwords. Cards purporting to have higher limits also command higher prices. Advertisers often claim that the cards have been recently obtained (thus, potentially not yet reported as stolen).
* **The location of the issuing bank** as well as the type and rarity of the credit card also influence asking prices. Credit cards issued in regions such as Asia, South America, and some European countries were advertised at higher prices than those in other regions because the availability of sensitive information in these regions is lower. In 2010, for example, credit cards from countries such as France and Brazil were commonly listed for $8 to $10, while cards issued from the United States were commonly listed at $2 or less per card. The United States was the top country advertised for credit cards on known underground economy servers, accounting for 65 percent of the total in 2010. This saturation of supply of credit cards on the underground economy and the total number of credit cards in circulation from the United States is a factor for the low advertised prices. Comparatively, the credit cards in circulation from France and Brazil are less than a quarter of the number in circulation in the United States.
* **Buy big and save:** Bulk rates kept advertised credit card information at low costs. Bulk rates for credit cards advertised varied from small amounts such as 10 credit cards for $17, to larger bulk amounts such as 1000 credit cards for $300. Advertisers even used the same marketing tactics as legitimate stores and offered Christmas sale specials for bulk orders.
* [CPSS – Red Book statistical update](http://bis.org/publ/cpss93p2.pdf)

**Promises of riches to be bilked:** Advertised prices for bank account credentials depend on the account type, location of the home branch account, and the funds advertised as available. In 2010, prices for these credentials observed on underground economy servers ranged from $10 to $900. The advertised bank account balances ranged from $400 to one account with a purported balance of $1.5 million. As in previous years, corporate accounts were typically advertised for a higher price than personal accounts. This is likely because these bank accounts often have larger balances than those of personal accounts.  
  
**Let’s make a deal:** Prices for bank account credentials are negotiable. Although the country in which the bank is located was sometimes included in advertisements, it did not noticeably affect the prices for this reporting period. Some advertisements for bank account credentials listed minimal details, such as the banking organization only. This may suggest that some advertisers prefer to negotiate rates on a per-customer basis rather than locking themselves into a set price.  
  
1Cashiers on the underground economy are people who convert stolen goods, such as bank account credentials, into true currency, either in the form of online currency accounts or through money transfers. In exchange for the service, cashiers will charge a fee, which is usually a percentage of the cash-out amount.

**Spam Delivered by Botnets**

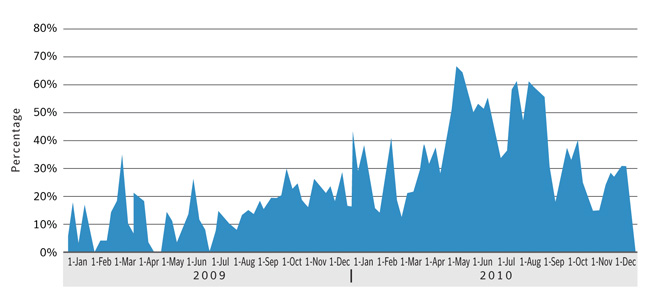
**Background**

This section discusses botnets and their use in the sending of spam. Botnets can be identified by SMTP patterns and in the structure of email headers. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis only reviews botnets involved in sending spam and does not look at botnets used for other purposes, such as for financial fraud or DoS attacks.

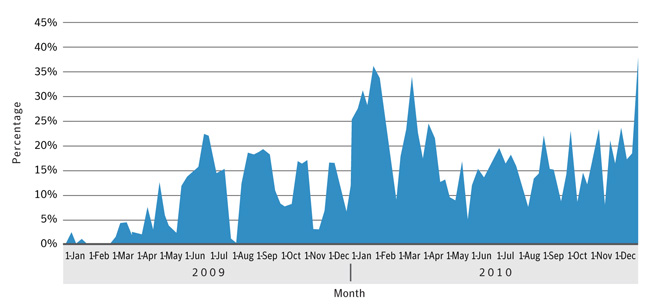
**Methodology**

MessageLabs Intelligence spam honeypots collected between 30-50 million spam emails each day during 2010. These are classified according to a series of heuristic rules applied to the SMTP conversation and the email header information. A variety of internal and external IP reputation lists are also used in order to classify known botnet traffic based on the source IP address of the sender. Information is shared with other industry insiders to ensure data is up to date and accurate.

**Data**



**Figure 24. Percentage of volume of botnet spam sent per day by Rustock botnet, 2009–2010**  
Source: MessageLabs Intelligence



**Figure 25. Percentage of volume of botnet spam sent per day by Grum botnet, 2009–2010**  
Source: MessageLabs Intelligence



**Figure 26. Spam from botnets as a percentage of total email, July 2009–October 2010**  
Source: MessageLabs Intelligence

**Commentary**

**Overall botnet spam decreases in 2010:** The total amount of global spam in circulation decreased toward the end of 2010, with a number of major botnets reducing their output. A major reason for the decrease in volume of spam email from botnets in 2010 is likely the shutdown of the SpamIt affiliate program in the fall of 2010. SpamIt was the largest known pharmaceutical spam affiliate—responsible predominantly for the “Canadian Pharmacy” brand—and the largest botnets send mostly pharmaceutical spam.

* [The recent drop in global spam volumes – what happened?](http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened)

**Changing tactics to send more spam using fewer bots:** One of the factors worth noting in the increased throughput from Rustock is that, in April 2010, its controllers stopped using TLS encryption to send spam, thus speeding up the email connections.1 For example, at its peak in March 2010, TLS-encrypted spam accounted for more than 30 percent of all spam, and as much as 70 percent of the spam from Rustock was sent using TLS-encrypted connections. However, since April 2010, the use of TLS in sending spam has fallen away dramatically, and by the end of 2010 accounted for just between 0.1 and 0.2 percent of spam. The use of TLS slows down a connection due to the additional encryption processing required. Symantec believes that the controllers of Rustock needed to recover this additional capacity in order to compensate for the recent contraction of the botnet in terms of its overall size. By turning off TLS, Rustock has been able to send more spam using fewer bots than it had previously with more bots and using TLS.

**Major botnet activity in 2010**

**Rustock** remained the most dominant botnet in 2010 with over 1 million bots under its control and its volume of spam more than double its 2009 percentage. It was the most dominant botnet throughout 2010 and was responsible for 36 percent of all spam during the year, with peak outputs of 64 percent of botnet spam in August and October. The output of spam from Rustock decreased at the end of 2010, likely due to the SpamIt shutdown, as mentioned previously.   
  
**Grum** was the second most active botnet for spam at the end of 2010, although both its number of active bots and volume of spam sent dropped off by the end of the year from peaks earlier in the year. Its volume dropped from 16 percent of the total at mid-year to 9 percent by year’s end, while the bots it controlled decreased by more than 50 percent, to between an estimated 310,000 to 470,000 bots worldwide.   
  
**Cutwail** ranked third, with approximately 6 percent of global spam in 2010. Its number of active bots increased by approximately 16 percent from the number of bots under its control at the end of 2009. Despite several takedown attempts during 2010, no action managed to do more than marginally reduce the spam output from Cutwail for a brief period. Each time it has returned to business-as-usual within a day or two. During 2010, Cutwail sent the widest variety of spam of any major botnets, including being the largest source of spam emails containing the Bredolab Trojan.  
  
**Maazben**—which had dropped out of the top 10 most active spam sending botnets by mid-2010—surged in the second half of the year to rank as the fourth most active botnet responsible for over 5 percent of spam by year’s end. The number of active bots under the control of Maazben control increased by more than 1,000 percent from March 2010, to between 510,000 and 770,000 bots by the end of the year.  
  
Toward the end of 2009, attempts to disrupt the **Mega-D** botnet seemed effectively to eliminate it. However, after only a few days, it resumed sending spam using a larger number of brand-new IP addresses. At that point, it was responsible for almost 18 percent of global spam. By the end of 2010, the amount of global spam sent by Mega-D was 2.3 percent of the total, the number of active bots under its control dropped by approximately 58 percent, and the spam output from each of its bots roughly halved every three months during the year—from approximately 428 spam emails every minute from each active bot in March, to 105 spam emails per bot per minute by the end of the year. It is likely that Mega-D was also reliant on a lot of business from the SpamIt affiliate and suffered after the shutdown in October.  
  
Since 2008, the **Storm** botnet has been a minor botnet; however, in April and May 2010 it made a significant reappearance when it was linked to a spam campaign making heavy use of legitimate shortened URLs that would redirect visitors to spam websites. Spam with shortened hyperlinks reached a peak of 18 percent at the end of April—equivalent to roughly 23.4 billion spam emails. In May 2010, spam from Storm accounted for nearly 12 percent of all the spam containing shortened hyperlinks.

* 1Transport Layer Security is a protocol that is intended to secure and authenticate communications across a public network through data encryption.

**Originating Sources of Botnet Spam**

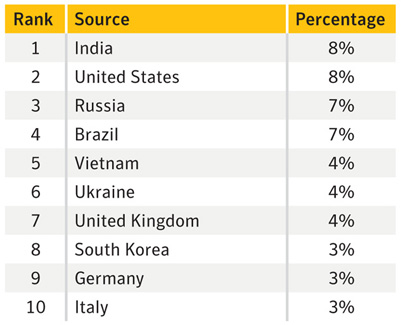
**Background**

This section discusses the top 10 sources of botnet spam origin in 2010. 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 location. In an attempt to bypass IP block lists, spammers use Trojans that relay email. This allows them to send spam from sites distinct from their location. To send large volumes of spam, spammers tend to take advantage of geographic areas with large networks of available broadband connections. This allows them to send out high volumes of spam by zombie connections at any time of the day.

**Methodology**

The data for this section is based on the analysis of email traffic collected from MessageLabs Intelligence global honeypots and from the analysis of malicious and unwanted email traffic data submitted by customers. The analysis of phishing trends is based on emails processed by Skeptic™ and recorded after perimeter traffic shaping and botnet connection mitigation techniques are applied. Botnet spam accounted for 88 percent of all spam in 2010, but does vary by client, so this analysis is based on the remaining 15-20 percent of email traffic not throttled at the perimeter. The honeypots are not affected in this way, and collected approximately 30-50 million spam emails each day during 2010.

**Data**



**Table 13. Top global sources of botnet spam, 2010**  
Source: MessageLabs Intelligence

**Commentary**

**India is single largest source of botnet spam:** The largest single source of botnet spam from one country was India, which accounted for 8 percent of global botnet spam. (The actual percentages before rounding for the top two sources are India at 8.4 percent and the United States at 8.2 percent) India remains a large source of infection for the top four major spam-sending botnets, Rustock, Grum, Cutwail, and Maazben. In 2010, these four botnets were responsible for 63 billion spam emails per day and two out of every three spam emails sent by a botnet could be attributed to one of these botnets. In addition, India was a major source of infection for smaller spam-sending botnets such as Bobax and Festi.   
  
**Spam from Rustock dominates in the United States.** The volume of spam coming from the United States increased during the first half of 2010, accounting for 8 percent of all global spam. The main factor for this high ranking is that the United States is the main source of infection for the largest spam-sending botnet, Rustock. Rustock had a significant spam output of over 44 billion spam emails sent per day, translating to almost half of all spam emails sent by botnets in 2010; this was almost double its volume output from 2009. It continues to be the largest botnet for spam, with an estimated size of between 1.1 and 1.7 million bots under its control during 2010.

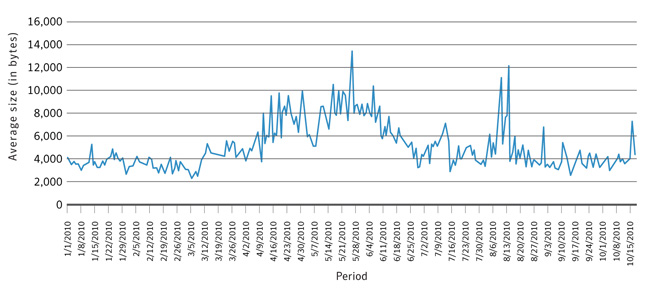
**Significant Spam Tactics**

**Background**

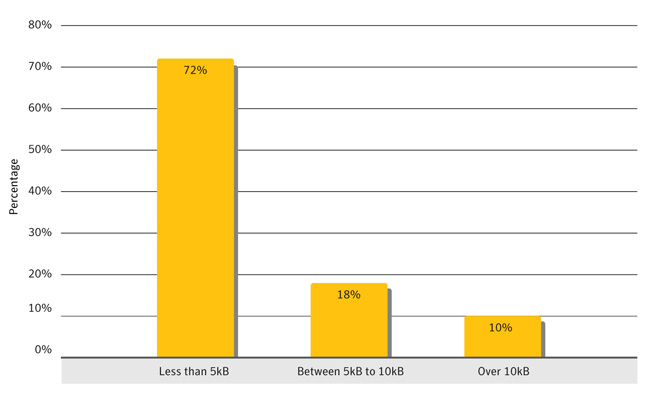
This section discusses significant spam tactics used throughout 2010, including the size of spam messages, how shortened URLs and the use of news and events shaped the content of spam, and how social engineering techniques have evolved.  
  
Tactics discussed include:

* Size of spam messages
* URL shortening and spam
* Tracking response rates for URL shortening services
* Spam by language
* File types found in spam messages

**Size of spam messages**

In 2010, the average size of a spam message was just over 5KB. In the last quarter of 2009, the average size was a little over 4KB. For spammers, smaller file sizes mean more messages can be sent using the same resources. That being said, the average size of spam emails increased from April to June, and again in August. The increased sizes were related to a long run of HTML format emails (with some attached images) being sent by both the Rustock and Cutwail botnets. The type of spam in these campaigns was mainly pharmaceutical, with some fake/replica watch spam.  
  


**Figure 27. Average size of spam messages, by week, January 2010–October 2010**  
Source: MessageLabs Intelligence



**Figure 28. Distribution of size of spam messages for 2010**  
Source: MessageLabs Intelligence

**Commentary**

From June 2010 onward, only 3 percent of spam had a file attached, with a peak of 11 percent for one day in September. The size of these messages is typically determined by whether or not there is an attachment included—which may include documents, images, or videos. An email with a file attached will always be bigger than one that contains a link to the file instead. This is important to spammers because the size of an email will have a direct effect on how many can be sent in a given time period. A larger file size for spam email implies that a spammer can send a smaller volume of email versus spam email with a small file size. Spammers would want to maximize their profits by delivering as much spam as possible.  
  
There was a rise in the daily average file size of spam emails in August 2010, with a peak of 12KB. This rise was likely due to a large run of compressed archives from the Cutwail botnet spreading the Bredolab family of malware. Emails containing malware are generally larger because they contain executable code or exploitable file attachments. In 2010, 88 percent of malicious spam emails were over 10KB, with over 26 percent ranging in file size from 90KB to 100KB. Malicious code in spam emails tends to be sent in batches, with each batch consisting of a different type of malicious code. A batch with an attachment will mean bigger files and fewer sent since the attachments are usually far larger than typical text-based spam.

**URL shortening and spam**

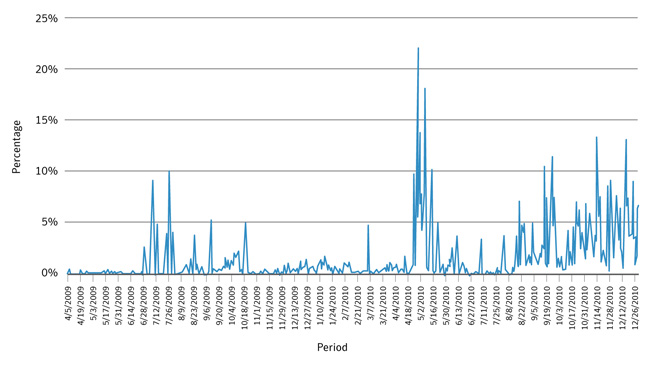
Shortened URLs have become popular in recent years as means of conserving space in character-limited text fields, such as those used for microblogging. Some URLs consist of a substantial number of characters that can eat up character limits, break the flow of text, or cause distortions in how Web pages are rendered for users. URL shortening services allow people to submit a URL and receive a specially coded, shortened URL that redirects to the submitted URL (figure 29). When a user clicks on the shortened URL, the service will redirect the person to the submitted Web page.  
  


**Figure 29. Example of a shortened URL**  
Source: Symantec Corporation

These services can be very convenient when referring people to Web pages that have very long URLs. However, attackers capitalize on these services because potential victims are usually unable to determine where the URL will send them. An example of this involves attackers mimicking popular posts but replacing legitimate URLs with shortened ones in the hopes that users will be less likely to notice that the URL has been changed.

* [Turning Good News into Bad News](http://www.symantec.com/connect/blogs/turning-good-news-bad-news)

**Data**



**Figure 30. Percentage of spam containing a shortened URL, April 2009 – December 2010**  
Source: MessageLabs Intelligence

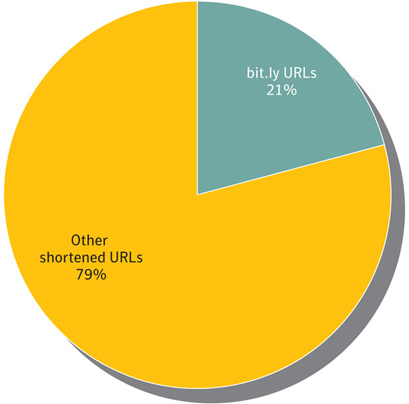
**Commentary**

**Cutwail and Grum send the most spam with shortened URLs:** MessageLabs Intelligence tracked a steady rise in the average percentage of spam containing shortened URLs from mid-August 2010 until the end of the year. From mid-August 2010, at least 1 percent of spam each day contained a shortened URL. By September 2010, the proportion of spam that contained a shortened URL reached 3 percent of spam and averaged approximately 2 percent of all spam by the end of the year. The botnets responsible for this sustained rise in the baseline proportion of spam containing shortened URLs were Cutwail and Grum, the majority of which were related to pharmaceutical and fake/replica watch spam.

**Tracking response rates for URL shortening services**

One of the most frequently seen shortened URL services in spam is the “bit.ly” service. bit.ly also provides a service in which users can view statistics on a given shortened URL by appending a ‘+’ after the shortened URL (e.g. http://bit.ly/d6nmLZ+). MessageLabs Intelligence is able to collect all of the statistics from these pages and analyze the click-through responses for shortened URLs using this provider. Note that some spam email messages contained more than one link.

**Data**



**Figure 31. Distribution of shortened URLs in spam emails, January 2010–October 2010**  
Source: MessageLabs Intelligence

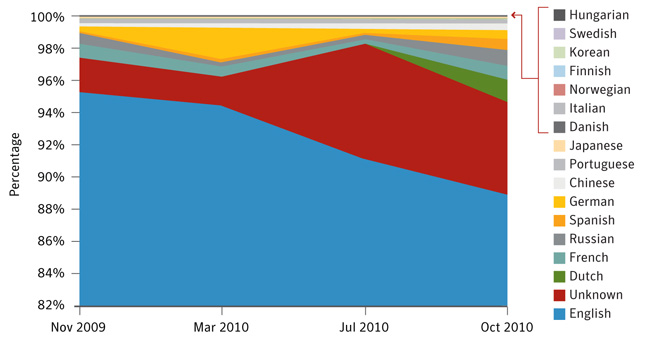
**Commentary**

**bit.ly links generate strong click-through response:** From January 1, 2010 to October 15, 2010, over 21 percent of shortened URL spam emails contained links to bit.ly URLs. These emails generated over 27 click-through responses per each email that contained a bit.ly URL. Since some emails contained more than one URL, there were over 44 click-through responses per bit.ly URL. The distribution of bit.ly shortened URLs mirrored all spam emails in general with a majority of the bit.ly shortened URLs in the categories of pharmaceutical products and watches.  
  
**The (brief) lifecycle of a bit.ly URL in the wild:** In early September 2010, a single shortened URL generated over 13,000 responses during one day. This large click-through response was a major contributing factor to a large peak in the amount of spam containing bit.ly URL spam emails. An estimated 352 million spam emails with this shortened URL were sent over a three-day period, generating over 17,000 click-through responses during that time. By the end of the observation period, the total of click-through responses was over 18,000. The URL in question redirected to a replica watch website and it is likely that the spammers’ income would have been generated from an affiliate scheme relating to the site. In cases like this, because most of the click-through responses are generated in the first few days of delivering the spam emails, and since many of the associated phishing websites are quickly shut down, it is in the spammers’ best interests to establish the shortened URLs and distribute the spam emails as quickly as possible in order to capture the maximum return in the shortest time.

**Spam by language**

The data for this section is based on the analysis of spam processed by Skeptic™ and recorded after perimeter traffic shaping and botnet connection mitigation techniques are applied. This means that the measurements are for language of spam not sent from a known botnet. Botnet spam accounted for 88 percent of all spam in 2010, but does vary by client, so this analysis is based on the remaining 15-20 percent of spam not throttled at the perimeter. The analysis is based on a random sample of 1,000 spam messages sent to each country. A series of checks are made against the language of the subjects and headers available from the Skeptic™ database.

**Data**



**Figure 32. Spam by language, November 2009–October 2010**  
Source: MessageLabs Intelligence

**Commentary**

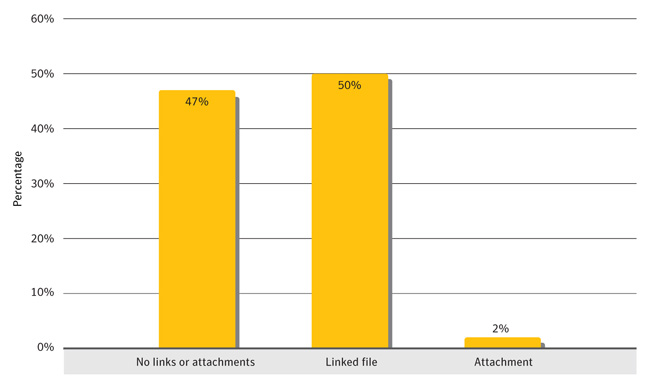
**Spam in English still dominates, but decreases over the year:** At the start of 2010, 96 percent of spam detected was in English. This declined slowly over the year, falling to 90 percent in August, where it has remained since. This indicates a growth in spam based in other languages.  
  
**The use of spam with only images or URLs rises:** Of the percentage of spam not in English, about half is classified as “unknown” (e.g., varying from just over 2 percent in November 2009 to nearly 6 percent in October 2010). An email is classified as unknown when there is not enough recognizable text within the body of the email to be able to determine a language. In most cases, this is because the body only contains a very small amount of HTML code, such as a hyperlink to a website or an image.  
  
**Brazil bucks the trend:** Brazil is the only country examined where the most common language is neither “unknown” nor English. Approximately 33 percent of spam sent to Brazilian recipients was in Portuguese. Brazil has one of the lowest percentages of English language spam at approximately 26 percent.

**File types found in spam messages**

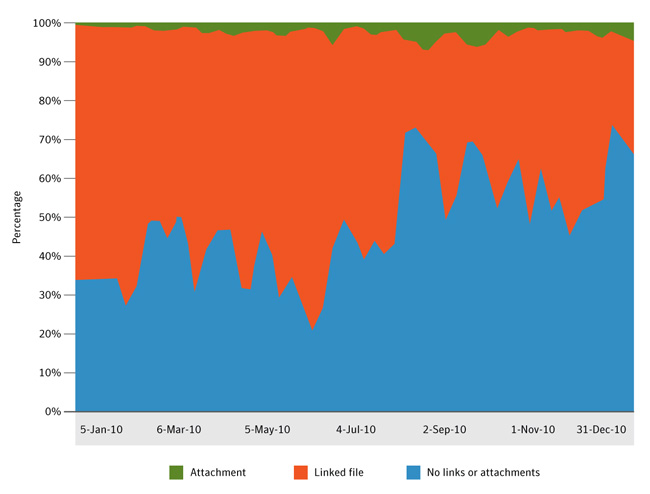
Spam email was classified into three categories for this metric:

1. Spam without links or attachments – no associated file
2. Spam with links to a file or Web page
3. Spam with attachments

**Data**



**Figure 33. Distribution of file types found in spam messages, 2010**  
Source: MessageLabs Intelligence (Due to rounding, percentages may not equal 100 percent)



**Figure 34. File types found in spam messages, by day, 2010**  
Source: MessageLabs Intelligence

**Commentary**

In 2010, 53 percent of spam emails contained links to files or a Web page, or the email had a file attached to the email itself. Files were either hosted online, or attached to the spam email, as follows:  
  
**Hosted files in spam:** Most of these files were not attached to spam emails, rather they were linked in HTML:

* **Remotely hosted images:** Of these remote files, almost 70 percent are image files. Typically, these image files form part of an email written in HTML format and are used either to make spam that looks like legitimate professional marketing spam (e.g. brand logos, product images) or to replace what would normally be a text body (so the image contains text) in an effort to evade text based spam filtering. These are often hosted using free online hosting services.
* **Specific Web file type links:** : The second most common type of file linked to is Web page files. This includes static HTML files, dynamic PHP files, ASP files, etc. Normal marketing emails often contain links, but generally they link to a website landing page (e.g. http://www.somesite.com) rather than a specific file (e.g. http://www.somesite.com/somefile.php). On some occasions, spammers are using links to compromised, legitimate websites to host this content.
* **Remotely hosted executables:** Other types of files that are linked to in emails are documents, compressed archives, and executables, although links to these types of files are rare because they are usually attached to the email rather than hosted remotely. In total, they accounted for a fraction of a percent of all linked files in spam since the end of May 2010.

**Attached files in spam:** In 2010, it was much less common to find spam with files attached, with only 2 percent of spam emails containing a file attached to it—peaking at 11 percent of all spam emails in September. There are several reasons why spammers do not attach files. First, many enterprises limit attachments in emails from external sources, especially from certain file types (such as .exe, .zip, etc.). Another reason is that an email with an attached file will always be bigger than one with just a link to the file instead. This is important because the size of an email determines how many can be sent in a given time. A bigger file size means less mail sent, and less mail sent means less potential income for the spammers.

**Spam by Category**

**Background**

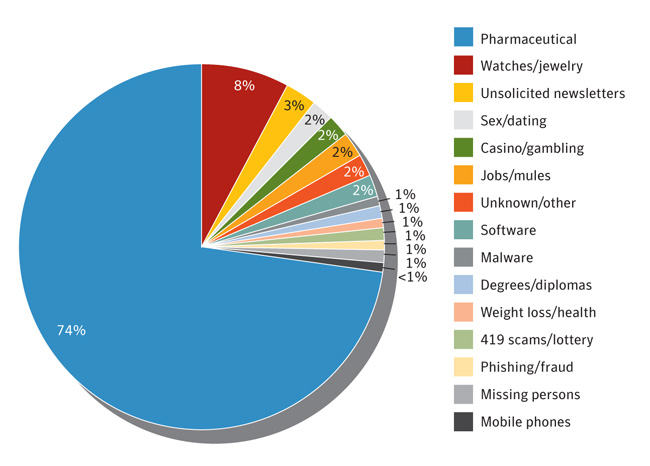
Spam is created in a variety of different styles and complexities. Some spam is plain text with a URL and some is cluttered with images and/or attachments. Some comes with very little in terms of text, perhaps only a URL. And, of course, spam is distributed in a variety of different languages. It is also common for spam to contain “Bayes poison” (random text added to messages that has been randomly scraped from websites to “pollute” the spam with words bearing no relation to the intent of the spam message itself). This is done in an attempt to thwart spam filters that typically try to deduce spam based on a database of words that are frequently repeated in spam messages.   
  
Any automated process to classify spam into one of the categories below would need to overcome this issue. For example, the word “watch” may appear in the random text included in a pharmaceutical spam message, posing a challenge as to classify the message as pharmaceutical spam or in the watches/jewelry category. Another challenge occurs when a pharmaceutical spam contains no obvious pharmaceutical-related words, but only an image and a URL.   
  
Spam emails are meant to be read by humans, and spammers thus attempt to get their messages through to the recipients without revealing too many clues that the message is spam. Any such clues found in the plain text content of the email can be examined using automated antispam techniques. A common way to overcome this is by using random text, but an equally effective way is to include very little in the way of extra text in the spam and to instead include a URL in the body of the message.   
  
Spam detection services often resist classifying spam into different categories because it is difficult to do (for the reasons above) and because the purpose of spam detection is usually to determine whether the message is spam and to block it, rather than to identify its subject matter. In order to overcome the ambiguity faced by using automated techniques to classify spam, the most accurate way to do it is to have a real person classify unknown spam manually. While time consuming, this provides much more accurate results. An analyst can read the message, understand the context of the email, view images, follow URLs and view websites in order to gather the bigger picture around the spam message.

**Methodology**

Once per month, 200 random spam samples are manually classified into one of the following categories:

* 419 scams/lottery
* Casino/gambling
* Degrees/diplomas
* Jobs/mules
* Malware
* Missing persons
* Mobile phones
* Pharmaceutical
* Phishing/fraud
* Sex/dating
* Software
* Unknown/other
* Unsolicited newsletter
* Watches/jewelry
* Weight loss/health

**Data**



**Figure 35. Spam by category**  
Source: MessageLabs Intelligence

**Commentary**

**Pharmaceutical products predominate:** Approximately three quarters of all spam in 2010 was related to pharmaceutical products—a great deal of which was related to “Canadian Pharmacy” websites and related brands. These sites sell a variety of drugs for anything from male enhancement, to weight loss, to stress relief. This type of spam was delivered by some of the largest spam-sending botnets in 2010, including Rustock, Grum, Cutwail, and Donbot. Because of the potential for profit in the underground economy, spammers line up to work with affiliate schemes such as SpamIt—distributing enormous volumes of rapidly changing spam and taking commission for their efforts. For example, even with a seemingly miniscule click-through conversion rate of one response per 12.5 million spam emails, some botnets send out millions of spam messages per day, which would thus still result in potential profits for the spammers.

* [BBC News article: Study shows how spammers cash in](http://news.bbc.co.uk/2/hi/7719281.stm)

**SpamIt shutdown only temporarily reduces pharmaceutical spam:** In October 2010, the closure of a well-known spam affiliate called SpamIt—the mainstay of the so-called Canadian Pharmacy business—resulted in a large drop of pharmaceutical-related spam. This closure can be seen in the drop of spam volumes of some of the major spam-sending botnets such as Rustock, as discussed elsewhere in this report. This drop, though, was only temporary because many spammers quickly switched to alternative affiliate schemes in order to continue sending spam. Despite the drop in spam volume, the percent of pharmaceutical spam at the end of 2010 returned to levels similar to those observed at the end of 2009.  
  
**A category with a low percentage still means millions of spam messages:** Although it is difficult to be certain what the true volume of spam in circulation is at any given time, Symantec estimates that 95.5 billion spam emails were sent globally each day in 2010. Where some of the categories above represent 0.5 percent of spam, this still equates to almost 500 million spam emails in a single day. Based on estimates of global broadband users—even for something as relatively rare as a 419 scam—that may be equivalent to one scam email per broadband user per day. For pharmaceutical spam, approximately 122 pharmaceutical spam emails are sent per broadband user per day, on average.1  
  
**Unsolicited newsletters are proliferating:** Although pharmaceutical spam dominates every year, in 2010, spam related to unsolicited newsletters, sex/dating, casino/gambling, job scams, and software all increased. Of particular note is the unsolicited newsletter category, which rose from less than 2 percent of spam at the beginning of the year to 5.6 percent in the summer, and then to 9 percent in October. In October, most unsolicited newsletters from botnets were sent using the Xarvester and Mega-D botnets. One reason for this may be because some companies may inadvertently or otherwise share their newsletter subscriber lists with third parties. Other causes include poor regulatory compliance and breaches from hackers infiltrating the enterprise.  
  
**Sex/dating spam is on the increase:** This type of spam became much more common in 2010. These were either mails containing sexual images or URLs that linked to adult or dating websites. In September 2009, sex/dating spam accounted for less than 1 percent of the total. One year later, it had increased to account for over 5 percent of all spam, most of which was being sent from the Cutwail and Mega-D botnets.

* [Dating scammers can be ingenious](http://www.symantec.com/connect/blogs/dating-scammers-can-be-ingenious)

1For current spam rates and other data, see <http://www.symantec.com/business/security_response/landing/spam>

**EMEA Introduction**

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify and analyse, to deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.  
  
More than 240,000 sensors in more than 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 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.  
  
In addition, Symantec maintains one of the world’s most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 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 24,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.  
  
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; as well as other Symantec technologies. Data is collected in more than 86 countries from around the globe. 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 secure their systems effectively now and into the future.  
  
In addition to gathering global Internet attack data, Symantec also analyses attack data that is detected by sensors deployed in specific regions. This report discusses notable aspects of malicious activity Symantec has observed in Europe, the Middle East and Africa (EMEA) for 2010.

**EMEA Threat Activity Trends**

The following section of the Symantec Europe, the Middle East and Africa (EMEA) *Internet Security Threat Report* provides an analysis of threat activity, malicious activity, and data breaches that Symantec observed in EMEA in 2010. The malicious activity discussed in this section not only includes threat activity, but also phishing, malicious code, spam zombies, bot-infected computers, and network attack origins. 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 activities can be found in their respective sections within this report.  
  
This section discusses the following metrics, providing analysis and discussion of the trends indicated by the data:

* Malicious activity by country
* Attack origin by country
* Web-based attack activity
* Bot-infected computers by country

**EMEA Malicious Activity by Country**

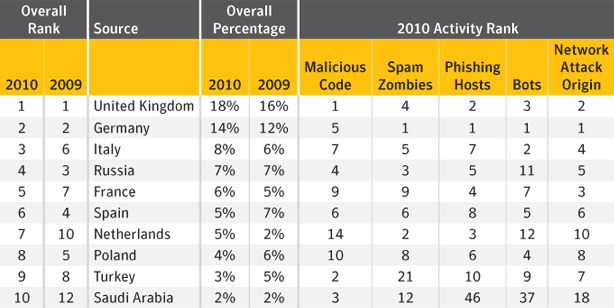
**Background**

This metric assesses the countries in the Europe, the Middle East, and Africa (EMEA) region in which the largest amount of malicious activity takes place or originates. Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically a more stable connection. Symantec categorizes malicious activities as follows:  
  
**Malicious code:** This includes viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, or compromising the security or integrity of a victim’s computer data.  
  
**Spam zombies:** These are compromised systems that are remotely controlled and used to send large volumes of junk or unsolicited emails. These emails can be used to deliver malicious code and phishing attempts.  
  
**Phishing hosts:** A phishing host is a computer that provides website services for the purpose of attempting to illegally gather sensitive, personal and financial information while pretending that the request is from a trusted, well-known organisation. These websites are designed to mimic the sites of legitimate businesses.  
  
**Bot-infected computers:** These are compromised computers that are being controlled remotely by attackers. Typically, the remote attacker controls a large number of compromised computers over a single, reliable channel in a bot network (botnet), which then is used to launch coordinated attacks.  
  
**Network attack origins:** These are originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.

**Methodology**

To determine malicious activity by country, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing hosts, bot-infected computers, and network attack origins. The proportion of each activity originating in each country is then determined within the region. 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. The rankings are then determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

**Data**



**Malicious activity by country, EMEA**  
Source: Symantec Corporation

**Commentary**

**The United Kingdom and Germany continue to have the highest percentages of malicious activity in the EMEA region:** In 2010, the United Kingdom and Germany were once again the top sources for overall malicious activity within EMEA. Globally, the United Kingdom ranked fifth and Germany ranked third overall for malicious activity. This indicates that attackers in the United Kingdom were more focused on the region, while attackers in Germany were more likely to target global systems.

* The continued top ranking of the United Kingdom in this metric is due to its high volume of malicious code activity.
* Germany’s high ranking is due to it ranking first in spam zombies, phishing hosts, bots, and originating network attacks. Germany has a firmly established broadband infrastructure with the most broadband users in the EMEA region. With almost 27 million broadband users, even if a small proportion of these systems are unpatched, these computers would still represent a large number of attractive targets for attackers and, thus, lead to a high percentage of malicious activity in the country.

**More than half of the world’s spam zombies were located in the EMEA region:** EMEA continues to be the region with the highest percentage of spam zombies, accounting for 54 percent of the global total in 2010. Germany, the Netherlands, and Russia had the highest percentages of spam zombies within the EMEA region, together accounting for over one-third of the regional total. One reason for this high percentage is that computers from EMEA are major sources of infection for major spam botnets such as Ozdok (Mega-D), Cimbot, Bobax, and Xarvester.

* [Read about the sources of infection for spambots](http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf)

**Turkey and Saudi Arabia continue to report high-levels of malicious code for 2010:** Although ranked ninth and tenth, respectively, for overall malicious activity in EMEA in 2010, Turkey and Saudi Arabia ranked second and third in the malicious code category in the region. This is likely due to the high volumes of potential virus and worm infections in the two countries for 2010. Turkey was the top ranked country for potential virus infections in 2010, mostly due to the Almanahe.B virus, which was very prominent there. Meanwhile, the Sality.AE and Mabezat.B worms had the most potential worm infection reports in Saudi Arabia in 2010.

**EMEA Attack Origin by Country**

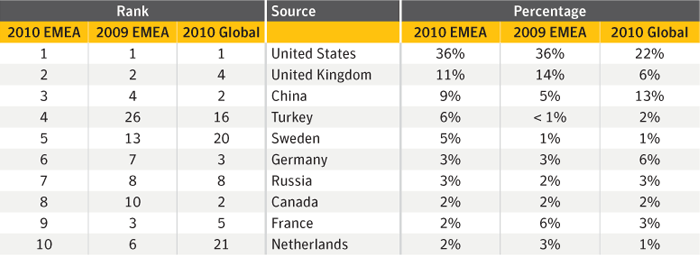
**Background**

This metric assesses the top global countries from which attacks originated that targeted the EMEA region in 2010. Note that, because the attacking computer could be controlled remotely, the attacker may be in a different location than the computer being used to mount the attack. For example, an attacker physically located in the United States could launch an attack from a compromised system in Germany against a network in the United Kingdom.

**Methodology**

This section measures the top originating countries of attacks that targeted computers in EMEA in 2010. A network attack is generally considered any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS), intrusion prevention system (IPS), or firewall.

**Data**



**Top attacks by country in EMEA, 2009-2010**  
Source: Symantec

**Commentary**

**The United States continues to dominate attacks on EMEA:** In 2010, 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. This is the same percentage as in 2009, when the United States also ranked first. 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 22 percent of that total. It also ranked first for overall global malicious activity, with 19 percent of that total. The United States also ranked first globally for bot-infected computers and malicious code, and much of the attack activity targeting EMEA countries would have been conducted through these malicious bot networks.   
  
**Attacks from Turkey increase:** Turkey experienced a significant rise as a country of origin for attacks on the EMEA region for 2010. The high rank of Turkey for malicious code activity within the EMEA region and top ranking in potential virus infections may have contributed to this rise. For example, the Almanahe.B virus, which propagates over networks, was very prominent in Turkey in 2010.

**EMEA Web-based Attack Activity**

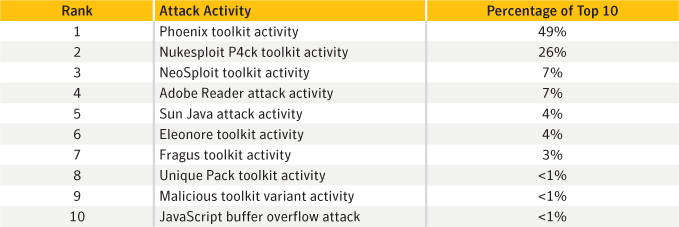
**Background**

The increasing pervasiveness of Web browser applications along with increasingly common, easily exploited Web browser application security vulnerabilities has resulted in the widespread growth of Web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to compromise specific networks to gain access to those computers. Symantec analyses attack activity to determine which types of attacks and attack toolkits are being employed by attackers. This can provide insight into emerging Web-based attack trends and may indicate the types of attacks with which attackers are having the most success.

**Methodology**

This metric assesses the top Web-based attack activity originating from compromised legitimate sites and intentionally malicious sites set up to target Web users in Europe, the Middle East, and Africa (EMEA) in 2010. To determine this, Symantec ranks attack activity by the volume of associated reports observed during the reporting period. The top 10 Web-based attack activities are analysed for this metric.

**Data**



**Web-based attack activity in EMEA, 2010**  
Source: Symantec

**Commentary**

**Cybercrime is global:** The top 10 rankings for Web-based attack activity in EMEA in 2010 differ very little from the rankings for the 2010 global figures. All of the top activities are the same with just slight variations in the rankings and percentages. This indicates the global nature of cybercrime and shows that, because these activities are Web-based, there are no immediate geographic limitations. This may be a significant factor in the rise of Web-based attacks in recent years, especially with considerations for financial gain. This is because a single malicious website can reach a widely dispersed pool of potential victims without being restricted to a specific country or region.  
  
**Phoenix is rising:** The most prominent volume of Web-based attack activity observed in 2010, both in EMEA and globally, was related to the Phoenix toolkit. This kit was first observed by security researchers in 2009, although it is rumoured to have been first released in 2007. This activity refers to attempts to download and execute exploit code on a victim’s Web client that is specific to the Phoenix toolkit. One version of Phoenix is known to exploit 16 vulnerabilities affecting multiple technologies. Successful attacks may install a rogue security software application called PC Defender Antivirus on compromised computers. Some of the vulnerabilities that Phoenix exploits affected a number of widely used technologies, including Sun Java, Microsoft Windows Media Player, Microsoft Internet Explorer, and Adobe Flash Player and Reader.

* [Read about rogue security software application PC Defender Antivirus](http://www.symantec.com/security_response/writeup.jsp?docid=2010-021812-5220-99)
* [Sun Java Runtime Environment and Java Development Kit Multiple Security Vulnerabilities](http://www.securityfocus.com/bid/32608)
* [Microsoft Windows Media Player Plugin Buffer Overflow Vulnerability](http://www.securityfocus.com/bid/16644)
* [Microsoft Active Template Library Header Data Remote Code Execution Vulnerability](http://www.securityfocus.com/bid/35558)
* [Adobe Flash Player Multimedia File Remote Buffer Overflow Vulnerability](http://www.securityfocus.com/bid/28695)
* [Adobe Acrobat and Reader Multiple Arbitrary Code Execution and Security Vulnerabilities](http://www.securityfocus.com/bid/27641)

**Java is being targeted:**

* **Java presents an attractive point of attack for attackers:** As evidenced by activity related to the Phoenix attack kit, as well as numerous other kits that successful employ Java exploits, Java presents an attractive point of attack for attackers. Furthermore, the sixth-ranked Sun Java attack activity refers to Java attacks that are not directly relatable to a specific attack toolkit. In some cases, the exploit code used in these attacks may be the same across multiple kits if the authors acquired the code from the same source.
* **Attackers may begin favouring Java exploits:** Detecting Java attacks can be challenging because the technology relies on a runtime environment that adds additional layers of processing that need to be analysed. While Java attacks that occurred in 2010 gained a significant amount of attention, they may not have been launched as frequently as attacks that exploited other technologies. One reason for this may be that attack toolkits often launch attacks in a sequence, trying one exploit after another until an exploit succeeds, all options are exhausted, or the source of the attacks is blocked by the victim. This could result in blocked or successful attacks occurring prior to the Java exploits being launched. Over time, attackers may begin weighting the sequence of attack attempts in favour of those that exploit Java vulnerabilities in order to increase their chances of success.
* **Symantec expects the volume of Java-related attacks to increase:** The authors of newly released kits such as Dragon Pack and Bleeding Life are touting the success of included Java exploits. As a result, Symantec expects the volume of Java-related attacks to increase.
* [Microsoft: ‘Unprecedented Wave of Java Exploitation’](http://krebsonsecurity.com/2010/10/microsoft-a-tidal-wave-of-java-exploitation/)
* [Exploit Packs Run on Java Juice](http://krebsonsecurity.com/2011/01/exploit-packs-run-on-java-juice/)

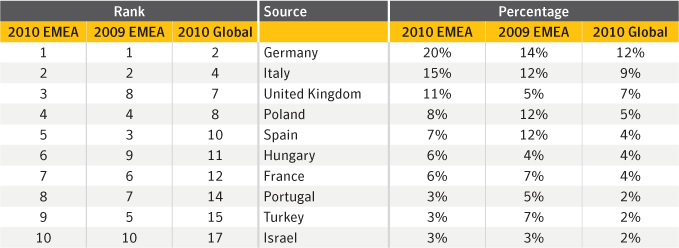
**EMEA Bot-Infected Computers by Country**

**Background**

This metric measures the countries of origin for bot-infected computers in Europe, the Middle East and Africa (EMEA) for 2010. Bot-infected computers, or bots, are programs that are covertly installed on a user’s machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet relay chat (IRC), P2P, or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a 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 that may be used in identity theft from compromised computers—all of which can lead to serious financial and legal consequences.   
  
Attackers favour bot-infected computers with a decentralized command & control (C&C) model because they are difficult to disable and allow attackers to hide in plain sight among the typically massive amounts of unrelated traffic occurring over the same communication channels. Most importantly, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate. For example, Symantec observed an advertisement on an underground forum in 2010 promoting a botnet of 10,000 bots for $15 USD. (The advertisement did not stipulate whether the cost was for purchase or rental).

**Methodology**

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. A distinct bot-infected computer is a distinct computer that was active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they can be classified as actively attacking bots, bots that send out spam (i.e. spam zombies), or bots that are used for DoS campaigns.



**Bot-infected computers by country in EMEA, 2009-2010**  
Source: Symantec

**Commentary**

**EMEA region dominates for bot-infected computers:** In 2010, the EMEA region accounted for 59 percent of all bot-infected computers detected globally, more than any other region. Of the top 10 countries for bot-infected computers in the EMEA region, seven were also in the top 10 countries for overall regional malicious activity. This may suggest that the number of bot-infected computers in these countries may be a reflection of the overall malicious activity occurring there.   
  
**Top 10 countries for bot-infected computers in the EMEA region remain unchanged from 2009:** Within the region, the distribution of bot-infected computers appears relatively stable, with countries listed in the top 10 from 2009 remaining in the top 10 for 2010. In fact, aside from Hungary, the remaining countries listed here in 2010 have been in the top 10 for this category since 2007.

**EMEA Malicious Code Activity Trends**

Symantec collects malicious code information from its large global customer base through a series of opt in anonymous telemetry programs, including Norton Community Watch, Symantec Digital Immune System, and Symantec Scan and Deliver technologies. Well over 100 million clients, servers, and gateway systems actively contribute to these programs. New malicious code samples, as well as detection incidents from known malicious code types, are reported back to Symantec. Reported incidents are considered potential infections if an infection could have occurred in the absence of security software to detect and eliminate the threat.   
  
Malicious code threats are classified into four main types— backdoors, viruses, worms, and Trojans:  
  
**Backdoors** allow an attacker to remotely access compromised computers.  
  
**Trojans** are malicious code that users unwittingly install onto their computers, most commonly through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.  
  
**Viruses** propagate by infecting existing files on affected computers with malicious code.  
  
**Worms** are malicious code threats that can replicate on infected computers or in a manner that facilitates them being copied to another computer (such as via USB storage devices).  
  
Many malicious code threats have multiple features. For example, a backdoor is always categorized in conjunction with another malicious code feature. Typically, backdoors are also Trojans; however, many worms and viruses also incorporate backdoor functionality. In addition, many malicious code samples can be classified as both worm and virus due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.  
  
This discussion is based on malicious code samples detected by Symantec in the EMEA region in 2010, with the following trends being analysed.

* Prevalence of malicious code features
* Top malicious code samples
* Top new malicious code families
* Threats to confidential information
* Propagation mechanisms

**EMEA Prevalence of Malicious Code Features**

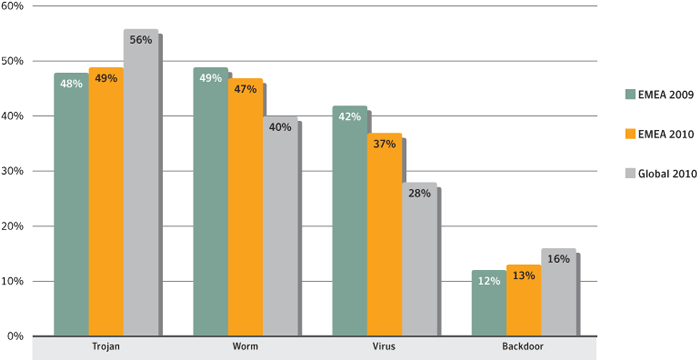
**Background**

As noted in the introduction to this section, Symantec categorizes malicious code features into four basic categories—backdoors, Trojans, viruses, and worms. Analysing the prevalence of each malicious feature provides insight into the general diversity of the threat landscape. Combined with the data from other metrics, this helps Symantec more accurately determine emerging trends in malicious code.

**Methodology**

This analysis focuses on the top 50 most prevalent malicious code samples of 2010 in Europe, the Middle East and Africa (EMEA). Each code sample is analysed and its features categorized into one of the four basic categories. The sum of this feature is measured by its volume proportional to the prevalence of each code sample in which it is found.   
  
As previously noted, malicious code samples are often characterized by more than one category; therefore, the volume of potential infections associated with each sample may apply to the proportions of multiple types. The proportions of the top 50 potential infections of the current period in EMEA are compared to those of the top 50 potential infections of the previous period in EMEA in order to observe shifting malicious code activity in the threat landscape. Since these are proportional figures, it should be noted that a change in proportion does not represent a year-over-year increase or decrease in potential infections.

**Data**



**Potential infections by type in EMEA, 2009-2010**  
Source: Symantec

**Commentary**

**Proportional stability:** Overall, the year-over-year similarity of proportions of each malicious code type in EMEA suggests that high profile malicious code (such as the Stuxnet worm) did not significantly affect the overall level of activity in the region (despite Stuxnet being active mostly in EMEA). This is further supported by the similar patterns in the top malicious code families observed year-over-year in the region.

* [Read about the Stuxnet worm](http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99)

**Worms and viruses:** Worms and viruses accounted for larger proportions of potential infections observed in EMEA than they did globally. One reason for this in 2009 was the prominence of the Downadup worm (a.k.a., Conficker). A significant contributor to this difference between proportions in 2010 was the Ramnit virus, which also has worm components. There was a high volume of Ramnit reports starting from its discovery early in 2010. Ramnit was the third ranked malicious code sample in EMEA and highest ranked new malicious code family EMEA in 2010.

**EMEA Top Malicious Code Samples**

**Background**

This metric assesses the top malicious code samples in EMEA in 2010. Symantec analyses new and existing malicious code samples to determine which threats types and attack vectors are being employed in the most prevalent threats. This information also allows administrators and users to gain familiarity with threats that attackers may favour in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

**Methodology**

To determine top malicious code samples, Symantec ranks each malicious code sample based on the volume of unique sources of potential infections observed during the reporting period.

**Data**



**Top malicious code samples, EMEA**  
Source: Symantec

**Commentary**

**The Sality.AE virus continues to dominate:** The top malicious code sample by volume of potential infections in EMEA for 2010 was Sality.AE. Reported activity by this virus was the primary contributor to the Sality family being the highest ranked malicious code family globally in 2010. Discovered in 2008, Sality.AE has been a prominent part of the threat landscape since then, including being the top malicious code sample identified by Symantec in 2009. Sality may be particularly attractive to attackers because it uses polymorphic code that can hamper detection. Sality is also capable of disabling security services on affected computers. These two factors may lead to a higher rate of successful installations for attackers. Sality propagates by infecting executable files and copying itself to removable drives such as USB devices. The virus then relies on Microsoft Windows AutoRun functionality to execute when those drives are accessed. This can occur when an infected USB device is attached to a computer. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Sality.AE (as well as SillyFDC and others) effective vehicles for installing additional malicious code on computers.

* [Read about Sality.AE](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99)
* [Read the *Global Internet Security Threat Report* 2009](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf)
* [Learn about SillyFDC](http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99)

**The Ramnit virus:** Ramnit is particularly interesting because it ranked third in EMEA in 2010 despite just being discovered in this reporting period (and making it also the highest ranked new malicious code family in EMEA for 2010). Newly discovered threats are often overshadowed in this metric by longer-running, existing threats. While Ramnit ranked ninth globally in 2010, 56 percent of its infections were reported from EMEA.

* [Read about Ramnit](http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99)

**EMEA Top New Malicious Code Families**

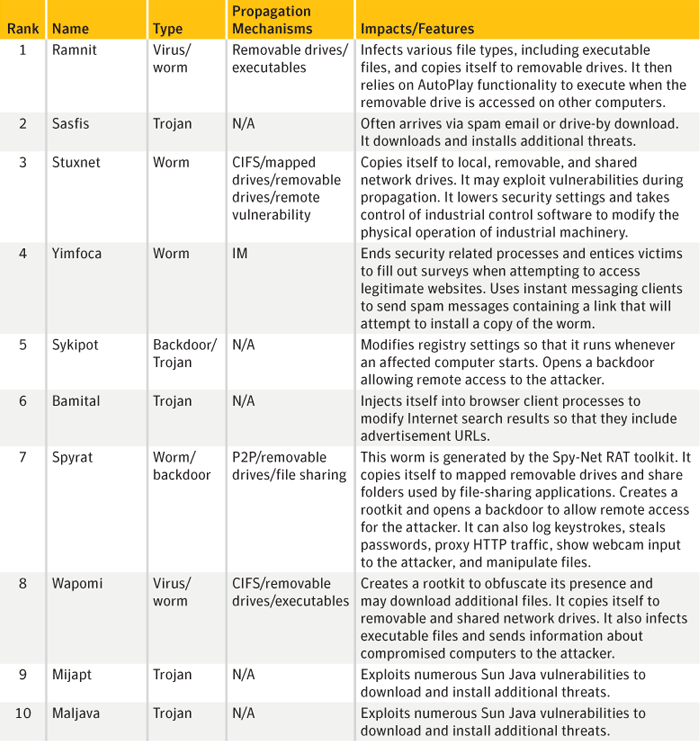
**Background**

Symantec analyses new and existing malicious code families to determine which threats types and attack vectors are being employed in the most prevalent threats. This information also allows administrators and users to gain familiarity with threats that attackers may favour in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

**Methodology**

A malicious code family is initially composed of a distinct malicious code sample. As variants to the sample are released, the family grows to include multiple variants. Symantec determines the most prevalent malicious code families by collating and analysing anonymous telemetry data gathered for the reporting period. Over the course of 2010, such products reported over 1.5 billion such malicious code detections. Malicious code is classified into families based on variants in the signatures assigned by Symantec when the code is identified. Variants appear when attackers modify or improve existing malicious code to add or change functionality. These changes alter existing code enough that antivirus sensors might not detect the threat as an existing signature.   
  
This metric assesses the top new malicious code families detected in EMEA in 2010. To determine this, Symantec ranks each malicious code family based on the volume of potential infections reported during the reporting period. The top 10 new malicious code families are analysed for this metric.

**Data**



**Top new malicious code families, EMEA**  
Source: Symantec

**Commentary**

**The Ramnit virus:** Along with being the top ranked new malicious code family in EMEA in 2010, Ramnit was also the third ranked malicious code sample in EMEA in 2010, which is unusual for a new threat. While Ramnit ranked ninth globally in 2010, 56 percent of its infections were reported from EMEA.

* [Read about Ramnit](http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99)

**The Sasfis Trojan:** Like the Ramnit virus, Sasfis made a significant impact in 2010, despite being newly discovered in this reporting period. While not nearly as striking as Ramnit, Sasfis managed to rank 15th in EMEA and 12th globally for top malicious code samples.

* [Read about the Sasfis Trojan](http://www.symantec.com/security_response/writeup.jsp?docid=2010-020210-5440-99)

**The Stuxnet worm:** Despite being developed for a very specific type of target, the number of reports of potential Stuxnet infections observed by Symantec in 2010 placed the worm at rank 29 among malicious code families. This may be a testament to the effectiveness of its ability to propagate on computers used to control system capacity in industrial sectors. The Stuxnet worm generated a significant amount of attention in 2010 because it was the first malicious code designed specifically to attack Programmable Logic Controller (PLC) industry control systems. Additionally, the worm also propagated using exploits for four zero-day vulnerabilities—a record for a piece of malicious code. Two of these were remote code execution vulnerabilities and two were local privilege escalation vulnerabilities. (Privilege escalation occurs when administrative abilities are enabled on a computer beyond what is allowed for the user.) Not only did Stuxnet exploit a number of what were, at the time, zero-day vulnerabilities, it also exploits a variety of other vulnerabilities—which indicates the extraordinary sophistication, thought, and planning that went into making this threat. This worm is important because the possibility of such an attack had been discussed in the past but never observed outside of lab environments. Notably, Stuxnet is the first malicious code family that can directly affect physical structures and proves the feasibility for malicious code to cause potentially dramatic physical destruction.

* [Learn about the Stuxnet worm](http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99)
* [Stuxnet: A Breakthrough](http://www.symantec.com/connect/blogs/stuxnet-breakthrough)
* [Wired article: Iran: Computer Malware Sabotaged Uranium Centrifuges](http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/)
* [Stuxnet Using Three Additional Zero-Day Vulnerabilities](http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities)

**EMEA Threats to Confidential Information**

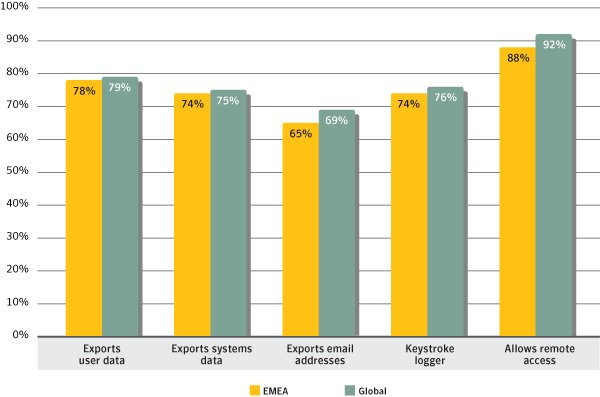
**Background**

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 backdoors, can give a remote attacker complete control over a compromised computer.  
  
Threats to confidential information are a particular concern because of their potential for use in criminal activities. Operators in the underground economy use these malicious threats to gain access to banking and credit card information, online credentials, and to target specific enterprises. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.  
  
Within the enterprise, the exposure of confidential information can lead to significant data loss. 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.

**Methodology**

This metric assesses the prominence of different types of threats to confidential information in Europe, the Middle East and Africa (EMEA) in 2010. To determine this, Symantec analysed the top 50 malicious code samples as ranked by the volume of potential infections reported during the year. Each sample is analysed for its ability to expose confidential information and these findings are then measured as a percentage of threats to confidential information.

**Data**



**Threats to confidential information, EMEA and global**  
Source: Symantec

**Commentary**

**Threats to confidential information that allow remote access:** In EMEA, malicious code that allows remote access accounted for 88 percent of threats to confidential information in 2010, up from 85 percent in 2009. Remote access has been the most prominent threat to confidential information for some time, likely because of the convenience and versatility it provides attackers. The ability to remotely access compromised computers allows attackers to perform a large variety of additional actions that need not be hardcoded in the malicious code that establishes the backdoor.  
  
**Threats to confidential information that export user data and log keystrokes:** In 2010, 78 percent of threats to confidential information exported user data, which is unchanged from 2009. The percentage of threats to confidential information that included keystroke loggers was down slightly from 75 percent in 2009 to 74 percent in 2010. Both of these threats are effective means for attackers to harvest sensitive financial information, online banking or other account credentials, and other confidential information.

**The continued growth of threats to confidential information:** As observed globally and in previous years of the Symantec *Internet Security Threat Report*, there has been increasing growth in each category of threats to confidential information—a trend that continued in this reporting period. Although global percentages were slightly higher than those for EMEA, the overall effect is nearly identical. The difference suggests that there were slightly more reports of malicious code that threaten multiple types of confidential information globally than in EMEA. The importance of these threats to the financial considerations of attackers is the primary driver behind this; the exposure of information that can be used or sold for monetary gain is an integral aspect of cybercrime that uses malicious code.

**EMEA Propagation Mechanisms**

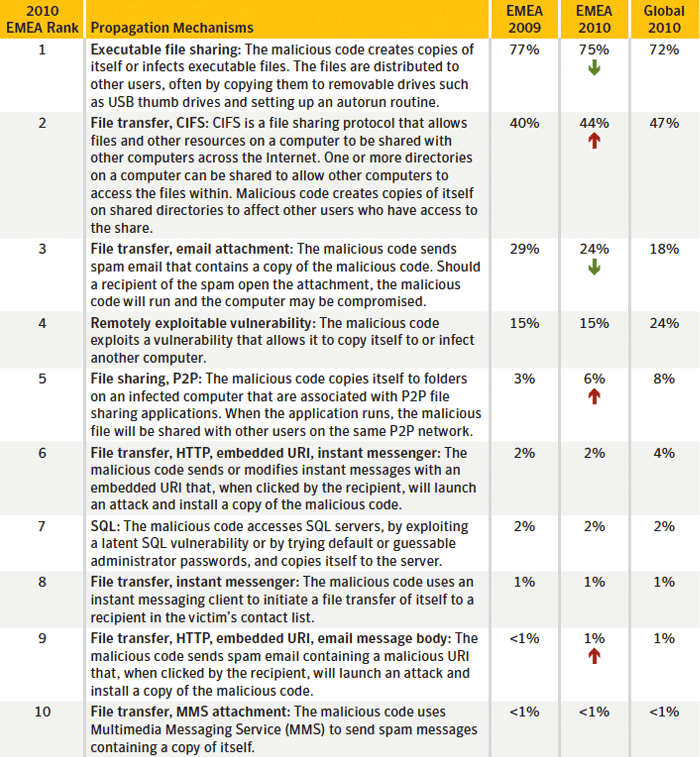
**Background**

Worms and viruses use various means to spread 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), peer-to-peer file transfers (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 backdoor server and using it to upload and install itself.

**Methodology**

This metric assesses the prominence of propagation mechanisms used by malicious code in Europe, the Middle East and Africa (EMEA) in 2010. To determine this, Symantec analyses the malicious code samples that propagate and then ranks associated propagation mechanisms according to the related volumes of potential infections observed in the region during the reporting period. Note that, because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

**Data**



**Top propagation vectors in EMEA**  
Source: Symantec

**Commentary**

**The exploitation of propagation mechanisms is relatively stable:** There were very few changes to propagation mechanism percentages in EMEA from 2009 to 2010. This suggests that attackers are seeing relatively stable success rates with the mechanisms they employ. When a propagation mechanism becomes less reliable, due to patching or other mitigations, attackers will incorporate other mechanisms and a new trend will emerge.  
  
**Executable file sharing:** In EMEA, 75 percent of malicious code propagated as executables, compared to 72 percent globally. This propagation mechanism is typically employed by viruses and some worms to infect files on removable media. The primary reason for this in 2010 was the prominence of the Ramnit virus/worm in EMEA, which also accounted for 56 percent of potential Ramnit infections globally. Several other prominent and notable malicious code samples employ this mechanism, such as the SillyFDC worm, Sality.AE virus, and the Stuxnet worm.

* [Read about the SillyFDC worm](http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99)
* [Read about Sality.AE](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99)
* [Learn more about the Stuxnet worm](http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99)

**Email attachments versus remotely exploitable vulnerabilities:** The percentages of malicious code samples that propagate through email attachments and those propagating through remotely exploitable vulnerabilities were nearly converse in EMEA and globally. Email attachments were at 24 percent in EMEA and 18 percent globally in 2010, while remotely exploitable vulnerabilities were at 18 percent in EMEA and 24 percent globally. Both Mabezat.B and Chir.B accounted for much of the malicious code samples that propagate through email attachments globally and the majority of these reports were from EMEA. However, the sources of reported prominent malicious code samples that propagate by exploiting malicious code are not as biased towards one specific region. Given the bias to EMEA for email propagation, the result is a slightly higher percentage of that mechanism in EMEA compared to all regions.

* [Learn about Mabezat.B](http://www.symantec.com/security_response/writeup.jsp?docid=2007-120113-2635-99)
* [Read about Chir.B](http://www.symantec.com/security_response/writeup.jsp?docid=2002-072920-3942-99)

**EMEA Fraud Activity Trends**

Fraud activity discusses trends in phishing and spam. Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. 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 end users to enter their 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).

* [419 – The Oldest Trick in the Book and Yet Another Scam](http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam)

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. Spam can also include URLs that often link to malicious sites that—without the user being aware of it—attack a user’s system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email gateways.

* [BBC News article: Spammers plunder Plusnet e-mail](http://news.bbc.co.uk/2/hi/technology/6676819.stm)

This section assesses phishing and spam trends that Symantec observed in the Europe, the Middle East and Africa (EMEA) region in 2010, with the following trends being analysed:

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

**EMEA Phishing URLs by Country and Top Targeted Sectors**

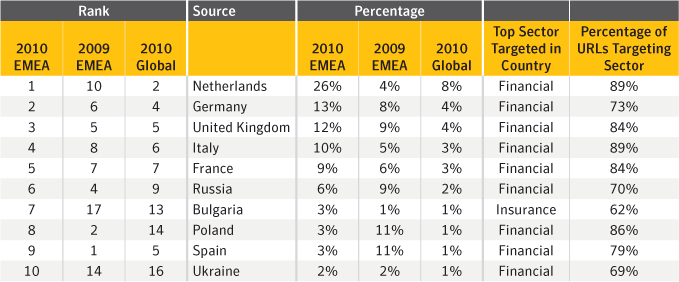
**Background**

This metric assesses the countries in the Europe, the Middle East and Africa (EMEA) region in which the most phishing URLs were hosted, as well as the sector targeted the most within each country. This data is a snapshot in time and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also 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.

**Methodology**

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 addresses. In this case, Symantec counts phishing URLs as the number of unique 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 URLs.

**Data**



**Top countries hosting phishing URLs and top targeted sectors in EMEA**  
Source: Symantec Corporation

**Commentary**

**Spam zombies lead to phishing:** The Netherlands hosted the highest percentage of phishing URLs observed in EMEA in 2010, with 26 percent of observed URLs in the region. The Netherlands was ranked second for spam zombies and third for phishing hosts in EMEA in 2010. It is likely that many of these spam zombies were used to disseminate spam that included links to phishing URLs.   
  
**Financial information most sought after in phishing URLs:** It is not surprising that the financial sector is the most spoofed by phishing URLs in nine out of the top 10 countries in this metric. Phishing URLs spoofing the financial sector attempt to steal a wide variety of information that can be used for identity theft and fraud such as names, government-issued identification numbers, credit card information, and bank account information. Cybercriminals are more focused on stealing financial information that can earn them a quick profit versus goods that require a longer time investment, such as scams.

**EMEA Countries of Botnet Spam Origin**

**Background**

This section discusses the top 10 countries of botnet spam origin in Europe, the Middle East and Africa (EMEA) in 2010. Botnets can be identified by SMTP patterns and in the structure of email headers. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis only reviews botnets involved in sending spam and does not look at botnets used for other purposes, such as for financial fraud or DoS attacks.

**Methodology**

Symantec spam honeypots collected between 30-50 million spam emails each day in 2010. These are classified according to a series of heuristic rules applied to the SMTP conversation and the email header information. Information is shared with other industry insiders to ensure data is up-to-date and accurate.

**Data**



**Top countries of botnet spam origin in EMEA**  
Source: MessageLabs Intelligence

**Commentary**

**Major spam-sending botnets are located in EMEA:** In 2010, half of all botnet spam detected by Symantec originated in the EMEA region. Within the region, Russia was the source of the most botnet spam, accounting for 14 percent of the EMEA total. Globally, Russia ranked third with 7 percent of the total. One of the main factors for this high ranking is because Russia is a large source of bot-infected computers for major spam botnets—such as Grum, Cutwail, Maazben, Ozkok (Mega-D), and Bobax—and by the end of 2010, Russia accounted for 9 percent of the global total for bot-infected computers that sent out spam. The Grum and Cutwail botnets were the second and third most active spam-sending botnets for volume of spam sent in 2010.

* [MessageLabs Intelligence: 2010 Annual Security Report](http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf)

**LAM Introduction**

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify and analyze, to deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.  
  
More than 240,000 sensors in more than 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 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.  
  
In addition, Symantec maintains one of the world’s most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 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 24,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.  
  
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; as well as other Symantec technologies. Data is collected in more than 86 countries from around the globe. Over 8 billion email messages, as well as over 1 billion Web requests are processed per day across 16 data centers. 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, analyze, 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 secure their systems effectively now and into the future.  
  
In addition to gathering global Internet attack data, Symantec also analyzes attack data that is detected by sensors deployed in specific regions. This report discusses notable aspects of malicious activity Symantec has observed in the Latin America (LAM) region for 2010.

**LAM Malicious Activity by Country**

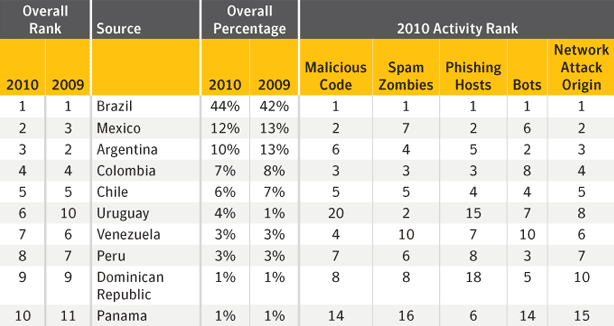
**Background**

This metric assesses the countries in the Latin America (LAM) region in which the largest amount of malicious activity takes place or originates. Malicious activity usually affects computers connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically a more stable connection. Symantec categorizes malicious activities as follows:   
  
**Malicious code:** This includes viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, or compromising the security or integrity of a victim’s computer data.  
  
**Spam zombies:** These are compromised systems that are remotely controlled and used to send large volumes of junk or unsolicited emails. These emails can be used to deliver malicious code and phishing attempts.  
  
**Phishing hosts:** A phishing host is a computer that provides website services for the purpose of attempting to illegally gather sensitive, personal and financial information while pretending that the request is from a trusted, well-known organization. These websites are designed to mimic the sites of legitimate businesses.  
  
**Bot-infected computers:** These are compromised computers that are being controlled remotely by attackers. Typically, the remote attacker controls a large number of compromised computers over a single, reliable channel in a bot network (botnet), which then is used to launch coordinated attacks.  
  
**Network attack origins:** These are originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.

**Methodology**

To determine malicious activity by country, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing hosts, bot-infected computers, and network attack origin. The proportion of each activity originating in each country is then determined within the region. 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. The rankings are then determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

**Data**



**Malicious activity by country in LAM, 2010**  
Source: Symantec Corporation

**Commentary**

**Brazil continues to have the highest percentage of malicious activity in the LAM region:** In 2010, Brazil was once again the top country for overall malicious activity in the LAM region. Globally, Brazil ranked fourth with 5 percent of the worldwide total. Brazil’s high ranking is due to it ranking first by a large margin in all malicious activities. In addition to being the country with the most broadband connections in the LAM region, the prominence of large, dominant botnets in Brazil contributes to its high rank in bot-infected computers, spam zombies, and phishing hosts. Brazil is a significant source for bot-infected computers of major botnets that send out spam emails such as Rustock, Maazben, and Ozdok (Mega-D).

* [Read about the Rustock botnet](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99)
* [Read about the Maazben botnet](http://www.symantec.com/connect/blogs/evaluating-botnet-capacity)
* [Read about the Ozdok (Mega-D) botnet](http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99)

**LAM Attack Origin by Source**

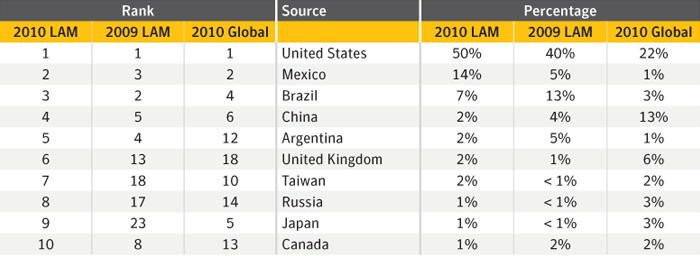
**Background**

This metric assesses the top global sources from which attacks originated that targeted the LAM region in 2010. Note that, because the attacking computer could be controlled remotely, the attacker may be in a different location than the computer being used to mount the attack. For example, an attacker physically located in the United States could launch an attack from a compromised system in Brazil against a network in Venezuela.

**Methodology**

This section measures the top originating sources of attacks that targeted computers in LAM in 2010. A network attack is generally considered any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS), intrusion prevention system (IPS), or firewall.

**Data**



**Attack origin by source**  
Source: Symantec Corporation

**Commentary**

**The United States dominates for originating attacks on LAM:** In 2010, the United States was the top originating source for attacks against LAM targets, accounting for 50 percent of all attacks detected by Symantec sensors in the region. This result is likely due to the high level of attack activity originating in the United States generally, as it was also the top source for originating network attacks globally, with 22 percent of the total worldwide. It also ranked first for overall global malicious activity, with 19 percent of that total. The United States also ranked first globally for bot-infected computers and much of the attack activity targeting the LAM region would have been conducted through these bot networks.

**LAM Bot-Infected Computers by Country**

**Background**

This metric measures the countries of origin for bot-infected computers in Latin America (LAM) for 2010. Bot-infected computers, or bots, are programs that are covertly installed on a user’s machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet relay chat (IRC), P2P, or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a 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 organization’s website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers—all of which can lead to serious financial and legal consequences.   
  
Attackers favor bot-infected computers with a decentralized command-and-control (C&C) model because they are difficult to disable and allow attackers to hide in plain site among the massive amounts of unrelated traffic occurring over the same communication channels. Most importantly, botnet operations can be lucrative for their controllers because bots are inexpensive and relatively easy to propagate. For example, Symantec observed an advertisement on an underground forum in 2010 promoting a botnet of 10,000 bots for $15 USD. (The advertisement did not stipulate whether the cost was for purchase or rental).

**Methodology**

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. A distinct bot-infected computer is a distinct computer that was active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they can be classified as actively attacking bots or bots that send out spam (i.e. spam zombies), or bots that are used for DoS campaigns..

**Data**



**Bot-infected computers by country in LAM, 2009-2010**  
Source: Symantec Corporation

**Commentary**

**Brazil continues to have more than half of the bot-infected computers in the LAM region:** Within the region, Brazil had the highest percentage of bot-infected computers, with 56 percent of the regional total. This is an increase from 2009, when Brazil also ranked first in this category with 54 percent of the regional total. Globally in 2010, Brazil ranked fifth with 8 percent of the worldwide total. One reason for this percentage of bot-infected computers in Brazil is that it is a large source of infection from botnets.   
  
**LAM is source of a relatively high percentage of bots globally:** The LAM region accounted for 15 percent of all bot-infected computers detected globally, likely driven by the high percentage of bots in Brazil. Compare that the LAM region has less than 10 percent of the world’s population and just over 10 percent of the global proportion of Internet users.

* [Read about the population of the LAM region](http://www.internetworldstats.com/stats10.htm)

**LAM Top Malicious Code Samples**

**Background**

This metric assesses the top malicious code samples in the Latin America (LAM) region in 2010. Symantec analyzes new and existing malicious code samples to determine which threats types and attack vectors are being employed in the most prevalent threats. This information also allows administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

**Methodology**

To determine top malicious code samples, Symantec ranks each malicious code sample based on the volume of unique sources of potential infections observed during the reporting period.

**Data**



**Top malicious code samples, LAM**  
Source: Symantec Corporation

**Commentary**

**The Sality.AE virus:** The top malicious code sample by volume of potential infections in LAM for 2010 was Sality.AE. Reported activity by this virus was the primary contributor to the Sality family being the highest ranked malicious code family globally in 2010. Discovered in 2008, Sality.AE has been a prominent part of the threat landscape since then, including being the top malicious code sample identified by Symantec in 2009. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Sality.AE (as well as SillyFDC and others) effective vehicles for installing additional malicious code on computers.

* [Learn more about Sality.AE](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99)
* [Read the Symantec *Global Internet Security Threat Report* 2009](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf)
* [Learn more about SillyFDC](http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99)

**The Downadup.B worm:** Downadup (a.k.a., Conficker) was initially discovered in December 2008 and garnered a significant amount of attention in 2009 because of its sophisticated attributes and effectiveness. Despite the release of a patch for the vulnerability on October 23, 2008 (i.e., before Downadup was even active), the worm was estimated still to be on more than 6 million PCs worldwide at the end of 2009. Although this number decreased during 2010, estimates are that it was still affecting between 4 and 5 million PCs by the end of the year. This worm was the top ranked malicious code sample in the region in 2009.

* [Learn about Downadup (a.k.a., Conficker)](http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99)
* [Read more about Downadup](http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker)
* [Learn more about Downadup](http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking#toc15)

**LAM Countries of Botnet Spam Origin**

**Background**

This section discusses the top countries of botnet spam origin in Latin America (LAM) in 2010. Botnets can be identified by SMTP patterns and in the structure of email headers. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis only reviews botnets involved in sending spam and does not look at botnets used for other purposes, such as for financial fraud or DoS attacks.

**Methodology**

Symantec spam honeypots collected between 30-50 million spam emails each day in 2010. These are classified according to a series of heuristic rules applied to the SMTP conversation and the email header information. A variety of internal and external IP reputation lists are also used in order to classify known botnet traffic based on the source IP address of the sender. Information is shared with other industry leaders to ensure that data is up-to-date and accurate.

**Data**



**Top sources of botnet spam, LAM**  
Source: Symantec Corporation

**Commentary**

**Brazil dominates the region for spam:** In 2010, 17 percent of all botnet spam detected worldwide by Symantec originated in the LAM region. Within the region, Brazil ranked first with 41 percent of originating spam. The high rate of spam from botnets originating in Brazil likely correlates to the high percentage of spam zombies located there, as Brazil ranked first for spam zombies both in the LAM region and, more significantly, globally in 2010. The prominence of large, dominant botnets in Brazil contributes to the high ranking in botnet spam. Brazil is a strong source of bot-infected computers to major botnets that send out spam emails, such as Rustock, Maazben, and Ozdok (Mega-D). Rustock was responsible for almost half of the global botnet spam sent at the end of 2010.

* [Read about Rusktock](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99)
* [Learn more about Maazben](http://www.symantec.com/connect/blogs/evaluating-botnet-capacity)
* [Read about Ozdok (Mega-D)](http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99)

**Enterprise Best Practices**

**Employ defense-in-depth strategies.** Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.  
  
**Monitor for network threat, vulnerabilities and brand abuse:**

* Monitor for network intrusions, propagation attempts, and other suspicious traffic patterns;
* Monitor for attempted connections to known malicious or suspicious hosts;
* Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation;
* Monitor brand abuse via domain alerting and fictitious site reporting.

**Antivirus on endpoints is not enough:** On endpoints (desktops/laptops), signature-based antivirus alone is not enough to protect against today’s threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

* Endpoint intrusion prevention that protects against unpatched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from ever making it onto endpoints;
* Browser protection for protection against obfuscated Web-based attacks;
* Heuristic file-based malware prevention to provide more intelligent protection against unknown threats;
* File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
* Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
* Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
* Device control settings that prevent and limit the types of USB devices to be used.

**Review software default settings:** Do not use the default settings on your endpoint security solutions. Work with your security provider or partner to ensure you have the most optimized settings. Where practical, use the enhanced security settings in common applications (e.g., document reader applications and browser plug-ins) to limit the use of unneeded features (e.g., disabling unneeded scripting capabilities).  
  
**Use encryption to protect sensitive data:** Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.  
  
**Use Data Loss Prevention to help prevent data breaches:** Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or websites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.   
  
**Implement a removable media policy:** Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.  
  
**Update your security content frequently and rapidly:** With more than 286M variants of malware detected by Symantec in 2010, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.  
  
**Be aggressive on your updating and patching:** Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors’ automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.  
  
**Investigate and use different security solutions for servers:** Securing mission-critical and single-purpose servers requires a different set of tools than for endpoints. Lightweight and robust protection solutions exist that can better secure a server. Turn off and remove unneeded services.   
  
**Turn off Autorun:** Malware such as Downadup and Stuxnet propagate from USB drives and network shares, spreading automatically using Autorun capabilities.

**Enforce an effective password policy.**

**Test security to ensure that adequate controls are in place:** If possible, employ vulnerability assessment services, a vulnerability management solution, and vulnerability assessment tools to evaluate the security posture of the enterprise.   
  
**Maintain a secure enterprise software profile:** Deploy only certified, up-to-date applications. In particular, audit Web applications for security prior to deployment. Certain applications may pose a greater security risk than others, including file-sharing programs, free downloads, and freeware and shareware versions of software. Avoid deploying unsupported products.  
  
**Be wary of unnecessarily broad user entitlements:** Limit privileges on systems for users who do not require such access and, on those systems where they do have access, ensure the entitlements match their business needs.  
  
**Restrict email attachments:** 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. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.

**Maintain an ongoing blacklist of malicious domains.**

**Take action on strong authentication to reduce the incidence of online identity theft, phishing attacks and other online fraud:** Attack technology has become too powerful to continue with passwords as the basis for account protection. Strong authentication mitigates this long-standing and often-exploited vulnerability by offering a significantly higher level of identity assurance.  
  
**Expand strong authentication from selective use to standardized practice:** Strong authentication is becoming a basic requirement for notions of due care for access to sensitive data and critical business applications. Enterprises should look to incorporate the widespread adoption of strong authentication into their security strategic planning.  
  
**Ensure that you have infection and incident response procedures in place:**

* Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
* Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
* Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
* Isolate infected computers to prevent the risk of further infection within the organization;
* If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
* Perform a forensic analysis on any infected computers and restore those using trusted media.

**Educate users on the changed threat landscape:**

* Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
* Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
* Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
* Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;
* Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
* Deploy Web browser URL reputation plug-in solutions that display the reputation of websites from searches;
* Only download software (if allowed) from corporate shares or directly from the vendors website;
* If users see a warning indicating that they are “infected” after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.

**Information security and compliance best practices**

**Actively manage and monitor IT Policy:**  
Develop, track changes and maintain IT management policy for:

* Regulatory and legal requirements;
* Monitoring and reporting;
* Maximum acceptable risk;
* Minimum acceptable service levels;
* Acceptable use standards;
* Actions for policy violations.

**Implement, track changes and maintain IT security operations policy for:**

* Employees, contractors, and third parties;
* IT security standards;
* Security controls for IT assets;
* Operations controls for IT assets;
* Monitoring and reports on IT assets;
* Access to information/IT assets;
* Acquisition, use, disposition of IT assets;
* Application development and production;
* Information handling standards;
* Incident response/management;
* Change management.

**Implement technical security and compliance controls:**

* Maintain an inventory of IT assets and configurations in a central location;
* Maintain an inventory of authorized users;
* Maintain an inventory of sensitive information;
* Monitor audit trails and settings on IT assets;
* Gather evidence about IT configurations and technical controls;
* Identify technical gaps for remediation and testing;
* Identify and remove orphaned user accounts and software services;
* Test IT assets, configurations and software services;
* Document changes to technical controls;
* Map technical controls to IT policies, legal and regulatory requirements;
* Define and maintain the roles and responsibilities of policy owners;
* Map regulatory mandates and legal statutes to information security policies;
* Document and report on conformance with policy.

**Implement security and compliance controls for procedures:**

* Implement segregation of duties to manage risk;
* Conduct background checks on employees;
* Deliver training to users about ethics, compliance, and IT policy;
* Survey employees on practices and procedures;
* Conduct penetration testing (social engineering) of procedural and operational controls;
* Identify gaps, remediate and document procedural controls.

**Protect critical IT assets:**

* Protect and harden critical IT assets;
* Monitor audit trails and settings;
* Automatically detect or prevent unauthorized access to IT assets;
* Conduct vulnerability scanning and penetration testing of IT assets;
* Patch and document vulnerabilities.

**Consumer Best Practices**

**Protect yourself:** Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

* Antivirus (file and heuristic based);
* Bidirectional firewall;
* Intrusion prevention to protect against Web-attack toolkits, unpatched vulnerabilities, and social-engineering attacks;
* Browser protection to protect against Web-based attacks;
* Reputation-based tools that check the reputation and trust of a file and website before downloading;
* Behavioral prevention that keeps malicious threats from executing even if they get onto your computer;
* URL reputation and safety ratings for websites found through online searches.

**Keep up to date:**

* Keep virus definitions and security content updated hourly, if possible. By keeping your virus definitions up to date, you can protect your computer against the latest viruses and malicious software (“malware”).
* Whenever possible, use the automated updating capability of your programs to keep your operating system, Web browsers, browser plug-ins, and applications current with the latest updated versions. Running out-of-date versions can put you at risk of being exploited by Web-based attacks.

**Know what you are doing:**

* Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically downloaded on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
* Downloading “free,” “cracked,” or “pirated” versions of software can also contain malware or social engineering attacks. This includes malware that tries to trick you into thinking your computer is infected and getting you to pay money to have it removed.
* Be careful which websites you visit. While malware can still come from mainstream websites, less reputable sites sharing pornography, gambling and stolen software often have a higher percentage of malware infections.
* Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them. Some security risks can be installed after you have accepted the EULA, or because of that acceptance.

**Use 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, since these are easier for cybercriminals to hack.
* Do not use the same password for multiple applications or websites.
* Use complex passwords (upper/lowercase, punctuation and symbols) or passphrases. (E.g., “I want to go to Paris for my birthday” becomes, “I1t2g2P4mb”)
* Consider using a “password vault” that can help you keep track of all your passwords. These tools allow you to have more complex passwords without having to remember them all, plus they protect you from threats that record your keystrokes. You can even use these tools to help you to automatically create a strong password.

**Think before you click:**

* Never view, open, or execute any email attachment unless you expect it and trust the sender. Even if it is coming from trusted users, be suspicious.
* A favorite tactic of malware authors is to try to trick you into clicking their infected links. Be cautious when clicking on URLs in emails, instant messages, and social media programs even when coming from trusted sources and friends. Remember that the attackers who have compromised a friend’s account may have lots of information about you too.
* Do not click on shortened URLs without expanding them first using “preview” tools or plug-ins to see where they actually lead.
* Do not click on links in social media applications with catchy titles or phrases - even from friends. If you do click on the URL, you may end up “liking it” and sending it to all of your friends – just by clicking anywhere on the page. Close or quit your browser instead.
* When searching for things online, use security software that shows the reputation and safety rating of websites in your search results.
* Be suspicious of search results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
* Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor’s website.

**Guard your personal data:**

* Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested by cybercriminals and used in targeted attacks, phishing scams, or other malicious activities.
* Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
* Review your bank, credit card, and credit information frequently for irregular activity, including small discrepancies. Cybercriminals will often steal a little bit of money over a long period of time instead of just wiping out your bank account all at once.
* Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
* Use only secured connections (HTTPS) when connecting via Wi-Fi networks to your email, social media and sharing websites. Check the settings and preferences of the applications and websites you are using to make sure that they are not exposing your sensitive information.
* Consider using software that protects all your Internet traffic when you are connected to a public hotspot. These “personal VPNs” will protect you from attackers who are trying to steal your email or social media information when you connect.