SYMANTEC ENTERPRISE SECURITY

Symantec™

Confidence in a connected world.

Symantec Internet Security Threat Report

Trends for 2010

Volume 16, Published April 2011

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. 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, Norton™ consumer products, and 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.

Marc Fossi
Executive Editor
Manager, Development
Security Technology and Response

Gerry Egan
Director, Product Management
Security Technology and Response

Kevin Haley
Director, Product Management
Security Technology and Response

Eric Johnson
Editor
Security Technology and Response

Trevor Mack
Associate Editor
Security Technology and Response

Téo Adams
Threat Analyst
Security Technology and Response

Joseph Blackbird
Threat Analyst
Security Technology and Response

Mo King Low
Threat Analyst
Security Technology and Response

Debbie Mazurek
Threat Analyst
Security Technology and Response

David McKinney
Threat Analyst
Security Technology and Response

Paul Wood
MessageLabs Intelligence Senior Analyst
Symantec.cloud

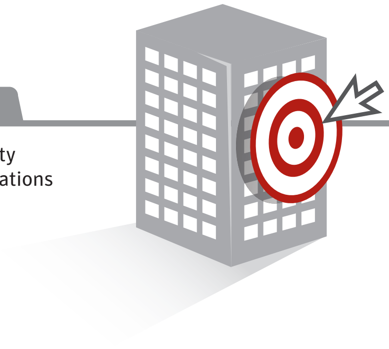
Spam and phishing data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; MessageLabs™ Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; as well as other Symantec technologies. 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.

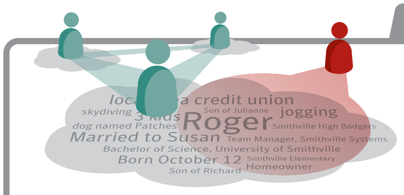
2010 in Review

Targeted Attacks continue to evolve

Targeted attacks, while not new, gained notoriety from high-profile attacks against major organizations (Hydraq) and significant targets (Stuxnet).



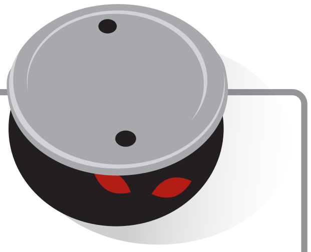
Social Networking + social engineering = compromise

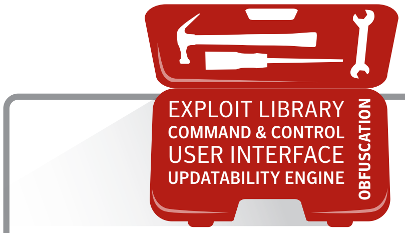


The ability to research a target online has enabled hackers to create powerful social engineering attacks that easily fool even sophisticated users.

Hide and Seek (zero-day vulnerabilities and rootkits)

Targeted attacks depend on their ability to get inside an organization and stay hidden in plain site. Zero-day vulnerabilities and rootkits have made this possible.



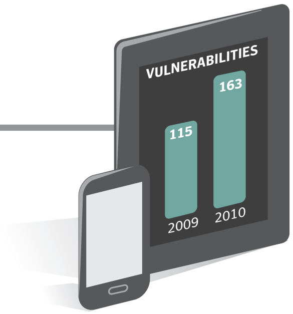


Attack Kits get a caffeine boost

Innovations from targeted attacks will make their way into massive attacks, most likely via toolkits.

Mobile Threats increase

All these types of attacks are moving to mobile devices, limited only by attackers getting a return on their investment.



Source: Symantec Corporation

Executive summary

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 cybersabotage 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. To access the supplemental analysis and best practices, please visit the Symantec *Internet Security Threat Report* online.

The Year in Numbers

Some of the more noteworthy statistics that represent the security landscape in 2010

286M+

Threats

Polymorphism and new delivery mechanisms such as Web-attack toolkits continued to drive up the number of malware variants in common circulation. In 2010, Symantec encountered more than 286 million unique variants of malware.

93%

Increase in Web Attacks

A growing proliferation of Web-attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to be playing a role here too. During a three-month observation period in 2010, 65% of the malicious URLs observed on social networks were shortened URLs.

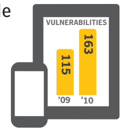
260,000

Identities Exposed per Breach

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.

42%

More Mobile Vulnerabilities

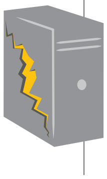


In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals, there was a sharp rise in the number of reported new mobile operating system vulnerabilities—up to 163 from 115 in 2009.

6,253

New Vulnerabilities

Symantec recorded more vulnerabilities in 2010 than in any previous year since starting this report. Furthermore, the new vendors affected by a vulnerability rose to 1,914, a 161% increase over the prior year.



14

New Zero-Day Vulnerabilities

The 14 zero-day vulnerabilities in 2010 were found in widely used applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player. Industrial Control System software was also exploited. In a sign of its sophistication, Stuxnet alone used four different zero-days.

74%

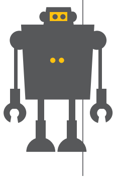
Pharmaceutical Spam

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.

1M+

Bots

Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control. Grum and Cutwail followed, each with many hundreds of thousands of bots.



$15

per 10,000 Bots

Symantec observed an underground economy advertisement in 2010 promoting 10,000 bots for $15. Bots are typically used for spam or rogueware campaigns, but are increasingly also used for Distributed Denial of Service attacks.

$0.07 to $100

per Credit Card

This was the range of prices seen advertised in the underground economy for each “stolen” credit card number, and, as in the real economy, bulk buying usually gets the buyer a significant discount.

Source: Symantec Corporation

Note: All currency in USD

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.

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.

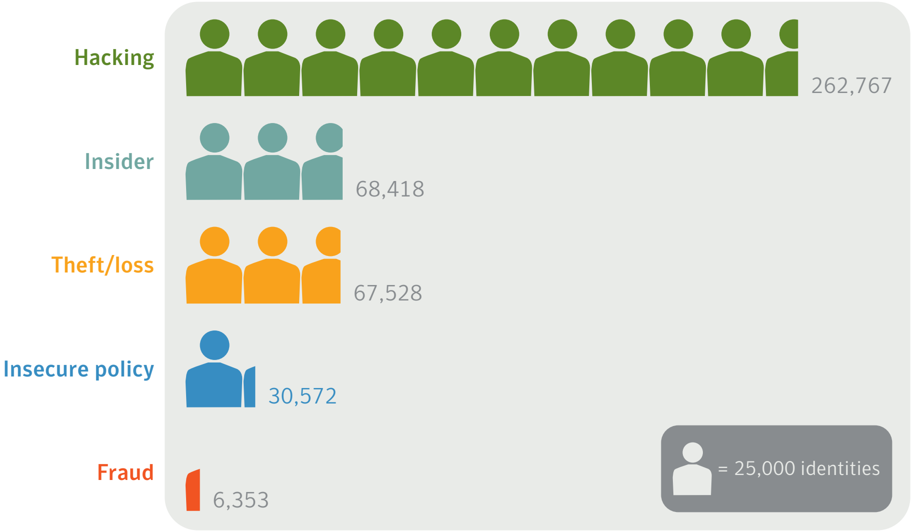
Rank	Propagation Mechanisms	2010%	2009%
1	**Executable file sharing.** The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	74% ↑	72%
2	**File transfer, CIFS.** CIFS is a file-sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within. Malicious code creates copies of itself on shared directories to affect other users who have access to the share.	47% ↑	42%
3	**Remotely exploitable vulnerability.** The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	24%	24%
4	**File transfer, email attachment.** The malicious code sends spam email that contains a copy of the malicious code. Should a recipient of the spam open the attachment, the malicious code will run and the recipient's computer may be compromised.	18% ↓	25%
5	**File sharing, P2P.** The malicious code copies itself to folders on an infected computer that are associated with P2P file-sharing applications. When the application runs, the malicious file will be shared with other users on the same P2P network.	8% ↑	5%
6	**File transfer, HTTP, embedded URI, instant messenger.** The malicious code sends or modifies instant messages with an embedded URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	4% ↓	5%
7	**File transfer, instant messenger.** The malicious code uses an instant messaging client to initiate a file transfer of itself to a recipient in the victim's contact list.	2% ↑	1%
8	**SQL** The malicious code accesses SQL servers, by exploiting a latent SQL vulnerability or by trying default or guessable administrator passwords, and copies itself to the server.	1% ↓	2%
9	**File transfer, HTTP, embedded URI, email message body.** The malicious code sends spam email containing a malicious URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	< 1%	< 1%
10	**File transfer, MMS attachment.** The malicious code uses Multimedia Messaging Service (MMS) to send spam messages containing a copy of itself.	< 1%	< 1%

Propagation mechanisms in 2010
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 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. 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 the messages seem legitimate. This tactic is commonly called spear phishing.

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, 2010
Source: Based on data provided by OSF DataLoss DB

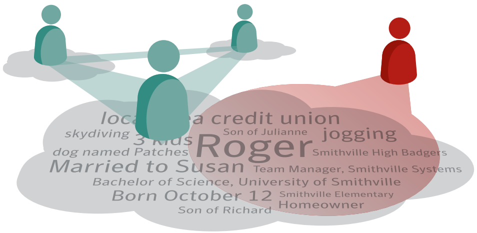
While much of the attention focused on targeted attacks is fueled by the sophisticated methods attackers use to breach their targets, the analysis often overlooks prevention and mitigation. In many cases, implementing best practices, sufficient policies, and a program of user education can prevent or expose a targeted attack. For example, restricting the use 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.

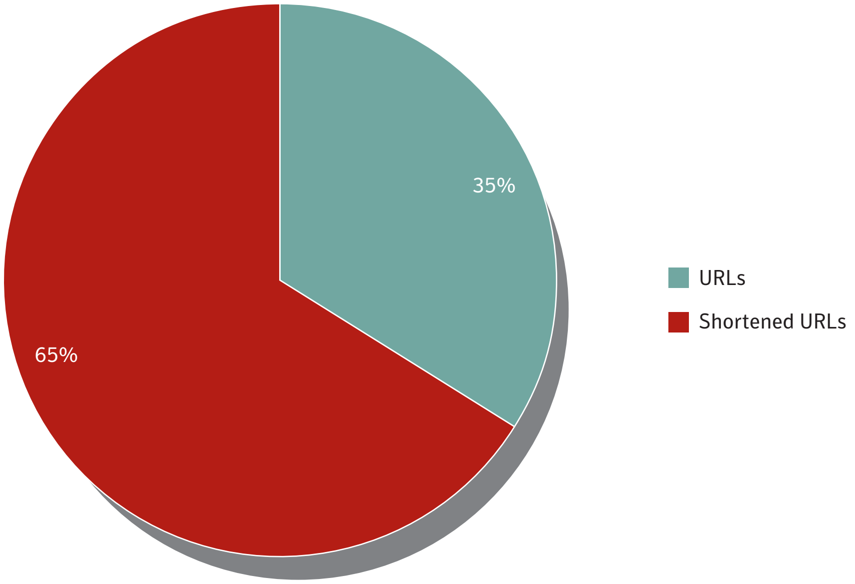
Attackers exploit the profile information available on social networking sites to mount targeted attacks. For example, many people list employment details in their profiles, such as the company they work for, the department they work in, other colleagues with profiles, and so on. While this information 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 and 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.

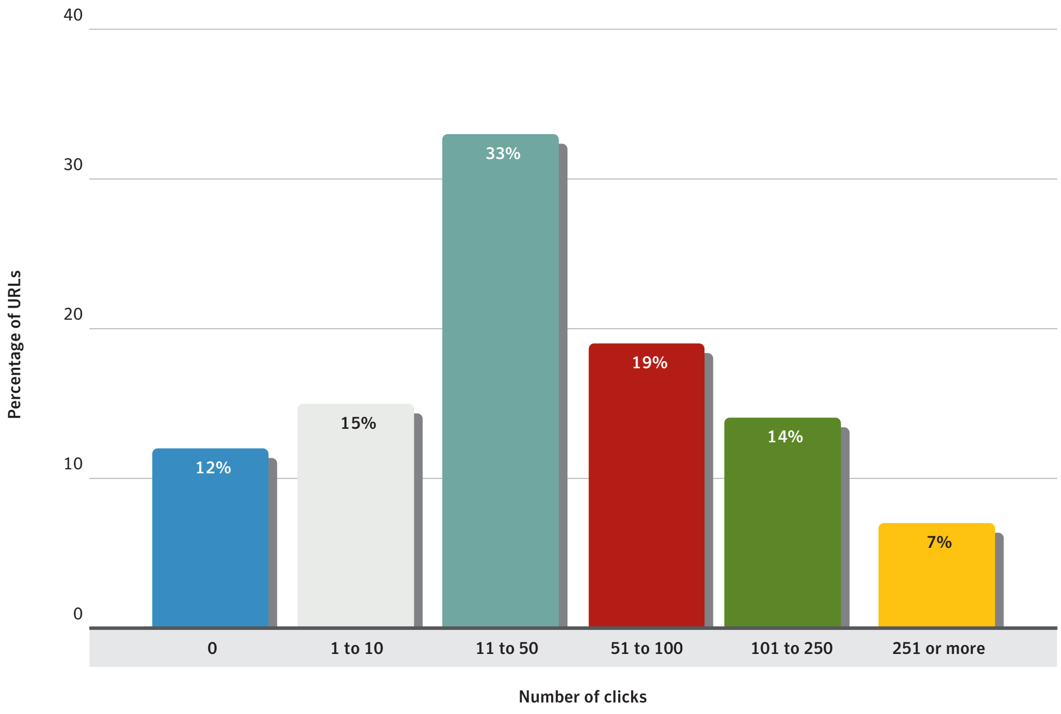
A favorite method used to distribute an attack from a compromised profile is to post links to malicious websites from that profile so that the links appear in the news feeds of the victim's friends. In addition, attackers are increasingly using shortened URLs for this because the actual destination of 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 over a three-month period in 2010
Source: Symantec Corporation

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.

[1] URL shortening services allow people to submit a URL and receive a specially coded shortened URL that redirects to the submitted URL.

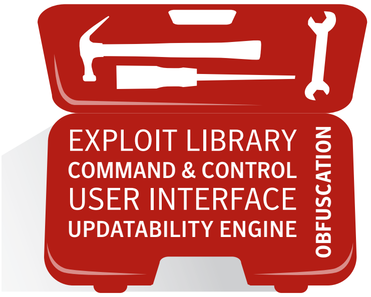


Clicks per malicious shortened URL during three-month period in 2010
Source: Symantec Corporation

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.

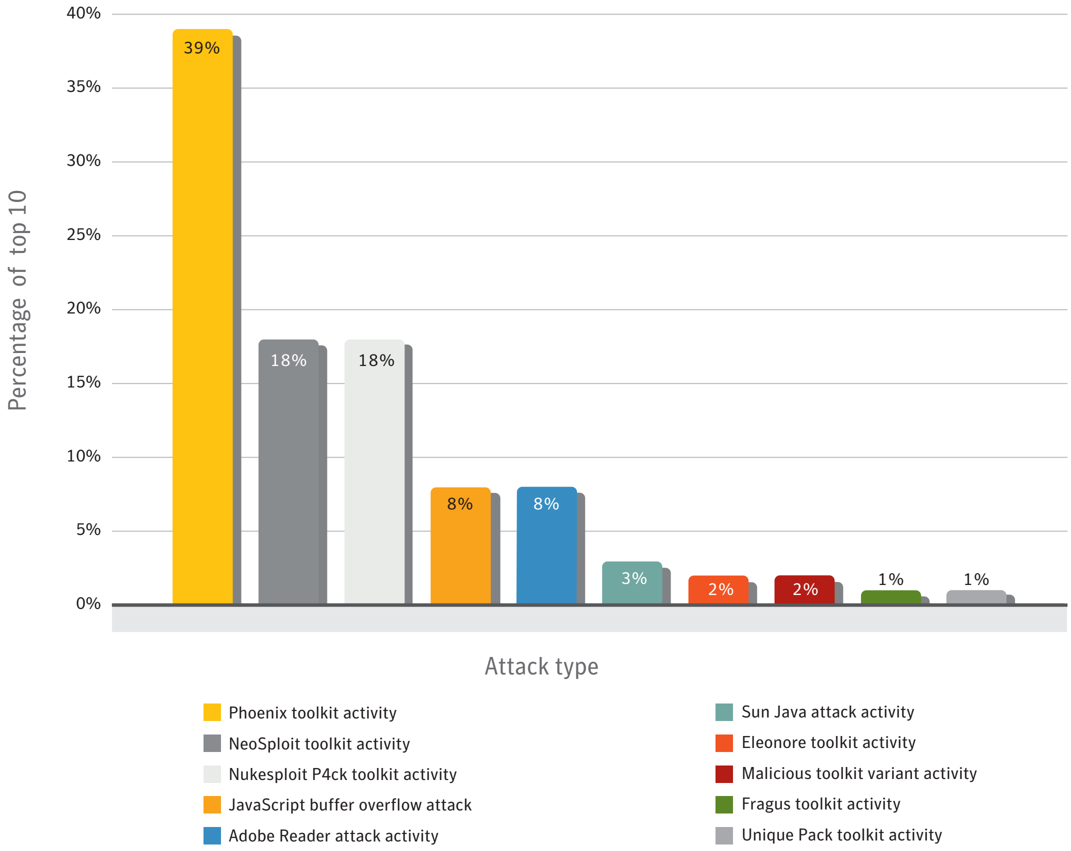
As more people join social networking sites and the sophistication of these sites grows, it is likely that increasingly complex attacks will be perpetrated through them. Users should ensure that they monitor the security settings of their profiles on these sites as often as possible, especially because 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



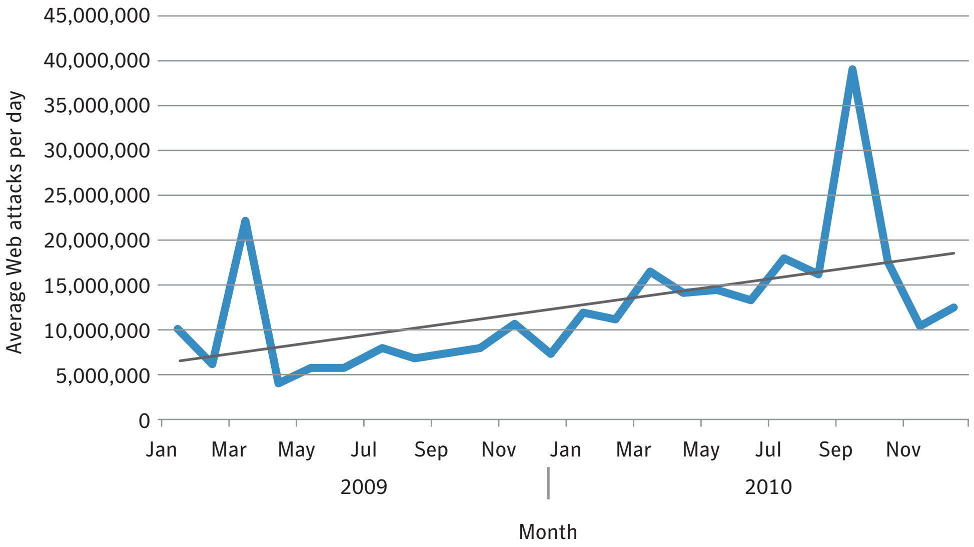
While targeted attacks are focused on compromising specific organizations or individuals, attack toolkits are the opposite side of the coin, using broadcast, blanket attacks that attempt to exploit anyone unfortunate enough to visit a compromised website. The previous edition of the Symantec *Internet 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.



Web-based attack activity, 2010
Source: Symantec Corporation

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-based attacks per day, by month, 2009–2010
Source: Symantec Corporation

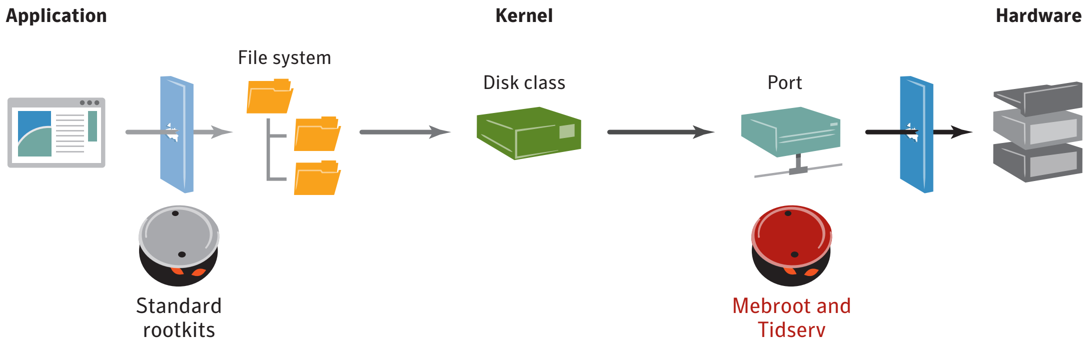
Because users are more likely to be protected against older vulnerabilities, attack toolkit developers advertise their toolkits based on the rate of success of the vulnerabilities that are included and the newness of the exploits. To remain competitive and successful, attack kit developers must update their toolkits to exploit new vulnerabilities as they emerge on the threat landscape. Thus, the kit developers must 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. 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 allow 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 canceling 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.

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.



Tidserv and Mebroot infection process
Source: Symantec Corporation

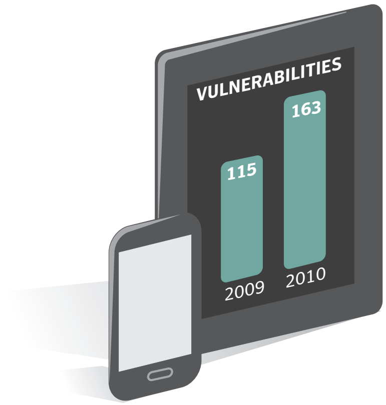
Many Tidserv infections were discovered by chance in February 2010 when they were uncovered by a patch issued by Microsoft® for an unrelated security issue in Windows. The malicious code made some changes to the Windows kernel that caused infected computers to "blue screen" every time they rebooted after 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 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.

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 being used. 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 be incorporated into targeted attacks.

Mobile threats

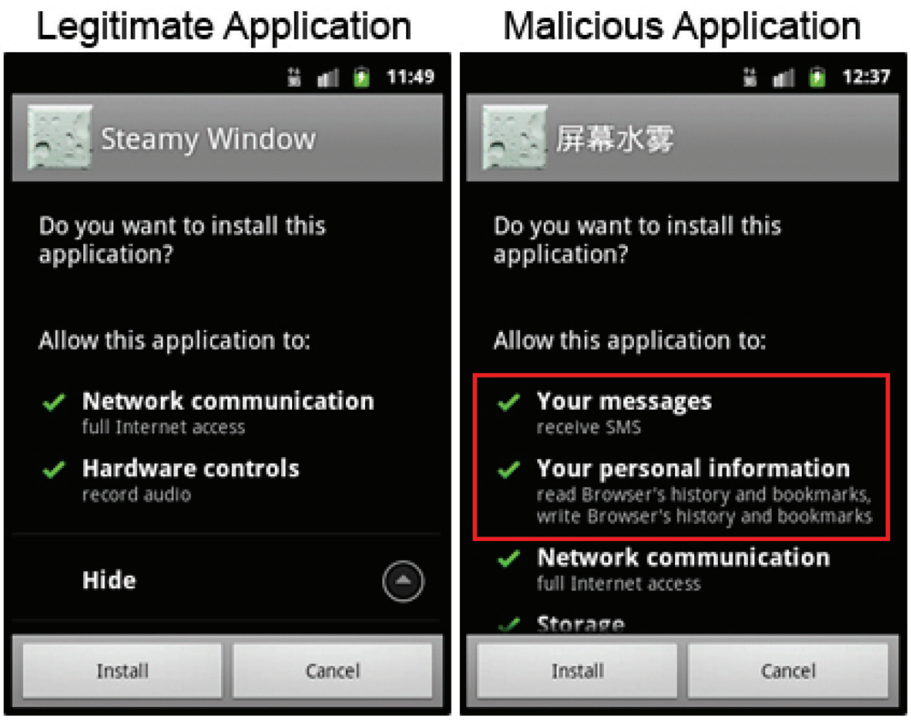


Since the first smartphone arrived in the hands of consumers, speculation about threats targeting these devices has abounded. While threats targeted early "smart" devices such as Symbian and Palm in the past, none of these threats ever became widespread and many remained proof-of-concept. Recently, with 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.

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 have also taken a popular legitimate application and added 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 permissions than should have been necessary.



Do you want to install this application?

Allow this application to:

✓ Network communication
full Internet access

✓ Hardware controls
record audio

Do you want to install this application?

Allow this application to:

✓ Your messages
receive SMS

✓ Your personal information
read Browser's history and bookmarks, write Browser's history and bookmarks

✓ Network communication
full Internet access

✓ Storage

Pjapps installation screen
Source: Symantec Corporation

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 these devices as a platform for cybercrime.

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 likely continue to use tried and true methods.

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, with the largest breach costing one organization $35.3 million to resolve. With stakes so high, organizations need to focus their security efforts to prevent breaches.

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, and 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 in 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.

2010 Timeline

A look back at some of the more newsworthy security-related events that took place in 2010

January

1 Trojan.Hydraq

News breaks of a high-profile targeted threat affecting multinational corporations around the globe.

27 iPad Announced

A whole new computing platform launches, marking yet another seismic shift in computing platforms. Hackers immediately launch SEO poisoning campaigns to leverage the worldwide interest.

February

15 SpyEye vs. ZeuS—Cybercriminal Toolkit Rivalry

ZeuS, king of the kits, is usurped by a new clone called SpyEye.

March

1 Chile Earthquake

Spammers leverage the Chilean earthquake for spam campaigns.

April

No notable events

May

No notable events

June

11 FIFA World Cup

Yet more fodder for spam and SEO poisoning.

17 Stuxnet

The first reports of a new threat leveraging a zero-day vulnerability. This threat would go on to become one of the biggest malware events of the year.

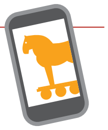
July

No notable events

August

18 First Android Trojan Discovered

AndroidOS.Tapsnake: Watching your every move.



September

9 Imsolk.B

In a remembrance of things past, an email worm called Imsolk.B—a.k.a. “Here you Have”—erupts to take the world by storm, spreading rapidly in a matter of hours.

29 Major ZeuS Bust

In a victory against cybercrime, UK police arrest 19 individuals believed to be part of an organized cybercrime network that used the ZeuS Trojan to steal $9.5 million from bank accounts there.

October

25 Trojan.Jnanabot

In perhaps a sign of things to come, researchers discover a Trojan that leverages Java to get on many different platforms, including Windows, OS X, and Linux.

November

No notable events

December

1 WikiLeaks and “Hacktivism”

The events highlight the new security issues of our age: protecting sensitive information and defending against hacktivism attacks.

Source: Symantec Corporation

NO WARRANTY. Symantec makes this document available AS-IS, and makes no warranty as to its accuracy or use. The information contained in this document may include inaccuracies or typographical errors and may not reflect the most current developments, and Symantec does not represent, warrant, or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Symantec reserves the right to make changes at any time without prior notice.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

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