White Paper

# CA 2007 Internet Threat Outlook

CA Security Advisor Team

January 2007

## A New Horizon in Cyber-Crime

According to urban legend, the notorious Willie Sutton once said when asked why he robbed banks: “Because that’s where the money is.”

Today, the money is online — in banks, at credit-card processors, in corporate web-based applications, and of course in your computers at home. Tomorrow, the money will be on smart phones, in MP3 players, search engines, and social networks. And the criminals will follow the money.

We’ve reached a new horizon in cyber-crime. Long gone are the days of teenage hackers seeking fame by causing widespread Internet outages or defacing well-known websites. Viruses, trojans, worms, spam, spyware — and panoply of other Internet-borne ills — are how cyber-criminals steal intellectual property, personal identities, the contents of bank accounts, and much more. Malware has become the tool of corporate espionage and cyber-terrorism.

The stakes have never been higher. More than 100 million records of United States residents have been exposed due to security breaches since February 2005, according to the Privacy Rights Clearinghouse. According to the research firm Gartner, 3.5 million Americans gave sensitive information to phishers in 2006, which was almost double the 2005 figure. The average cost was $1,244, compared with just $256 in 2005. Total U.S. financial losses exceeded $2.8 billion.

A growing number of regulations mandate the protection of personally identifiable information. If a business fails to comply with these laws, it can be subject to significant penalties, including fines and jail time for corporate executives. The lasting damage to the company’s reputation cannot be understated: Customers will certainly think twice about buying from a company that doesn’t bother to protect their private information. What’s potentially even more damaging is that cyber-attacks are used for corporate espionage and to steal military secrets. A company that experiences a loss of its intellectual property, be it engineering drawings, source code, or even marketing plans, can find itself out of business.

At the same time, the threats have become highly sophisticated. The criminals are organized. They operate in the underground and across international borders, making them difficult to stop and prosecute. They use state-of-the-art professional development techniques and constantly evolve their tactics to avoid detection by the security community. They send their malicious software through multiple distribution channels, including e-mail, peer-to-peer networks, and instant messaging. They take advantage of unpatched or newly discovered software vulnerabilities so that users don’t actually have to do anything — not open an attachment, not click on a link — for their computers to be compromised.

As criminals have followed the money online, they’ve become highly sophisticated and organized in their efforts to steal, commit fraud, extort and more.

The purpose of this report is to provide awareness of cyber-security trends as observed by the CA Security Advisor team. The analysis in this report is based on incident information that has been observed by the CA Security Advisor Team, submitted by CA customers and public sector information. This report also provides

information on key security topics, including malware trends and emerging threats.

## Trends in Malware

2006 was a year for cross-over. The dividing lines among trojans, worms, and viruses have blurred. Trojans — malicious software unable to spread of their own accord — have replaced worms as the most prolific and widespread from of malware.

- **Trojans dominate.** Trojans are now the dominant form of malicious application. In 2006, 62 percent of new types of malware were trojans, while worms accounted for 24 percent of new malware. The flexibility of trojans, coupled with a broad range of distribution channels enabled by the Internet, has made them the cyber-weapon of choice by attackers. Trojans may be just one step in multi-component attack which culminates in a compromised machine, stolen data, fraud — or worse.

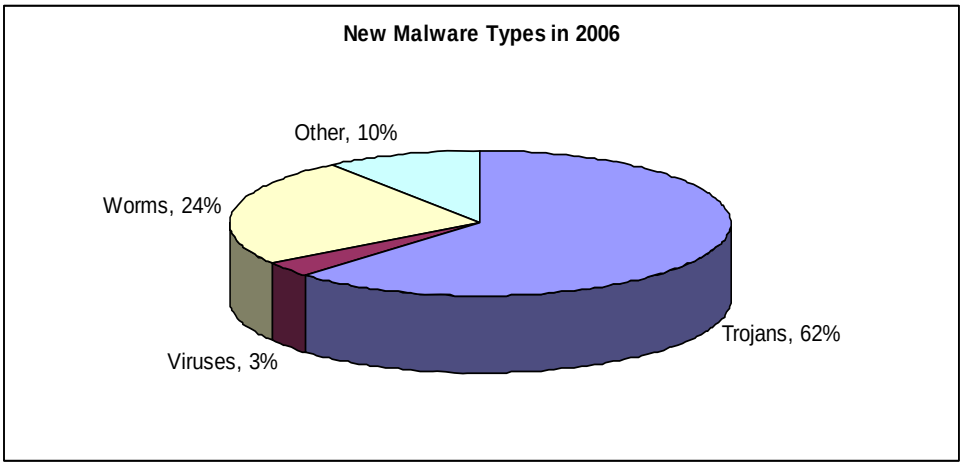


**Figure 1: In 2006, most of the new malware activity surrounded the development of trojans. More than 60 percent of new malware were trojans. Worms accounted for 24 percent of new malware detected.**

If a user downloads a program from a chat room, a freeware site, or even from an unsolicited e-mail, the program is likely to contain malware, and that malware is most likely to be a trojan. The payload of a trojan may unleash a wide variety of ills on unprotected computers. Users may not become aware that their computers have a trojan until they run some form of an anti-spyware program.

- **Many new channels of distribution.** Trojans are unable to spread on their own, but they take advantage of the wide variety of distribution channels available on the Internet. The number of distribution channels continues to grow in new and challenging ways. Spam is the primary channel to distribute malware, but peer-to-peer file sharing networks, instant messaging, and network shares are commonly used. Malware can also be dropped or downloaded by other malware. Malicious web pages can exploit vulnerabilities. Malicious programs can masquerade as useful or enticing programs, thereby tricking users into compromising their computers.

- **Multi-component malware.** Malicious attackers use increasingly sophisticated techniques, including creating multi-component malware. Once multi-component malware hits a computer, that computer becomes vulnerable to any number of infections.

Multi-component malware is appealing to malicious attackers for several reasons. It leverages the inherent flexibility that comes with having several distinct yet cooperative components, which allows attackers to gain control of a wide distribution of machines. It's also a survival tactic, because it allows malware to live longer and survive some level of detection. Although having multiple components means more

visibility to the security community, it also means that if one component is detected by anti-virus software, the other components may continue to function. Ultimately, multi-component malware allows the author greater control, so he or she can update and replace components, changing functionality or replacing components that have become non-functional. Multi-component malware is also highly configurable. It tends to rely on backdoor functionality and is driven by information contained on host servers on the Internet, so the authors retains control over specific instructions about where and what to download.

The Lufoure family is an example of the complex interoperability seen in multi-component malware. Lufoure usually arrives on a computer via spam that attempts to distribute a downloader or by exploiting browser vulnerabilities. From this point, the affected system is vulnerable to infection by malware that's associated with the Lufoure family. The behavior is highly configurable, but it is often used to steal private information.

- **Anti-detection and removal techniques.** Attackers are using more advanced anti-detection and removal mechanisms, such as polymorphism, packers, cryptors, and rootkits.
  - ***Polymorphism*** has been used with viruses and even some worms for a decade, but the use of polymorphism as an anti-detection technique became widespread in 2006. In this technique, a malicious encrypted application mutates its decryptor on each replication, so it can take a different form that will presumably evade detection.

    Recently, the disseminators of malware have used polymorphism to produce different generations of malware on remote sites, from where they are inadvertently downloaded by victims. The result is thousands of functionally identical versions of the application, which otherwise look very difficult and may pose a problem for some types of detection techniques. Some of these malicious applications may produce new generations every few hours or even every few minutes. Some produce new generations upon each and every download.

    Two new (and widespread) families of malware featured polymorphism — Win32/Stration and Win32/Polip. Stration, which first appeared in fall 2006, uses the server-side polymorphism which we just described. Stration is a family of multi-component, mass-mailing worms. Some Stration variants send spam. They usually contact a particular domain and download a file that contains a list of URLs. This list includes the location of the e-mail to be downloaded and sent out by the worm, as well as the location of the files that contain the lists of e-mail recipients. Stration downloads these files and after a certain period of time begins sending out e-mail.

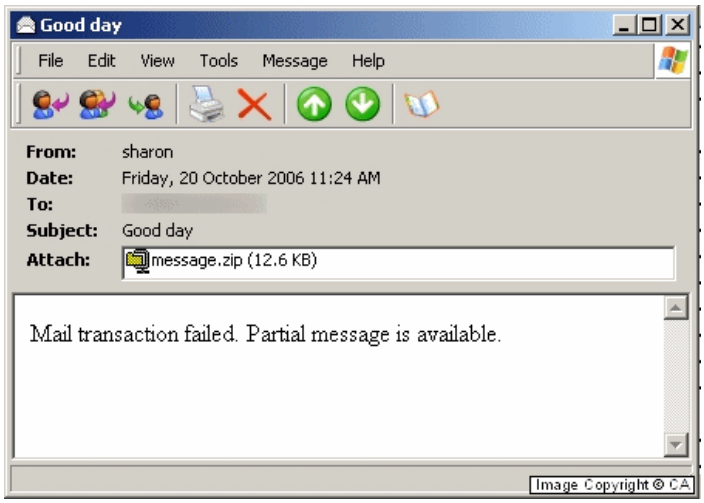


**Figure 2: Stration is a new family of worms that uses polymorphism to evade detection. It can disguise itself as a "mail failure" e-mail that even an experienced user might open. Some variants of Stration are responsible for the explosion of image-based spam in late 2006.**

In fact, Stration can be blamed for contributing to the explosion of image-based spam in the fall of 2006.

Win32/Polip was also new in 2006. Polip is a polymorphic, entry-point obfuscating virus that infects Windows executable files. Unlike Stration, it uses the more traditional approach and mutates its code on each replication. Polip searches for and infects files in the Program Files directory, and then stays resident and infects certain files, such as Windows console and GUI applications that have the extension .exe or .scr. It may also spread via the Gnutella file sharing network.

– Malware authors continue to use ***packers and cryptors*** to evade detection. Run-time executable packers are legitimately used to compress a program's code or data so it takes up less space on the hard drive and load faster. But packers and cryptors can be used for nefarious purposes. A side effect is that the program's contents and structure are no longer recognizable. For an anti-virus scanner to detect a packed program, it must unpack it or contain a separate signature in its database for the program's packed state. Run-time cryptors work in a similar fashion, but they encrypt (or more commonly encrypt and compress) a program's content to obfuscate it We saw a large increase in the number of different packers and cryptors being used for malicious intent and the complexity of these programs have also risen.

– Another troublesome trend is the increased use of ***rootkits***. A rootkit is a set of software tools intended to conceal running processes, files, or system data from the operating system. In recent years, rootkits have been used increasingly by malware to help intruders maintain access to systems while avoiding detection.

## Trends in Spyware

Trojans now dominate the triumvirate of viruses, worms and trojans, but the prevalence of Spyware marks a similarly disturbing trend. Spyware burst onto the malware scene a few years back, and its names and forms are many. It's a pointless debate as to whether the user actually agreed to get the adware (or toolbar, keylogger, etc.) as part of an overly dense end-user license agreement that virtually no one bothers to read anyway. Be it adware, toolbars, keyloggers, ransomware or something else, the many types of Spyware out there are essentially trojans. They are malicious software and are used to steal private information and conduct other nefarious activities.

Trojans now dominate the triumvirate of viruses, worms and trojans, but the prevalence of Spyware marks a similarly disturbing trend.

Spyware writers have learned well from the authors of viruses and worms. The WMF exploit in 2006 was the first time that the exploitation of a zero-day threat was associated with spyware distribution. (A zero-day exploit is one that takes advantage of a security vulnerability previously unknown to the general public.) Users must remember that their computers could be infected merely by visiting a website. Cyber-criminals don't need to entice people to open an attachment in an e-mail to deliver a payload. They can simply exploit a new or known vulnerability in software if the users' computers have lax security settings.

Adware was by far the most prevalent type of Spyware seen in 2006. Let's look at each common type of Spyware in greater detail.

- **Adware** is software that displays pop-up/pop-under advertisements when the primary user interface is not visible, or which do not appear to be associated with the product. In 2006, adware was the most prevalent spyware threat, accounting for 45 percent of the volume of threats. The most common adware in 2006 is WhenU.SaveNow, which pops up ads based on the keywords that a user enters into a search engine. Ezula, also widespread, can alter pages viewed in Microsoft Internet Explorer by adding extra links to words and phrases targeted to advertisers.

- **Hijacker.** Hijacking is a type of network security attack in which the attacker takes control of a communication. In respect to malware, there are many forms of hijackers, including DNS, browser, error and homepage hijackers. Each form of the hijacker attacks or takes control of a different type, path, or kind of software. A browser hijacker is a type of malware program that alters your computer's browser settings so that you may be redirected to Web sites that you had no intention of visiting. A browser hijacker might install in a location that is difficult to detect. Your machine might be reconfigured to run it at boot. When run, it might delete your 'favorites' info for Microsoft Internet Explorer, and replace your selected home page with another web page. Hijackers as a category accounted for 14 percent of Spyware in 2006. Common hijackers in 2006 included ISTbar and CnsMin.

- **Trojans** is a term applied to programs that do something their programmers intended, but that the user would not approve of if they knew about it (that is, a program with a hidden intent). The defining feature of a trojan is that it is a malicious program that is unable to spread of its own accord. Another often defining feature of trojans is remote access and control of the affected system. The most prevalent spyware-related trojans seen in 2006 are Pcast, SysSecuritySite, and MediaCodec. Trojans as a Spyware category accounted for 11 percent of all threats. Due to the blending of threats, a trojan can be both a type of malware category as well as a category of Spyware.

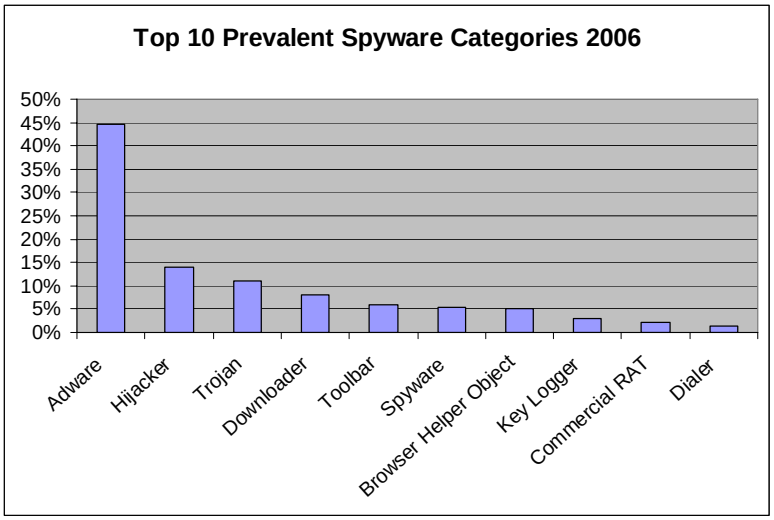


**Figure 3: Adware was the most prevalent form of *Spyware* in 2006. Following far behind adware were hijackers and trojans. As a category of *Spyware*, trojans were the third most prolific form chosen by malware writers**

- **Downloaders** can download and may execute or install software without a user's permission. Downloaders have risen in popularity because they allow their distributors to change the malware more readily, and are often part of a multi-phased installation of malware. In 2006, downloaders accounted for 8 percent of the total volume of Spyware. The effects of a downloader span the gamut from keyloggers to browser hijackers. The most prevalent downloaders in 2006 are TrojanDownloader.Win32.Xlob.ci and Downloader-AK, both of which download trojans.

- **Toolbars,** which are a group of buttons that perform common tasks in a web browser, accounted for 6 percent of Spyware in 2006. Toolbars may be created by Browser Helper Objects. For instance, WhenU.Search, the most prevalent toolbar seen in 2006, changes the user's default search engine without the user's permission.
- **Spyware** is any software that employs a user's Internet connection in the background without their knowledge and gathers/transmits info on the user or their behavior. As noted earlier with the blending of threats blurring the lines of distinction, spyware can also be a category within the malware type referred to in general terms as "Spyware". Many spyware products collect information from a user's web browser, IP address, system information, such as time of visit, type of browser used, the operating system and platform, and CPU speed. Spyware, as a category, accounted for 5 percent of the threats in 2006. The most common spyware was New.Net.Domain.Plugin, which changes the browser settings without the user's permission, displays pop-up/pop-under ads, and can silently connect to an unintended location to transmit user data.
- **Browser Helper Objects** A Browser Helper Object (BHO) is a DLL module that's designed as a plug-in for Internet Explorer to provide added functionality. For instance, a BHO may allow you to display a file format that the browser can't ordinarily display, reading a PDF file within your browser. The security risk is that a BHO doesn't need any kind of permission to install malicious components and thus spyware may be spread without the user's knowledge.

  The most common BHOs seen in 2006 were TopSearch (which is bundled with KaZaA) and VX2 (which monitors web pages requested and data entered into forms and sends this information to its home server and install pop-up advertisements). BHOs accounted for 5 percent of Spyware in 2006.
- **Keystroke loggers** are programs that run in the background, recording all the user's keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then reads them in the hopes of finding passwords or other useful information that could be used to compromise the system or be used in a social engineering attack. Advanced Keylogger and SafeSurfing were the two most common keyloggers seen in 2006. Keyloggers accounted for 3 percent of Spyware in 2006.
- **Commercial RAT** A Remote Administration Tool (RAT) is a trojan that provides an attacker with the capability of remotely controlling a computer. Commercial RAT accounted for 2 percent of the Spyware, with Sepro and Pest being the two most common RATs in 2006.

## Rogue Spyware

An ongoing problem is rogue, or fake, anti-spyware programs. Rogue anti-spyware pretends to provide a service to the customer when in actuality it uses social engineering and extortion to get the user to pay for the ineffective detection and removal capabilities it advertises. These deceptive practices prey on consumers and small businesses that don't recognize that some of the free anti-spyware programs may actually contain the malware they purport to address.

Typically, we find rogue anti-spyware distributed via online advertisements for free anti-spyware software. On occasion we have also witnessed these applications installed via exploitation of Microsoft Windows vulnerabilities as part of a drive-by download bundle or zero-day exploit.

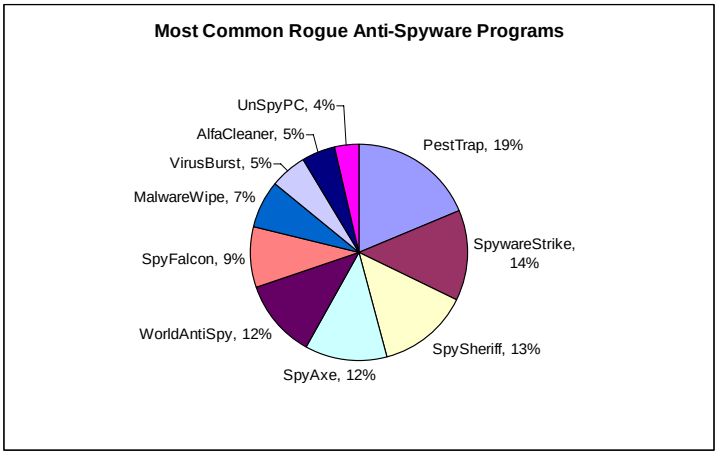


**Figure 4: PestTrap, SpywareStrike, and SpySheriff were the most common rogue anti-spyware programs seen in 2006. Typically, we find rogue anti-spyware distributed via online ads for free anti-spyware software.**

Users should be aware that some of these programs do in fact contain malware or are simply relatively useless against the majority of the spyware threats that exist today. After scaring the customer into believing that his or her system has security problems, the rogue anti-spyware software offers to sell the user a license that will enable the removal of the supposed problem. After the user pays up, the scheme will either undo the threat it itself installed or offer no fix at all.

## Trends in Application Vulnerabilities

As it becomes more difficult to evade anti-virus products, we see that cyber-criminals are increasing their activities around exploiting new and not-so-new application vulnerabilities. Criminals take advantage of known vulnerabilities in operating systems, applications, plug-ins, and other software. Many security researchers actively seek to find new vulnerabilities with no fix and disclose them “for the greater good” or, in some cases, for exploitation.

Compounding this situation is the reality that many companies and individuals fail to keep their computers up-to-date with the latest anti-virus definitions, anti-spyware software, and software patches. Or they buy illegal copies of software, for which they cannot get software patches, leaving themselves exposed to a raft of known exploits. Many times, those too-good-to-be-true offers for pirated software contain malware.

- **Windows Platforms.** Microsoft Windows platforms continue to be a favorite target because of wide market penetration. Most of the newly identified vulnerabilities were on Windows XP, but Windows 2000 continues to be a viable target. Old vulnerabilities are still being exploited by malware authors because so many computers remain unpatched and thus vulnerable.
- **Mac OS X.** The Apple Mac OS X operating system has become a target because of its increased popularity and ability to run on Intel processors as well as the PowerPC architecture. More than 100 vulnerabilities were identified in Mac OS X in 2006, with more than half rated as high or medium risk, according to NIST. No longer can Mac users be lax about security protections and patches.
- **Web browsers.** Online criminals have also turned more of their attention to the web browser, as businesses now rely on web-

based applications for many of their critical business functions. In 2006, about 45 percent of the newly identified web browser vulnerabilities were in Mozilla Firefox and about 40 percent were in Microsoft Internet Explorer, according to NIST. Many of these vulnerabilities were no doubt discovered and disclosed because of vulnerability researchers' "Month of Browser Bugs" in July 2006. Apple's Safari browser also had about 10 percent of the discovered vulnerabilities in web browsers.

- **Databases.** Databases are at the core of most companies' operations, as they contain vital business and customer data. In 2006, the Oracle platform had more discovered vulnerabilities than Microsoft SQL Server or the open source MySQL. Some vulnerability researchers have targeted Oracle, because they contend that Oracle doesn't address vulnerabilities quickly enough.
- **Microsoft Office.** Many of the obvious vulnerabilities have been previously identified and exploited, so criminals are turning their attention to Microsoft Office, and in particular Word and PowerPoint. In particular, these exploits target vulnerabilities in Microsoft Office that allow remote code execution. Several Office platforms are affected and some were targeted very specifically. For instance, some exploits only worked on systems with a particular service pack installed.

  One such example is the W97M/Kukudro family. CA received reports that Kukudro was actively spammed out to users in mid-2006. The payload for this trojan is to drop another trojan, which tries to download and execute arbitrary files. We saw it download a polymorphic virus, which has many payloads, including stealing system information, downloading and executing arbitrary files, running an HTTP proxy, and harvesting e-mails.

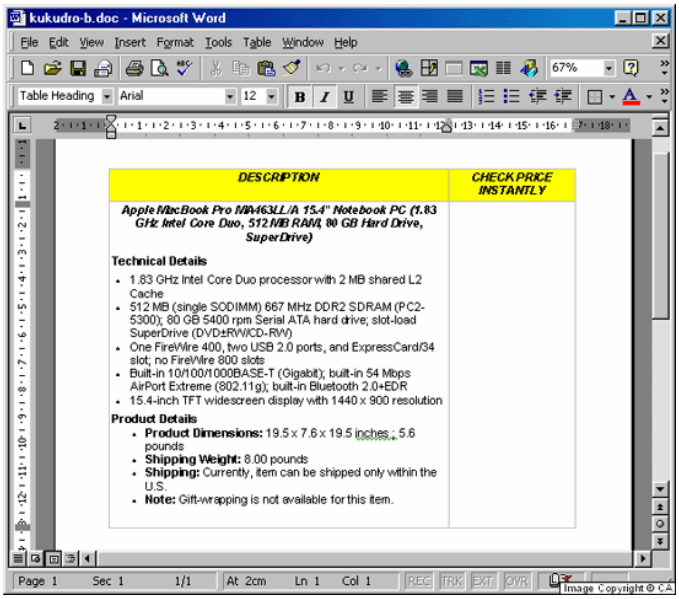


**Figure 5: 2006 saw a number of exploits targeting vulnerabilities in Microsoft Office. For example, in the Kukudro trojan above, the body of text of this infected document doesn't have any clickable buttons within the document, but it drops another variant of the trojan.**

This marks a shift from the opportunistic targeting of victims to selective targeting of individuals and organizations. CA saw several cases in which attackers sent specially crafted PowerPoint presentations via e-mail into businesses and government agencies. The files contained downloaders, which took advantage of Office's remote code execution capabilities. The downloader later pulled the real payload from a web server, and that payload was used for a targeted attack against the organization. Damages can range from gathering users' e-mail address books to stealing information from hard drives. Now imagine that these attacks are targeted at a company's engineering team — or their corporate executives.

- **Mobile Platforms.** While 2006 did not see many vulnerabilities reported for the mobile phone platforms, such as Windows Mobile, Palm, or Nokia/Symbian, that trend will likely change in upcoming years. As business

adoption of mobile devices grows — as will the criticality of the data they contain — the CA Security Advisor Team expects mobile phone operating systems to become a viable target in the near future.

## Seven Predictions for 2007

Based on ongoing research and vulnerability analysis, the CA Security Advisor Team has identified these seven key trends and areas to watch for the upcoming year:

- **Targeted attacks.** Criminals or disgruntled employees can use malware for corporate espionage or to steal intellectual property. By infecting an employee's machine, often through an online porn or gambling site the employee visits using his work computer, the criminal can plant malware that harvests information that can be used to steal intellectual property or credit card numbers. Or they can use ransomware to "kidnap" a user's data by encrypting it until they're willing to pay to get their data back.

  Today's phishing attacks are largely targeted at the consumer. Expect to see social engineering tactics become more convincing and targeted at the knowledgeable user. Those obviously fake phishing e-mails "to verify your account" will be replaced by more clever attempts. E-mail worms can disguise themselves as mail-failure notices. Or the seeds of identity theft may be planted in a credible e-mail from your bank that notifies you of the breach of your account. We expect to see an increase in sophisticated social engineering tactics that target how people use different types of content.

- **The rise of rootkits.** Criminals are increasingly using rootkits to help intruders maintain access to systems while avoiding detection. We expect to see a rise in kernel rootkits, which are especially dangerous because they can be difficult to detect without appropriate software. Kernel level rootkits add code or replace a portion of kernel code with modified code to help hide malicious applications.

- **Busting out web browser and other software vulnerabilities**. Cyber-criminals will increasingly exploit vulnerabilities in web browser and application platforms. As business embrace Web applications at the core of their operations, the browser will become a richer target for criminals. New software versions provide especially fertile ground for discovering vulnerabilities to exploit.

  For example, Microsoft Internet Explorer version 7 is new, and the ease of installing plug-ins may create the opportunity for abuse. Microsoft Vista, designed with security in mind, may actually turn out to be "too" secure, and users will turn off the security features for ease of use, thereby increasing their risk of exploitation. As businesses move to web-based software, rather than PC-based software, as their primary platform, we'll see increased vulnerabilities.

- **Stealing game passwords**. We expect to see a large amount of malware that was created with the express purpose of stealing passwords for particular online games.

- **More Mac malware.** We expect to see more malware development for Mac OS X, as the platform becomes a new target for adventurous malware writers. The release of Intel-based Macs also presents new challenges and opportunities as the number of systems running OS X increases.

  Perhaps the most worrying trend is the release of the OS X/Macarena virus in late 2006. Macarena is a parasitic file infector that was released for Intel first and for PowerPC shortly afterward. Macarena may be a harbinger of what to expect next — malware that uses a universal binary format and is capable of running on both PowerPC and Intel applications.

- **Distribution of underground utilities.** We saw the increase in the volume and complexity of packers and protectors in 2006, both to protect legitimate software from being cracked and to protect malware from reverse engineering and detection. We expect to see more of these underground executable protectors to be shared among malware authors, and thus their prevalence will rise.
- **Increasing complexity**. In 2006, we saw malware authors using increased levels of complexity and sophistication. Multi-component malware and the diversification of distribution channels are two good examples. As behaviors that were new in 2005 became mainstream in 2006, we expect to see more of the same. What was cutting-edge in 2006 will be mainstream in 2007 as more perpetrators use advanced techniques.

## What Can You Do?

You may have a lock on the front door of your house but simply having that lock isn't enough to protect you if you don't use it. Similarly, when protecting your company, yourself, and your family from online threats, acting responsibly is nearly as important as having the right software installed.

### For Businesses

To protect yourself and your company's data, you should get back to basics. The rise of a raft of compliance regulations have caused companies to shift to a strategic model for security risk assessment. But despite the sophisticated risk models taking both information security and regulatory compliance into account, companies need to take the basic steps needed for security blocking and tackling.

A multi-layered approach to security provides the most complete protection for your corporate systems and networks. Ensure that anti-virus definitions are current, especially for employees who are mobile. Use anti-spyware software to prevent attackers from establishing a beachhead in your company. Protect the network perimeter with firewalls and Internet gateway protection. Larger organizations should use host intrusion prevention (including firewall) and anti-rootkit utilities. Taking proactive action such as monitoring and patching vulnerabilities will also lessen your risk exposure.

Keep your users informed of the security risks — and stay informed yourself. Make sure your organization has clear, written security policies and that your IT department can enforce those policies. Patch critical business applications and operating systems. Enable automatic updates for Microsoft products and other popular software, so users will always have the latest protections without having to spend time manually updating their software. Extend your vigilance to applications such as Adobe Acrobat Reader, Flash, and Windows Media Player. Take into consideration the possibilities of instant messaging and voice over IP as channels for attack.

### At Home

To protect yourself and your family, follow these simple do's and don'ts:

- Do run anti-virus, anti-spyware, **and** personal firewall software.
- Do keep this software **on** and keep it **up-to-date**.
- Do read license agreements for software downloads.
- Do only download from websites you trust.
- Don't accept online offers that appear too good to be true — they usually are. "Free" file sharing or many other "free" things on the Internet are potentially spyware.
- Don't click on attachments from unknown sources either in e-mail, in instant messages or on social networking sites.
- Be wary of clicking on attachments from known sources such as friends since they may not be aware of the email; don't be afraid to

ask them if they really intended to send you the attachment.

- Don't click "ok" or "yes" to close out of a pop-up ad, use the "x" on the corner to get rid of it.
- Don't participate in group e-mails, they are common sources of malware.

## Rely on the CA Security Advisor Team

The CA Security Advisor Team delivers around-the-clock, dependable security expertise that has provided trusted security advice to the world for more than 16 years. Providing a complete threat management resource, CA's Security Advisor Team is staffed by industry-leading researchers and skilled support professionals delivering the knowledge to secure.

CA Security Advisor Team is a complete threat management resource that computer users can depend on. It is comprised of a network of rapid response centers — that vigilantly monitor threats around-the-clock. New security threats may include malicious code, computing vulnerabilities, and network attacks. Upon the discovery of a new security threat, the CA Security Advisor Team responds with solutions to detect and protect against a malicious attack. In addition, the CA Security Advisor Team provides information and assistance on combating the outbreak, including expert advice and descriptions of threats including risk, impacts, affected versions, distribution methods, detection signature files, validated recommendations and instructions for fixing the problem, and clean-up utilities.

The CA Security Advisor Team consists of industry-leading researchers and skilled support professionals who help ensure CA's award-winning Threat Management Solutions —*e*Trust® Antivirus, *e*Trust® PestPatrol® Anti-Spyware Corporate Edition r8, CA Host-Based Intrusion Prevention System, *e*Trust® Secure Content Manager, *e*Trust® Intrusion Detection, *e*Trust® Policy Compliance and *e*Trust® Vulnerability Manager, CA Internet Security Suite 2007, CA Anti-Virus 2007, CA Anti- Spyware 2007, CA Personal Firewall, and CA Anti-Spam 2007 — are always ready to address tomorrow's security threats today. Additionally, the security expertise and resources of the CA Security Advisor Team provide benefits to help your organization:

- **Effectively manage business risk.** With the comprehensive security information, tools, and support available from the CA Security Advisor Team, enterprises are empowered to manage risks and business impact proactively — rather than simply react to security threats.
- **Protect critical computing assets.** IT security personnel stay updated on the latest security threats, enabling the correct protection to proactively secure an organization's critical computing infrastructure. This helps reduce the risk of information compromise or costly downtime.
- **Respond faster to security threats.** The vigilant monitoring by CA's global network of CA Security Advisor Team Rapid Response Centers allows for the immediate discovery and notification of new security threats — no matter when or where they may surface — so enterprises can rapidly respond to an attack.

Get more information about security for your business at CA Security Advisor.

Get more information about security for your home computers or home office at CA Consumer Solutions.