TechTarget Windows Media

SearchWinIT.com
SearchWindowsSecurity.com
SearchWinComputing.com
SearchExchange.com
SearchSQLServer.com
SearchDomino.com
LabMice.net

SearchWindowsSecurity.com E-Guide

Antimalware E-Guide

Malware is evolving. Even with the advent of Windows Vista and Microsoft's promise of enhanced security, the forecast is that malware will still be a significant factor that every organization must address. This E-Guide from SearchWindowsSecurity.com and Sunbelt Software defines the problem, discusses the enhancements and gaps in Windows Vista and offers some suggestions of how to remove malware from your windows systems. Lastly, Sunbelt Software has provided a free trial download link and information about its product—Counterspy Enterprise—award winning antimalware solution.

Sponsored By: Sunbelt Software

TechTarget®
The Most Targeted IT Media

SearchWindowsSecurity.com E-Guide

Antimalware E-Guide

Table of Contents:

What is malware?

By Benjamin Vigil

Malware can be loosely defined as a malicious computer executable. The definition requires some flexibility because the term can describe a wide variety of different types of unwanted programs. The one certainty when discussing malware is the magnitude of the problem it poses—the damage inflicted globally by malware is usually measured in billions. This overview briefly covers the history of malware, the different strains, what makes today's computers so hospitable and what the future holds.

Malware first entered the computer lexicon when the people responsible for chronicling such topics—journalists, analysts and industry pundits—realized they needed a broader term to describe the profusion of malicious software running rampant across the Internet. Before malware became a commonly used term, any dangerous software was referred to as a virus or worm, which still holds true today in the mainstream media. What distinguishes the term malware from words like virus and worm is that malware refers to the intention of the software's creator rather than a particular feature of said software. While the term may be fairly new, the software it describes is not.

Viruses and worms

Worms have probably been around the longest, though when they first started surfacing they were hardly as malicious as today's malware. A worm, as well as a virus for that matter, is a self-propagating computer program.

The first well-known worm was known as the Morris Worm and it used an early version of the Internet and a BSD Unix flaw to propagate itself. In the recent past, hackers would often write these pesky programs simply to prove that it could be done. That was before every computer on earth was networked together via the Internet, and viruses and worms often had to be physically distributed to computers via floppy disk.

Viruses usually distinguish themselves from worms by requiring a host, like a Word document. Though both viruses and worms can be spread through e-mail, viruses and unwanted e-mail attachments have become synonymous. The first widespread e-mail-distributed virus was 1999's Melissa virus, which was a macro virus that exploited Microsoft Word and Outlook to mail itself to an infected computer's address book. Although viruses and worms can be damaging, their implementation is often haphazard and less beneficial to their creators than other forms of malware, which helps explain why this oldest form of malware is dying out.

Spyware and adware

Just as widespread e-mail use provided an enormous highway for virus traffic, the growth of the Internet helped spawn spyware. Spyware is an Internet browser-based malady that is largely fueled by the prospect of monetary gain. In its least virulent form, spyware or adware causes sluggish systems, slow Web browsing and annoying pop-ups. The more dangerous spyware might track browsing habits or sensitive information and transmit that information back to its creator.

The term spyware is most commonly used to refer to the less damaging adware. The surreptitious activity attributed to spyware usually requires another piece of malware like a keylogger.

Bots, Trojans and keyloggers

The most recent trends in malware are related to the increasing criminalization of online threats. One of these threats, bots, is either on the rise or people are just starting to realize the dangers of being infected by one. Bot makers and distributors infect multiple systems to create massive botnets that can be used to launch Distributed Denial of Service attacks or as spam distributors—which is, unfortunately, a lucrative endeavor.

Next on the list of growing Internet threats is the Trojan horse. By definition a Trojan horse is just a means of secretly installing a piece of malware on a system. That malware could be as innocuous as adware or as dangerous as a keylogger or rootkit. The name of the game for Trojans is subversion—sneaking their way onto a system and delivering an unexpected and potentially devastating payload.

Flaws and vulnerabilities

So what makes malware so pervasive? You can often chalk up the reasons for this deluge of depravity to software bugs, but even perfectly operating software can be susceptible to attack. For example, lax default configurations can either open up or exacerbate vulnerabilities—like when Windows 2000 Server had IIS turned on by default, which contributed to the massive damage inflicted by the Code Red worm of 2000. Often Microsoft’s zeal for introducing new functionality opens security holes in software, especially in Internet Explorer. But Microsoft is not solely to blame for the rise of malware. A significant number of the most vile threats require user interaction.

The future of malware

The bad news is that malware, once characterized by harmless viruses and annoying adware, is increasingly used for criminal activities. So much so that it is introducing new terms to the computer world, like crimeware. Even completely novel applications of computer code to the crimeware cause are surfacing. A new form of malware known as ransomware attempts to hold a user’s computer files hostage.

Gone are the days when a hacker would announce his triumph with an obvious mass-mailing virus. Nowadays, more malware writers are creating subversive software. They wish to sneak onto systems and secretly acquire sensitive user information or to even enslave vulnerable machines. While wrong-doing is on their minds, financial gain is usually the primary incentive.

Rootkit dangers at an ‘all-time high’

By Dennis Fisher

SAN FRANCISCO—The rootkit problem is not going away any time soon. In fact, it’s likely to get much worse before it gets better, according to the members of a panel on the topic at RSA Conference 2007 Tuesday.

“Rootkit capability is at an apex, an all-time high for the attackers,” said Jamie Butler, director of engineering at software security firm HBGary Inc. in Chevy Chase, Md. “Once you’re at ring zero, which is where all rootkits need to be in order to work well, it’s impossible to block their actions. They can write executable code, hijack legitimate threads, all kinds of things.”

Rootkits are not a new class of technology; they’ve been around for decades in one form or another. But in the last couple of years, their popularity and sophistication has grown by leaps and bounds as organized crime groups have adopted them as their weapons of choice for infiltrating PCs. The tools typically are designed to be installed stealthily, hide their presence on the system and allow the attacker to access the machine at any time.

As their use has grown in recent years, rootkits have steadily moved down deeper into the guts of PCs, from the operating system kernel all the way to the hardware. This, the panelists said, is a good indication of just how serious the problem now is.

“Each generation of rootkit moves lower into the system. They’re implementing them in hardware now, with virtual rootkits,” said Bill Arbaugh, an assistant professor of computer science at the University of Maryland and president and CTO of College Park, Md.-based rootkit detection firm Komoku Inc.

“It’s a business and they’re doing a pretty decent job of it,” he added. “These gangs have a QA process. They do not want their software to be detected. Malware writers are using the exact techniques that security guys have been using for years.”

And the advances being made by malicious hackers are constantly pushing the envelope. A new rootkit, called Unreal, that hit the Web late last month has the ability to hide both files and drivers. It’s designed specifically to bypass rootkit-detection software, Arbaugh said, and does the job quite well.

All of this has attracted the attention of a number of legitimate software companies and other corporations that are interested in preventing users from modifying or misusing their products. Some legitimate software makers have taken rootkit technology and adapted it to prevent users from reverse-engineering their applications or modifying them in unauthorized ways. In 2005, Song BMG Music Entertainment Inc. set off a firestorm of controversy and customer anger after a researcher discovered the company had included a rootkit on some of its audio CDs. The technology was meant to prevent illegal copying, and the company initially defended it, but quickly backtracked and eventually settled with both the Federal Trade Commission and consumers who had sued.

“It’s legitimate to self-detect whether you’re software is being modified,” said Greg Hoglund, who runs the Rootkit.com Web site and is a well-known software security expert. “But a lot of this other stuff is clearly not legitimate.”

Polymorphic viruses call for new antimalware defenses

By Ed Skoudis

Polymorphic code is actually a pretty simple idea, but a nasty one. Think of the word “polymorphic” in its piece parts: “poly” means “many,” and “morphic” means “form.” So, polymorphic refers to two or more pieces of code that have exactly the same functionality, but different code.

Two snippets of code could do exactly the same thing when they run, for example, but they might have entirely different sets of instructions. These pieces are “polymorphs” of each other.

Why would someone implement such code? To dodge strict signature-based detection, a major function of most antivirus and antispyware tools today.

Strict signature detection technologies match an exact sequence of bits on the hard drive or in memory. By self-morphing for each newly infected system, polymorphic code can create a new version that dodges the latest signatures. And, taken to the extreme, code could morph whenever it runs, each time creating a new version of itself that still performs the same function.

But, here’s the good news. Most major antivirus tools today employ heuristic checks. Think of these like “fuzzy” signatures; instead of matching the exact contents of a file in the file system or in memory, heuristic technologies only require certain crucial piece parts of code to match. And, because the bad guys so frequently utilize key parts of their old code when creating new evil specimens, the heuristics catch a lot of the nastiness. There are often still enough patterns left even in polymorphic code for an antivirus tool to detect it.

So what preventative measures can you take? Make sure you have up-to-date antivirus and antispyware signatures and that you are using an AV/spyware tool that supports heuristics. Most of the antivirus tools have this type of functionality, but not all of the antispyware tools do. Check with your vendor if you really want to know for sure.

As always though, things are in flux. The bad guys are starting to experiment with radically polymorphic code that thwarts heuristic controls by removing as many patterns from the original code as possible. The vendors, in turn, are working to improve the intelligence of their heuristics. Other antimalware vendors are starting to move toward behavior-based detection. Such techniques monitor the behavior of malware rather than look for any pattern in the actual code. If a piece of malware, for example, alters some critical files, the antimalware product can detect such behavior and kill the infection.

I happen to like a blend of both heuristic and behavior-based defenses myself, but be aware that some vendors are devoted to one side or the other.

Additional Resources from Sunbelt Software

CounterSpy Enterprise Assets

Protect Your Network Against Blended Malware Threats: Test Drive CounterSpy Enterprise
Does your antivirus software protect your organization against keyloggers, backdoor trojans, adware and spyware? Find out if it does!

Sunbelt's CounterSpy Enterprise Version 2.0 is powered by the industry's first hybrid antispyware scanning engine with **VIPRE** technology (Virus Intrusion Protection Remediation Engine). Version 2.0 delivers protection against malware using a hybrid technology that merges the 'system cleaning' properties of traditional antispyware products with the efficiency of powerful antivirus-based technology. You cannot afford to have a false sense of security when your organizations security is at stake. So give CounterSpy Enterprise a try. Download your complimentary, 30-day evaluation copy today!

Spyware in the Enterprise: The Problem and the Solution (white paper)
Spyware is a serious threat to the enterprise network, and the threat is growing. Awareness campaigns and user education are useful, but they're not enough. Download this informative white paper to learn more about:

- The truth about spyware
- The costs associated with spyware
- The right solution to protect your network from spyware

How Effective Is Your Antivirus? (white paper)
Your antivirus software may stop viruses and worms, but what about keyloggers, backdoor Trojans, and other malware? A lack of aggressive malware detection and removal can result in spyware wreaking havoc throughout an organization's IT network.

Read this paper to learn about the key differences between antivirus and antispyware products.

Controlling Spyware in an Enterprise Environment
This brief demo of CounterSpy Enterprise demonstrates how to easily configure and deploy desktop spyware protection throughout your organization with policy-based deployment, Active Directory support, an easy Admin Console for centralized management and the one of the most robust spyware threat databases in the industry.

Protecting Patient Data from Spyware and other Malware
Malicious spyware applications present an ever-increasing privacy and security threat to all companies, especially for healthcare organizations that must keep patient information secure and confidential. Keeping your healthcare IT networks safe from spyware that can steal personally identifiable information or patient records is critical. With the help of a robust, best-of-breed enterprise antimalware solution you can confidently know that your patient and company data are protected from security breaches associated with spyware while continuing to reinforce your ongoing security initiatives that help you meet HIPAA requirements.