Realtime publishers
"Leading the Conversation"

The Essentials Series: Modern Malware Threats and Countermeasures

Understanding the Modern Malware Landscape

sponsored by

Sunbelt Software

by Greg Shields

Copyright Statement

Understanding the Modern Malware Landscape

The word “spyware” is often used incorrectly to describe all types of unwelcome software that makes its way onto computers. Spyware, by definition, is only a small portion of the possible types of malware found in the wild. This terminology misuse highlights one of the central problems with truly understanding the landscape of bad code that could potentially infect unprotected servers and desktops: Each class of bad software has its own mechanisms for infection. Each arrives with different payloads, some attempting to do data destruction, others for financial gain. Virtually all arrive with a bent towards replicating themselves anywhere possible. As an IT professional, it is your responsibility to keep bad code away from systems, all the while rooting it out of those that become infected.

Malware, short for “malicious software”—and the correct term used to identify all classes of unwanted and potentially unwanted software—is a major problem in IT environments. Like all types of software, it evolves over time with new versions exploiting newly found vulnerabilities in operating systems (OSs). But malware as a class of software is changing as well. In the old days, malware was often written by disgruntled or bored code developers as a way to prove their mettle or enact revenge upon some segment of the online world. The malware of the early days often resulted in total destruction of computers and their data.

These days, malware development is big business. No longer relegated to computer hackers writing code in their mothers’ basements, malware is used most often these days as a tool for extorting money out of its victims. Fraud and scare tactics are a major priority of current malware creation. Malicious software in the form of rogue security programs are used to convince uneducated computer users to purchase removal software from the very people who wrote the malware itself. Other types collect proprietary information, such as credit card and Social Security numbers left in browser cache locations, and send it off for inappropriate use. Even more nefarious types work together in swarms for large-scale, massively parallel computing activities such as spam mail transmission, Denial of Service (DoS) attacks, and other activities.

The issue with all these types of unwanted software is the wide spread of their mechanisms for attacking systems and their payloads once an infection has occurred. The next article of this series will discuss in-depth those technologies, behaviors, and practices, and how the level of sophistication with this software has increased substantially with its monetization. In this article, let's take a look through a current list of known malware classes commonly seen in the wild. Understanding the types of malware you're up against will help you improve your ability to keep it out of your environment.

Adware

This class of malware describes software that monitors Internet use for known e-commerce sites. When a user attempts to reach a site, adware can pop up an alternate suggested site, which may or may not be legitimate. Not long ago, adware was a substantial component of all malware infections, with legitimate companies crafting specially-worded End User Licensing Agreements (EULAs) that made many infections deceptively legal. Recent litigation along with user education has resulted in the closure of many of these early organizations or their reconfiguration from legitimate to illegitimate entities. The financial gain associated with adware has lessened somewhat in recent years, with a resulting reduction in instances of this type.

Porn Dialers

Another aged malware class is the dialer or porn dialer. This software was used heavily in the days when modems were a primary mechanism for connecting to the Internet. This class of malware could silently disconnect a modem from its service provider and redial to another premium-rate telephone number. The resulting phone number charges, usually to far-removed countries, would be found by the user on their next telephone bill. Dialers have gone out of vogue as more Internet connections are broadband-based, and as telephone companies update their policies to find and eliminate the businesses that use such practices.

Rogue Security Programs

A much more modern construct, rogue security programs are a common occurrence in today's malware landscape. These software bundles download and install one or more obvious malware packages onto a targeted machine, while simultaneously installing code that alerts the user to the infection. The "rogue" in rogue security programs is named so because users are then shown how to purchase specialized software that will remove the malware. In essentially all cases, utilizing the suggested software does not actually remove the initial infector itself, keeping the system open for continued use by the attacker.

Backdoors

Backdoors are software tools that are installed to bypass existing security mechanisms present in either an OS or an application. Backdoors can be used to get around OS authentication systems, identify and replicate themselves around local networks, or send spam email from the infected host. Backdoors are often a component of other malware packages, enabling a mechanism for later download of additional malicious code.

Exploits

An exploit is a generic term used to describe any software code specifically designed to take advantage of a known weakness in OS or application code. When desired software on a computer system has not been coded properly and vulnerabilities exist on that system, exploits can be created to grant the attacker administrative privileges, complete some task, or destroy or disclose proprietary data. A common exploit in recent years has been the buffer overflow attack. This type of exploit software attempts to "overflow" existing pre-established areas of memory, pushing its malicious data into the next area of memory where it is later executed by the system. This type of attack is usually done in an attempt to acquire administrator privileges on the system, which are then used to process additional malware.

Keyloggers

Keyloggers are the original "spyware." Although, as discussed earlier, the term "spyware" is used loosely by many to describe all forms of bad software, spyware as a class of malware is actually used to "spy" on the user of a system. One way to accomplish this goal is to log every keystroke typed into that system. When all keystrokes are logged, it is possible to data mine the results to find credit card and Social Security numbers, password information, bank account information, and other personal information. Keyloggers need not necessarily be malware, as they are sometimes used in high-security corporate environments to monitor the activities of users on corporate networks.

Remote Control/Remote Access Tools

Another example of software that can be used for both legitimate and illegitimate means, remote control and remote access tools enable an individual to access areas of an infected computer remotely over the Internet. The level of remote access with this class of malware depends on the sophistication of the software itself. Some uses grant the user command-line access, while others can involve complete control of the desktop itself. Although used for illegitimate purposes, not all remote control or remote access tools are malware. Tools exist on the market today for the legitimate remote access of systems across the Internet.

Trojans

Like the fabled wooden horse in Greek mythology, a Trojan in computing relates to a piece of software that illegitimately performs some action that is different than its stated purpose. With Trojan software, the software may appear to be a legitimate software package that accomplishes a task desired by the user. However, in installing the software, it also performs some illegitimate task at the same time, destroying or exposing personal data, or any of the other payloads discussed to this point.

Trojan Downloaders

One class of Trojans commonly seen on the Internet is the Trojan downloader. A type of Trojan, the subversive task completed by this software once installed is to silently download additional malware packages to the machine. Because the initial application is installed to the computer through legitimate means by a privileged user, the Trojan itself gains the administrative rights necessary to download, install, and execute its follow-on packages. Often, the Trojan downloader itself does not perform any further function, masking its nefarious alternative purpose and leaving the further infection to the later downloaded code.

Rootkits

A particularly nasty class of malware, today's rootkits are created to hide the presence of software code on an infected system. That hidden code can be the rootkit itself as well as additional malware that is brought down to the infected system along with the rootkit. What makes rootkits challenging to locate and eliminate is the mechanism by which they hide themselves. Digging deep into the files and file system of the infected computer, rootkits install themselves by "patching" onboard system files for the OS itself. The result of the patching enables the rootkit to intercept user requests to view files on the system. It then replaces the results provided by the system with results of its own, hiding the presence of files and folders on the system.

Worms

Worms are a class of malware with a programmed drive to replicate. Although virtually all malware is written and distributed to spread itself across computers, worms include the code necessary to replicate themselves directly from the infected computer. The difference between malware that exhibits worm-like behaviors and other types of malicious code is the ability of the infected machine itself to spread the malware further. Worms can arrive on-system with a payload to accomplish some task like those discussed to this point, or can be written with no other reason than to simply replicate themselves.

Viruses

Along with worms are viruses. These common forms of malware are different than worms in that they actively attempt to infect files on-board a system. The infection can involve the wholesale replacement of a file, or more likely, the injection of malware code into the file itself. This injection of code into existing files allows the virus to run on the infected computer without being obviously seen through common systems monitoring tools. Because of this, virus scanning utilities are required to locate and remove instances of the injected code.

Summary

The economics associated with malware have grown to make malware production big business for the underground IT industry. Although many of the early mass-infection events were highly publicized and very obvious events to the user, modern malware is usually designed to be much more subtle in its behaviors. Similar to how the Ebola virus is significantly more virulent and deadly to its victims than the common cold, it also has a tendency to burn itself out rather quickly while the common cold remains prevalent today. The same holds true with today's malware landscape. Some are designed to create big results, while most quietly infect computers with the intention of keeping their presence hidden as long as possible for maximum gain.

These days, the war between good software and bad no longer pits the individual IT person against an individual malware developer. Entire underground industries have been built that write and test code against unsuspecting systems with an eye towards profit. As such, effective tools that incorporate fast responses against all these categories are critical to ensuring the security posture of today's IT environment.