By Michael Kassner

With all the different terms, definitions, and terminology, trying to figure out what's what when it comes to computer malware can be difficult. To start things off, let's define some key terms we'll use throughout the article:

- **Malware**: Is **mal**icious soft**ware** that's specifically developed to infiltrate or cause damage to computer systems without the owners' knowledge or permission.
- **Malcode**: Is **mal**icious programming **code** that's introduced during the development stage of a software application and is commonly referred to as the malware's payload.
- **Anti-malware**: Includes any program that combats malware, whether it's real-time protection or detection and removal of existing malware. Antivirus and anti-spyware applications and malware scanners are examples of anti-malware.

It's important to remember that like its biological counterpart, malware's number one goal is reproduction. Damaging a computer system, destroying data, or stealing sensitive information are all secondary objectives.

Keeping the above definitions in mind, let's take a look at 10 types of malware.

1: The infamous computer virus

A computer virus is malware that's capable of infecting a computer but has to rely on some other means to propagate. A true virus can spread from the infected computer to a non-infected computer only by attaching to some form of executable code that's passed between them. For example, a virus could be hidden in a PDF file attached to an e-mail message. Most viruses consist of the following three parts:

- **Replicator**: When the host program is activated, so is the virus, and the viral malcode's first priority is to propagate.
- **Concealer**: The computer virus can employ one of several methods to hide from anti-malware.
- **Payload**: The malcode payload of a virus can be purposed to do just about anything, from disabling computer functions to destroying data.

Some examples of computer viruses currently in the wild are W32.Sens.A, W32.Sality.AM, and W32.Dizan.F. Most quality antivirus software will remove a computer virus once the application has its signature file.

2: The ever-popular computer worm

Computer worms are more sophisticated than viruses, being able to replicate without user intervention. If the malware uses networks (Internet) to propagate, it's a worm rather than a virus. The main components of a worm are:

- **Penetration tool**: Malcode that leverages vulnerabilities on the victim computer to gain access.
- **Installer**: The penetration tool gets the computer worm past the initial defense mechanism. At that point, the installer takes over and transfers the main body of malcode to the victim.
- **Discovery tool**: Once settled in, the worm uses several methods to discover other computers on the network, including e-mail addresses, Host lists, and DNS queries.
- **Scanner**: The worm uses a scanner to determine if any of the newly found target computers are vulnerable to the exploits available in its penetration tool.
- **Payload**: Malcode that resides on each victim's computer. This could be anything from a remote access application to a key logger used to capture user names and passwords.

This category of malware is unfortunately the most prolific, starting with the Morris worm in 1988 and continuing today with the Conficker worm. Most computer worms can be removed by using malware scanners, such as MBAM or GMER.

3: The unknown backdoor

Backdoors are similar to the remote access programs many of us use all the time. They're considered malware when installed without permission, which is exactly what an attacker wants to do, by using the following methods:

- One installation method is to exploit vulnerabilities on the target computer.
- Another approach is to trick the user into installing the backdoor through social engineering.

Once installed, backdoors allow attackers complete remote control of the computer under attack. SubSeven, NetBus, Deep Throat, Back Orifice, and Bionet are backdoors that have gained notoriety. Malware scanners, like MBAM and GMER, are usually successful at removing backdoors.

4: The secretive Trojan horse

It's difficult to come up with a better definition for Trojan horse malware than Ed Skoudis and Lenny Zelter did in their book *Malware: Fighting Malicious Code*:

"A trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality."

Trojan horse malware cloaks the destructive payload during installation and program execution, preventing anti-malware from recognizing the malcode. Some of the concealment techniques include:

- **Renaming** the malware to resemble files that are normally present.
- **Corrupting** installed anti-malware to not respond when malware is located.
- **Using Polymorphic code** to alter the malware's signature faster than the defensive software can retrieve new signature files.

Vundo is a prime example; it creates popup advertising for rogue anti-spyware programs, degrades system performance, and interferes with Web browsing. Typically, a malware scanner installed on a LiveCD is required to detect and remove it.

5: Adware/spyware: more than an annoyance

Adware is software that creates popup advertisements without your permission. Adware usually gets installed by being a component of free software. Besides being irritating, adware can significantly decrease computer performance.

Spyware is software that collects information from your computer without your knowledge. Free software is notorious for having spyware as a payload, so reading the user agreement is important. The Sony BMG CD copy protection scandal is probably the most notable example of spyware.

Most quality anti-spyware programs will quickly find unwanted adware/spyware and remove it from the computer. It's also not a bad idea to regularly remove temp files, cookies, and browsing history from the Web browser program as preventative maintenance.

Malware stew

Up until now, all the malware discussed has distinctive characteristics, making each type easy to define. Unfortunately, that's not the case with the next categories. Malware developers have figured out how to combine the best features from different types of malware in an attempt to improve their success ratio.

Rootkits are an example of this, integrating a Trojan horse and a backdoor into one package. When they're used in this combination, an attacker can gain access to a computer remotely without raising any suspicion. Rootkits are one of the more important combined threats, so let's take a deeper look at them.

Rootkits: Completely different

Rootkits are in a class all their own, choosing to modify the existing operating system instead of adding software at the application level, like most malware. That's significant, because it makes detection by anti-malware much more difficult.

There are several types of rootkits, but three make up the vast majority of those seen in the wild: user-mode, kernel-mode, and firmware rootkits. Let's look at user-mode and kernel-mode first:

- **User-mode**: Code has restricted access to software and hardware resources on the computer. Most of the code running on your computer will execute in user mode. Due to the restricted access, crashes in user-mode are recoverable.
- **Kernel-mode**: Code has unrestricted access to all software and hardware resources on the computer. Kernel mode is generally reserved for the most trusted functions of the operating system. Crashes in kernel-mode aren't recoverable.

6: User-mode rootkits

It's now understood that user-mode rootkits run on a computer with the same privileges reserved for administrators. This means that:

- User-mode rootkits can alter processes, files, system drivers, network ports, and even system services.
- User-mode rootkits remain installed by copying required files to the computer's hard drive, automatically launching with every system boot.

Hacker Defender is one example of a user-mode rootkit. Luckily Mark Russinovich's well-known application Rootkit Revealer can detect it, as well as most other user-mode rootkits.

7: Kernel-mode rootkits

Since rootkits running in user-mode can be found and removed, rootkit designers changed their thinking and developed kernel-mode rootkits. Kernel-mode means the rootkit is installed at the same level as the operating system and rootkit detection software. This allows the rootkit to manipulate the operating system to a point where the operating system can no longer be trusted.

Instability is the one downfall of a kernel-mode rootkit, typically leading to unexplained crashes or blue screens. At that point, it might be a good idea to try GMER. It's one of a few trusted rootkit removal tools that has a chance against kernel-mode rootkits, like Rustock.

8: Firmware rootkits

Firmware rootkits are the next step up in sophistication, with rootkit developers figuring out how to store rootkit malcode in firmware. The altered firmware could be anything from microprocessor code to PCI expansion card firmware. This means that:

- When the computer is shut down, the rootkit writes the current malcode to the specified firmware.
- Restart the computer and the rootkit reinstalls itself.

Even if a removal program finds and eliminates the firmware rootkit, the next time the computer starts, the firmware rootkit is right back in business.

9: Malicious mobile code

In relative anonymity, malicious mobile code is fast becoming the most effective way to get malware installed on a computer. Mobile code is software that's:

- Obtained from remote servers.
- Transferred across a network.
- Downloaded and executed on a local system.

Examples of mobile code include JavaScript, VBScript, ActiveX controls, and Flash animations. The primary idea behind mobile code is active content, which is easy to recognize. It's the dynamic page content that makes Web browsing an interactive experience.

What makes mobile code malicious? Installing it without the owner's permission or misleading the user as to what the software does. To make matters worse, it's usually the first step of a combined attack, similar to the penetration tool used by Trojan horse malware. After that, the attacker can install additional malware.

The best way to combat malicious mobile code is to make sure that the operating system and all ancillary software are up to date.

10: Blended threat

Malware is considered a blended threat when it seeks to maximize damage and propagate efficiently by combining several pieces of single-intentioned malcode. Blended threats deserve special mention, as security experts grudgingly admit they're the best at what they do. A blended threat typically can:

- Exploit several known vulnerabilities or even create vulnerabilities.
- Incorporate alternate methods for replicating.
- Automate code execution, which eliminates user interaction.

Blended threat malware, for example, may send an HTML e-mail message containing an embedded Trojan horse along with a PDF attachment containing a different type of Trojan horse. Some of the more famous blended threats are Nimda, CodeRed, and Bugbear. Removing blended threat malware from a computer may take several pieces of anti-malware, as well as using malware scanners installed on a LiveCD.

Final thoughts

Is it even possible to reduce the harmful effect malware causes? Here are a few final thoughts on that subject:

- Malware isn't going away any time soon. Especially when it became evident that money, lots of money, can be made from its use.
- Since all anti-malware applications are reactionary, they are destined to fail.
- Developers who create operating system and application software need to show zero tolerance for software vulnerabilities.
- Everyone who uses computers needs to take more ownership in learning how to react to the ever-changing malware environment.
- It can't be stressed enough: Please be sure to keep operating system and application software up to date.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our 10 Things Newsletter
- Check out all of TechRepublic's free newsletters
- 10+ answers to your questions about IPv6
- 10 ways to avoid IT security breaches
- 10 answers to your questions about botnets

Version history

Version: 1.0
Published: July 17, 2009

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team