10 typical malware types

Currently, more and more sophisticated and more malicious new malware types appear. Anyone can know the harmful effects of malware, but not everyone knows how they work. This article will point out the 10 most dangerous types of malware ever.

TipsMake.com - Currently, more and more sophisticated and more malicious new malware appear. Anyone can know the harmful effects of malware, but not everyone knows how they work. This article will point out the 10 most dangerous types of malware ever.

Here are some of the terms used in the article:

1. *Malware* : A malware written specifically to infiltrate and destroy computer systems without users' knowledge.
2. *Malcode* : Is a malicious programming code embedded in the development phase of a software application and usually in the payload of malware, used to perform destructive, steal information on the computer.
3. *Anti-malware:* Includes programs against malware, helps protect, detect and remove malware.Antivirus , anti-spyware applications and malware detection applications are examples of anti-malware.

1. The infamous computer virus

Computer virus is a malware that can be infected but must rely on other means to spread. A true virus can spread from infected computers to an uninfected computer by attaching a code to the executable file that is passed on to each other. For example, a virus can hide in a PDF file attached to an email. Most viruses consist of the following three components:

1. **Replicator:** When activating the host program, the virus is activated at the same time, and they immediately distribute malcode.
2. **Concealer: The** virus used to evade anti-malware.
3. **Payload:** As mentioned, this payload is usually a virus's malcode, used to disable computer functions and destroy data.

Some recent computer virus samples include W32.Sens.A, W32.Sality.AM, and W32.Dizan.F. Most good antivirus software will remove viruses based on their virus data file.

2. Deep (Worm)

Computer worms are much more sophisticated than viruses. They can copy themselves without user intervention. Malware will look deeper than viruses if you use the Internet to spread. The main components of the worm include:

1. **Penetration tool** : Malcode exploits vulnerabilities on the victim's computer to gain access.
2. **Installer** : The penetration tool helps the computer worm get past the first defense system. The installer will then receive and convert the main component of malcode to the victim's computer.
3. **Discovery tool** : Once it has entered the machine, the worm uses a method to retrieve other computers on the network, including email addresses, server lists and DNS queries.
4. **Scanner** : The worm uses a test tool to determine if the new target computers in the penetration tool have vulnerabilities to exploit.

5. **Payload** : Malcode exists on each victim's computer. These codes can be anything from a remote access application to a key logger used to steal user names and passwords.

Unfortunately, this malware grows very fast. Starting with Morris worm in 1988 and now is Conficker worm. Most computer worms can be removed with a malware scanner.

3. Backdoor

Backdoor is similar to the remote access programs that we often use. They are considered malware if installed without permission, this is exactly what the hacker wants, according to the following methods:

1. Exploiting vulnerabilities on the target computer.
2. Trap the user to install the backdoor through another program.

Once installed, the backdoor allows hackers to have complete remote control of the hacked computers. Backdoor types, such as SubSeven, NetBus, Deep Throat, Back Orifice and Bionet, are known for this method.

4. Trojan horse

According to Ed Skoudis and Lenny Zelter, Trojan horse is a program that at first glance seems useful, but it contains many malicious 'features'.

Trojan horse malware contains many destructive payloads while installing and running the program, preventing malware from recognizing malcode. Some cloaking techniques include:

1. Rename the malware to the same file as the normal file on the system.
2. Make an antivirus software installed on your computer, to prevent it from responding when malware is detected.
3. Using different types of code to change the malware's registration is faster than security software.

Vundo is the typical Trojan horse type. It creates multiple popup ads to harass antispyware programs, degrade system performance and hinder web browsing. If you stick this trojan, you will have to install antivirus software on the LiveCD to detect and remove it.

5. Adware / spyware

Adware is software that creates advertising popup without user permission. Adware is usually installed by a component of free software. In addition to disturbing, adware can significantly reduce computer performance, slow down, and hang up.

Spyware is a software that steals information from a computer without users' knowledge. Free software usually has a lot of spyware, so before you install it, read the user agreement carefully. The most notable case of spyware related to Sony's BMG CD copy scandal.

Most good antispyware programs will quickly find and remove adware / spyware from your computer. You should also regularly delete temporary files, cookies and history from Web browsers to prevent this group of malware.

Malware stew

So far, all known malware types are quite different, helping to distinguish each type. However, this type of malware is not the same. The writers studied how to combine the best features of different types of malware to improve its capabilities.

Rootkits are a good example of this malware, which includes the features of a Trojan horse and a Backdoor. When used in combination, hackers can gain control of remote computers without being suspected.

Rootkits

Rootkits are completely different types, they often modify the current operating system instead of adding software at the application level that other types of malware often do. This is very dangerous because anti-malware programs will be very difficult to detect.

There are many types of rootkits, including the three most dangerous, including user-mode, kernel mode and firmware rootkits.

User-mode rootkits

User-mode includes code that limits access to software and hardware resources on the computer. Most of the code running on the computer will run in user-mode. Because access is limited, user-mode failures are not recoverable.

User-mode rootkit runs on the computer with admin rights. That means:

1. User-mode rootkits can change processes, files, system drives, network ports, and even system services.
2. User-mode rootkit maintains itself by copying the required files to the computer's hard drive and automatically launching each time the system starts.

Hacker Defender is a typical user-mode rootkit. This type of rootkit and many others were discovered and removed by Luckily Mark Russinovich's famous application.

Kernel-mode rootkits

Kernel-mode includes destructors that limit access to all hardware and software resources on the computer. Kernel-mode is often used to store the most reliable functions of the operating system. Damages in kernel-mod cannot be recovered either.

Since rootkits run in user-mode detection and removal, rootkit programmers have changed their minds and developed kernel-mode rootkits. Kernel-mode means that rootkits are installed at the same level as the system and rootkit detection programs. So rootkits can make the system unreliable.

Unstable is a downfall of a kenel-mode rootkit system, even leading to unexplained crashes or screen crashes. At that time, you should try GMER, one of the few reliable rootkit removal tools to fight kernel-mode rootkits like Rustock.

Firmware rootkits

Firmware rootkit is a sophisticated rootkit installed because these rootkit developers have studied the rootkit's malcode storage method in firmware. Any firmware can be changed, from the microprocessor code to the firmware of the expansion slot. That means:

1. When shutdown, the rootkit writes the current malcode to different firmware.
2. When restarting, the rootkit computer will also perform the reinstallation itself.

Even if a program detects and removes the firmware rootkit, the next time you start your computer, this firmware rootkit will still work normally.

6. Malicious mobile code (Mobile malicious code - MMC)

MMC quickly became the most effective method of installing malware on computers. They can:

1. Occupy remote server.
2. Move in the network.
3. Download and install on a local system

MMC includes Javascript, VBScript, ActiveX Controls and Flash Animations. The main purpose of MMC is easily recognizable as the way it works, making the web page content of the web browser more interactive.

Why is MMC toxic? Because the installation does not require user permission and misleading users. In addition it is often a stepping stone for a combined attack like the intrusion tool used by Trojan horse malware. Hackers can then install more malware.

The best way to combat MMC is to always update the system and all sub-programs.

7. Blended threat (Mixed threat)

Malware is thought to be a blended threat when it causes large damage and spreads rapidly through combinations of many targeted malcode. Blended threat deserves special concern because many security experts say they are 'experts in their work'. A typical blended threat can:

1. Exploit and create many holes.
2. Use many different reproductions.
3. Automatically run code to cancel user intervention.

Blended threat malware may send an HTML-formatted email embedded with a Trojan horse along with an attached PDF file containing a different type of Trojan horse. Some familiar blended threats are Nimda, CodeRed and Bugbear. Removing blended threat from a computer requires many anti-malware programs, as well as using installed malware scans that run directly from the CD.

8. Bots

Robots are automatically executed or bots are quite popular in modern Internet. They are often used to automate boring, repetitive tasks, most commonly in online auctions, online checks, chat and gaming.

However, there is a dark side to the fact that bots used for malicious purposes such as spamming, spreading other malware and joining the botnet network: a huge computer network, which has been infected with malware. and used to carry out large-scale network attacks. You can read more about botnets at: What is a botnet, who does it use to attack, and how can you prevent botnet?

Antivirus software can protect your computer from these bots, but there are some cases where the rootkit is pre-installed, preventing antivirus software from detecting bots, so regular rootkit scanning is a good precaution. Best.

9. Ransomware

Ransomware is one of the hacker's biggest money-making tools. In essence, it encrypts data on the computer, requiring a ransom to unlock the data.Some " ransomware " only lock the computer (allowing easy removal in Safe Mode), while the more dangerous ones will encrypt the entire hard drive, blocking user access until The attacker receives money (usually in the form of Bitcoin or through anonymous transfers like Western Union).

Hackers often threaten users that they find illegal or suspicious documents on their hard drive. For more evidence, hackers can use webcams to capture victims. This hacker's strategy can cause panic, causing the victim to pay ransom for fear and despair.

Ransomware infects a computer in a manner very similar to Trojan horse, through downloading files and running files. Another way for ransomware to infect a computer network is through a network or rootkit vulnerability. In general, an updated anti-virus program can detect malware of this type before they can be executed.

In the future, with the growing and deeper penetration of the Internet into life, the number and form of malware will increase. Although the application publishers, the operating system also regularly release vulnerability patches, provide additional tools to prevent malware but that is not enough. We need to regularly update software versions, new operating systems, practice the habit of careful clicking, downloading files, surfing the net to minimize the risk of malware infection.

Read more: What to do if your computer has a virus?