Risks from malware and how to prevent it

The article will focus on recent malware threats and suggest possible solutions to deal with these threats.

TipsMake.com - At the present time, it's hard to believe that low-level codes can still run in the background without being detected. Governments also recognize that current defense measures are not enough and they can easily lose control of the intranet or website to others. The article will focus on recent **malware** threats and suggest possible solutions to deal with these threats.

Along with the development of software technology, developers also give warnings and at the same time deploy more security measures to ensure their products are protected. However, the malware threat is not reduced. When countermeasures come out, bad guys find more sophisticated and complicated ways to invade the system vulnerability. Now they can even fake software services and when the machine updates, instead of patches and security software, the malware is downloaded and installed on the system.

New attacks are being developed to suit the era of social networks, such as spreading social networking sites. In addition, similar attacks previously caused heavy losses. Traditional viruses are still secretly infecting files, compromising the computer's performance and can turn our computers into servers that infect sites and other computers and networks.

Malware can be described as follows:

1. **Advertising program (Adware)** : Put ads on the computer screen with many different means.

2. **Spyware (Spyware)** : Used to collect data information on a computer and redirect it to another address. Information such as personal user information, browser history, username and password and credit card number.
3. **Hijacker** : Hijacker targets Internet Explorer. They control parts of the web browser, including the home page, search pages and the search bar. They redirect you to sites you don't want to visit.
4. **Toolbars** : A toolbar is installed via unclear media that entails a series of malware.
5. **Dialer** : The program that changes the configuration of the modem so that a device turns to a certain number increases the phone bill, causing damage to the user and earning a profit for the bad guys.
6. **Deepware** : This is a new term for malicious code to work deeper into the OS and behave like a very low-level rootkit, almost impossible to detect by normal antivirus programs.

Effect of malware on the computer

1. Slow down the connection.
2. Slow down the machine, causing a computer error by malicious code.
3. Causing the display of continuous error messages.
4. Cannot turn off the computer or restart when the malware maintains for certain processes to work.
5. Bad guys take advantage of malware to collect personal information or data from computers.
6. 'Robbery' browser, redirecting users to intentional sites.
7. Infecting the machine and using it as a host promotes many different files or performs other attacks.
8. Send spam and go to user mailboxes.
9. Send emails that impersonate users, cause trouble for users or the company.
10. Grant system control and resources to attackers.
11. Make new toolbars appear.
12. Create new icons on the desktop.
13. Run underground and hard to detect if programmed well.

Types of malware that stand out

In the past few months, dangerous malware has been identified. The latest malware includes:

1. Flame
2. Trojan Flashback
3. Trojan.Win32.Generic
4. Artemis Trojan
5. Scrinject.b

Flame

New flame was discovered in May. It is also known as Flamer or Skywiper and is believed to have appeared two years ago but was only discovered until recently. With over 1000 initial attacks on many computers of government institutions, educational institutions and individuals, Flame is described as the most sophisticated malware ever discovered.

Flame is the first malware to use cryptographic, pre-collision attack technology, allowing viruses to falsify digitized authentication information to spread. This malware attacks computers running Microsoft Windows and easily spreads to other computers via LAN or USB. Flame collects data through recordings, photos, keyboard operations, Skype conversations and network traffic. It also uses a host as a Bluetooth receiver station that can attempt to download information from surrounding Bluetooth enabled devices. All collected data is sent to command and control server settings around the world. Once done, all traces of malware are erased from the computer because Flame supports a Kill command in it.

The most ominous of this kind of malware is that it works stealthily but cannot be detected but still silently gathers important information. Its level of harm can be endless thanks to the modular structure, after infecting a malware-based computer, many modules are easily added to accomplish different purposes.

Trojan Flashback

The absolute safety of Apple users is only past. Years ago, the attacks targeted Apple users with worms, viruses and hackers were very small. Trojan Flashback, first discovered at the end of 2011 is described as the worst security disaster happening on Macs. Global attacks on Macs and Macbooks running OS X have achieved huge numbers of victims, more than 600,000 devices and no sign of diminishing.

Trojans target vulnerabilities on Mac OS X. A user is redirected to a fake site where JavaScript code downloads an application. An executable file stored on the device can download and run malicious code on the device. Trojans are capable of doing everything they want on infected machines.

The increase in Apple's user base makes these devices a great target for attacks. Hackers will definitely continue to search for vulnerabilities or ways to infiltrate this system.

Trojan.Win32.Generic

The Trojan is ranked among the top 10 most infectious malware recently and is the most widely spread malware in a short time. Trojan.Win32.Generic infiltrates the computer via backdoor, installs itself and proceeds with vandalism. It takes advantage of vulnerabilities in computer software to grant remote access to hackers to the host.

Artemis Trojan

Artemis Trojan is capable of spreading on a computer and then displays false information such as fake security websites. Although it appeared a few years ago, this Trojan suddenly increased its activity this year. The biggest problem when dealing with Artemis is that in many cases, the antivirus program cannot determine if it is actually a virus.

Scrinject.b

When translating data into the cloud is the mainstream today, this is really a big concern. Scrinject.b is a system of cloud-based malware. It is capable of collecting data on a global scale.

Steps to prevent malware

Activate and always maintain the firewall. If you don't trust the firewall feature on the OS, you can also try one of the many firewalls on the network.

1. Update your computer regularly.
2. Update the new antivirus program and the latest antispyware / malware software.
3. Browse the web safely, set security for your browser enough to detect invalid downloads.
4. Install multiple anti-spyware programs on your computer, since all programs are imperfect and can compensate for each other. The combination of programs will detect a wider range of malware.
5. Computer monitoring. Perform regular virus scans.

1. After installing the new software, always perform a virus scan on the computer.
2. Caution when installing software. We often do not read the EULA carefully but quickly click to accept the installation. It's best to read the EULA and make sure that any middleware is allowed to be installed.
3. Understanding malware. Make sure you stay up to date on the latest malware.
4. Regularly backup data, prepare in case of computer problems.
5. Do not click on the link or attachment in the email unless you are sure about their content.
6. Download and install software from trusted websites.
7. Use pop-ip blocker and don't click on any link in the pop-up.
8. Use sandbox to test the program. If downloading an application that is unsure about safety, install it on the sandbox first to test .
9. Check for process detection and fake service. This is simple enough to do, but you should make a habit of doing it regularly to make sure nothing runs in the background.
10. Use virtual machines for unclear software, just like the sandbox.

Conclude

The motivation behind malware has changed a lot over time. The first malware versions were only developed for the purpose of teasing more than intentionally damaging. Everything changed and bad guys tried to develop malware for a special purpose like making money or collecting important information. But users also have ways to protect themselves against malware according to the steps mentioned above.

Malware is still part of today's computing world. When research is conducted to quickly develop tools to deal with them, it's time for malware creators to develop new programs and find new ways to infect our systems. And the chase will continue forever.

See also: Theory - What is Ransomware?