How many types of malware do you know and how to prevent them?

Currently, computer criminals use a lot of different malware (malware) to attack the system. Here are some of the most common malware types and ways to prevent them.

Computer criminals use a lot of different malware (malware) to attack the system. Here are some of the most common malware types and ways to prevent them.

IT security experts often use generic terms without precisely defining their meaning. That can make users wonder about basic questions like *what is malicious software? or how are malware and viruses different? What are the similarities between Crimemare and malware? And what exactly is spyware (ransomware)?* In the following article, we will answer all these questions.

1. How to kill Malware with effective Zemana AntiMalware software
2. Top 10 most dangerous malware types with bank accounts
3. Remove root malware (malware) on Windows 10 computers

So what is Malware?

Malware is actually an abbreviation for malicious software. Basically, malware is software that you don't want to appear on your computer or mobile device. Obviously this is a large software group that includes many different types of malicious software. Malware includes viruses, worms, trojans, adware and ransomware .

The following sections will provide definitions for some of the most common types of malware.

Adware

Adware is a type of malware that downloads or displays pop-up ads on a user's device. Normally, Adware does not steal data from the system, but it forces users to view ads that they do not want on the system. Some extremely annoying forms of advertising for users are creating pop-ups on the browser that cannot be closed. Sometimes users infect themselves with adware installed by default when downloading other applications without knowing it.

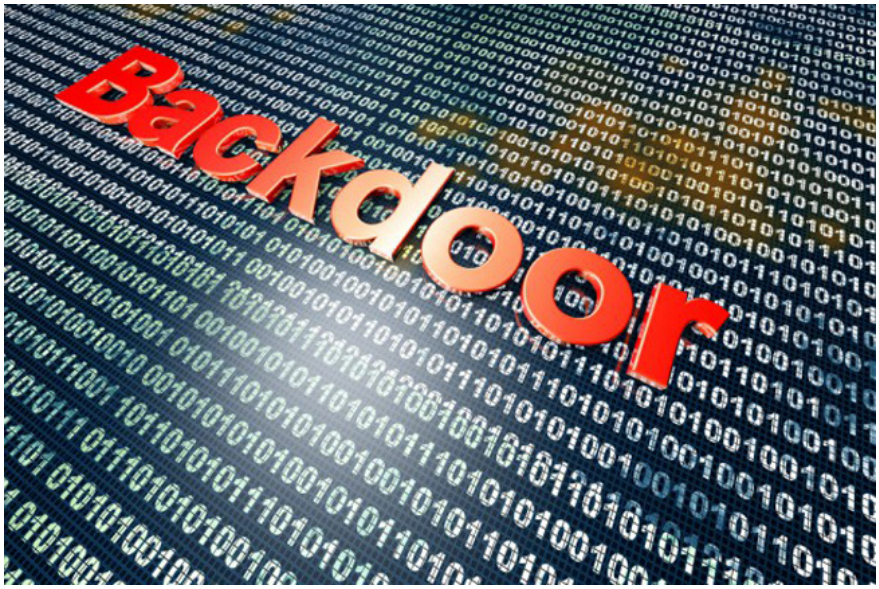
So how to block these adware?

The solution is to install anti-malware capable of blocking adware. Disable pop-ups on browser pages and observe the process of installing new software, making sure to uncheck the boxes for installing additional software by default.

1. Completely remove Adware and Spyware on your system

Backdoor

Backdoor is a secret program that can access a user's device or network. Typically, manufacturers of equipment or software create backdoors in their products or intentionally let corporate employees infiltrate the system through coding practices. Backdoor can also be installed by other malware such as virus or rootkit.



How to prevent backdoor

Backdoor is one of the biggest threats that is hard to prevent. Experts say the best protection strategy is firewall installation, anti-malware software, network monitoring, intrusion prevention and data protection.

Bot and botnet

Generally, bots are software that runs automated tasks, and there are many useful bots. For example, Internet data collection programs and index pages for search engines and chatbot sometimes answer customer questions on the company website.

However, when discussing IT security, bots are often used to refer to a device that has been infected with malicious software that could harm the computer that the user has not allowed or known. Bonet is a large group consisting of bots gathered to do the same task. Attackers often use bonet to send a series of spam messages, scams or perform distributed denial of service (DDoS) attacks to websites. Recently, Attacker has started to combine devices of all things Internet connectivity (IoT) into their bonet attacks.

Instructions on how to fight bonet

Organizations can help prevent computers from becoming part of bonet by installing anti-malware software, using firewalls, constantly updating software and forcing users to use strong passwords. In addition, network monitoring software may be useful in determining whether the system has become a part of bonet. Also, you should regularly change the default password for any IoT device you install.

Browser hijacker

Browser hijacker, also known as Hijackware can change your web browser behavior, for example by sending users a new search page, changing the homepage, installing toolbars, switching. direct users to unwanted websites and display ads that users don't want to see. Attacker often makes money from this kind of malicious software through receiving advertising fees. They can also use a hacked browser to redirect users to sites that download more malware into the system.

How to prevent browser hijacker

Be very careful when installing a new software on the system by many browser hijackers that will insert into the software you have installed, such as adware. In addition, you should install and run the anti-malware software on the system and security settings for the browser to a higher level.

Bug

Bug is a generic term for a hole in a code. All software has errors but is almost unnoticed or only causes minor discomforts. However, there are times when bugs represent a serious security hole, using software that contains this type of bug to attack the user's system.

How to prevent bugs

The best way to prevent an attack from exploiting a security vulnerability in software is to update the software continuously. When the Attacker is aware of vulnerabilities, vendors often quickly release a patch to prevent damage to the customer's system.

Organizations that want to prevent security errors on software that they write should implement safe encryption methods and fix bugs as soon as possible. They will also reward researchers who find security holes in their products.

Crimeware

Some vendors use the term "crimeware" to refer to malware used to commit crimes, often a crime related to financial interests. Like malware, crimeware is a broad category of a wide range of other malicious software.

How to prevent crimeware?

To protect your system from crimeware, you should take the best security measures, including firewall use, intrusion prevention, network monitoring and logging, data protection and security information. , network security monitoring system (SIEM) and intelligent security tools. You should also use strong passwords and update passwords regularly.

Keylogger

Keylogger is a keystroke monitor that records all the keys that users click, including email, documents and passwords entered for certain purposes. Typically, attackers often use this kind of malicious software to get passwords and hack into network or user accounts. However, employers sometimes also use keyloggers to determine if their employees have any offenses in the company's system.

How to prevent Keylogger

Replacing passwords is one of the best ways to prevent or mitigate the damage caused by keyloggers. Remember to use strong passwords and update regularly. In addition, you should also use network firewall and anti-malware solutions.

Malicious mobile application

Not all applications available on Apple's App Store or Google Play are secure applications. Although application operators have tried to prevent malicious applications, some still slip through. These applications can steal user information, blackmail or attempt to access the company's network, forcing users to view unwanted advertisements or engage in other unwanted activities.

How to block malicious mobile applications

Equipping users with knowledge is one of the most powerful ways to prevent malicious mobile applications because users can avoid these software by not downloading or accessing third-party app stores. Be careful when downloading new applications to mobile devices. Mobile anti-malware apps also help users avoid these bad apps.

Organizations can block these malicious applications by creating strong mobile security policies and deploying mobile security solutions to enforce those policies.

Phishing

Phishing is a type of email attack that attempts to trick users into revealing passwords, downloading attachments or accessing a website that has been installed on their systems with malicious software. Spear phishing is a phishing campaign targeting specific users or organizations.

How to prevent phishing

Because phishing is based on social engineering techniques (security terminology to trick users into doing something), equipping users with knowledge is one of the best measures to avoid being attacked. Users should implement anti-spam and anti-malware solutions as well as not disclose personal information or email passwords. In addition, they need to be warned about being careful when downloading attachments or clicking links in mail even if they appear from a common source because attackers often disguise a company or a someone that users know. Email is also often an active Ransomware object.

Ransomware

In recent years, Ransomware has quickly become one of the most popular types of malware. In fact, according to Malwarebytes' report, the Ransomware incident caused an increase of 267% between January and November 2016. These most popular software variants will lock the system, block any operation. done until the victim pays a ransom for the attacker. Other types of Ransomware will threaten to publicly disclose bad information about users, such as user activity on adult websites if users do not pay ransom.

How to prevent Ransomware infection

Often organizations can reduce attacks by updating backups. In addition, organizations should educate users about threats, patch software when needed and establish common security methods. However, some types of Ransomware are said to be difficult to block, so many individuals and organizations have lost money unfairly.

Rogue fake security software

Rogue security software is often described as a form of Ransomware and Scareware. This software deceives users into thinking that the computer system has security issues and suggests they buy fake security software to solve the problem. In fact, instead of providing security features, counterfeit software often installs more malicious software.

How to prevent Rogue security software

Like most malware, you can block fake security software by installing a firewall or using preventive methods like Phishing.

Rootkit

Rootkits are one of the most dangerous types of malware because they allow attackers to have admin-level access to the system without users' knowledge. When an attacker accesses the system, they can do anything to the system, including recording operations, changing system settings, accessing data and attacking other systems. Famous attacks like Stuxnet and Flame are two examples of rootkits.

Prevention

The way to prevent rootkits is similar to those of other malicious software. However, one thing worth noting is that if the rootkit infects the system, users will find it difficult to detect and remove. In many cases, you must clean up the hard drive and start over again to remove it.

Spam

In IT security, Spam is unwanted email. Typically, spam includes unnecessary advertisements, but it may also contain malicious software installation links or attachments to the user system.

How to stop

Most email solutions or services include spam protection features. Using those methods is the best way to prevent spam messages from appearing on the system.

Spyware

Spyware Spyware are software that collects information about users that they do not know or agree with. For example, websites that enable cookies that track a user's web browser can be considered a form of Spyware. Other types of Spyware software can steal information from individuals or businesses. Sometimes, government agencies and police forces also use this spy software to investigate suspects or foreign governments.

Prevention

You can install anti-spyware software on your computer, or anti-virus and anti-malware packages that also contain anti-spyware features. Similarly, you should also use a firewall and be careful when installing software on the system.

Trojan

In Greek mythology, a number of Greek soldiers were hiding inside a wooden horse outside of Troy and then retreating. When the Trojan brought the horse into the city thinking it was a spoils, the Greek warriors got out of the horse's belly and opened the gate for the Greeks to attack and capture Troy. In computer security, the Trojan horse, also known as Trojan - is a malicious software hidden under a harmless program but actually serves a bad purpose. For example, a Trojan may appear as a free game, but once installed, it can destroy your hard drive, steal data, install backdoor malware or perform malicious actions. Other harms.

How to stop

Similar to other malware prevention methods.

Viruses

Sometimes people use the word "virus" and "malware" instead, but the virus is actually a specific type of malware. To be considered a virus, malware must infect other programs and other systems. Viruses also often perform some unwanted activity on an infectious system such as combining systems into botnets, sending spam, stealing credit card information, passwords or locking the system.

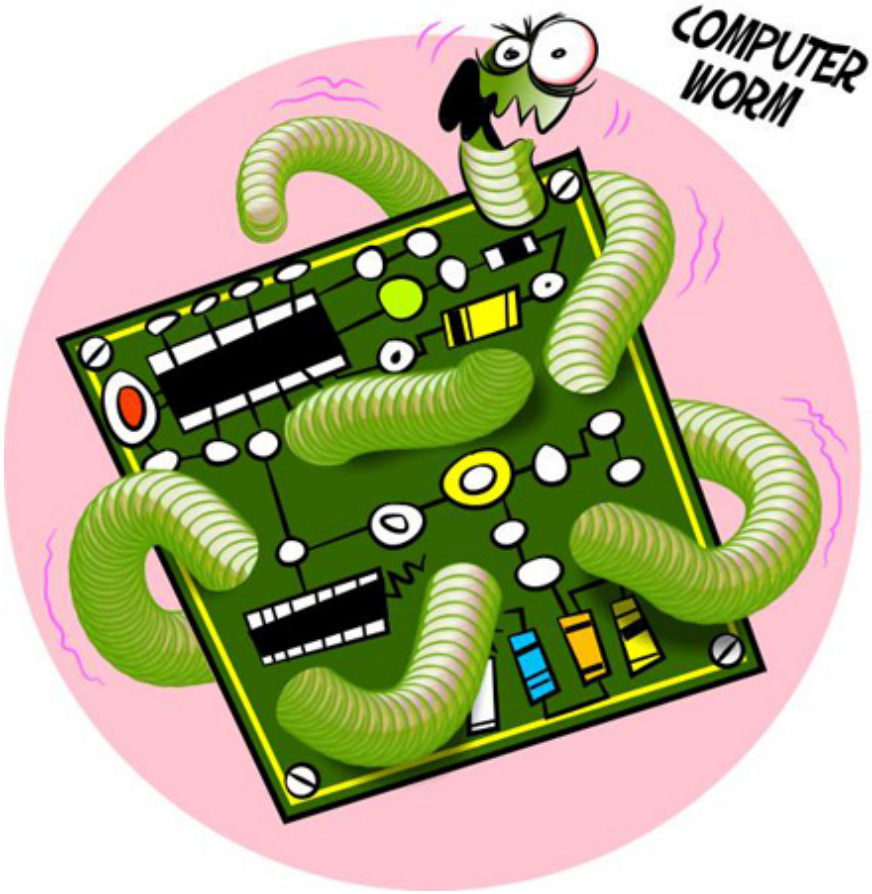
1. 7 types of "infamous" computer viruses most frightening

The same way to prevent other malware.

Worm

The worm is created similar to a virus because it spreads itself, but another point is that it does not infect other programs. Instead, it is an independent part of malware, spread from one computer to another or from one network to another. It may cause similar types of damage to viruses on the system.

1. Summary of the most frightening "virus worms" on computer systems



Prevention

Like viruses, the best way to avoid being infected with Worm is to use antivirus or anti-malware software. Just like with other types of malware, users should only click on email links or attachments when they really know the content.

What kind of popular malware that TipsMake.com has not mentioned in the post, you can give comments by commenting below! TipsMake.com hope that the article will bring useful information for you.

You finished reading the article "**How many types of malware do you know and how to prevent them?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
