

Common types of computer viruses

Understanding and identifying viruses on your computer makes it easy for you to identify and protect yourself when using your computer in an open connection environment. TipsMake.com shares with readers knowledge about popular computer viruses.

Understanding and identifying viruses on your computer makes it easy for you to identify and protect yourself when using your computer in an open connection environment. In today's article, TipsMake.com shares with readers knowledge about popular computer viruses, invites you to read along.

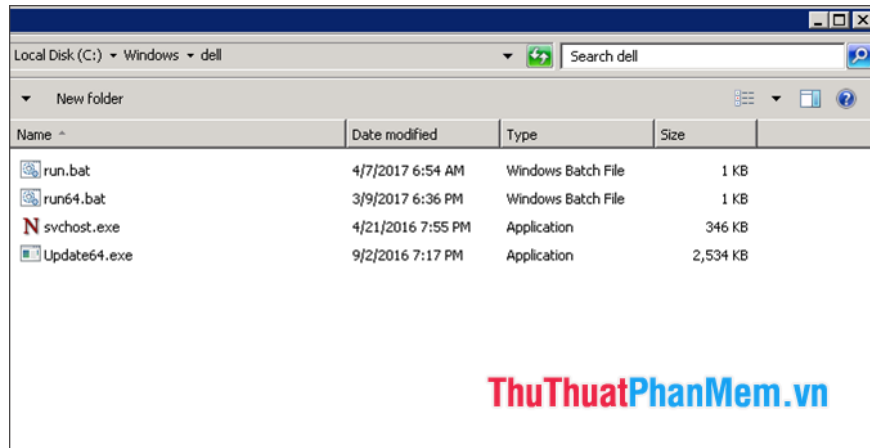


1. Virus Boot



This virus is quite common in the late 20th century and early 21st century when weak computer systems used floppy disks to boot. This virus is loaded into the Boot Sector - the area responsible for booting the operating system on disk. Today, we hardly see the Boot Sector Virus because they are easily detected and destroyed by anti-virus software and with the development of the Internet, the target to attack computers with this virus is no longer suitable. .

2. Virus File



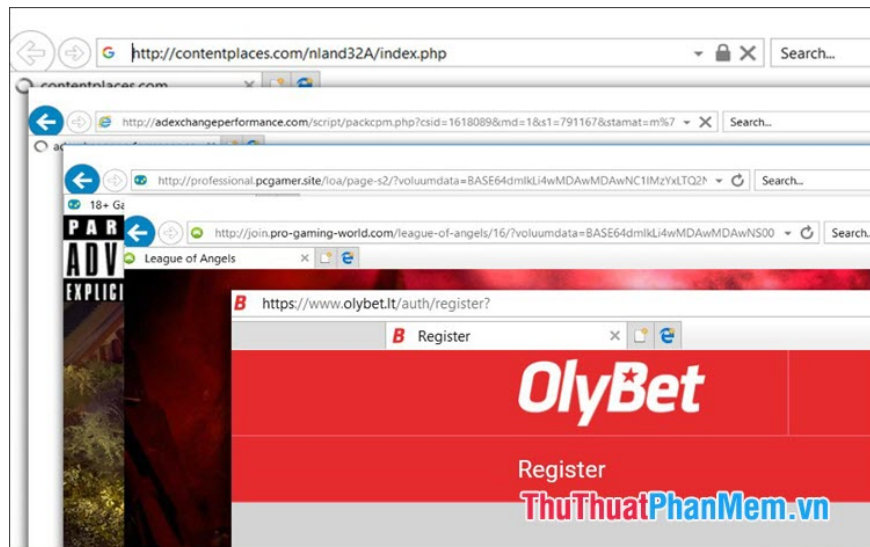
This is a fairly common computer virus from the era of the Internet, not really popular to this day. This type of virus often selects program executable files (.exe, .dll, .inf .) to infect. This virus spreads quite quickly and the recovery is quite difficult because we have to delete the file infected by the virus to fix it. When you open the software with the .exe extension, the virus starts to work and continues to search for other files to infect. Worse when these viruses infect important operating system files with the task of booting, booting up, checking hardware . and the only way to fix it is to reinstall the operating system.

3. Macro Virus



Macro virus is a virus that uses the application's macro programming language to load resources and conduct infection. The same way that a file is transmitted via a virus file, but this virus usually looks for text files and documents such as Microsoft Office and they are often included in emails containing document files.

4. Virus web scripting



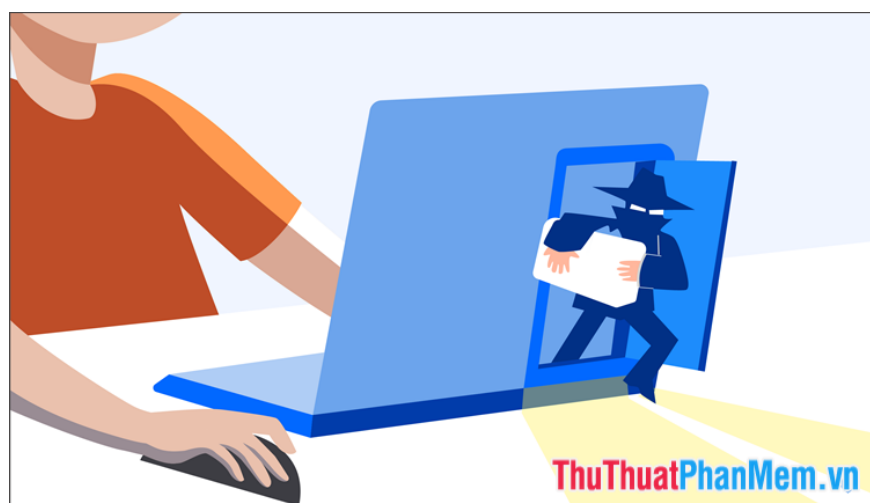
With the strong development of the Internet and platforms, web scripting viruses have become more popular and unpredictable than ever. Virus scripting is programmed with scripting languages such as Visual Basic Script, Batch Script, JavaScript, and spreads on other website scripts such as images, videos. Then they insert ads, banners, causing users to accidentally click and your computer may be bothered by ads, consuming system resources. The recent variant of this virus is the Crypto Mining virus - a virtual currency mining on the web that makes your computer turn into a virtual currency mining machine, making it slow and sluggish.

5. Trojan Horse Virus



The virus is associated with an ancient Greek story: in a siege of a failed Trojan castle, Greek soldiers devised a reconciliation plan that gave the Trojan people a giant wooden horse and When the wooden horse was brought into the city, the soldiers hid inside the wooden horse and stormed to occupy the city. Trojan Horse was born with the same purpose, it is hiding under the cover of file system and silently stealing data or spreading different types of viruses. Besides the data theft trojans, some new concepts that will divide the Trojan into the main categories are Backdoor, Adware, Spyware.

6. Backdoor



Backdoor, also known as "backdoor" - a type of Trojan when entering the computer will try to open a service port and exploit that port, allowing hackers to access the remote computer via the secondary port to collect data or hijack computers.

7. Adware illegal adware



Adware is a branch of Trojan that displays annoying pop-up ads to users when visiting infected websites. Adware, by its nature, is harmless, but it annoys and annoys users when pop-up ads are offered on the screen. Worse, those ads may contain virus scripting or spyware when users accidentally click on them and follow the instructions on them.

8. Spyware



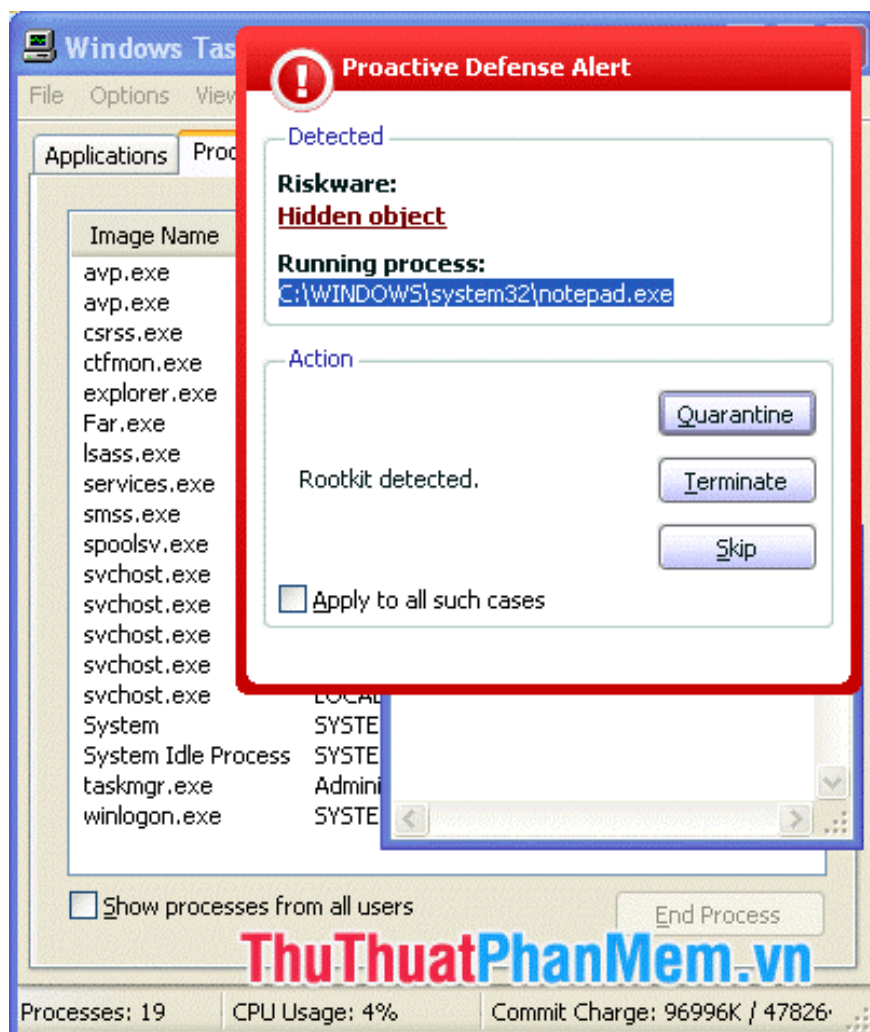
Spyware was born with the purpose of "spying" - hiding itself to steal information. Spyware usually spreads by attaching to Adware and users accidentally activate it when clicking on Adware or are attached to "pirated" programs, "cracked" software. Some popular Spyware models include Keylogger (recording keyboard input), Banking Trojan (stealing user banking information), Password stealer (collecting information about types, passwords) and Info stealers (steals login information, documents .).

9. Worm - Worm computer



Worm is widely spread thanks to the Internet and its intelligence. Worms can "corrode" the data on your computer and "sabotage" your computer to become more sluggish and even inoperable. Worms have been present for a long time but their sabotage is indisputable, including a few names like Melissa or ILOVEYOU that have caused tens of millions of computers to be infected and caused billions of dollars in damage. Worms can spread through the Internet environment with infected emails automatically sending copies of the Worm to other email addresses or via USB memory devices.

10. Rootkit

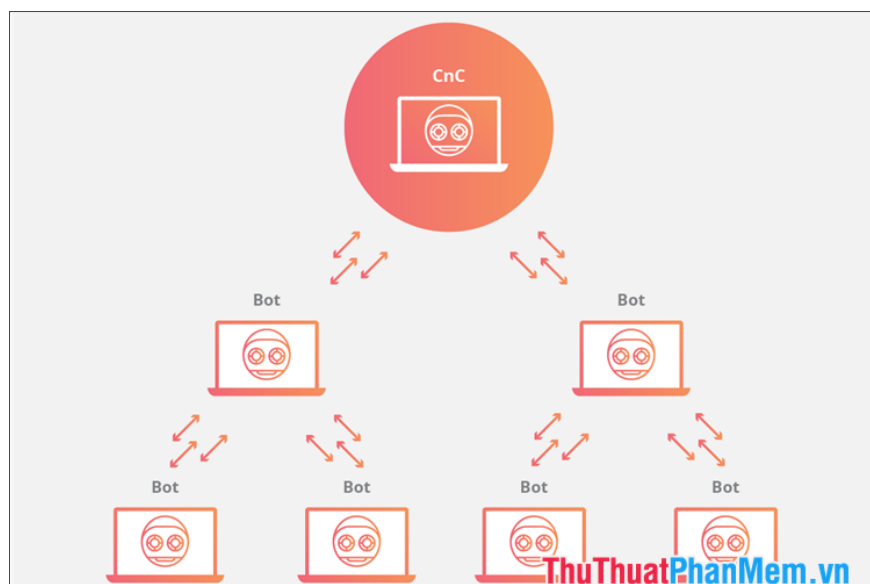


Basically, Rootkit is just a toolkit with the purpose of protecting other computer virus files on the system. Rootkits trick users by hiding into tools on the operating system such as the Registry and Task Manager, and they are often there to receive hacker commands to do things like open a backdoor, install spyware. (spyware). Rootkits are divided into two main types based on their activity level:

+ **Rootkit hides in normal applications:** With this operation, the rootkit can hide in Microsoft Office applications or utilities on Windows (Notepad, Paint .) to create some code snippets. fake to hide the true identity of other viruses operating on the computer such as Worm, Trojan Horse.

+ **Rootkit hides in the operating system kernel (Kernel):** The kernel is the kernel of the operating system with the task of managing system resources. When a rootkit works on a kernel, it can easily help a hacker control both the computer and be harder to detect. In addition, it can change and cause driver drivers to fail, making your computer more "abnormal".

11. Botnet



Botnets are known as "ghost networks" - where infected computers are connected and receive commands from a hacker 's server (temporarily called Botmaster). Computers that become botnets can be infected with various viruses such as trojans, spyware, rootkits, backdoors, etc. which are programmed by hackers to perform network attacks. Large numbers of botnets that are accessed from a website can overload the site and generate a denial of service (DDos) error.

With the sharing of common computer viruses in the article, readers are equipped with the basic knowledge about viruses and can protect themselves by being aware of their abnormal activities. Have a nice day!

You finished reading the article "**Common types of computer viruses**" 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.