What is Safe Malware? Why is it so dangerous?

Remote Access Trojan (RAT) is a type of malware that allows hackers to monitor and control the victim's computer or network.

Remote Access Trojan (RAT) is a type of malware that allows hackers to monitor and control the victim's computer or network. But how does RAT work, why do hackers use them and how do you avoid this malware? Let's find out with **TipsMake.com** through the following article!

Learn about SV - Malware remote access to computers

1. The RAT allows hackers to remotely access the victim's computer
2. SV works best when not being noticed
3. Don't worry because SV is easy to prevent!
4. Use antivirus software to find and destroy SV

The RAT allows hackers to remotely access the victim's computer

If you've ever had to call technical support for a PC, you might be familiar with the concept of remote access. When enabling remote access, authorized computers and servers can control everything that happens on your PC. Authorized computers can open documents, download software and even move the cursor on the screen in real time.

SV is a type of malware, very similar to legitimate remote access programs. Of course, the main difference is that the SV is installed on the computer without users knowing. Most legitimate remote access programs are implemented for technical support and file sharing, while RAT is created to spy on, hijack or destroy the computer.

Like most other malicious software, RAT is "hidden" under files that seem legitimate. Hackers can attach the RAT to documents in emails or in a large software package, such as video games. Ads and nefarious websites can also contain RAT, but most browsers feature automatic download compartments from websites or notify users when an unsafe website is detected.

Unlike some other malware and viruses, it can be difficult to know when you mistakenly downloaded the RAT to your computer. Generally, RATs do not slow down computers and hackers are not easy to detect by deleting files or rolling the cursor around the screen. In some cases, users have been infected with SV for many years without knowing it. But why is the SV capable of hiding so well? How useful are they for hackers?

SV works best when not being noticed

Most computer viruses are created with a single purpose. Keylogger automatically records everything you enter, ransomware restricts access to computers or files until you pay ransom and adware to put suspicious ads on your computer to make money.

But SV is very special. They give hackers total, anonymous control over infected computers. As you can imagine, a hacker in the RAT can do anything, as long as the goal is undoubted.

In most cases, SV is used as spyware. A "thirsty" hacker (or terrifying) can use the RAT to steal keystroke (the keystrokes you press on the keyboard, such as when entering a password) and files from the infected computer. Keystrokes and files can contain bank information, passwords, sensitive photos or private conversations. In addition, hackers can use the RAT to securely activate a webcam or microphone. Being watched by some anonymous guys is quite annoying, but it is nothing compared to what some hackers do through SV.

Because RAT provides hackers with admin access to infected computers, hackers can freely change or download any file. This means that a hacker in the RAT can wipe the hard drive, download illegal content from the Internet through the victim's computer or install additional malware. Hackers can also control remote computers to perform illegal online activities in the name of victims or use home networks as proxy servers to perform anonymous crimes.

A hacker can also use a SV to control home networks and create botnets. Basically, botnets allow hackers to use computer resources for super strange (and often illegal) tasks, such as DDOS attacks, bitcoin digging, file storage and torrenting. Sometimes, this technique is used by hackers for the sake of cybercrime and creating cyberwar. A botnet of thousands of computers can create a lot of Bitcoin or destroy large networks (or even a country) through DDOS attacks.

Don't worry because SV is easy to prevent!

If you want to avoid RAT, don't download files from sources you don't trust. You should not open email attachments from strangers, you should not download games or software from funny websites or torrent files unless they come from a trusted source. Always update your browser and operating system with security patches.

Of course, you should also activate antivirus software. Windows Defender built into the PC is really a great antivirus software, but if you feel you need some additional security measures, you can download a commercial antivirus software like Kaspersky or Malwarebytes. .

Use antivirus software to find and destroy SV

It is likely that the computer is not infected with SV. If you haven't noticed any weird activity on your computer or haven't been stolen recently, you may still be safe. But check your computer regularly to make sure your system is not infected with SV.

Since most hackers use well-known RATs (instead of self-development), anti-virus software is the best (and easiest) way to find and remove RAT from your computer. Kaspersky or Malwarebytes has a large and constantly growing SV database, so you don't need to worry about obsolete antivirus software.

If you have already run an antivirus program, but still worry that the RAT may still be on your PC, reformat the computer. This is a drastic measure but has a 100% success rate, completely eliminating malware that may have been ingrained in the computer's UEFI firmware. New undetected RAT malware by antivirus software takes a lot of time to create and they are often intended to 'cope' with large corporations, celebrities, government officials and wealthy people. If the antivirus software does not find any RAT, then your system is probably still very safe.