# 107 new rootkit lines appeared in Vietnam within 30 days

The software that hackers use as a 'shield' for the existence of viruses, Trojans, spyware, adware on victims' computers appeared more than half a month ago in April. According to the BKIS Center, of these, over 80% are rootkits

**Software that hackers use as a "shield" for the existence of viruses, Trojans, spyware, and adware on victims' computers appears more than half a month ago in April. According to the BKIS Center, of these, over 80% are online game rootkits.**

Rootkits in online games are "shields" that block malicious code that runs on this environment with stealing passwords and gamer account information. When the online game virus "raises" the computer, it will "extract" the rootkit so that they can interfere with Ring 0 operating system (the lowest level of the system) and thereby hide the virus destructive processes. . They also hide files, registry code of the attack code.

This technique helps computer worms "bypass" most of the methods of manual testing such as checking by Task Manager, Registry Editor, MsConfig, Services .


" *In order to prevent rootkits, users need to use the latest anti-virus software to keep up to date with the latest identities. It is not recommended to handle rootkits themselves, but requires direct support from the expert. Control the system, if manually processed, it can make the operating system corrupted and lose data* ", Mr. Vu Ngoc Son, expert of BKIS recommended.

Computers with viruses but clean software that cannot be "scanned" are very popular phenomenon recently. According to the BKIS Center, there are two main reasons for this phenomenon.

First of all, the user has not updated to the latest version of the kill, so the malware identification forms are incomplete and undetectable. This situation often falls into the case of using non-copyrighted anti-virus software, the identity pattern is not automatically updated. The solution is to update to the latest version or use the copyright program.

Besides, when the computer is infected with a new virus and it has some behavior similar to the old worm that anti-software has updated. Therefore the virus will be detected. However, at that time, although new viruses were detected, the software could not kill new intruders because it was still waiting for the correct identification. As a result, users will constantly see warnings about viruses but they have not been destroyed. To resolve this case, just notify the antivirus software manufacturer to have the sampling, analysis, and update expert update to the latest version, the problem will be thoroughly handled.