If infected with this new virus, your chances of data recovery are 0%

If nCoV-infected patients still have a high chance of being cured, then the computer system infected with this new virus is almost unable to recover data.

Recently, the world has been buzzing about the new strain of Corona virus that causes pneumonia (nCoV - 2019) originating from Wuhan city, China, and still happening very complicatedly in many countries. and different territories. Coincidentally, the field of carrier security has also recorded the emergence of a new extremely dangerous computer virus. If nCoV-infected patients still have a high chance of being cured, then the computer system infected with this new virus is almost unable to recover data.

Computer viruses and worms were once common malicious agents for a while, but now make way for more sophisticated and diverse threats, including real-world cryptocurrency mining tools. Legal, Trojans, ransomware and sophisticated monitoring software designed to infiltrate mobile devices.

However, when the virus reappears, it will be extremely scary. This is true for KBOT, a new virus discovered by researchers from the Kaspersky team.

KBOT can be spread via Internet access systems, local area networks and removable hard drives. When a system is infected, the virus will write itself to the Startup and Task Scheduler, spreading to all .exe files on the system and shared network folders in its path.

During a scan of the system's drives, the virus attaches polymorphic code to the .exe files and the override function of the IWbemObjectSink interface, a basic feature of the Win32 application. In addition, KBOT can also identify all connections between drives and use the NetServerEnum and NetShareEnum API functions to access links to other network resources to spread malware.

More dangerous, KBOT uses a variety of sophisticated tools and techniques to conceal its operations, including RC4 chain encryption, scanning antivirus software-related DLLs to disable them and inject code. into valid running processes.

Not only does it interfere with the .exe files, the malware tries to steal the victim's personal data, which may include the login information used to access financial services and online banking. gland. Using fake websites is KBOT's preferred method and to do so, the virus interferes with the browser code, as well as the code of the system functions that handle traffic.

Of course, before stealing the victim's data, the virus will have to establish a link to its command and control server (C2), in which the associated domain names are stored in hosts.ini. The configuration and connection parameters C2 are encrypted and will send bot IDs, computer names, operating systems and local user data lists as well as security software that they have installed on the system.

C2 commands include deleting and updating files, instructions for updating bot modules, or performing self-destruction. In addition, KBOT can also download additional malware modules that collect user data including login information, files, system information and data related to cryptocurrency wallets.

With all the above characteristics, KBOT is considered a new extremely dangerous computer virus. Global cybersecurity experts are closely monitoring malicious code and response plans will be launched soon.