Hackers break into chats on Microsoft Teams to spread malware

International security researchers have just warned about a relatively new form of attack related to the traditional enterprise application platform Microsoft Teams.

International security researchers have just warned about a relatively new form of attack related to the Microsoft Teams enterprise communication application platform. In it, the hacker will try to break into the target's Microsoft Teams account, then access the chats and distribute the malicious executable file targeting the participants in that chat.

More than 270 million people are interacting on Microsoft Teams every month, from millions of organizations and businesses around the world. Most of them completely trust this application, but in fact Microsoft Teams currently does not have an effective measure against malicious files spreading on the platform.

Simple but effective form of malware distribution

Researchers at Avanan, a security company that primarily targets cloud email and collaboration platforms, were the first to detect this form of malware distribution targeting Microsoft Teams users.

The attacks appear to have begun in January. In it, hackers insert into the chat they successfully break into an executable file named 'User Centric' to convince and fool other members to launch it.

After the program is executed, the malware writes data to the system registry, then installs DLL files and establishes its stability on the infected Windows computer.

The method used by the hacker to gain access to the victim's Teams account is still unclear. But some possible possibilities include stealing email or Microsoft 365 credentials through phishing, or breaching a partner organization.

Analysis of malware distributed in this way shows that the trojan can establish persistence on the target system through Windows Registry Run keys, or by creating an entry in the startup directory. .

At the same time, the malware also collects detailed information about the operating system and the hardware it runs on, along with the security status of the machine based on the operating system version and installed patches.

Although the overall attack process is quite simple, the actual effectiveness is high because the common mentality of many Microsoft Teams users today is to completely trust the files that their colleagues share, researchers say. by Avanan said.

The company analyzed data from several hospitals that use Teams, and found that doctors often use the platform to share medical information unrestricted. In addition, impersonation on Microsoft Teams is also a big problem.

Researchers say the problem is exacerbated by 'the fact that Microsoft Teams is lacking default protections, as scanning for malicious links and files is limited' and 'multiple security solutions' email security does not provide strong protection for Teams'.

To 'defence' against such attacks, Avanan recommends the following:

1. Implement measures to scan downloads to detect malicious content early
2. Deploy comprehensive, powerful security for the system.
3. Encourage end users to contact IT when suspicious files are distributed on the system