Activity

Chat

Teams

Calendar

Calls

Hackers are spreading Trojan malware in Teams chats

Cybercriminals are abusing Microsoft Teams by attaching malicious executables to the conversations, in an attempt to spread them among participants. At present, Microsoft Teams has around 270 million monthly active users which makes it a lucrative target. Researchers from Avanan discovered thousands of attacks against Microsoft Teams accounts since January. Hackers obtain access to Teams accounts by spoofing a user with East-West attacks via malicious emails or using credentials collected from some other phishing attacks. They log in to these accounts and insert an executable file ‘User Centric.exe’ inside a chat to dupe participants into opening it. When executed, the malicious code installs DLL files and creates shortcut links to self-administer.

The Possible attack scenarios:

- In one scenario, the attackers may launch the attack by targeting a partner organization and listening in on inter-organizational chats.

- In another possibility, they may compromise an email address to access Teams.

- Attackers may use Office 365 credentials stolen from previous attacks.

Hackers are spreadin...

Search in Document

Home Insert Draw Design Layout References Mailings Review Share

Paste

Cyscom 20

Styles Styles Pane

THE SAFETY TIPS:

The use of Microsoft Teams as an infection vector is concerning because some users may have no knowledge regarding it. Experts recommend using extra layers of security such as downloading and inspecting the suspected files in a sandbox first. Additionally, organizations should deploy email gateway security that secures communication applications, and employees should contact IT whenever a suspicious file is observed.

Page 3 of 3 221 words Focus 118%