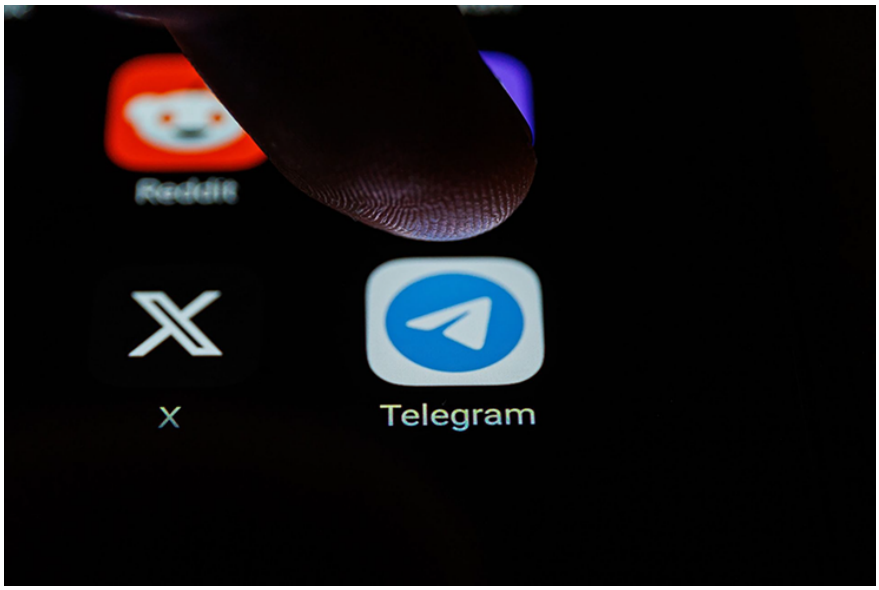
Malware that specializes in eavesdropping and sabotage is discovered hiding on Telegram

New Golang malware is using Telegram as a 'lever' to spread itself everywhere.

A new cybersecurity threat has just been discovered by experts, using the popular messaging app Telegram as a "base" to carry out destructive acts. This Golang malware not only has the ability to eavesdrop, but can also spread itself and execute many other dangerous commands.

Researchers from Netskope have discovered a backdoor built in the Golang programming language. Notably, this backdoor uses Telegram as a command and control (C2) station. Instead of using complex servers, the attackers leverage Telegram to send commands and receive information from the backdoor.



Telegram is the "base" of Golang malware to carry out destructive acts.

Specifically, this backdoor creates a Telegram bot via Botfather, then uses this bot to continuously listen for commands sent from a Telegram chat. Before performing any action, the backdoor checks the validity of the command.

The use of Telegram as a C2 channel makes it extremely difficult to detect and block this backdoor. It is difficult for security experts to differentiate between malicious and normal information flows on Telegram.

'While using cloud applications as a C2 channel is not something we see every day, it is a very effective method used by attackers not only because it does not require deploying an entire infrastructure for it, making the attacker's life easier, but also because it is very difficult, from a defense perspective, to differentiate between

what is a normal user using the API and what is C2 communication,' Netskope said.

In addition to Telegram, threat actors often use other cloud services such as OneDrive, GitHub, Dropbox, etc. to carry out attacks. Netskope did not disclose the number of potential victims, but emphasized that this malware is most likely of Russian origin.

The emergence of this Golang backdoor is a warning about the potential risks from familiar applications. Users need to be vigilant, update security software regularly, and not open suspicious links or files.