Warning: New DISGOMOJI malware uses Discord emoji to steal data!

First discovered by security research firm Volexity, DISGOMOJI malware can use Discord emoji to execute commands on infected devices.

What is DISGOMOJI malware?

Volexity discovered the DISGOMOJI malware in June 2024, linking it to a Pakistan-based group tracked as UTA0137.

The malware targets Linux devices using the BOSS distribution, mainly used by Indian government agencies. However, it could theoretically be used against any Linux distribution and written in the adaptable Golang programming language.

However, the most interesting part of DISCOMOJI is the use of Discord emoji to control infected devices. Instead of sending verbal commands like you see with most malware, DISCOMOJI operators can send specific Discord emojis to perform actions.

How does this emoji-controlled malware work?

First, malware must be installed for the attacker to gain control of the target device. The target device is sent a fake document containing a malicious file, which when executed, downloads the DISCOMOJI malware. Upon launch, DISCOMOJI steals data from the target machine, such as local information, usernames, hostnames, malware installation folders, and data from any connected USB devices.

The malware then connects to a Discord server controlled by the attacker, calling back to wait for new instructions. The attackers used something called discord-c2, an open source command and control project that uses Discord as a control point for infected devices. Once the malware connects to the Discord server, the attacker can use multiple emojis to prompt the malware, with a range of different parameters available.

The Discord emojis used by this malware are summarized below:

emoji	Emoji name	Command description