Vultur banking malware reappears with many dangerous features

Recently, NCC Group researchers discovered a new version of Vultur banking malware, allowing crooks to remotely interact with phones and collect sensitive data.

Researcher Joshua Kamp (NCC Group), said: 'Vultur has encrypted communication information between the control server (C2 server) and infected devices, impersonating legitimate applications to perform many harmful actions'.

When communication between the control server and the victim's device is encrypted, the transmitted data becomes harder for security systems to read and analyze, making it difficult to detect and prevent malicious activities. harm becomes more difficult.

What is Vultur banking malware?

Vultur is one of the first Android banking malware families with screen recording capabilities, primarily targeting banking applications to record keystrokes and remote controls. Vultur was first discovered by ThreatFabric in late March 2021.

This malware was observed to be distributed through trojanized droppers on Google Play, masquerading as authenticator apps and productivity apps to trick users into installing them.

As observed by NCC Group, dropper applications use a combination of SMS messages and phone calls to spread malware. Once installed by the user, the dropper will execute 3 related payloads (2 APKs and 1 DEX file) register the bot with the C2 server, obtain accessibility service permissions for remote access via AlphaVNC, and ngrok, while also running commands fetched from the C2 server.

One of Vultur's new features is the ability to remotely interact with an infected device, including performing clicks, scrolls, and swipes through Android accessibility services, as well as downloading, uploading, and swiping. delete, install and find files.

Additionally, the malware prevents victims from interacting with a predefined list of apps, displays custom notifications in the status bar, and even disables Keyguard to bypass screen security measures. lock up.

Vultur improves remote control

Kamp said: 'Vultur's recent developments have demonstrated a shift in focus towards maximizing remote control of infected devices. With the ability to dictate scrolling, swiping, clicking, controlling volume, blocking app launches, and even incorporating file management functionality, it's clear that the main goal is to gain full control over compromised devices. '

This development comes as Team Cymru revealed the transition of Android banking trojan Octo (also known as Coper) to operating as a service, providing malware for other threat actors to conduct. information theft.

'This malware offers many advanced features, including keystroke logging, blocking SMS messages and push notifications, and controlling the device's screen,' the company said.

Octo's campaigns are estimated to have compromised 45,000 devices, mainly spread across Portugal, Spain, Türkiye and the United States. Some other victims were in France, the Netherlands, Canada, India and Japan.

Broadcom-owned Symantec said in a news release that the malware 'targets stealing banking information, SMS messages and other confidential information from victims' devices'.