SpyNote malware spies on Android users steals banking credentials

Hackers are increasingly using a new variant of SpyNote malware to secretly observe and modify infected Android smartphones, according to research published by ThreatFabric on Monday.

SpyNote is a “powerful” spyware family designed to monitor, manage, and modify a device. Its most recent sample, SpyNote.C, has been the first variant to openly target online banking applications, according to ThreatFabric.

The Android spyware is one of the most common malware used by hackers to track a user’s location, steal sensitive information, such as passwords and credit card numbers, record phone calls, intercept SMS messages and remotely manage a device.

Hackers distribute spyware through fake mobile apps which infect Android smartphones with SpyNote.

The malware’s new variant impersonates the apps of “reputable financial institutions” like HSBC, Deutsche Bank, Kotak Bank, and BurlaNubank to exfiltrate the personal data of their customers.

This malware also disguises itself as well-known mobile apps like WhatsApp, Facebook, and Google Play, as well as more generic apps such as wallpaper apps, productivity apps, or gaming apps.

The use of SpyNote.C increased significantly in the last quarter of 2022, according to ThreatFabric. Hackers used a Telegram channel to sell a spyware under the name CypherRat.

At least 80 people purchased CypherRat with cryptocurrency between August 2021 and October 2022.

In October 2022, CypherRat’s code became public on GitHub after a leak and several fraud incidents on hacker forums, when threat actors impersonated the real CypherRat developers to steal money from other criminals.

Since the release of the source code, there’s been a drastic increase in the number of SpyNote attacks, particularly focusing on online banking applications. Malware developers have shifted their focus to a new spyware project, CraxsRat — a paid app with similar capabilities as CypherRat.

SpyNote.C can track SMS messages, calls, videos, and audio recordings, as well as update and install new apps on a user’s device. Without any user input, SpyNote can click on the “install” and “update” buttons, according to ThreatFabric.

One of the malware’s most dangerous capabilities allows hackers to access a device’s camera and send videos right to their server. With complete control over the device’s camera, the attacker can spy on the user with it.

SpyNote can also obtain two-factor authentication codes by exploiting the Google Authenticator app without the user’s knowledge. SpyNote can also steal social app credentials by tricking users into entering a password, email address, or username on a fake banking app login page.

Researchers predict that hackers will keep using SpyNote to collect essential data. It is also very likely that different forks of SpyNote will continue appearing, following the release of its source code, according to ThreatFabric.