New Octo Banking Trojan Spreading via Fake Apps on Google Play Store

thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html

April 7, 2022

A number of rogue Android apps that have been cumulatively installed from the official Google Play Store more than 50,000 times are being used to target banks and other financial entities.

The rental banking trojan, dubbed **Octo**, is said to be a rebrand of another Android malware called ExobotCompact, which, in turn, is a "lite" replacement for its Exobot predecessor, Dutch mobile security firm ThreatFabric said in a report shared with The Hacker News.

Exobot is also likely said to have paved the way for a separate descendant called Coper, that was initially discovered targeting Colombian users around July 2021, with newer infections targeting Android users in different European Countries.

"Coper malware apps are modular in design and include a multi-stage infection method and many defensive tactics to survive removal attempts," Cybersecurity company Cyble noted in an analysis of the malware last month.

Like other Android banking trojans, the rogue apps are nothing more than droppers, whose primary function is to deploy the malicious payload embedded within them. The list of Octo and Coper droppers used by multiple threat actors is below -

- Pocket Screencaster (com.moh.screen)
- Fast Cleaner 2021 (vizeeva.fast.cleaner)
- Play Store (com.restthe71)
- Postbank Security (com.carbuildz)
- Pocket Screencaster (com.cutthousandjs)
- BAWAG PSK Security (com.frontwonder2), and
- Play Store app install (com.theseeye5)

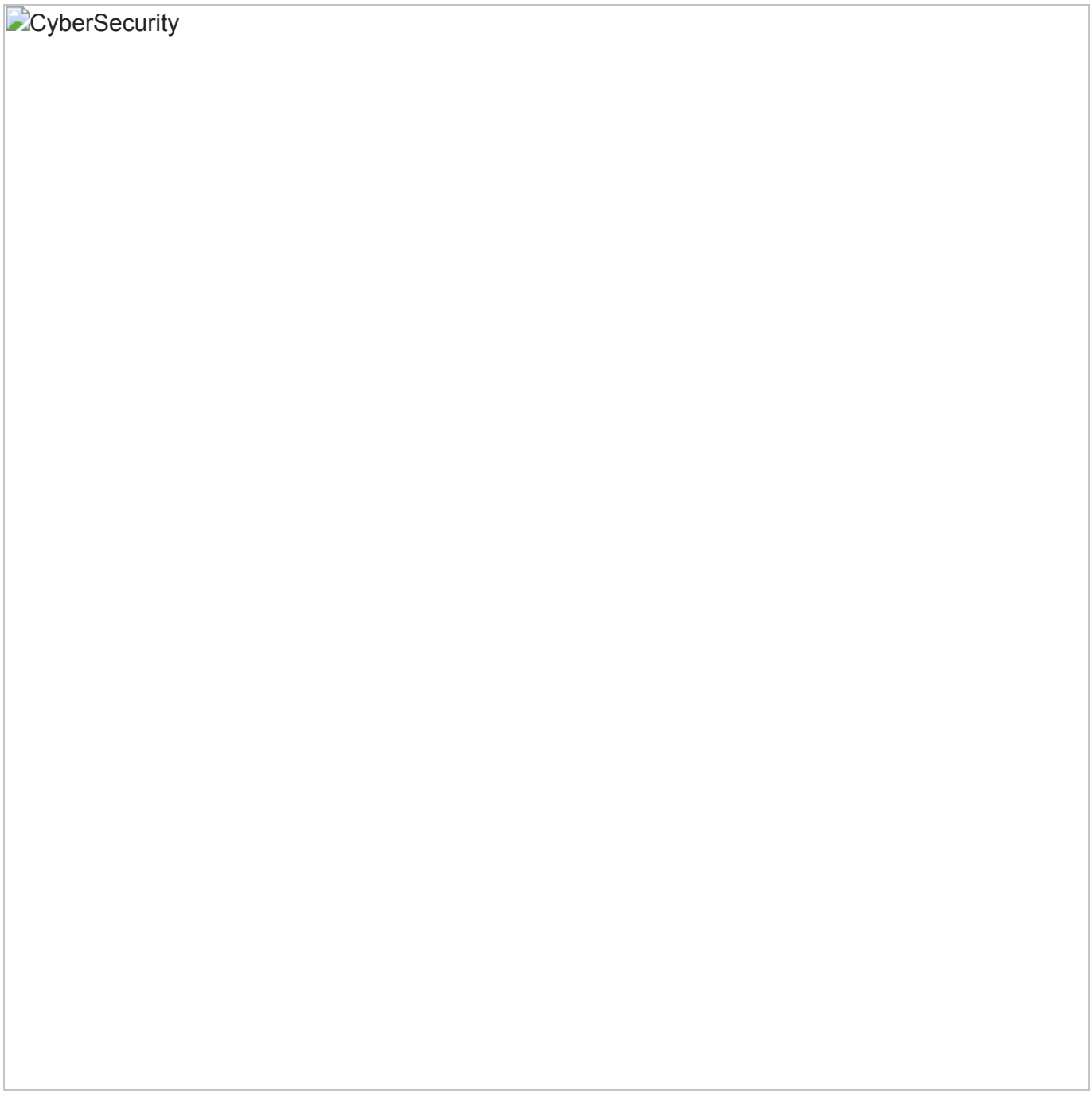
These apps, which pose as Play Store app installer, screen recording, and financial apps, are "powered by inventive distribution schemes," distributing them through the Google Play store and via fraudulent landing pages that purportedly alert users to download a browser update.

The droppers, once installed, act as a conduit to launch the trojans, but not before requesting users to enable the Accessibility Services that allow it a wide breadth of capabilities to exfiltrate sensitive information from the compromised phones.

Octo, the revised version of ExobotCompact, is also equipped to perform on-device fraud by gaining remote control over the devices by taking advantage of the accessibility permissions as well as Android's MediaProjection API to capture screen contents in real-time.

The ultimate goal, ThreatFabric said, is to trigger the "automatic initiation of fraudulent transactions and its authorization without manual efforts from the operator, thus allowing fraud on a significantly larger scale."

Other notable features of Octo include logging keystrokes, carrying out overlay attacks on banking apps to capture credentials, harvesting contact information, and persistence measures to prevent uninstallation and evade antivirus engines.



"Rebranding to Octo erases previous ties to the Exobot source code leak, inviting multiple threat actors looking for opportunity to rent an allegedly new and original trojan," ThreatFabric noted.

"Its capabilities put at risk not only explicitly targeted applications that are targeted by overlay attack, but any application installed on the infected device as ExobotCompact/Octo is able to read content of any app displayed on the screen and provide the actor with sufficient information to remotely interact with it and perform on-device fraud (ODF)."

The findings come close on the heels of the discovery of a distinct Android bankbot named GodFather — sharing overlaps with the Cereberus and Medusa banking trojans — that has been observed targeting banking users in Europe under the guise of the default Settings app to transfer funds and steal SMS messages, among others.

On top of that, a new analysis published by AppCensus found 11 apps with more than 46 million installations that were implanted with a third-party SDK named Coelib that made it possible to capture clipboard content, GPS data, email addresses, phone numbers, and even the user's modem router MAC address and network SSID.

SHARE □ □ □ □ □
SHARE □