Cerberus Enters the Android Malware Rental Scene

By Tara Seals

Published: 2019-08-13 · Archived: 2026-04-05 15:56:21 UTC

The mobile banking trojan has a few unusual features and bears watching, researchers said.

A never-before-seen Android banking trojan, dubbed Cerberus, is being rented out on underground forums by a threat group that likes to engage with the defense community publicly via Twitter.

According to a Tuesday posting from ThreatFabric, Cerberus isn't based on the leaked Anubis source code that underpins many new trojans on the market. Its authors claim that it's completely bespoke, with no code re-use, and it comes with infrastructure support. That offers an important differentiator, according to the researchers, given that the Android banking trojan market is in a transition phase.

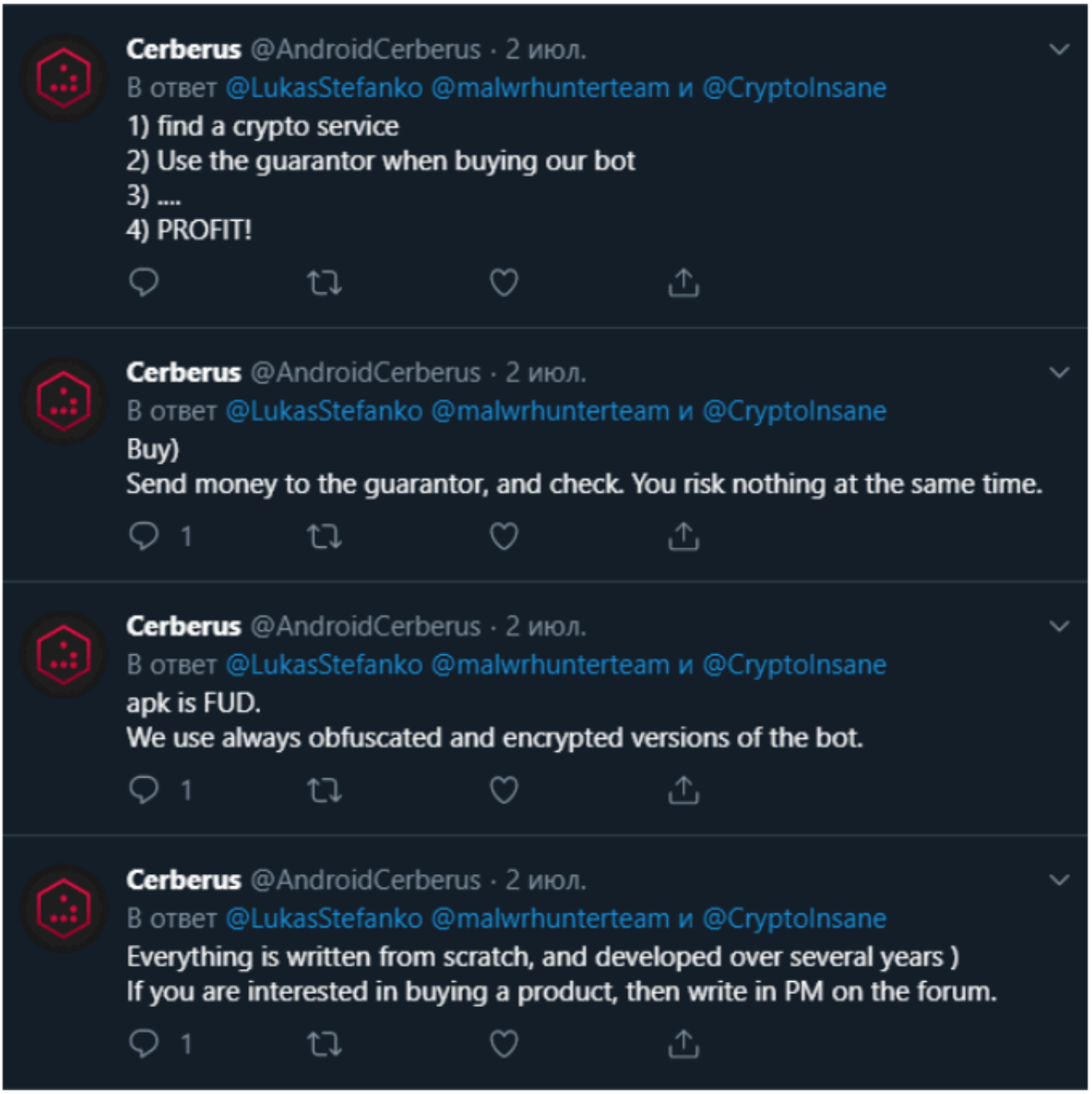
"After the actor behind [the previously dominant] RedAlert 2 [trojan] decided to quit the rental business, we observed a surge in Anubis samples in the wild. After the Anubis actor was allegedly arrested and the source code was leaked there was also huge increase in the number of Anubis samples found in the wild, but the new actors using Anubis have no support or updates. Due to this, Cerberus will come in handy for actors that want to focus on performing fraud without having to develop and maintain a botnet and command-and-control (C2) infrastructure."

Cerberus sets itself apart in a couple of ways. For one, it uses an interesting method to determine that it's not running in a sandbox environment: It uses the device's accelerometer sensor to measure movements of the victim with a pedometer function; researchers said that it uses the step-counter to activate the bot once it hits a preconfigured threshold.

It also has an unusually small list of mobile apps for which it's set up to do overlay attacks. It obtains the package name of the foreground application and determines whether or not to show a phishing overlay window to harvest credit-card information, banking credentials, email credentials and so on. So far, it only works with seven French banking apps and seven U.S. banking apps; one Japanese banking app; and 15 non-banking apps, according to the analysis.

"This uncommon target list might either be the result of specific customer demand, or due to some actors having partially reused an existing target list," the researchers said.

The other unusual thing about Cerberus is the behavior of its authors.



“One peculiar thing about the actor group behind this banking malware is that they have an ‘official’ Twitter account that they use to post promotional content (even videos) about the malware,” ThreatFabric researchers wrote. “Oddly enough, they also use it to make fun of the AV community, sharing detection screenshots from VirusTotal (thus leaking IoC) and even engaging in discussions with malware researchers directly.”

Otherwise, the trojan has standard features, the researchers noted, such as SMS control, contact-list harvesting and keylogging to broaden the attack scope; it lacks advanced features such as a back-connect proxy, media streaming and remote access control.

It sets itself up by requesting accessibility permission.

“After the user grants the requested privilege, Cerberus starts to abuse it by granting itself additional permissions, such as permissions needed to send messages and make calls, without requiring any user interaction,” according to

ThreatFabric. “It also disables Play Protect (Google’s preinstalled antivirus solution) to prevent its discovery and deletion in the future. After conveniently granting itself additional privileges and securing its persistence on the device, Cerberus registers the infected device in the botnet and waits for commands from the C2 server while also being ready to perform overlay attacks.”

The malware-as-a-service market is ripe for Cerberus, the researchers wrote.

“The lifespan of many well-known rented Android bankers is usually no more than one or two years,” they said. “When the family ceases to exist a new one is already available to fill the void, proving that the demand for such malware is always present and that therefore Cerberus has a good chance to survive.”

While it’s still immature, Cerberus “should not be taken lightly,” the researchers said.

“In addition to the feature base it already possesses and the money that can be made from the rental, it could evolve to compete with the mightiest Android banking trojans,” according to the analysis. “Next to the features, we expect the target list to be expanded to contain additional (banking) apps in the near future.”

Black Hat USA and DEF CON 2019 just wrapped up in Las Vegas. For all of Threatpost’s stories, podcasts and videos from Black Hat and DEF CON, click here.
