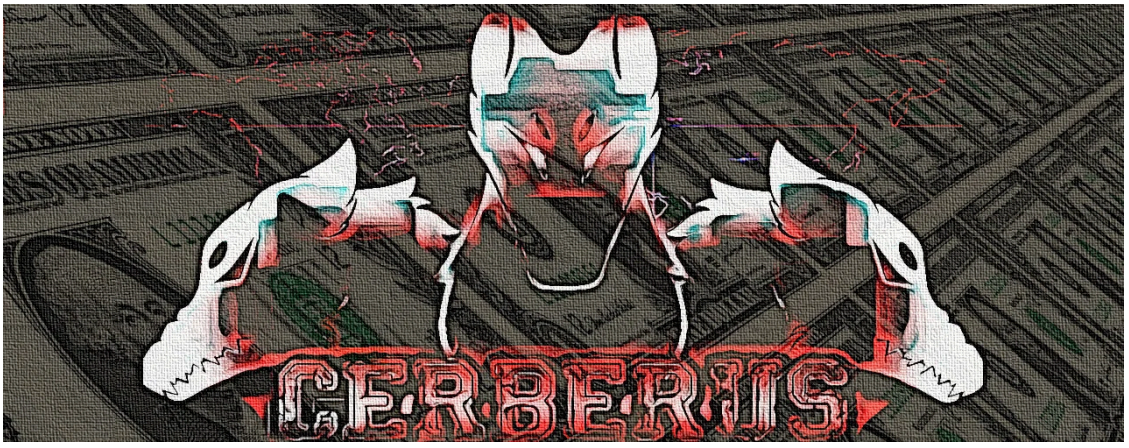
Cerberus Android malware source code offered for sale for $100,000

By Ionut Ilascu

Published: 2020-07-27 · Archived: 2026-04-05 12:42:37 UTC



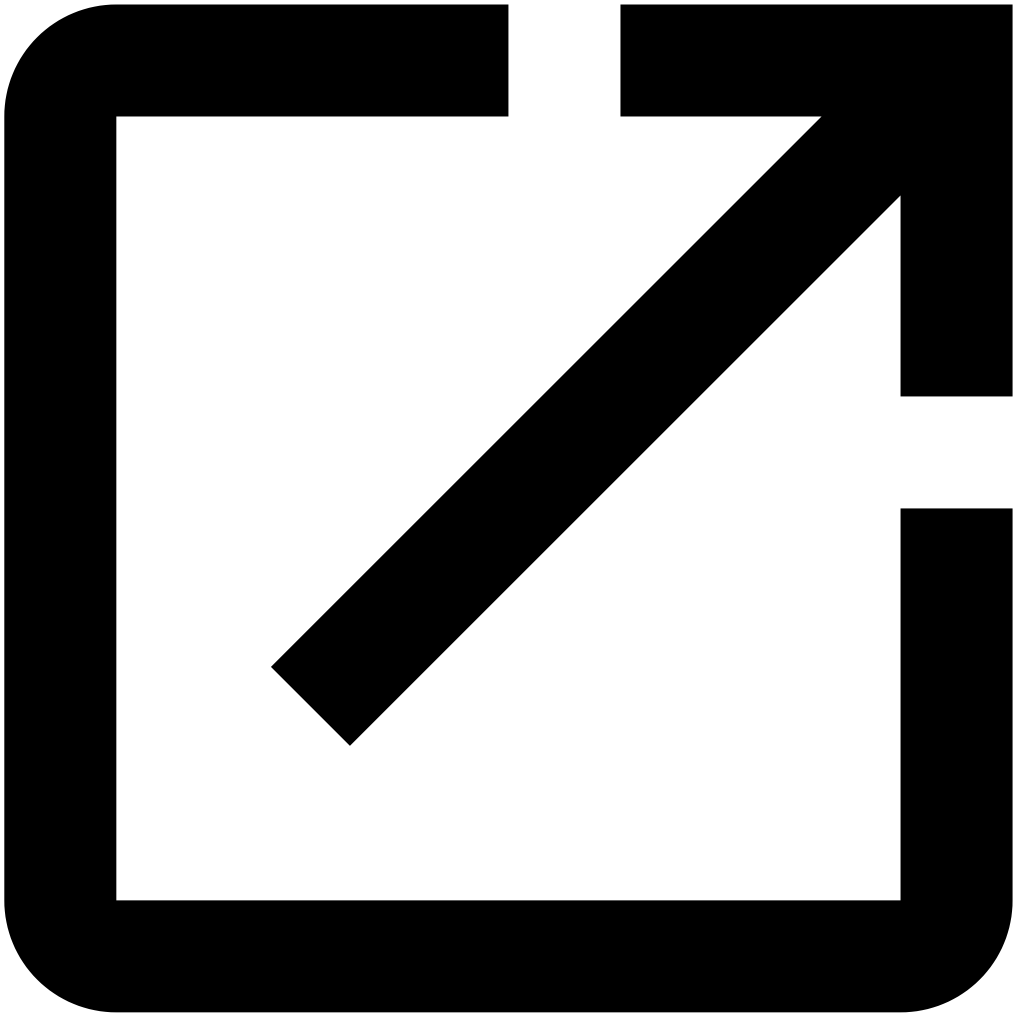
The maintainer of Cerberus banking trojan for Android is auctioning the entire project for a price starting at $50,000 or close the deal for double the money.

The price includes everything from source code to customer list along with installation guide and the scripts to make components work together.

Profit potential

For at least one year, the group behind Cerberus advertised their business and rented the malicious bot for up to $12,000 per year. They also offered a license for shorter periods ($4,000/3 months, $7,000/6 months).


DIE LINKE.
0:00



According to a post from the seller on a Russian-speaking underground forum, the business is currently generating $10,000 every month.

Striking a deal with Cerberus maintainer would get the buyer the source code for the malicious APK as well as the module, the admin panel, and the servers.

Motivating that the Cerberus crew split up and they no longer have the time to 24/7 support, the seller is getting rid of everything, including the customer base with an active license, contacts for customers and potential buyers.

Alon Gal, CTO of cybercrime intelligence firm Hudson Rock, told BleepingComputer that a price tag of $100,000 for a piece of malware like Cerberus is likely to attract sophisticated threat actors with capabilities to maintain and improve the project.

Cerberus has been analyzed by malware researchers at ThreatFabric, who found that it was not a clone of Anubis banker, whose source code got leaked in 2019.

The malware stands on its code that can detect movement of the infected device to determine a real system and avoid running in a sandbox environment.

Cerberus bot has extensive functionality, being able to spoof notifications from the banking service present on the device to prompt the victim to type in login credentials, and steal two-factor authentication codes, run any installed apps.

The seller included in their thread a post from the summer of 2019 showing all the capabilities available in Cerberus:

The malware has been heavily promoted on public channels and is well-known in cybercriminal communities. When the actors behind it started renting it, they claimed it had been used privately for two years.

It emerged in a time when Anubis-based bankers were very common and stood out as a more reliable alternative for collecting banking credentials.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
