

# Cerberus banking Trojan source code released for free to cyberattackers

By Written by

Archived: 2026-04-05 17:04:06 UTC

The source code of the Cerberus banking Trojan has been released as free malware on underground hacking forums following a failed auction.

## Security

- 
- 
- 
- 

Speaking at Kaspersky NEXT 2020 on Wednesday, Kaspersky cybersecurity researcher Dmitry Galov said that the leaked code, distributed under the name Cerberus v2, presents an increased threat for smartphone users and the banking sector at large.

Cerberus is a mobile banking Trojan designed for the Google Android operating system. In circulation since at least July 2019, the Remote Access Trojan (RAT) is able to conduct covert surveillance, intercept communication, tamper with device functionality, and steal data including banking credentials by creating overlays on existing banking, retail, and social networking apps.

The malware is able to read text messages that may contain one-time passcodes (OTP) and two-factor authentication (2FA) codes, thereby bypassing typical 2FA account protections. OTPs generated through Google Authenticator may also be stolen.

**CNET:** [Razer leak exposes thousands of customers' private data](#)

In early July, Avast researchers discovered [Cerberus in Google Play](#), wrapped up and disguised as a legitimate currency converter. It is thought that when the application was submitted to Google for approval, the functions were innocent and legitimate -- but once a large user base was established, an update package deployed the Trojan on victim devices.

Later in the same month, Hudson Rock spotted Cerberus [going to auction](#). An advert was posted by the maintainer of the malware, revealing that the development team was breaking up, and so a new owner was being sought.

The operator set a starting price of \$50,000 -- with the aim of generating up to \$100,000 -- for the malware's .APK source code, client list, servers, and code for administrator panels. The auctioneer claimed that Cerberus generated \$10,000 in revenue per month.

However, it seems there were no takers.

**TechRepublic:** [Cyberattacks against schools are on the rise](#)

"Despite Cerberus' Russian speaking developers earmarking a new vision for the project in April this year, auctions for the source code began in late July due to the breakup of the development team," Kaspersky says.

"Due to an unclear culmination of factors, the author later decided to publish the project source code for premium users on a popular Russian-speaking underground forum."

The cybersecurity firm says that following the free release of Cerberus source code in the underground, there was an "immediate rise" in mobile app infections across Europe and Russia. Of particular note, Galov says, is that previous clients were not encouraged to strike Russian mobile device users -- but the moment the code was released, the attack landscape changed.

When Cerberus was offered as Malware-as-a-Service (MaaS), the scope of the threat was contained to attack groups able to pay for the code, on subscription from \$4,000 for one month to \$12,000 for a year. Now the developer has washed their hands of the project and released the source code for free, we may not only see rising adoption of Cerberus, but also potentially new variants based on the leaked code in the future.

**See also:** [Your email threads are now being hijacked by the QBot Trojan](#)

"We continue to investigate all found artifacts associated with the code, and will track related activity," Galov commented. "But, in the meantime, the best form of defense that users can adopt involves aspects of security hygiene that they should be practicing already across their mobile devices and banking security."

**The worst IoT, smart home hacks of 2020 (so far)**

### Previous and related coverage

- [Cerberus banking Trojan infiltrates Google Play](#)
- [Cerberus banking Trojan team breaks up, source code goes to auction](#)
- [Android malware can steal Google Authenticator 2FA codes](#)

---

**Have a tip?** Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

---

---

Source: <https://www.zdnet.com/article/cerberus-banking-trojan-source-code-released-for-free-to-cyberattackers/>