Attacks Using Cerberus Banking Trojan Surge

By Chinmay Rautmare

Account Takeover Fraud , Cybercrime , Fraud Management & Cybercrime

Release of Code on Russian Darknet Forums Leads to Broader Use, Enhancements (@crautmare) • September 18, 2020

The code for the Cerberus banking Trojan, named after the mythical three-headed beast, was posted on darknet forums.

The posting on Russian underground forums of source code for the Android mobile banking Trojan Cerberus has led to an increase in attacks as well as updates to the malware, the security firm Kaspersky reports.

See Also: OnDemand | Transform API Security with Unmatched Discovery and Defense

"We're already seeing an increase in attacks on users since the source code was published," Kaspesky states. "It's not the first time we've seen something like this happen, but this boom of activity since the developers abandoned the project is the biggest developing story we've tracked for a while."

The researchers note that Cerberus' source code was made available for free to premium members of certain Russian darknet forums. Previously, the Trojan was available as a malware-as-a-service tool.

In July the malware's development team had a falling out and opted to auction off the source code, Kaspersky notes. "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 report says.

Kaspersky dubbed the free version Cerberus v2.

Code Analysis

The posting of the source code has led to a surge in attempts steal money from Russian and European consumers as additional threat actors have taken advantage of the free malware, Kaspersky says. Another result has been the enhancement of the Trojan's capabilities.

The malware has been upgraded to stealthily send and steal SMS codes as well as use a bank's website as an overlay to hide malicious domains and steal credentials. Kaspersky found the malware can read text messages that use one-time passwords and steal two-factor authentication passcodes - even those using Google Authenticator.

"Additional capabilities include accessing customer credit card and contact details, the ability to redirect calls or tamper with mobile functionality via its [remote access Trojan] features and to automatically grant required permissions as part of its authentication attributes," the report says.

In June, the FBI warned that fraudsters are increasingly using Trojans to target banking customers and disguising the malware as legitimate apps, games or other tools (see: *FBI Warns Of Increasing Use of Trojans in Banking Apps*).

The bank website overlay is activated when a mobile banking customer launches their banking app. This triggers the Trojan and prompts a fake login page that overlays the legitimate app to entice the user to provide their login information, according to the FBI.

History of Cerberus

Researchers discovered Cerberus in the summer of 2019. In July, Avast uncovered a fake currency converter app in the official Google Play store that hid the Trojan (see: *Cerberus Banking Trojan Targeted Spanish Android Users*).

The fake app, “Calculadora de Moneda," appears to have only targeted Android users in Spain, Avast says. Researchers determined this app managed to bypass security features embedded in the Google Play store that are designed to keep out malware.

Google Play has security features designed to scan and block apps that contain malware such as Cerberus, but researchers have noted that fraudsters have upped their game when it comes to creating malicious apps that avoid can detection (see: *Spyware Campaign Leverages Apps in Google Play Store*).
