Upgraded Cerberus Spyware Spreads Rapidly via MDM

By Tara Seals

Published: 2020-05-01 · Archived: 2026-04-05 20:54:53 UTC

No longer a simple Android banker, Cerberus is now a full-fledged RAT that can take complete control of devices and automatically spread via mobile device management servers.

A newly discovered variant of the Cerberus Android trojan has been spotted, with vastly expanded and more sophisticated info-harvesting capabilities, and the ability to run TeamViewer.

It was spotted by researchers being used in a targeted campaign on a multinational conglomerate. Unusually, the sample propagated through the employee pool via the infected company's mobile device management (MDM) server.

Cerberus first emerged last August on underground forums, offered in a malware-as-a-service (MaaS) rental model. At the time it was presented as a standard banking trojan that set itself apart mainly in the way it determines whether it's running in a sandbox environment: It uses the device's accelerometer sensor to implement a step-counter. It activates the malware's functions once it hits a preconfigured threshold.

At the time, researchers at ThreatFabric said that Cerberus was clearly still in active development, with a limited set of features. However, Check Point analysts earlier this year discovered a freshened-up sample, showing that Cerberus has moved far beyond those initial, simple banking trojan capabilities to become a full-fledged spyware.

To wit: The latest sample can steal a whole raft of users' information, such as call logs, SMS, credentials and installed applications. And perhaps most damagingly, cyberattackers can gain complete remote control of the device by running the TeamViewer remote access application.

"This new variant is equipped with more than the average banker – it has mobile remote access trojan (MRAT) capabilities," according to Check Point's writeup this week. "These capabilities include logging all keystrokes on the device (credentials included), stealing Google Authenticator data and any SMS received (two-factor authentication included), and commanding the device remotely via TeamViewer."

Cerberus: Full-On Spyware

When the researchers took a look under the hood of the new variant, they noticed that the malware, when first installed, first shows a window that purports to be an update for the phone's Accessibility service. If dismissed, the window keeps popping up until the user accepts the update.

Once the user accepts, the malware then uses the Accessibility service to automatically click on menu options and bypass user interaction. For instance, the application registers a receiver for SMS, and uses that status to collect incoming SMS messages and send them to the command-and-control (C2) server. It also collects device fingerprinting information and a raft of other potentially sensitive data.

“The main module can use the Accessibility service to steal Google authenticator credentials, Gmail passwords and phone unlocking patterns,” according to the writeup. “This module can send the C2 a list of files and installed applications, and can even upload a specific file upon request from the C2 server. In addition, all the user’s keystrokes are logged and sent to the server, showing the actor all activities being performed on the device. The malware waits for the Google Authenticator application to be accessed, at which point all available information is read and stored to be sent to the C2.”

It also runs the TeamViewer application while keeping the device unlocked. When running TeamViewer on Samsung devices, the malware utilizes Samsung KNOX to automatically grant permissions. The module also blocks attempts to uninstall TeamViewer and prevents the user from using it themselves, so as not to interfere with the attacker’s actions on the device.

One of the other functions of the main application is to receive a DEX file from the C2, which is an additional payload module.

“The application receives a list of commands to perform – which are configurable by the actor,” according to the Check Point analysis. “Once the appropriate command is received, the malware downloads an encoded DEX file, and saves it on the device’s external storage as ‘ring0.apk.'”

This module is responsible for additional nefarious activities beyond data exfiltration.

“The ring0.apk module can collect all contacts, SMS and installed applications and send it to the C2,” according to Check Point. “This module also can perform phone-related actions such as sending specific SMS messages, making calls and sending Unstructured Supplementary Service Data (USSD) requests. In addition, this module can show notifications, install or uninstall applications and open popup activities with URLs.”

USSD, sometimes referred to as “quick codes” or “feature codes,” is a communications protocol responsible for communication between phones and a wireless carrier’s infrastructure.

The ring0.apk module is also responsible for cleanup, and can remove itself both from the device’s administrators list, and from the device itself. It also grants itself permissions and can fetch updated payload modules.

MDM Expands Corporate Damage

Check Point became aware of Cerberus’ upgrade after it infiltrated a multinational conglomerate. It quickly went on to infect more than 75 percent of the company’s devices, prompting the company to do a factory reset for all of its mobile devices.

“We know that every credential used from an unprotected device was reported to the C2 server,” according to the report. “We also know that every SMS message was intercepted. This makes it possible for us to speculate regarding the potential damage for the affected company.”

Two malicious applications harboring the same Cerberus sample were found to be installed on a large number of the customer's devices. The apps had been installed "in a very short window of time," suggesting automation. That led the forensics team to discover that the customer's MDM had been breached.

"This is the first time we have a reported incident of mobile malware distribution that uses the MDM server as an attack vector," according to Check Point. "MDM's most prominent feature, arguably the reason for its existence, is also its Achilles' heel – a single, central control for the entire mobile network. If that platform is breached, so is the entire mobile network."

The attack, given how it unfolded, appeared to be a targeted attack against the company. In terms of attribution, Check Point was able to determine that the C2 listens on port 8888, and there is no hostname, just a Russian IP address.

While all communications with the C2 could have been blocked, to err on the side of caution, the company went forward with a factory reset on all devices.

"If one unprotected device was used by an administrator who then tried to access corporate resources with his credentials, those credentials, along with any 2FA SMS codes, are compromised," said the researchers. "This type of response is extremely costly, both in conducting the damage assessment and re-establishing the entire mobile network after the factory reset."

Source: https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/