Cerberus

Threat: **Android Banker**

Author: **Jeffrey Farnan** Date Originally Published: **September 31th, 2021**

1. SUMMARY

- Cerberus is the name of an Android banking malware first discovered in 2019 on Google Play. It is disguised as a legitimate Android App such as a flash player, currency converter or delivery app. Cerberus is very advanced Android malware, it can bypass security measures, access text messages and commands can be sent to user's devices and perform dangerous actions. The main purpose of Cerberus is gain access to financial information such as to banking credentials and sensitive information, to generate revenue.

2. MALWARE FAMILY

- **Type** = Android Banker.
- **Sub-type** = Trojan / RAT / Bot / Spyware.

- Cerberus is a sophisticated Android banking malware, which was actively distributed on a MaaS (Malware-as-a-Service). It is called an Android Banker because it gains unauthorized access to confidential data, such a credit card and bank details without the user's knowledge. It can also be referred to as a Trojan, Rat or Spyware because it carries out many of these services and functions:
    - **Trojan**: Fake malicious apps designed to infect Android smartphones.
    - **Rat:** (Remote Administration Tool) is designed to control a victim's Android device.
    - **Bot:** Your mobile device can added to a botnet and controlled by a botmaster from afar.
    - **Spyware:** Can steal personal information such as messages, contacts and device details.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Ukraine.
- **First seen date/period** = 2019.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = September 28th, 2021.

4. MALWARE HISTORY

- Cerberus is named after the Greek, three headed mythological creature which guards the entrance of the underworld ruled by Hades.
- Cerberus is the name of an Android banking malware first discovered in Spain in 2019 on Google Play. Posing as a currency converter app, it and was downloaded more than 10,000 times.
- This malware (Malware-as-a-service) could be rented from the Russian hacking forum XSS[.] from 2019. It was actively promoted with an official page on twitter, where the creators, claiming to be from Ukraine, boast about their superior technical competence.

- You could rent it depending on how long you wish to use it:
    - 3 months - $4,000,
    - 6 months - $7,000,
    - 12 months - $12,000
- In July 2020 adverts were posted in hacking forums stating the APK source code, client list, servers, and code for administrator panels for Cerberus was being put up for auction due to the development team breaking up and departing. The operator set a starting price of $50,000. The auctioneer claimed that Cerberus generated $10,000 in revenue per month.
- No one was interested in taking on their criminal operations and the developers instead released the source code of the Cerberus malware into the wild.
- After the release of the source code there was a rise in infections across Europe and Russia. When the malware was offered as Malware-as-a-Service (MaaS) the threat was contained to groups able to pay for the code. Once the source code was available for free there, saw a rise in Cerberus infections, plus new variants were created based on the leaked code.

5. MALWARE DESCRIPTION

- Security Researchers discovered Cerberus in Google Play, wrapped and disguised either as a legitimate flash player app, currency converter or delivery app. The code is developed by a team who claim to have written all the code from scratch and features advanced obfuscation, anti-detection and anti-analysis techniques. It uses no components featured in other banking Trojans.
- This malware is able to conduct covert surveillance, intercept communication, and tamper with device functionality and steal data including banking credentials by creating overlays on existing banking, retail and social networking apps.

- When Cerberus is installed on a device, it deploys a pedometer to detect when the person is moving, the malware only operated when the victim was on the go.
- It attempts to deceive users into providing increased privileges through the Accessibility Service. When these privileges are granted it connects to a botnet and can receive commands from a command and control (C2) server.
- Cyber criminals can perform various actions on the victim's device, such as keylogging, ability to take screenshots, get a list of installed apps, access contacts list, enable call forwarding to a number, launch specific apps, delete apps, send text messages, lock the screen.
- This malware is very advanced it's able to read text messages that may contain one-time passcodes (OTP) and two-factor authentication (2FA) codes, thereby bypassing typical 2FA account protections.
- This malware is capable of performing 'overlay attacks'. This type of attack displays an overlay on top of legitimate mobile banking apps and tricks users into entering their credentials onto a fake login screen. All information is sent to the attackers C2 server.
- The permissions are: READ_CONTACTS, SEND_SME, CALL_PHONE, RECEIVE_SMS, RECORD_AUDIO, READ_PHONE_STATE, INTERNTE, WRITE_EXTERNAL_STORAGE and Read_SMS. Given these permissions, many capabilities can be identified, such as those that are consistent with a remote access Trojan gaining access to, and controlling the device.
- The Activities, Receivers and Services use obfuscation to hide their activity with random letters and numbering.

6. POTENTIAL CUSTOMER DEFENSE

- Cerberus malware relies on social engineering tactics to get on a victim's device, so be careful what you download, specifically from unofficial sites and third party apps. Recently there have been Covid related apps promoted on coronavirus-related domains, which contain the Cerberus malware.
- Many people think Google play which is the official site to download Android apps is safe and protected from malicious software, unfortunately this is not true. Google states it only allows certified apps on its site, the problem is the certificates, can be fake, stolen or copied. At the present moment the Play Store is lacking in security to stop these malicious apps. The sheer size and popularity of Google play means it's a high target for malware authors to slip malicious apps onto the site without been detected.
- Other helpful advice:
    - Android software and files should be downloaded from official websites and through direct links while avoiding downloading lesser-known apps.
    - Before downloading a new app, check its user ratings. If other people had a bad experience don't download it.
    - Pay attention to the permissions the app requests, if it's requesting more than it delivers its best to avoid it. Sometimes an app will request admin permissions to take control of your device, don't give this permission unless you know this is necessary for the app to work.
    - Android operating systems should be protected with trusted antivirus products or anti-spyware software.
    - Stay on top of the latest mobile security news and current threats.

Research Sources:

- https://gbhackers.com/cerberus-android-banking-malware/
- https://www.technadu.com/new-android-malware-cerberus-available-renting/76740/
- https://www.anomali.com/blog/leashing-cerberus
- https://www.darkowl.com/blog-content/the-rise-of-android-specific-malware-on-the-darknet
- https://www.pcrisk.com/removal-guides/17387-cerberus-banking-trojan-android
- https://www.mcafee.com/blogs/consumer/consumer-threat-reports/cerberus-banking-trojan/
- https://blog.avast.com/avast-finds-banking-trojan-cerberus-on-google-play-avast
- https://www.bleepingcomputer.com/news/security/new-cerberus-android-banker-uses-pedometer-to-avoid-analysis/