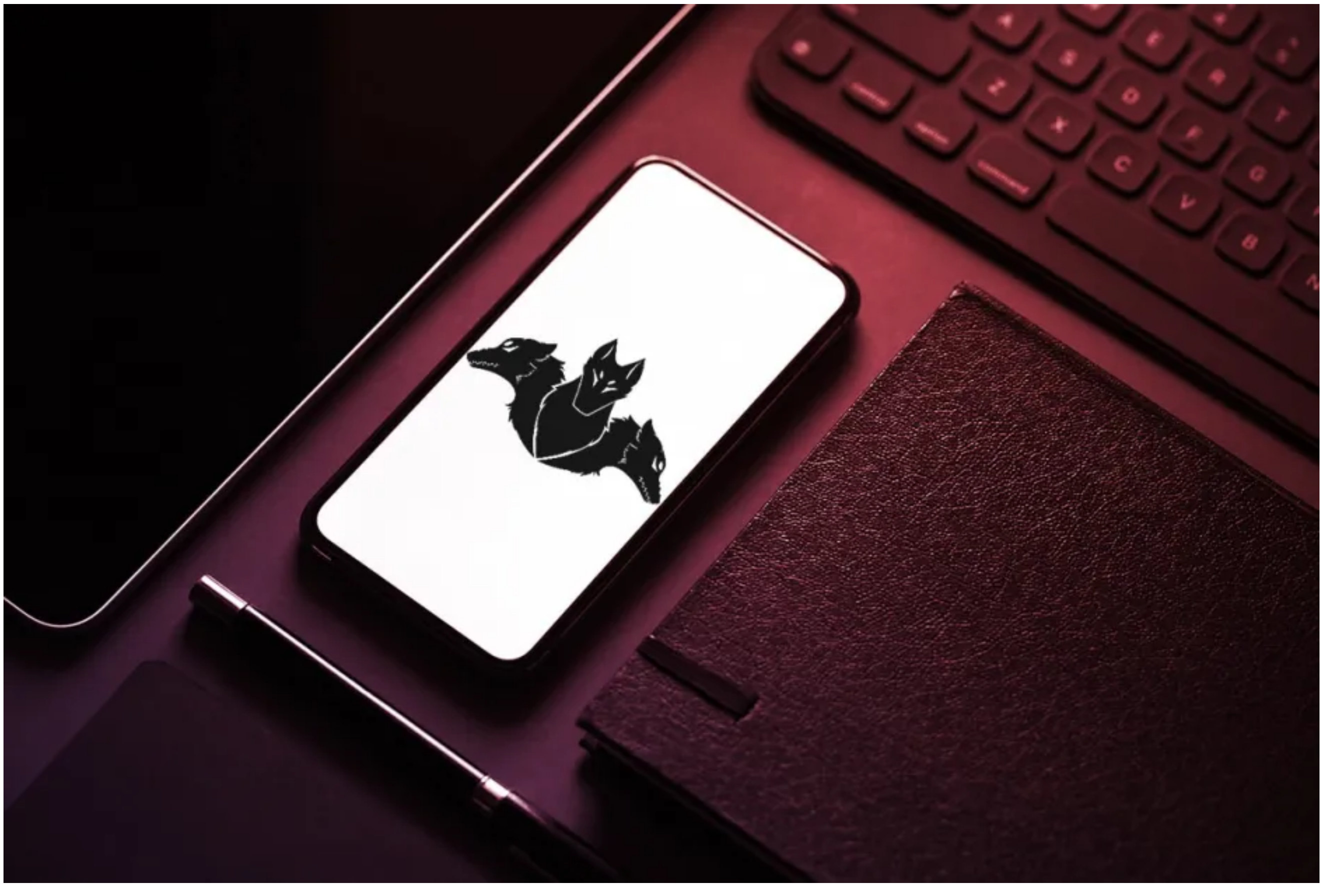
Cerberus and Alien: the malware that has put Android in a tight spot

preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/

September 29, 2020



2020 is the year of the rat, and we actually aren’t talking about the Chinese horoscope. According to several cybersecurity researchers, 2020 has seen an explosive increase in Remote access Trojans, or “RATs”.

This threat is not minor: a RAT can take control of your computer in the same way that a remote administrator would normally do, using tools such as TeamViewer or VNC. In this case, it’s a malicious control: a RAT steals your personal information trying to carry out bank or identity fraud.

However, and with the migration of PC users to the mobile world, hackers changed their strategy. Now there is a whole series of malware focused on bank credentials and identity theft, especially designed for Android mobile devices. These RATs have reached a high level of sophistication, and most are offered in the form of “malware as a service”, or MaaS.

Between 2019 and 2020 these attacks have become increasingly common. Names like Anubis, Hydra, Ginp, or Gustuff appear on all mobile malware lists on a recurring basis. However, the one that has dominated the arena this year –for several reasons– is Cerberus: a nightmare-inducing rodent.

Cerberus, the king of all RATs

Cerberus is a highly sophisticated Android malware, in circulation since 2019. It has been actively distributed on dark web forums, in a “malware-as-a-service” (MaaS) format. For a sum between $4,000 and $12,000, cybercriminal groups capable of paying it have had all the malware tools at their disposal. And by tools, we mean an arsenal of destruction.

> Yesterday was released Cerberus v2 (banking Trojan)
>
> I received their master C&C
>
> Please, don't try to hack it, don't RT so it wont be shared with many skilled whitehat pentesters.#StayHome and don't help to reveal its developers, clients and victims.
>
> reil424lawk6u65o .onion pic.twitter.com/3iaXv3ABG2
>
> — Lukas Stefanko (@LukasStefanko) April 4, 2020

Cerberus was conceived as a run-of-the-mill banking and phishing malware, and seeing Anubis’s success with cybercriminals, the team decided to integrate RAT capabilities into their toolset. Its victim is the banking apps inside your smartphone, but its functionality is much more complex. Like any Remote Access Trojan worth its salt, Cerberus is capable of deep surveillance within your device, interfering with the encrypted communications the phone has with its apps, and outside.

Basically, Cerberus can intercept and steal your phone’s unlock pattern or PIN, as well as Google Authenticator numbers, and any SMS necessary to perform a two-step verification. Likewise, this malware can interpose itself between you and your bank’s app through an overlay, the most common method for carrying out a phishing attack. In short, Cerberus can enter your computer, extract all the necessary data to perform a bank fraud, and wait for the best moment to take the money from your account. All without you doing anything.

Cerberus and its complex functionality

Regarding what Cerberus can do, it is necessary to point out two possibilities within its functionality. We already mentioned that Cerberus is a RAT, but to achieve such control of the phone, it is necessary to have control of a vulnerability. In this case, it is the Android Accessibility Service.

This service, which normally assists users with disabilities in certain applications, is abused by Cerberus to give itself more permissions without user interaction. Having control of the Accessibility Services, the malware proceeds to ensure its persistence in different ways, either by disabling Play Protect or by removing itself from the applications in use.

On the other hand, Cerberus is capable of generating an instance of TeamViewer on mobile, and through the aforementioned Accessibility permissions, authorizing said session while the equipment is in use, all without user interaction.

From that point, and as soon as the C2 server has the computer’s data, the rest of the functionalities are available to the attackers remotely. Abusing both the Accessibility Service and the TeamViewer session, Cerberus is capable of a lot. Its possibilities include:

- A keylogger
- Listing, retrieval, sending and forwarding of SMS
- Forwarding or transferring calls
- Installation and deletion of apps
- Locking and unlocking the screen (without user interaction)
- Collection of device data
- List of device applications
- Device file collection and extraction
- Phishing attacks via preloaded overlays
- Various protection capabilities, such as emulation detection

The rocky history of Cerberus

As we mentioned, Cerberus has been on the market for a long time, to the detriment of users and banks alike. However, there are two reasons why it is now a growing concern: on one hand, the rapid evolution of its functionalities and on the other, the release of its source code.

Cerberus was born in 2019 as an espionage suite. While its design made it capable of bank fraud, at the time the malware lacked the level of sophistication required to steal two-step authentication (2FA) data from apps like Google Authenticator. However, a ThreatFabric report analyzed the second version of the malware in early 2020. Cerberus v2 was still in development by the same Eurasian team that brought it to life, with increasingly powerful functionality.

Months later, An Avast team made a disturbing finding. An app for the Spanish market, called “Calculadora de Moneda” (“Currency Calculator”), contained malicious code related to Cerberus in its APK. The app was hosted on the Google Play Store, which supposedly contains software from legitimate and safe sources.

However, after weeks in hibernation, a connection to the attackers’ C2 servers activated code on the app that downloaded another APK containing Cerberus, and the smartphones were infected with the malware.

As the days passed, the Cerberus team became fragmented. In July, the developers decided to leave the project in the hands of anyone who could pay for it. The operators decided to auction everything: the servers, the malicious APK’s source code, and the admin panel codes in addition to the modules. With a profit of aproximately $10,000 per customer, the creators of Cerberus promised potential buyers to recover the expense in no time.

However, the lack of interest –or buyers willing to pay that sum– put the sale at risk. The worst happened a couple of weeks later. Cybersecurity researcher Dmitry Galov revealed that the auction had failed and that Cerberus operators released the source code of the malware. This opened the door to the worst-case scenario: developers taking Cerberus and transforming it into something nasty.

Alien, the new player

It took less than two weeks for another MaaS to take the crown. Alien, considered by experts as a full-blown ‘fork’ of Cerberus, entered the market aggressively after the fall of its predecessor.

The ThreatFabric report on Alien is concerning. Although Alien comes from a different version than the one released, it retains many of the functions that make this type of malware dangerous. First of all, it’s a very streamlined RAT with tons of features. It is also capable of running its own TeamViewer instance, and of displaying fake logins for more than 226 applications. These include not only banking apps, but social media, email, and even popular cryptocurrency wallets.

Alien is distributed in the same way as Cerberus in its early days: through malware forums on the dark web. Its price has not yet been published, but it is believed that it would be similar to Cerberus given the similarity in functionality.

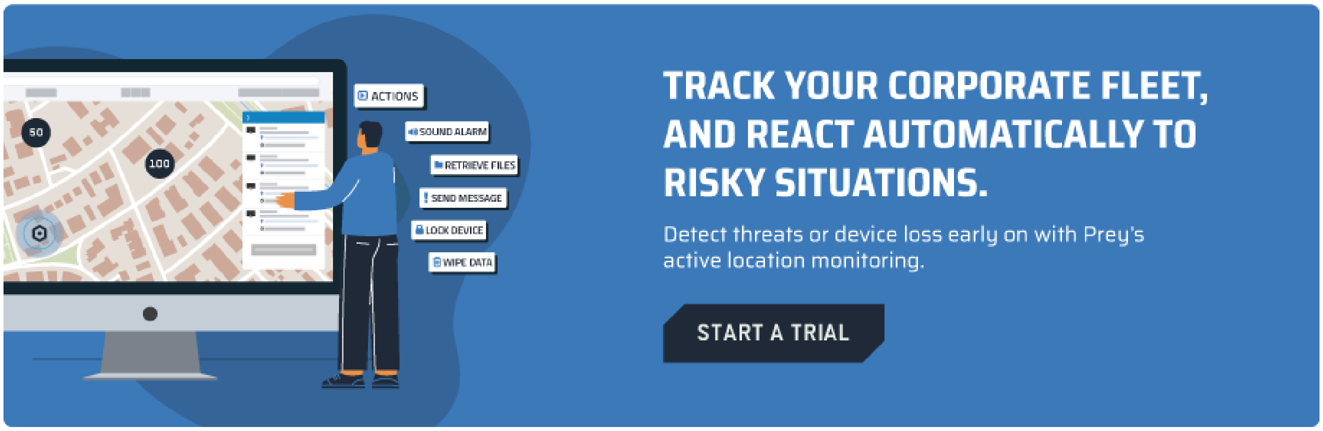
Conclusions

The smartphone malware landscape is becoming more complex as 2020 progresses. Malicious actors are taking advantage of user-authorized vulnerabilities to access our phones, and then exploit all avenues for financial gain. This practice has generated a very profitable market, one that all Android users can fall victim to.

Recommendations for a threat this organized are straightforward. First and foremost, review any application installed on our Android devices, especially the requested permissions. Also, and even if it is used by many applications in a completely legitimate way, it's necessary to pay attention if a suspicious application needs access to Google's Accessibility Services.

Along the same lines, there is a need to educate users about the risks of this type of malware, whether personal or work-related. It should not be forgotten: although there are strong economic motivations, malware such as Cerberus is still a powerful spying tool. The coexistence of private data on our mobiles may well be an attack vector for our organizations.

Back to the Basics – What is Cybersecurity?


50
100
ACTIONS
SOUND ALARM
RETRIEVE FILES
SEND MESSAGE
LOCK DEVICE
WIPE DATA
TRACK YOUR CORPORATE FLEET, AND REACT AUTOMATICALLY TO RISKY SITUATIONS.
Detect threats or device loss early on with Prey's active location monitoring.
START A TRIAL