TLP:AMBER

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

7 DECEMBER 2021

FLASH Number

CP-000157-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:AMBER**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI CyWatch immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email: cywatch@fbi.gov | Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Anatomy of Alien Mobile Malware Infection

Summary

Mobile malware represents an increasing threat to the US financial services sector as more users shift toward mobile banking—accelerated as a result of the COVID-19 pandemic, and nearly universal smartphone usage with as many as 169 million mobile banking users in the US. As a result, malware purpose built to target devices supporting mobile banking has emerged. Many common mobile malware variants, such as Eventbot, Anubis, and Cerberus, possess the preprogrammed and automated ability to compromise SMS-based two-factor authentication by reading and deleting SMS messages.

Alien mobile malware (Alien), which was first observed in January 2020, is likely a variant of the v1 Cerberus mobile malware. Alien employs a wide variety of tools and capabilities as both an Android Banking Trojan and Malware-as-a-Service. Alien possesses traditional mobile malware capabilities, as well as SMS listing and forwarding. The malware allows cyber actors to generate custom Android Application Packages (APKs) based on desired settings, and is often distributed through smishing and phishing. Alien malware often targets non-financial applications to attempt to take advantage of users' potential decreased caution when interacting with seemingly more innocuous applications, but once deployed targets the user's financial applications.

Technical Details

Alien is a feature-rich mobile malware banking trojan with an extensive range of malicious capabilities, including:

- Injection of phishing pages for legitimate applications in order to steal credentials, financial information, and other sensitive data
- Automatically disabling security services such as Google Play Protect
- Uninstalling applications from the infected device
- Interception of all SMS messages received by the device [including two-/multifactor authentication (TFA/MFA) codes]
- Sending SMS messages through the device using the device phone number
- Sending arbitrary push notifications to the device
- Sending USSD requests (USSD codes are carrier specific codes that can be used to query the carrier network for information about the sending device, such as the device phone number or IMEI number)
- Forwarding calls through the device using the device phone number
- Recording audio using the device microphone
- Proxying arbitrary traffic through the device via a SOCKS5 proxy service
- Controlling the device remotely via the Microsoft Teamviewer Application
- Executing applications on the device
- Opening specified URLs using the device
- Receiving and installing updates for the malware
- Uninstalling itself from the device

Alien is also capable of exfiltrating the following sensitive data from the device:

- The locally stored Google authentication token
- The pattern used to lock the device
- Saved SMS messages (including messages that may have been on the device pre-infection)
- The device's contact list
- Files located on the device such as documents, photos, videos, etc.
- A list of installed applications

Once Alien has been installed on a victim device, the actor essentially has complete control of the device, including access to multiple types of data stored on there, as well as the ability to use that device for additional malicious activities via the RAT and SOCKS5 services.

Alien allows the malicious actor to bypass the majority of TFA/MFA security, which tend to rely on emails, SMS alerts, or authenticator apps to distribute their authentication codes, all of which are likely to reside on the victim's infected device in some form.

At the time of writing, Alien was equipped with injects for 271 different Android applications, 36 of which are applications belonging to companies based in the United States. Alien has been observed targeting the following categories:

- Financial/Banking applications
- Retail/Shopping services
- Cryptocurrency vendors/exchanges
- Email services
- Social media applications
- Instant message/encrypted chat applications

Alien, as well as multiple other mobile malware banking trojans, is known to abuse Android Accessibility services and Background execution permissions to conduct its malicious activity. Accessibility services allows Alien to mimic user actions (e.g., taps, swipes) to disable security services and grant additional permissions to itself via auto-click routines, as well as monitor and intercept system events (e.g., receiving text messages). Background execution allows Alien to constantly operate in the background without risk of being suspended by Android's power management service, allowing it to function at all times, even when not in focus.

Alien is a malware-as-a-service variant, in which criminal affiliates conduct attacks and the proceeds are shared with the malware developers. Overall, the Alien command and control structure can be divided into three parts: the network of mobile devices infected with Alien, the affiliate-owned Alien command and control server, and the developer-owned hidden service hosting the Alien control panel.

It can be exceptionally difficult to associate cases of fraud with Alien, as the methods used to conduct the fraud once sensitive credentials have been stolen using Alien can vary widely across its users.

Infection Vectors

- Phishing links received from untrusted sources (spoofed sites, malicious SMS alerts, untrusted websites, phishing emails).
- Installation of applications from untrusted third-party app stores.
- Installation of unknown apps created by unverifiable publishers on trusted vendor platforms, *(Multiple instances have been observed of apps bypassing Google Play Store protections by not displaying any malicious behavior until a later period in time, at which point a malicious app update is pushed that can result in Alien being dropped onto the device.).*

Infection Process

Due to the nature of mobile operating systems and their tendency to sandbox applications, a significant amount of user interaction is required for Alien to gain the necessary permissions to run. These are normally acquired by tricking the user by posing as a legitimate application and through repeated promptings.

A successful infection relies heavily on a user's lack of security awareness regarding mobile malware, and a lack of understanding of the two primary permissions needed: accessibility services and background operation. Both of these permissions are rarely requested in legitimate applications, provide a great amount of control over the target device, and are commonly abused by multiple strains of mobile malware to conduct their malicious activity.

A sample infection from the perspective of an end user is laid out below:

1. Upon downloading the malicious APK, the Android OS will prompt the user on if they wish to install the application.
2. If the user has enabled Google Play Protect, Play Protect may display an additional message advising the user that the publisher of the application is unverified.
3. Once installed, Alien will display a customizable push notification advising the user on how to enable accessibility permissions for the app.
4. Lastly, Alien will request background execution permissions. If the user grants these, the malware will be fully operational and active on the device.

Information Requested

The FBI may seek the following information, including:

- Monetary loss as a result of the infection.
- Fraud method, (e.g. victim device used in an unauthorized transaction, login from a foreign IP, etc.).
- Recovered malicious APK file (if available).
- Device images (if available).
- Initial infection vector (if determined).
- Associated Indicators Of Compromise (IOCs):
    - Email addresses
    - Phone numbers
    - IP addresses
    - C2 Domains
    - Developer account names
    - Malicious app names
- Any forensic analysis performed on infected devices.

Best Practices to Mitigate Infection

The FBI recognizes that financial institutions largely do not possess the ability to mitigate user device infection that may then target financial applications. These end-user best practices are included for awareness.

- Receiving unsolicited alerts or messages should always be treated with a level of suspicion, even if they appear to be from legitimate sources.
- Users should only install applications from their vendors trusted app store (e.g. Google Play Store, or Apple App Store) in order to minimize the risk of infection.
- Only install applications that are necessary, and that originate from a verifiable publisher (e.g. the official published banking app for your banking institution).
- If applications from unverified publishers are installed, be on the lookout for app updates that cause the app to request elevated permissions (e.g. background execution or accessibility services) that it did not request during the original installation.
- NEVER enable Accessibility Services or Background Execution for apps that do not explicitly require it, as the permissions are almost never needed for legitimate applications and are commonly abused amongst many strains of mobile malware as their primary means of conducting malicious activity.
- Once installed, Alien employs several methods that make it difficult for a victim to remove by regular means. It is recommended to perform a complete factory reset of the infected device to completely remove the infection.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at cywatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked TLP:AMBER. The information in this product may be shared with members of your organization, and with clients and customers who need to know the information to protect themselves or prevent future harm.

Your Feedback Regarding this Product is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.