AbstractEmu

Threat: **Rooting Malware**

Author: **Jeffrey Farnan** Date Originally Published: **November 29th, 2021**

1. SUMMARY

- A newly discovered Android malware called AbstractEmu uses known security flaws to gain root permissions giving it greater system ability and privileged access. The malware is a Trojan which comes hidden in legitimate-looking apps (like password managers, app launchers, and data savers) found in Google Play Store, the Amazon App Store, Samsung Galaxy Store and other Android app markets. This malware is well designed and the app function works as advertised, the user would not notice anything wrong or suspect any malware was on their device. The main motivation is financial gain by collecting sensitive data by gaining a high level of access to the mobile operating system.

2. MALWARE FAMILY

- **Type** = Rooting Malware.
- **Sub-type** = Trojan / Spyware.

- **Rooting Malware:** Gains privileged access to the Android operating system, granting itself further permissions to change system systems and install additional malware. Widely-distributed malware with root capabilities and this level of access is very rare.
- **Trojan:** This malware is a Trojan which comes hidden in utility security and privacy apps found on Android App Stores.
- **Spyware:** With rooting access and commands from Command and Control server the threat actors can track notifications, take screenshots, lock the device and disable Google Play Protect. With this high level of rooting access threat actors can gain access to contacts, call logs, SMS messages, GPS location, camera and microphone. They also have the ability to reduce the security of the Android device.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** =2020.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = November 19th, 2021.

4. MALWARE HISTORY

- This malware was found by a security firm called Lookout Threat Lab. It is named AbstractEmu due to its use of code abstraction and anti-emulation checks to avoid detection while running under analysis and sandboxes.
- It was found on Google Play store and other third-party app stores, it has since been removed from Google Play store.
- This malware attempts to gain root access by exploiting several vulnerabilities identified in 2019 and 2020, as well as two from 2015. It is the first widespread rooting malware campaign in five years.
- This malware was aimed at users globally, users in 17 countries were affected, with the United States hit the hardest.

5. MALWARE DESCRIPTION

AbstractEmu poses as a functional app, when the user downloads and opens the app the malware will be activated, here are the steps involved:

- Once this malware is installed it performs device checks, and checks to see it if it real android device or an emulated device.
- It starts gathering large amount of information from the device. This information is sent to its C&C server, along with what commands the mobile device supports. Based on the commands gives the malware can collect files, get contact information and details about the device.
- AbstractEmu obtains permissions through root access using exploited vulnerabilities, allowing access to data and apps on the device without user interaction.
- The malware can execute embedded root exploits, allowing it to install new apps using its root access. The apps are hidden with encoded files, including exploit binaries targeting different vulnerabilities. These apps can also contain encoded shell scripts which are used to execute the exploit binaries to gain further access.
- The Package Manager is an application to manage system and user apps on Android phones. The Package Manager is modified and granted a number of intrusive permissions, such as access to contacts, call logs, SMS messages, location, camera and microphone. This app will modify settings to grant itself risky capabilities or reduce the device's security.
- One of the installed apps is called "Settings Storage" which is actually spyware disguised as a storage manager. If a user tries to run this app it will exit and open the legitimate settings app. This app is given extensive permissions, including access to the camera, microphone, contacts, calls, messages and location data. The data is collected and controlled through the C&C server.

With root permissions and elevated privileges it is also able to receive and collect sensitive data from other apps on the phone. With these capabilities the app can be used to conduct phishing attacks and provide the actor with all the information needed for illicit access to user accounts. This malware's capabilities go far beyond stealing financial and sensitive data, so the full aim or goal of the attackers is not known.

6. POTENTIAL CUSTOMER DEFENSE

The mobile phone is the perfect tool for the cyber criminals to exploit, as they have countless functionalities and hold an immense amount of sensitive data. There are numerous vulnerabilities within the Android ecosystem which been found and has been exploited by this malware. The command-and-control server has since gone off-line and all flaws have been patched as of March 2020 in an official Android security update. To protect yourself from this malware here are a number of tips:

- To be infected with mobile malware like AbstractEmu can lead to financial loss and stolen sensitive data. The best advice is to avoid 3rd party apps and only download apps from official stores.
- To stay secure experts suggest keeping the operating system updated.
- Have an Android antivirus app on your phone, to keep one step ahead of the nasty malware.

Research Sources:

- https://www.tomsguide.com/news/abstract-emu-android-malware
- https://cyware.com/news/abstractemu-the-rooting-malware-with-a-global-spread-92f9b995
- https://www.pcrisk.com/removal-guides/22385-abstractemu-malware-android
- https://www.techzine.eu/news/security/67784/abstractemu-malware-completely-takes-over-android-devices/
- https://blog.lookout.com/lookout-discovers-global-rooting-malware-campaign