New AndroRAT Exploits Allow for Permanent Rooting

By By: Veo Zhang, Jason Gu, Seven Shen Feb 13, 2018 Read time: 3 min (734 words)

Published: 2018-02-13 · Archived: 2026-04-05 16:17:06 UTC

Trend Micro detected a new variant of Android Remote Access Tool (AndroRAT) (identified as ANDROIDOS_ANDRORAT.HRXC) that has the ability to inject root exploits to perform malicious tasks such as silent installation, shell command execution, WiFi password collection, and screen capture. This AndroRAT targets CVE-2015-1805, a publicly disclosed vulnerability in 2016 that allows attackers to penetrate a number of older Android devices to perform its privilege escalation.

RATs have long been a commonnews- cybercrime-and-digital-threats Windows threat, so it shouldn't be a surprise that it has come to Android. A RAT has to gain root access — usually by exploiting a vulnerability — in order to have control over a system. Discovered in 2012, the original authors intended AndroRAT — initially a university project — as an open-source client/server application that can provide remote control of an Android system, which naturally attracted cybercriminals.

Figure 1. Code snippet of the malware executing the exploit

This new variant of AndroRAT disguises itself as a malicious utility app called TrashCleaner, which is presumably downloaded from a malicious URL. The first time TrashCleaner runs, it prompts the Android device to install a Chinese-labeled calculator app that resembles a pre-installed system calculator. Simultaneously, the TrashCleaner icon will disappear from the device's UI and the RAT is activated in the background.

Figure 2. Icon of the malicious TrashCleaner

Figure 3. Icon of the Chinese-labeled calculator app

The configurable RAT service is controlled by a remote server, which could mean that commands may be issued to trigger different actions. The variant activates the embedded root exploit when executing privileged actions. It performs the following malicious actions found in the original AndroRAT:

- Record audio
- Take photos using the device camera
- Theft of system information such as phone model, number, IMEI, etc.
- Theft of WiFi names connected to the device
- Theft of call logs including incoming and outgoing calls
- Theft of mobile network cell location
- Theft of GPS location
- Theft of contacts list
- Theft of files on the device

- Theft of list of running apps
- Theft of SMS from device inbox
- Monitor incoming and outgoing SMS

Apart from the original features of the AndroRAT, it also performs new privileged actions:

- Theft of mobile network information, storage capacity, rooted or not
- Theft of list of installed applications
- Theft of web browsing history from pre-installed browsers
- Theft of calendar events
- Record calls
- Upload files to victim device
- Use front camera to capture high resolution photos
- Delete and send forged SMS
- Screen capture
- Shell command execution
- Theft of WiFi passwords
- Enabling accessibility services for a key logger silently

Targeting CVE-2015-1805

Google already patched CVE-2015-1805 in March 2016, but devices that no longer receive patches or those with a long rollout period are at risk of being compromised by this new AndroRAT variant. Older versions of Android, which are still being used by a significant number of mobile users, may still be vulnerable.

Countermeasures

Users should refrain from downloading apps from third-party app stores to avoid being targeted by threats like AndroRAT. Downloading only from legitimate app stores can go a long way when it comes to device security. Regularly updating your device's operating system and apps also reduce the risk of being affected by exploits for new vulnerabilities.

[Read: Secure your mobile device through these easy stepsnews article]

End users and enterprises can also benefit from multilayered mobile security solutions such as Trend Micro™ Mobile Security for Android™products, which is also available on Google Play. For organizations, Trend Micro™ Mobile Security for Enterpriseproducts provides device, compliance and application management, data protection, and configuration provisioning. It also protects devices from attacks that leverage vulnerabilities, prevents unauthorized access to apps, and detects/blocks malware and fraudulent websites.

Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies. The service protects users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

We disclosed our findings to Google and worked with them on further analyzing the apps that carried the new AndroRAT variant. Google said that the abovementioned apps were never on Google Play, and that they already incorporated detection for CVE-2015-1805 into their compatibility tests. Ideally, any device launched or updated after April 2016 will not be vulnerable.

Indicators of Compromise (IoCs)

SHA256	App Label	Package Name
2733377c14eba0ed6c3313d5aaa51171f6aef5f1d559fc255db9a03a046f0e8f	TrashCleaner	com.cleaner.trashcleaner
fde9f84def8925eb2796a7870e9c66aa29ffd1d5bda908b2dd1ddb176302eced	TrashCleaner	com.cleaner.trashcleaner
2441b5948a316ac76baeb12240ba954e200415cef808b8b0760d11bf70dd3bf7	TrashCleaner	com.cleaner.trashcleaner
909f5ab547432382f34feaa5cd7d5113dc02cda1ef9162e914219c3de4f98b6e	TrashCleaner	com.cleaner.trashcleaner

---