Lookout

WHITEPAPER

AndroRATIntern:

A Japanese Mobile Threat With Global Implications for Mobile Data Security

I. INTRODUCTION

Mobile remote access trojans (mRATs) enable attackers to quickly spin up new mobile threats using off-the-shelf malicious toolkits. Attackers often trojanize mobile apps to include mRATs so they can carry out data exfiltration and device surveillance. Two notable Android mRATs include AndroRAT, a toolkit first published in 2012 by academics, and Dendroid, a commercially-sold, criminal toolkit first released in 2014.

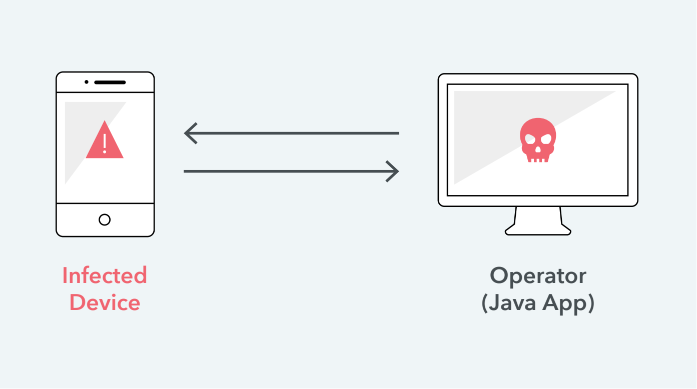
Recently, Lookout detected a new, more sophisticated Android mRAT evolved from the AndroRAT toolkit that has troubling implications for mobile security. This new threat, AndroRATIntern, offers attackers commercial surveillanceware targeted at Japanese devices and it is publicly marketed under the name AndroidAnalyzer. AndroRATIntern boasts a range of new features over its predecessor, AndroRAT, including improved scalability, data encryption, and expanded data collection through a novel abuse of the Android accessibility service[1] that allows it to collect data from LINE, Japan's most popular mobile messaging app.

AndroRATIntern represents the first time Lookout has observed a mobile threat abusing the Android accessibility service to attack and exfiltrate mobile data. While not a vulnerability, strictly speaking, this accessibility-service abuse illustrates a limitation of the Android Application Sandbox intended to segregate app data and code execution from other apps. Moreover, it raises the possibility that attackers could more widely abuse this particular service to exfiltrate otherwise protected data when it's accessed and displayed for end users. Encryption solutions such as app containers are only as secure as the operating systems on which they depend, and threats like AndroRATIntern that undermine or abuse the operating system could potentially circumvent these data protections.

II. ARCHITECTED FOR SCALE

AndroRATIntern has evolved noticeably from its predecessor with respect to operational control. Consider the relatively straightforward operation of AndroRAT in the following figure:

Figure 1. AndroRAT Operational Control

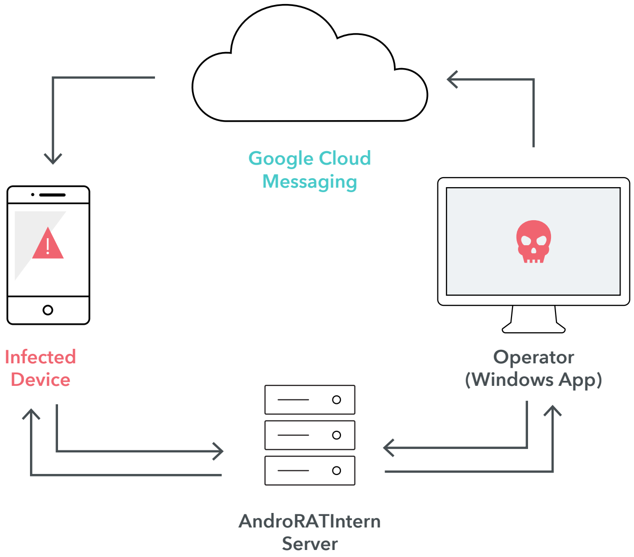


AndroRAT's C2 server is designed to acquire data from and issue commands to a single device. With AndroRAT, attackers must rely on a custom protocol and need to run a Java app on their computer as a command and control server. AndroRATIntern, on the other hand, is designed for operation as a service to collect data from a greater number of devices under control of multiple subscribing operators. In contrast to its predecessor, AndroRATIntern is effectively Surveillance-as-a-Service.

The AndroRATIntern server implements RESTful API interactions that enable attackers to manage more infected clients and increase the stability of their operations, using the Google Cloud Messaging service to initiate commands to infected devices. All communications between infected clients and the AndroRATIntern server, including data exfiltration events, occur over HTTP and are encrypted using a static key, then encoded using Base64.

[1] Android's accessibility service helps users with visual or physical disabilities use their devices through extended features like text-to-speech.

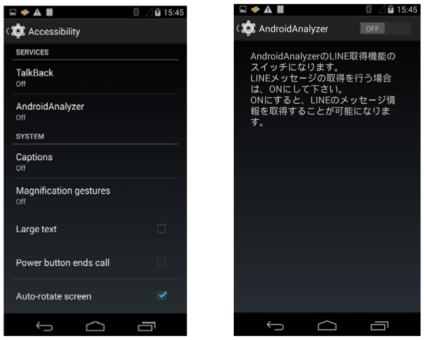
Figure 2. AndroRATIntern Operational Control



The authors have also packaged this tool with a Windows PC application that automates the installation/infection process on target devices.

As commercial surveillanceware, AndroRATIntern relies on local installation to the Android device and also requires an attacker to enable Android Debug Bridge (ADB)[2] and sideloading, as well as activate the accessibility service on the target's device (shown in Figure 3).

Figure 3. AndroRATIntern's Accessibility Enablement Prompt



15:45

Accessibility

SERVICES

TalkBack
Off

AndroidAnalyzer
Off

SYSTEM

Captions
Off

Magnification gestures
Off

Large text □

Power button ends call □

Auto-rotate screen ☑

15:45

AndroidAnalyzer OFF

AndroidAnalyzerのLINE取得機能のスイッチになります。
LINEメッセージの取得を行う場合は、ONにして下さい。
ONにすると、LINEのメッセージ情報を取得することが可能になります。

English Translation: "This is the switch used to obtain LINE acquisition functionality for AndroidAnalyzer. If you'd like to acquire LINE messages, please set to ON. Once you set this to ON, you will be able to acquire LINE Message data."

The Windows application can automatically install, start, and configure the threat on the target mobile device. AndroRATIntern was designed for stealth as it has no launcher icon nor visible activities that would alert an individual to its presence on a device unless the attacker wants to specifically prompt the user of the infected device. After initial installation, AndroRATIntern will wait silently in the background until an attacker issues a wake command via Google Cloud Messaging service.

III. STEPPING OUT OF THE APP SANDBOX

In theory, the Android Application Sandbox should prevent an app from gaining access to data belonging to other applications without explicit user permission. While Lookout has observed prior AndroRAT variants rooting devices to exfiltrate messaging data from the popular messaging app WhatsApp, AndroRATIntern marks the first time Lookout has detected a mobile threat using the Android accessibility service to access otherwise protected data by "reading" the screen as it displays data, in this case, messages sent and received by the LINE app.

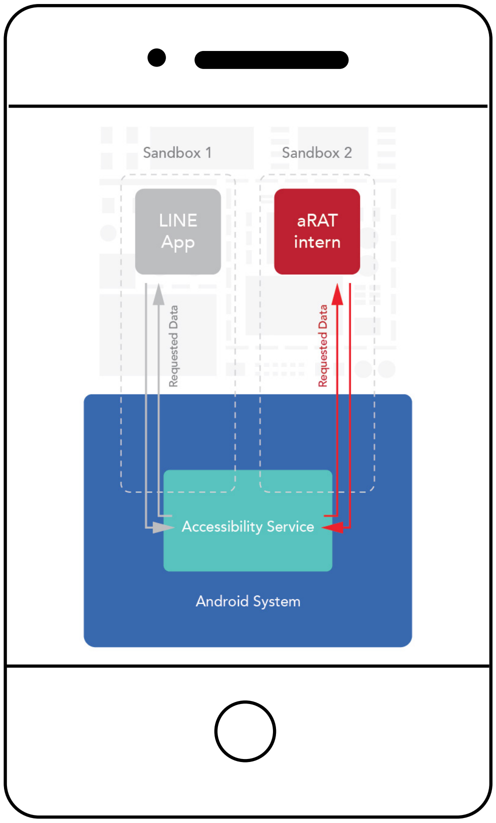
To be clear, the Android accessibility service is a legitimate service that helps users with visual or physical disabilities use their devices through extended features such as text-to-speech and haptics (touch feedback).[3] The text-to-speech feature requires access to displayed content, however accessibility service only has permission to retrieve content from a currently active window, so AndroRATIntern can only capture message content when the LINE app is in use, as opposed to retroactively collecting all the messages from the logs.

[2] A client-server program that lets developers communicate with an emulator instance or Android device.

[3] See: https://developer.android.com/guide/topics/ui/accessibility/index.html

It should come as no surprise that AndroRATIntern's author(s) went to the trouble of creating this feature specifically to capture data from the LINE application. LINE dominates the Japanese mobile messaging market and has achieved significant global penetration as well: analysts expect the app to exceed 700 million users worldwide by the end of 2015.[4]

Figure 4. AndroRATIntern's Abuse of Android Accessibility Service



IV. MOTIVATION

AndroRATIntern is offered for sale online as a commercial surveillanceware product under the name "AndroidAnalyzer". It's advertised as a product for monitoring individuals and employees and offers a range of price points and capabilities, as shown in Table 1 below.

Table 1. AndroidAnalyzer product packges

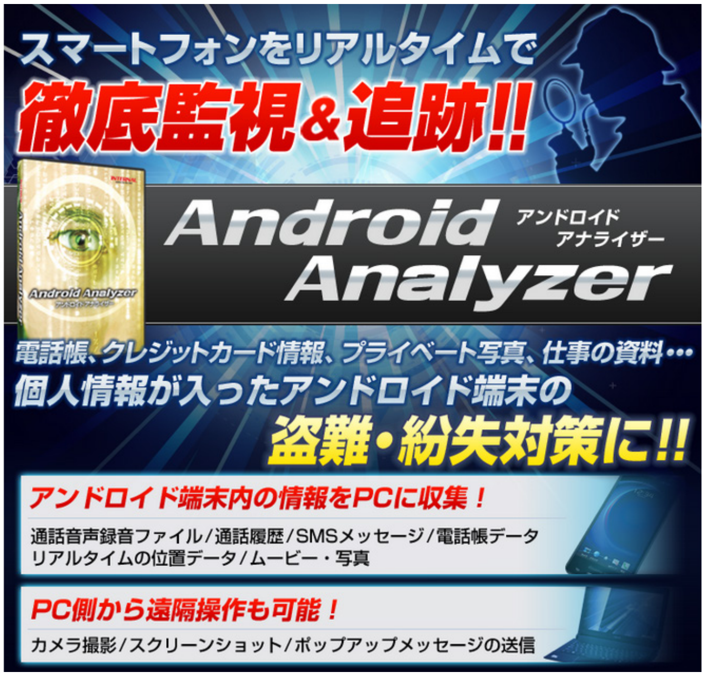
Package	Cost	Description
AndroidAnalyzer (Basic)	9,800 Yen	Tracks one device.
AndroidAnalyzer (Pro)	14,800 Yen	Tracks two devices; expands data collection capabilities to include GPS location and photos and videos.
AndroidAnalyzer (Enterprise)	59,800 Yen	Tracks multiple devices; offers maximum data collection capabilities.

That AndroidAnalyzer has no launcher icon on the device's home screen suggests the its author(s) may not intend for this software to operate under the informed consent of a device owner, despite warnings to the contrary found on the product's webpage (see Figure 6 on next page).

Lookout's detections of AndroRATIntern are currently low and restricted to Japan. Surveillanceware threats like AndroRATIntern are designed for targeted deployments and due to their local installation requirements cannot be widely distributed via drive-by-download campaigns.

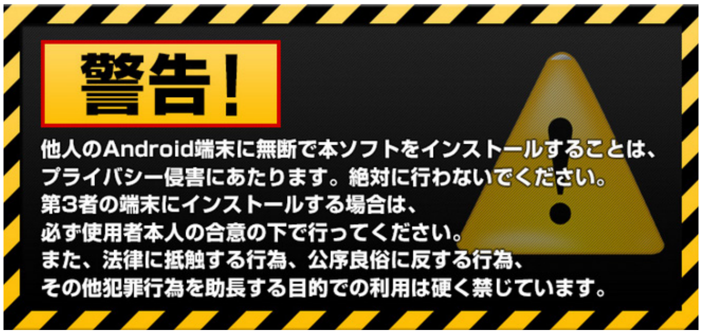
[4] "Number of Line users to top 700 mil. this year". Korea Times. February 2015. http://www.koreatimes.co.kr/www/news/tech/2015/02/419_173201.html

Figure 5. Advertisement for AndroidAnalyzer (found on the product's website)


スマートフォンをリアルタイムで
徹底監視&追跡!!
Android Analyzer
アンドロイド アナライザー
Android Analyzer
電話帳、クレジットカード情報、プライベート写真、仕事の資料…
個人情報が入ったアンドロイド端末の
盗難・紛失対策に!!
アンドロイド端末内の情報をPCに収集！
通話音声録音ファイル/通話履歴/SMSメッセージ/電話帳データ
リアルタイムの位置データ/ムービー・写真
PC側から遠隔操作も可能！
カメラ撮影/スクリーンショット/ポップアップメッセージの送信

English Translation for Figure 5: "Smartphone real time monitoring & tracking! Your device stores lot of personal info such as contact, credit card, private photos, work documents...Protect your Android device from theft & loss!! Collect data in Android device and store them on your PC! Recording of phone conversations, call history, SMS messages, contacts, real-time GPS data, movies and pictures. Remotely control your device from PC! Take photos and screen-shots, send pop-up messages."

Figure 6. Legal disclaimer warning buyers not to install it without device owner permission (found on the product's website)



警告！

他人のAndroid端末に無断で本ソフトをインストールすることは、
プライバシー侵害にあたります。絶対に行わないでください。
第3者の端末にインストールする場合は、
必ず使用者本人の合意の下で行ってください。
また、法律に抵触する行為、公序良俗に反する行為、
その他犯罪行為を助長する目的での利用は硬く禁じています。

English Translation for Figure 6: "Warning! Installing this app on an Android device without device owner's consent is an invasion of privacy. Never install this app without the owner's consent. If you plan to install the app on a device owned by someone else, please obtain the owner's consent. It is strictly prohibited to use this app for any activities which violates laws, public order and morality, and encourages other criminal acts."

V. THE MOBILE SECURITY RISK

While not specifically designed to target enterprise devices, as commercial surveillanceware AndroRATIntern could nonetheless put enterprise data at risk if installed on an employee's device given its expansive data collection capabilities (see Table 2 on the following page).

Table 2. AndroRAT vs. AndroRATIntern Data Collection

Capabilities	AndroRAT	AndroRATintern
Capture contact data	Y	Y
Capture call log data	Y	Y
Capture SMS data	Y	Y
Capture photo	Y	Y
Capture audio	Y	Y
Capture video	Y	Y
Capture GPS location	Y	Y
Capture LINE messaging data	N	Y
Launch browser	Y	Y
Monitor SD card for file changes	N	Y
Monitor SD card for file changes	N	Y

AndroRATIntern's ability to remotely activate and capture audio, video, and photos make it a potentially powerful tool for corporate espionage, expanding the security risk beyond data already stored on the device to data communicated or presented in near proximity to a compromised device, such as communications in a corporate boardroom.

Fortunately, there's no evidence to suggest that AndroRATIntern is being specifically seeded en masse or in a targeted fashion to compromise enterprises. The manual-installation requirement of AndroRATIntern greatly reduces the risk to enterprises since employees cannot unwittingly install this threat and attackers would need physical, unmonitored access to an unlocked mobile device to successfully infect it. While people rarely leave mobile devices unattended and unlocked, it would only take a few minutes to successfully install this software on a target device and this scenario should not be discounted as implausible.

Nonetheless, in an enterprise context there remains a risk that relevant data could be captured via audio, photos, or messages that expose corporate secrets. With the recently documented compromise of the surveillanceware product mSpy[5] there is also reason to be concerned that Surveillance-as-a-Service operators can be a vector for exposing sensitive data captured illicitly from user devices.

Lastly, AndroRATIntern's abuse of the Android accessibility service raises troubling concerns around device security in the enterprise. As an Android system service, the accessibility service operates outside of the normal app permission model and AndroRATIntern uses these capabilities to violate app sandboxing measures intended to protect mobile data. To be clear, the LINE application is not vulnerable or at fault for data being compromised in this scenario, since this attack method could work across all apps. Instead, it's another stark reminder that device security measures such as sandboxing, encryption, and app containerization are only as secure as the underlying operating system on which they depend. If an attack can abuse a loophole in an OS, as AndroRATIntern does with its abuse of Android accessibility service, then otherwise protected device data could be breached.

VI. CONCLUSION

AndroRATIntern, as a powerful piece of surveillanceware, demonstrates the path by which attackers can build more advanced threats on the backs of standard mobileRAT toolkits. Successfully installed on an enterprise device, the data exfiltration and surveillance capabilities of AndroRATIntern would make it a potent enterprise threat and a potential attack vector to breach sensitive systems and services by capturing sensitive credentials. This risk is mitigated by its manual installation requirement for attackers and limited geographic distribution (currently only detected in Japan). Ultimately, AndroRATIntern's novel abuse of the Android accessibility service shows that relying on OS-dependent security measures alone for data protection may not be enough.

[5] "Mobile Spyware Maker mSpy Hacked, Customer Data Leaked". Krebs On Security. May 2015. https://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/