NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Mobile: Android Operating System Increasingly at Risk

October 1, 2015

TLP: **WHITE** | ***The NJCCIC assesses with high confidence that vulnerabilities, exploits, and malware variants targeting the Android operating system (OS) will continue to proliferate as Android maintains a majority share of the global mobile device market and users increasingly rely on mobile devices for email, web browsing, banking, and shopping – both for professional and personal use.*** Additionally, as more organizations establish 'bring your own device' (BYOD) policies to reduce costs and increase connectivity, state-sponsored espionage groups and cybercriminals are likely to dedicate more resources to developing mobile exploits as a means to compromise user credentials, steal data, and to serve as an initial breach vector onto corporate networks. The threats targeting mobile devices range from various criminal schemes such as ransomware, exploits kits, and malvertising, to malicious applications that masquerade as legitimate software and stealthily exfiltrate user data, including phone call audio, text messages, photos, and emails. The NJCCIC recommends organizations and individual users implement strategies to mitigate the risk associated with the developing threat posed by mobile devices; this not only includes the patching of vulnerabilities and implementation of endpoint protections, but the training and awareness of best practices and the ability to recognize a potential threat.

Threat Overview

Android is an open source, Linux-based, mobile OS marketed by Google Inc. and commercially available through a range of device manufacturers and mobile carriers. The Android OS reportedly powers more than one billion mobile devices, representing 82.8 percent of the global smartphone market.[1] The OS runs on a wide variety of smartphones, tablets, televisions, wristwatches, and an increasing number of home automation devices. Android gained popularity with users and device manufacturers alike due to its affordability and openness, allowing for easy customization of the platform. Likewise, it appeals to application developers because of low barriers to entry into the Android application marketplace, Google Play. However, these characteristics are also advantageous to malicious actors who have capitalized on the ability to inject malicious code, develop malware, and carry out fraud schemes targeting the Android ecosystem.

- In 2014, the security firm Symantec found that fourteen percent of all Android applications—nearly one million in total— were actually malware in disguise.[2] In the first half of 2015, researchers at the digital security company G DATA observed a 25 percent increase in new Android malware, from an average of 4,900 per day in the first quarter to 6,100 per day in the second quarter.[3, 4] By the end of 2015, G DATA predicts there will be two million new Android malware variants in circulation.[5] In addition to volume, the sophistication of Android malware has increased as threat actors refine their malicious code and employ techniques previously seen only affecting desktop and server operating systems.
- Since 2009, a total of 77 Common Vulnerabilities and Exposures (CVEs) affecting the Android OS have been documented, with nearly half of those discovered in 2015 alone. In August, IBM researchers identified a severe serialization vulnerability that opens the door to application privilege escalation.[6] In July, a Zimperium researcher discovered the widely reported vulnerability called "Stagefright" which allows for remote code execution via multimedia messages.[7] One of the key challenges in mitigating Android vulnerabilities is the lack of a centralized system for the dissemination of patches; instead, developers, device manufacturers, and network carriers are responsible for deploying security updates. This often results in a window of opportunity for hackers to exploit.
- The NJCCIC recommends that all Android OS users immediately apply patches and updates supplied by their network carriers and application developers. Users are urged to avoid downloading third-party applications from unauthorized sources, and avoid "rooting" their devices, which allows the user to retain administrative privileges and provides attackers with ample opportunity to control a device. Organizations operating with BYOD policies are urged to educate employees on mobile threats and vulnerabilities, implement monitoring and endpoint protection on all mobile devices, and establish the capability to remotely wipe lost or compromised devices.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Android Infection Vectors

The most common vector for Android device infections is a user downloading a seemingly legitimate application that contains malicious code. These infected applications are often free to download and may come packaged to appear as if they perform legitimate functions. Applications downloaded from unknown and questionable sources put the device at risk for infection as reputable application markets routinely test their digital inventory for standalone and bundled malware. Android devices may also become infected due to a "drive-by download," when the victim inadvertently visits a malicious website using the device web browser. Similarly, Android devices can become infected through phishing tactics if the user clicks on a malicious link contained within an email or text message. Malware can also be delivered to a vulnerable Android device through a connection to an unsecured WiFi hotspot, or via a multimedia text message that targets a weakness within the media file processing code. Unpatched and "rooted" Android devices are particularly at risk, as they may not have the security in place to protect against various threats.

Indicators of an Android Malware Infection

Not all Android malware infections are obvious to the victim and some variants are difficult to detect. However, the following are potential indicators that an Android device is infected:

- **Unusually large phone bills**: Some Android malware variants send text messages to premium-rate numbers, racking up many unauthorized charges on the victim's phone bill.
- **Spam text messages:** If the contacts on a victim's phone start receiving spam text messages from the victim or unusual texts appear in the victim's sent folder, it is likely the result of a malware infection.
- **Abnormally heavy data usage**: Malware that siphons and transmits information from an infected device can cause a spike in data usage that will be reflected on the victim's bill.
- **Reduced battery life**: Android malware that is constantly running in the background will drain the device battery quicker than under normal use.
- **Slow system performance**: An infected device may experience sluggish performance and the victim may need to reboot the device several times in a day. Monitoring the Random Access Memory (RAM) and Central Processing Unit (CPU) can assist in determining if malware is present.
- **Pop-up messages, advertisements, or unusual push notifications:** If a message unrelated to any current application appears on the device screen, it is very likely a malware infection; a message demanding money in exchange for restored access to your data or device is the result of a ransomware infection.
- **Unusual actions or sounds**: Some malware can affect various functions of the Android device, like changing settings, installing additional apps, and even controlling the camera or microphone without user-initiated actions.
- **Dropped calls or degraded phone service**: If a device suddenly experiences poor signal strength and the problem is not carrier-related, it could be the result of an infection.

Android Malware Variants

The following is a list of Android malware variants known to be impacting US users of devices running the Android OS, from Froyo (2.2) to Lollipop (5.1.1). **Note**: See the appendix for full descriptions and links to additional resources with technical details and Indicators of Compromise (IOCs).

Exploit Kit Variant:

- **BrainTest**: malware that bypassed detection by the Google Play store twice and comes bundled with a dropper, opens a backdoor, roots the device, downloads additional malicious files, and maintains persistence.

Android Ransomware Variants:

- **LockerPIN**: an advanced variant of Android-specific ransomware that locks infected devices, generates a new PIN number for the lock screen, and then demands payment from the victim in order to regain access.
- **Simplelocker**: the first TOR-enabled Android ransomware that encrypts device files before demanding payment from the victim.

- **Koler**: blocks the device screen with a hoax law enforcement warning and a demand for ransom payment.

Data Stealing Variants:

- **Gunpoder**: a family of malware that embeds itself into popular game emulators, then siphons data from infected devices and spreads via SMS messages.
- **SocialPath**: disguises itself as legitimate applications and requests personal information from victims, steals data from infected devices, and spreads via malicious shortened URLs posted on social media websites.
- **Android/Badaccents**: a banking Trojan designed to look like a video downloader app for the film, *The Interview*, and targeted international Citibank customers and various South Korean bank customers.
- **Android.HeHe**: a family of malware that disguises itself as a seemingly legitimate Android security app but actually lets attackers intercept phone calls, steal SMS messages, and remotely wipe devices.
- **MisoSMS**: an advanced mobile botnet that disguises itself as seemingly legitimate Android applications and transmits device data to China via a C2 server.
- **NickiSpy**: masquerades as legitimate Android applications but allows attackers to eavesdrop on victims by secretly recording phone calls and collecting data such as GPS coordinates, contact lists, and SMS messages.

Mitigation Strategies

Below is a list of prevention and mitigation strategies to help protect Android devices against infection and exploitation:

- Keep the device's OS and applications current by promptly applying patches and updates when they are released.
- Do not install unknown or unfamiliar applications.
- Only install applications from trusted and reputable Android app stores, like Google Play and the Amazon Appstore. Avoid "sideloading" applications from questionable sources.
- Uncheck the "Unknown Sources" box under the device's settings menu to prevent the installation of apps from unauthorized sources.
- Prior to purchasing and downloading any app, make sure to review what permissions it's requesting. Be skeptical of any app that requests access to the device's controls or system that are unrelated to the main function of the app (i.e., a game that requests permission to access or send text messages).
- Read user reviews of apps prior to installation and avoid apps with an excessive amount of negative reviews or very few reviews.
- Consider installing and running an antivirus app but be sure that it is developed by a trusted company to avoid fake antivirus software.
- Do not visit suspicious websites using your Android device.
- Avoid clicking on suspicious links in emails and text messages.
- Be mindful of any noticeable changes to the device (i.e., slow system performance, browser redirection, pop-up ads, altered user interface, etc.) and wipe the device or run antivirus software to detect any infections.
- Regularly backup data from the device to prevent data loss should the device become infected and need to be restored to its original state.
- Avoid connecting the device to open and unsecured Wi-Fi signals.

Reporting

If you or your organization encounters Android malware, or you would like to learn more about the NJCCIC, please contact a Cyber Liaison Officer at NJCCIC@cyber.nj.gov or visit www.cyber.nj.gov.

Appendix

BrainTest, discovered by Check Point Mobile Threat Prevention in September 2015, is a sophisticated piece of Android OS malware that managed to evade detection by Google's security service, Google Bouncer, twice, after employing an obfuscation method. This malicious app can determine if it is being run from an IP address or domain that is mapped to Google Bouncer and, if so, will hide its malicious behavior. BrainTest gains root access to the infected device by using four privilege escalation exploits, opens a backdoor, and subsequently installs additional malware to maintain persistence and monitor removal attempts. If the user removes one malware app, BrainTest will download and install another one. Currently, the only way to completely remove this malware from an infected Android device is to re-flash the ROM.

- Check Point Software Technologies, Ltd. provides a full analysis of BrainTest here.

LockerPIN, also known as Android/Lockerpin.A, is an advanced and aggressive variant of Android ransomware discovered by ESET in September 2015. It disguises itself as an adult video viewing application called "Porn Droid" and, once installed, it prompts the user to install an update and then obtains administrator privileges. LockerPIN sets a new code for the lock screen to prevent the user from gaining access to the device. It then displays a bogus FBI warning directing the user to submit a ransom payment of $500 USD via a link labeled "Payment Penalties." LockerPIN is coded to avoid detection and removal by various Android antivirus applications and, even if the user successfully removes the malicious file, it randomly generates the access code (PIN) permanently locking the user out of the device. There are currently only three ways to restore access to a device infected with LockerPIN:

1. Restore the device to factory settings (this will delete all saved data).
2. Connect the device to a computer via USB and use the Android Debug Bridge (ADB) utility to remove the file containing the PIN (for rooted devices).
3. Use a mobile device management (MDM) solution that is capable of resetting the PIN (must be installed on the device prior to infection).

- ESET provides more information on Android/Lockerpin.A, including IOCs, here.

Simplocker, also known as Simplelocker, Android/Simplocker.A, and Android/SLocker-A, was detected by ESET in June 2014 and is described as the first file-encrypting, TOR-enabled Android ransomware variant. Simplocker infections occur when an Android device user installs a malicious video player app. This malware targets images, documents, and video files stored on the device's SD card and begins the encryption process after installation is complete. It also collects data from the device such as the OS version, make and model number, and IMEI number, then sends it to a Command and Control (C2) server via the anonymous TOR network. Next, it displays a warning on the screen accusing the user of viewing and distributing various pornographic material and then demands payment for the decryption key. Currently, there are two versions of this ransomware in the wild but both use the same code and AES password for file decryption.

- ESET provides more information about Android/Simplocker.A here, and a decryption tool here.
- A full dissection of this variant by SecureHoney.net can be found here.

Koler, also known as AndroidOS.Koler.A, was first detected by Kaspersky Lab in May 2014. This ransomware variant does not encrypt files but it does block the screen with a fake warning from law enforcement along with a demand for a $100 payment to unlock the device. Koler infections can occur when an Android device user visits a malicious website and manually installs the malicious app when prompted. The website redirects the browser to a server that hosts the malicious Android application package (APK), a browser-based screen lock utility, or an exploit kit. Koler operates by using a complex Traffic Distribution System (TDS) called Keitaro to manage website traffic and redirections. A newer variant, known as Worm.Koler, is similar to the original but has the added capability of spreading via text messages containing a malicious URL. Both Koler variants can be removed by rebooting the device in Safe Mode, then uninstalling the malicious app by selecting Settings, Manage Applications, selecting the app, and then the Uninstall button.

- Kaspersky Lab provides a full report on the Koler variant of ransomware here.

Gunpoder, a family of data-stealing malware, was discovered in July 2015 by the Unit 42 research team of Palo Alto Networks. Gunpoder embeds itself into emulators of popular Nintendo Entertainment System (NES) games and, once installed, will ask users to pay for a permanent use license. Because Gunpoder's malicious code is packaged within legitimate applications, it managed to evade detection by all of the antivirus software listed on VirusTotal.com. This malware variant steals information from devices, propagates itself through text messages, pushes fraudulent and potentially malicious advertisements, and maintains the ability to execute further payloads.

- Palo Alto Networks provides more information about Gunpoder, including IOCs, here.

SocialPath, discovered by Lookout, Inc. in January 2015, promotes itself either as an online reputation management application or a data backup tool. It spreads through malicious shortened links posted on social media websites. After the victim's device is infected, it begins requesting personal information which it then sends back to the attacker along with the contact list, text messages, call logs, and the device's make and model information, MAC address, and carrier. Once this step is complete, SocialPath deletes its own icon and hides on the device to continue to steal information. A month later, another variant snuck onto the official Google Play store under the name **SaveMe**, disguised as a security application. Both variants have since been removed from the Google Play store.

- Lookout, Inc. provides more information about SocialPath here.

Android/Badaccents, a banking Trojan, was discovered in December 2014 by researchers at McAfee and the Technische Universität Darmstadt and the Centre for Advanced Security Research Darmstadt (CASED). Originally hosted on Amazon Web Services, it masqueraded as an app that claimed to download the film, *The Interview*. It targeted Citibank customers worldwide as well as customers of various South Korean banks but included a feature that prevented installation on North Korean devices. Approximately 20,000 bank account credentials were stolen and sent back to Chinese servers within two months of the beginning of this malware campaign. Amazon removed the malicious app as soon as researchers notified them of their findings.

- The full technical report on Android/Badaccents is located here.

Android.HeHe, discovered by a FireEye threat researcher in January 2014, is an Android malware family that contains six variants. Android.HeHe disguises itself as an Android security app that, once installed, grants attackers with the ability to monitor, intercept, and block phone calls, steal text messages, and remote-wipe devices. It also transmits the device model, Android OS version, and network back to the attacker via a C2 server. It also checks for the presence of a sandbox to deter analysis. Android.HeHe can be removed automatically by using a reputable antivirus application or manually by selecting Settings, Manage Applications, then select the malicious app, and tap the Uninstall button.

- FireEye, Inc. provides a full report on Android.HeHe, including IOCs, here.

MisoSMS, first discovered by FireEye in December 2013 and touted as "one of the largest advanced mobile botnets," has been used in at least 64 spyware campaigns. The original MisoSMS malware disguises itself as an Android settings app called "Google Vx." A more recent variant, discovered in March 2014, presents itself as an app called "Gplay Dsc." Both variants send copies of the victims' text messages to servers in China via a C2 server, the former transmitting data via email over SMTP and the latter communicating in C++ and using an encryption algorithm. This Android malware was prevalent in South Korea around the time of its discovery but Korean law enforcement, U.S. security researchers, and the Chinese webmail vendor involved worked together to put an end to this malicious campaign.

- FireEye, Inc. provides a full report on MisoSMS malware here and here.

NickiSpy is a large and sophisticated family of Android malware variants that began targeting victims in July 2011. This malware comes bundled with, or masquerades as, legitimate applications to avoid detection by antivirus software, although they can only be downloaded through third-party markets and not through official Android app stores. NickiSpy has the ability to record phone calls and store them on the SD card in the device, allows attackers to eavesdrop on victims, and collects GPS coordinates, text messages, and contact lists to send back to the attacker. It is important to note that, because of changes made to the Android OS, this malware only affects versions up to and including Froyo (2.2).

- Trustwave provides more information on the NickiSpy malware family here.

Sources

[1] International Data Corporation (IDC). "Smartphone OS Market Share, 2015 Q2." Worldwide Quarterly Mobile Phone Tracker. August 2015. URL: http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[2] "Internet Security Threat Report 2015." Symantec. April 2015. URL: http://www.symantec.com/security_response/publications/threatreport.jsp.

[3] "Mobile Malware Report – Threat Report Q1/2015". G DATA. 2015. URL: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q1_2015_US.

[4] "Mobile Malware Report – Threat Report Q2/2015". G DATA. 2015. URL: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_EN.pdf.

[5] "Mobile Malware Report – Threat Report Q2/2015". G DATA. 2015. URL: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_EN.pdf.

[6] Peles, Or. "One Class to Rule Them All: New Android Serialization Vulnerability Gives Underprivileged Apps Super Status." IBM. August 10, 2015. URL: https://securityintelligence.com/one-class-to-rule-them-all-new-android-serialization-vulnerability-gives-underprivileged-apps-super-status/.

[7] Z Team. "Experts Found a Unicorn in the Heart of Android." Zimperium Mobile Security. 27 July 2015. URL: https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/.