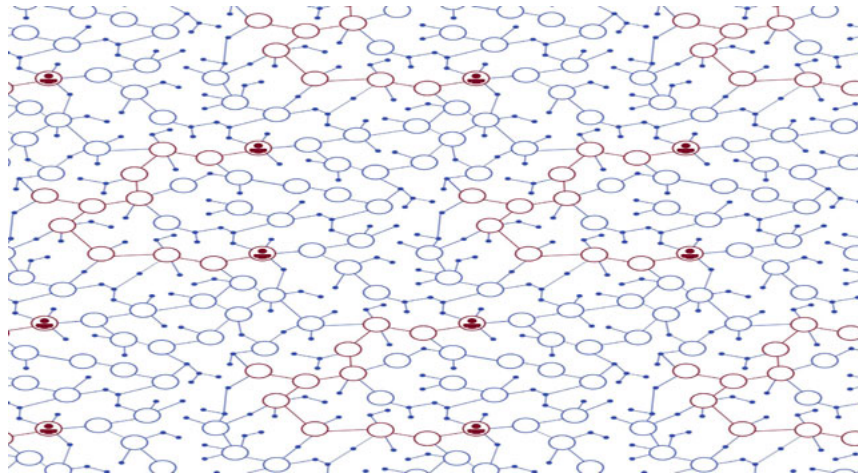


First Binder Exploit Linked to SideWinder APT Group

blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/

January 6, 2020



Mobile

We found malicious apps that work together to compromise devices and collect user data. One of the apps, called Camero, exploits CVE-2019-2215, a flaw that exists in Binder. This is the first instance in the wild that exploits said UAF vulnerability.

By: Ecular Xu, Joseph C Chen January 06, 2020 Read time: (words)

Updated January 8, 2020 5PM EST with a video showing the exploit of CVE-2019-2215.

We found three malicious apps in the Google Play Store that work together to compromise a victim's device and collect user information. One of these apps, called Camero, exploits [CVE-2019-2215](#), a vulnerability that exists in Binder (the main Inter-Process Communication system in Android). This is the first known active attack in the wild that uses the [use-after-free vulnerability](#). Interestingly, upon further investigation we also found that the three apps are likely to be part of the SideWinder threat actor group's arsenal. SideWinder, a group that has been active since 2012, is a known threat and has [reportedly targeted military entities' Windows machines](#).

The three malicious apps were disguised as photography and file manager tools. We speculate that these apps have been active since March 2019 based on the certificate information on one of the apps. The apps have since been removed from Google Play.

 [Figure XX](#)

Figure 1. The three apps related to SideWinder group

 [Figure 2](#)

Figure 2. Certificate information of one of the apps

Installation

SideWinder installs the payload app in two stages. It first downloads a DEX file (an Android file format) from its command and control (C&C) server. We found that the group employs [Apps Conversion Tracking](#) to configure the C&C server address. The address was encoded by Base64 then set to referrer parameter in the URL used in the distribution of the malware.

 [Figure 3](#)

Figure 3. Parsed C&C Server address

After this step, the downloaded DEX file downloads an APK file and installs it after exploiting the device or employing accessibility. All of this is done without user awareness or intervention. To evade detection, it uses many techniques such as obfuscation, data encryption, and invoking dynamic code.

The apps Camero and FileCrypt Manger act as droppers. After downloading the extra DEX file from the C&C server, the second-layer droppers invoke extra code to download, install, and launch the callCam app on the device.

 [Figure 4](#)

Figure 4. Two-stage payload deployment


 [Figure.5](#)

Figure 5. Code showing how the dropper invokes extra DEX code

To deploy the payload app callCam on the device without the user's awareness, SideWinder does the following:

1. Device Rooting

This approach is done by the dropper app Camero and only works on Google Pixel (Pixel 2, Pixel 2 XL), Nokia 3 (TA-1032), LG V20 (LG-H990), Oppo F9 (CPH1881), and Redmi 6A devices. The malware retrieves a specific exploit from the C&C server depending on the DEX downloaded by the dropper.

 [Figure.6](#)

Figure 6. Code snippet from Extra DEX downloaded by Camero

We were able to download five exploits from the C&C server during our investigation. They use the vulnerabilities CVE-2019-2215 and MediaTek-SU to get root privilege.


 [Figure.7](#)

Figure 7. CVE-2019-2215 exploit


 [Figure.8](#)

Figure 8. MediaTek-SU exploit

After acquiring root privilege, the malware installs the app callCam, enables its accessibility permission, and then launches it.


 [Figure.9](#)

Figure 9. Commands install app, launch app, and enable accessibility

2. Device Rooting

This approach is used by the dropper app FileCrypt Manager and works on most typical Android phones above Android 1.6. After its launch, the app asks the user to enable accessibility.

 [Figure.10](#)

Figure 10. Steps FileCrypt Manager prompts user to do

Once granted, the app shows a full screen window that says that it requires further setup steps. In reality, that is just an overlay screen that is displayed on top of all activity windows on the device. The overlay window sets its attributions to `FLAG_NOT_FOCUSABLE` and `FLAG_NOT_TOUCHABLE`, allowing the activity windows to detect and receive the users' touch events through the overlay screen.

 [Figure.11](#)

Figure 11. Overlay screen

Meanwhile, the app invokes code from the extra DEX file to enable the installation of unknown apps and the installation of the payload app callCam. It also enables the payload app's accessibility permission, and then launches the payload app. All of this happens behind the overlay screen, unbeknownst to the user. And, all these steps are performed by employing Accessibility.


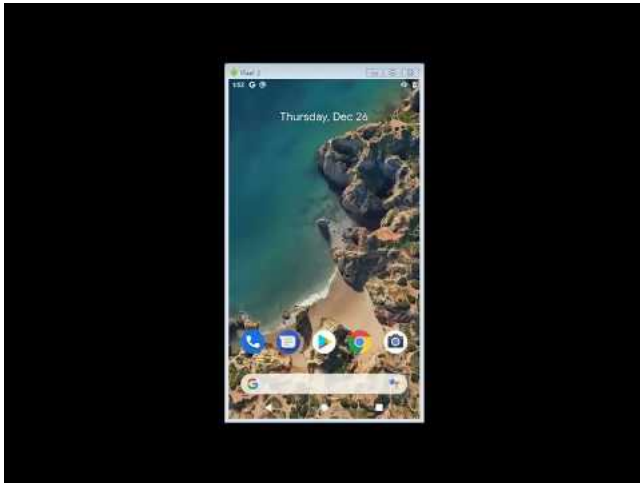
 [Figure.12](#)

Figure 12. Code enabling install of unknown apps and new APK

 [Figure.13](#)

Figure 13. Code enable accessibility permission of the newly installed app

The video below demonstrates payload deployment via CVE-2019-2215 on Pixel 2:



Watch Video At: <https://youtu.be/zyVgQurr33U>

callCam's Activities

The app callCam hides its icon on the device after being launched. It collects the following information and sends it back to the C&C server in the background:

- Location
- Battery status
- Files on device
- Installed app list
- Device information
- Sensor information
- Camera information
- Screenshot
- Account
- Wifi information

The app encrypts all stolen data using RSA and AES encryption algorithms. It uses SHA256 to verify data integrity and customize the encoding routine. When encrypting, it creates a block of data we named headData. This block contains the first 9 bytes of origin data, origin data length, random AES IV, the RSA-encrypted AES encrypt key, and the SHA256 value of AES-encrypted origin data. Then the headData is encoded through the customized routine. After the encoding, it is stored in the head of the final encrypted file followed by the data of the AES-encrypted original data.


 [Figure.14](#)

Figure 14. Data encryption process

 [Figure.15](#)

Figure 15. Customized encoding routine done

Relation to SideWinder

These apps may be attributed to SideWinder as the [C&C servers it uses are suspected to be part of SideWinder's infrastructure](#). In addition, a URL linking to one of the apps' Google Play pages is also found on one of the C&C servers.


 [Figure. 16](#)

Figure 16. Google Play URL of FileManager app found in one of the C&C servers.

Trend Micro Solutions

Trend Micro solutions such as the [Trend Micro™ Mobile Security for Android™](#) can detect these malicious apps. End users can also benefit from its multilayered security capabilities that secure the device owner's data and privacy and safeguard them from ransomware, fraudulent websites, and identity theft.

For organizations, the [Trend Micro Mobile Security for Enterprise](#) suite provides device, compliance, and application management, data protection, and configuration provisioning. It also protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps, and detects and 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 to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerabilities.

Indicators of Compromise

SHA256	Package Name/File type	App Name/Detection N
ec4d6bf06dd3f94f4555d75c6daaf540dee15b18d62cc004e774e996c703cb34	DEX	AndroidOS_SWinderSp
a60fc4e5328dc75dad238d46a2867ef7207b8c6fb73e8bd001b323b16f02ba00	DEX	AndroidOS_SWinderSp
0daefb3d05e4455b590da122255121079e83d48763509b0688e0079ab5d48886	ELF	AndroidOS_MtkSu.A
441d98dff3919ed24af7699be658d06ae8dfd6a12e4129a385754e6218bc24fa	ELF	AndroidOS_BinderExp./
ac82f7e4831907972465477eebafc5a488c6bb4d460575cd3889226c390ef8d5	ELF	AndroidOS_BinderExp./
ee679afb897213a3fd09be43806a7e5263563e86ad255fd500562918205226b8	ELF	AndroidOS_BinderExp./
135cb239966835fefbb346165b140f584848c00c4b6a724ce122de7d999a3251	ELF	AndroidOS_MtkSu.A
a265c32ed1ad47370d56cbd287066896d6a0c46c80a0d9573d2bb915d198ae42	com.callCam.android.callCam2base	callCamm

Package Name/File type	App Name/Detection Name
com.abdulrauf.filemanager	FileCrypt Manager
com.callCam.android.callCam2base	callCamm
com.camero.android.camera2basic	Camera

C&C Servers

- ms-ethics.net
- deb-cn.net
- ap1-acl.net m
- s-db.net
- aws-check.net
- reawk.net

MITRE ATT&CK Matrix™

 [Figure 17](#)