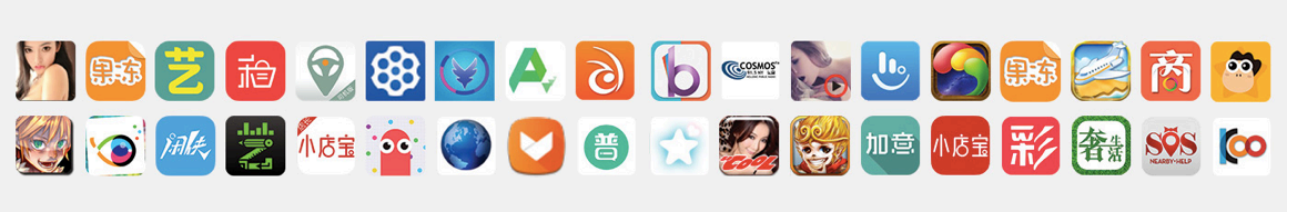
RedDrop: the blackmailing mobile malware family lurking in app stores

By Nell Campbell

Security | February 27, 2018 at 1:52 pm by

As soon as the threat research community collectively gets to grips with a new malware variant, another more aggressive strain rears its ugly head. The latest zero-day threat to be discovered by Wandera's mobile threat research team is RedDrop, a family of mobile malware inflicting financial cost and critical data loss on infected devices. The most worrying part? The 53 malware-ridden apps are exfiltrating sensitive data – including ambient audio recordings – and dumping it in the attackers' Dropbox accounts to prepare for further attacks and extortion purposes.

The infection was first unearthed at several global consultancy firms, when Wandera's machine intelligence engine – MI:RIAM – blocked a suspicious app download. Since then, Wandera's threat research team has investigated the app and its hidden functionality in more detail to gain a clearer understanding of the previously undiscovered mobile malware family which we have termed RedDrop.



- *Zero-day threat previously unknown within the mobile security community*
- *Group of at least 50 functioning apps containing the sophisticated RedDrop malware*
- *Apps are distributed from a complex network of 4,000+ domains registered to the same underground group*
- *Once the app is opened, at least seven further APKs are silently downloaded, unlocking new malicious functionality*
- *When the user interacts with the app, each interaction secretly triggers the sending of an SMS to a premium service, which is then instantly deleted before it can be detected*
- *These additional APKs include spyware-like components, harvesting sensitive data, including passively recording the device's audio, photos, contacts, files and more*
- *RedDrop then exfiltrates this data, uploading it straight into remote file storage systems for use in extortion and blackmailing purposes*

RedDrop: Wandera's research findings

A total of 53 new malicious applications have so far been discovered to be harbouring this malware variant. The applications range from practical tools like image editors and calculators, to more recreational apps covering topics like space exploration or learning new languages. Each one is intricately built to provide entertaining or useful functionality – to act as a seemingly innocent guise for the malicious content stored within.

Apps within the RedDrop family request invasive permissions enabling the attack to be conducted without requesting further interaction from the user. One of the more destructive permissions allows the malware to be persistent between reboots. Granting it the ability to constantly communicate with command and control (C&C) servers, permitting the covert activation of its malicious functionality.

1. The complex distribution network

Wandera's machine learning detections first uncovered one of the RedDrop apps when a user clicked on an ad displaying on popular Chinese search engine **Baidu**. The user was then taken to **huxiawang.cn**, the primary distribution site for the attack. The landing pages that follow host various content to encourage and incite the user to download one of the 53 apps within the RedDrop family of malicious apps.

RedDrop's creators utilise an intricate content distribution network (CDN) of over 4,000 domains to distribute the applications serving the malware. In Wandera tests, upon clicking on **huxiawang.cn,** users were taken through a complex series of network redirects in an attempt to circumvent and evade malware detection techniques, prior to being presented with the download.

> *We believe the group developed this complex CDN to obfuscate where the malware was served from, making it harder for security teams to detect the source of the threat. Senior Security Researcher at Wandera*

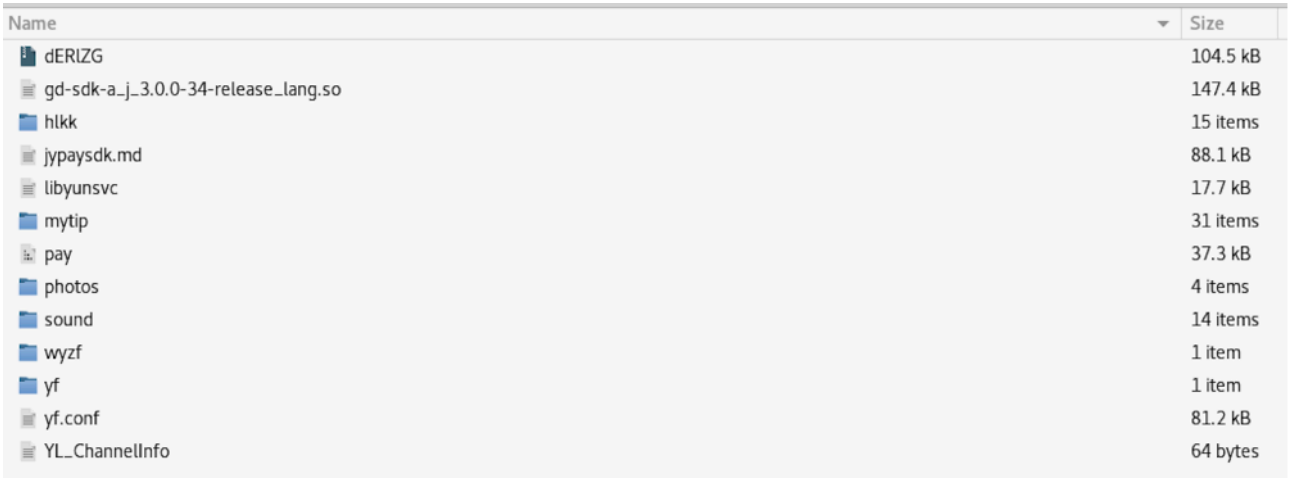
2. The malicious functionality

RedDrop is highly destructive due to the sophistication of its distribution network and the powerful hybrid functionality which delivers multiple malicious actions in one package. Through static and dynamic analysis of

the RedDrop drive-by, Wandera's threat research team uncovered a mechanism whereby 7+ additional APKs are silently installed onto the device from the C&C server. These additional APKs contain the following functionality:

A) Trojan

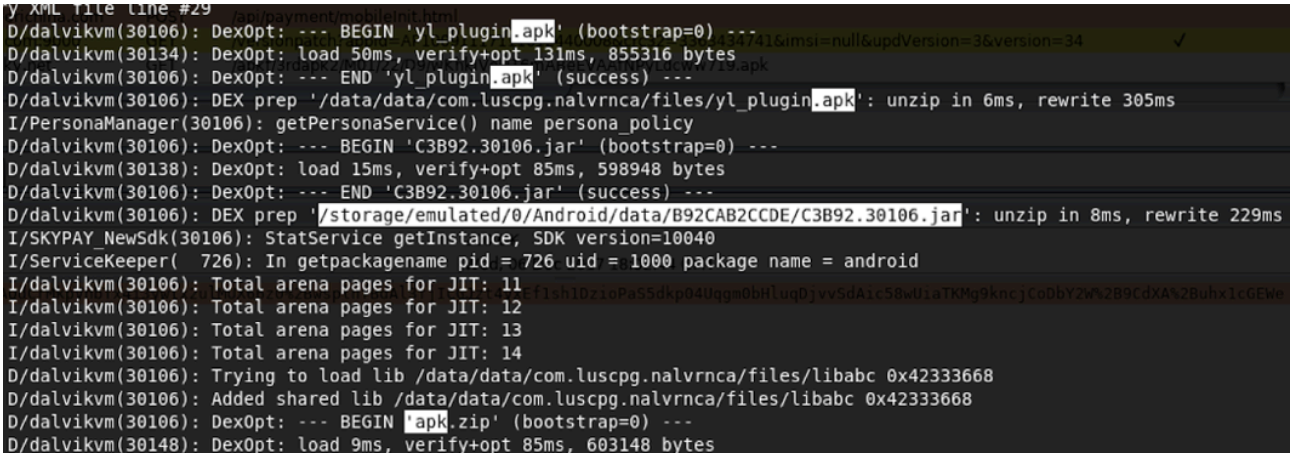
When the RedDrop apps are unzipped (static analysis) they're found to contain malicious embedded files, which are then compiled in order to initiate the malicious functionality. These files are located in the assets folder of the application shown below.



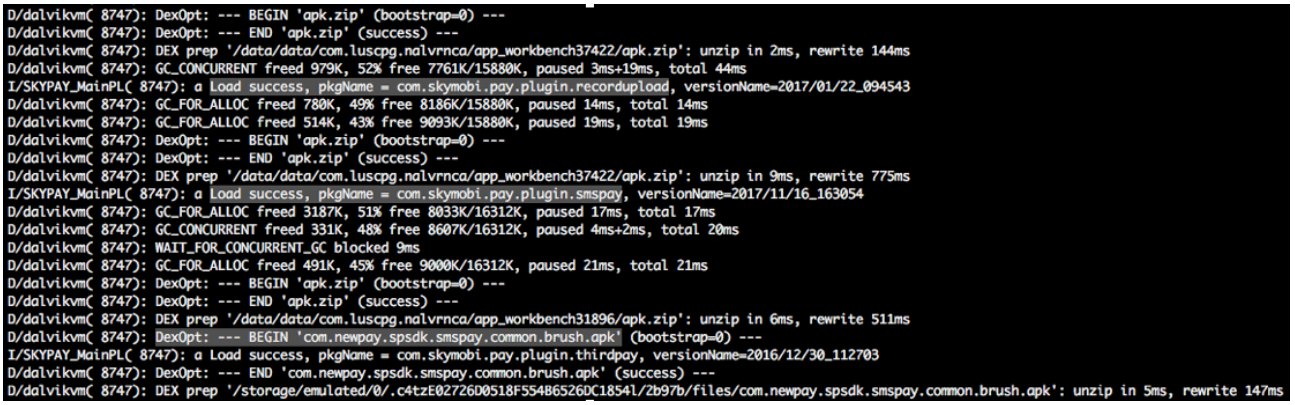
Contents of RedDrop malware application package (APK)

B) Dropper

Immediately after installation, the malware downloads additional components (APKs, JAR files) from different C&C servers, storing them dynamically into the device's memory. This technique allows the attacker to stealthily execute additional malicious APKs without having to embed them straight into the initial sample. This can be seen from both the network communication and the device logs.



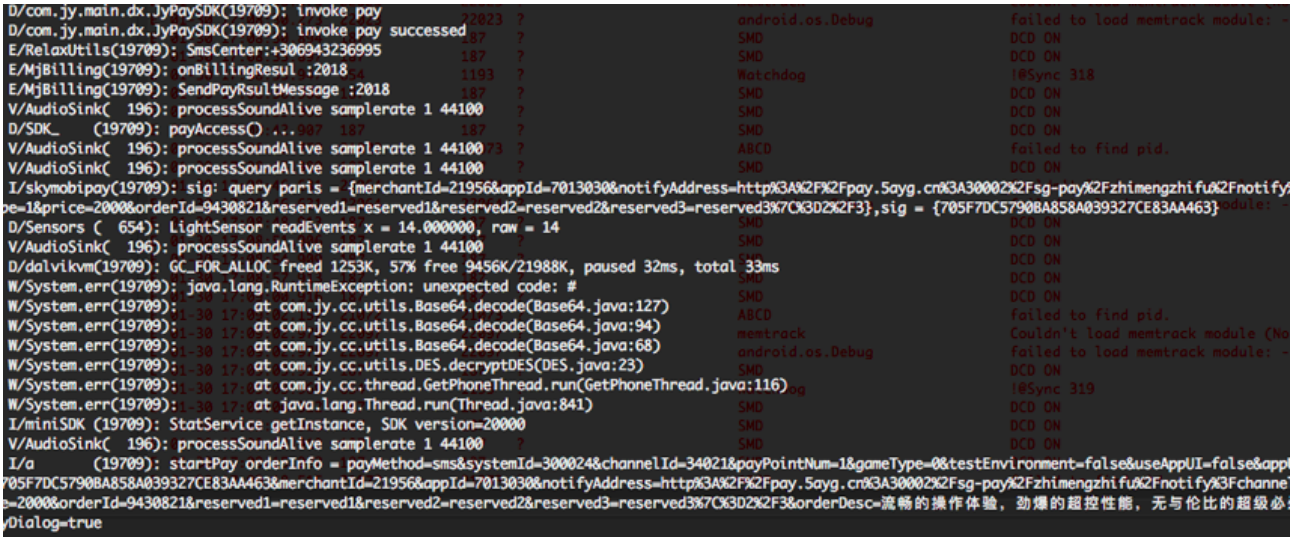
Optimizing malicious components for execution



Loading Dropped APKs

C) SMS fraud and Spyware

Apps within the RedDrop family each provide clear functionality to the user, which requires the victim to interact with their mobile device. In one such sample, each time the screen is touched within the app, the user is unwittingly sending an SMS message to a premium service incurring substantial charges. Crucially, the malware is able to delete these messages almost instantly, meaning the evidence of these premium SMS is destroyed.



Payment service through SMS method

Perhaps the most perverse aspect of the RedDrop malware family, is its invasive set of spyware tools. Firstly, the malicious application is spying to identify when the user is present in order to initiate the rest of the malicious functionality. Then, the app records and exfiltrates data to a variety of servers and cloud storage services.

3) Critical data loss

When all of the functionality is combined, RedDrop aims to extract valuable and damaging data from the victim. As soon as the information is collected, it is transmitted back to the attackers' personal Dropbox or Drive folders to be used in their extortion schemes and as the foundation to launch further attacks.

Data stolen includes:

1. Locally saved files – photos/contacts/images
2. Live recordings of the device's surroundings
3. Device Related Info (IMEI, IMSI, etc)
4. SIM Related Info (MNC, MCC, etc)
5. Application data
6. Nearby WiFi Networks

Wandera revealed different types of information exfiltration by the RedDrop malware family, including encrypted and unencrypted data, encoded data and TCP streams.

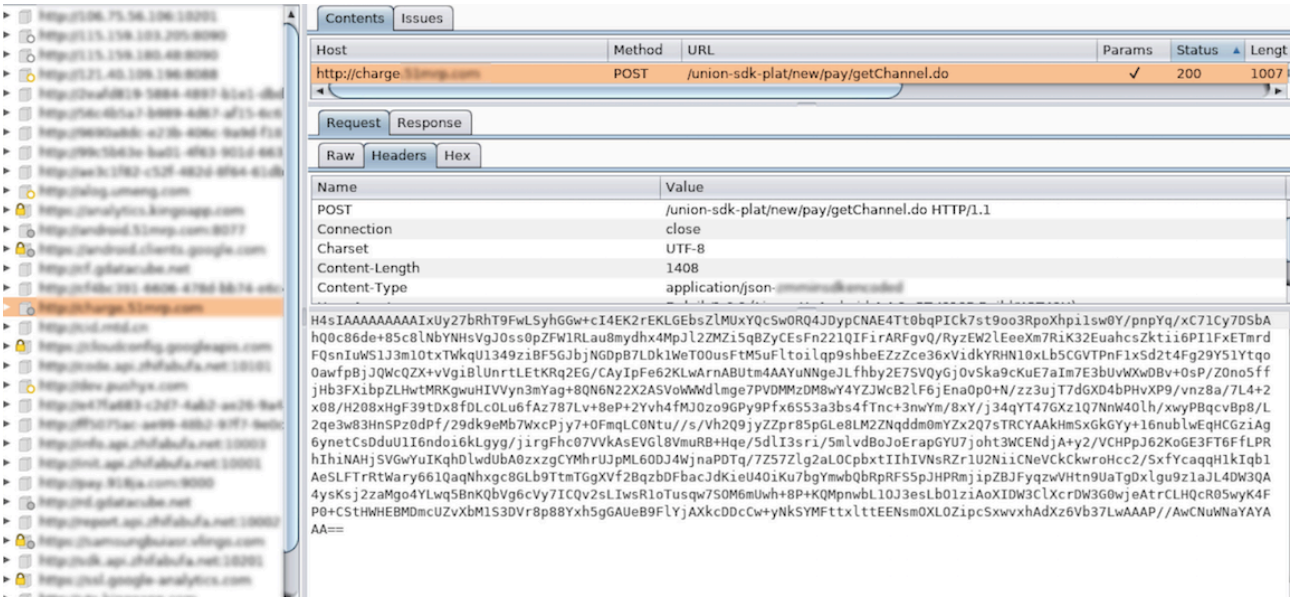
The data exfiltrated provides the attacker with more device-centric information. Ranging from whether the device is on Wi-Fi or Cellular, the operating system and manufacturer details of the device up to checking if the device is already rooted or not. Sim card related information (ICCID) also is being transmitted.

In more detail, the parameters of the request are:

- netConnectionType
- osVersion
- imei
- appId
- os_ui_version
- ourVersion
- packageName
- channelId
- iccid
- isRoot
- deviceManufacturer
- type
- deviceNo
- mac
- deviceType
- imsi

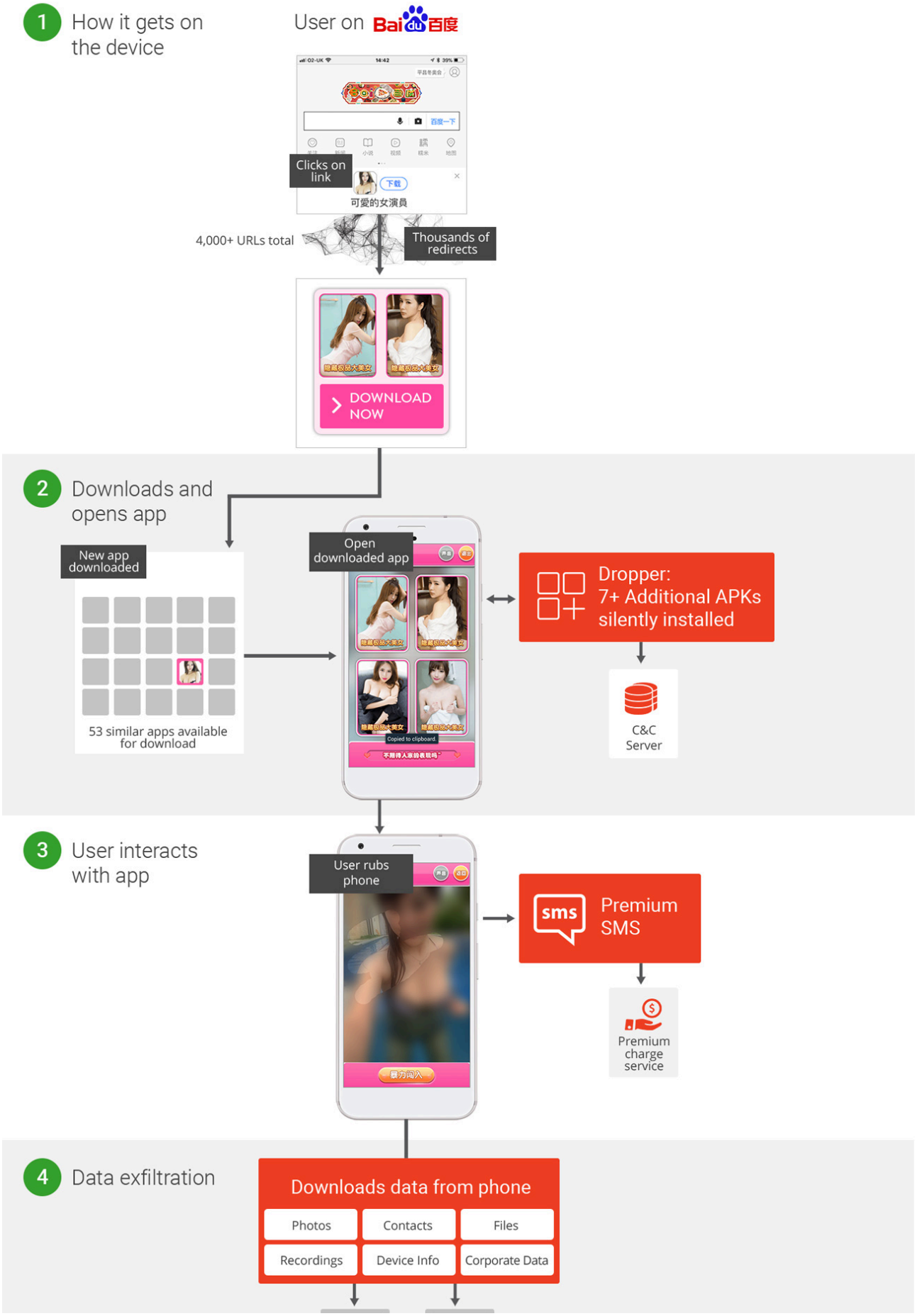
Example of exfiltrated data transfer

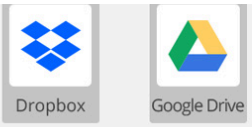
Below we can see how data related to the SMS payments and internal network details are being exfiltrated. The encoded payload is visible on the bottom right part of the screenshot:



Case study: CuteActress

Zero-day mobile malware: A RedDrop application in the wild


1
How it gets on the device
User on Baidu 百度
Clicks on link
可愛的女演員
4,000+ URLs total
Thousands of redirects
DOWNLOAD NOW
2
Downloads and opens app
New app downloaded
53 similar apps available for download
Open downloaded app
Copied to clipboard.
Dropper: 7+ Additional APKs silently installed
C&C Server
3
User interacts with app
User rubs phone
sms
Premium SMS
Premium charge service
4
Data exfiltration
Downloads data from phone
Photos
Contacts
Files
Recordings
Device Info
Corporate Data



The CuteActress app ostensibly functions as an adult-themed game in which the user must rub the screen in order to reveal a seductively-dressed female. Each time the screen is 'rubbed', the user is unknowingly sending an SMS message to a premium service. After installation the app dynamically loads 7 additional APKs with trojan, dropper, spyware and data exfiltration functionality, like the rest of the apps in the RedDrop mobile malware family.

Conclusion

RedDrop is one of the most sophisticated pieces of Android malware that we have seen in broad distribution. Not only does the attacker utilize a wide range of functioning malicious applications to entice the victim, they've also perfected every tiny detail to ensure their actions are difficult to trace. From the complex distribution network of over 4,000+ domains and concealed APKs to SMS functionality and the data exfiltration – the group that built this malware have planned it exceedingly well.

In order to protect themselves from these types of threats, individuals and organizations with vulnerable devices should disable downloads from third-party app stores, unless absolutely necessary for business functionality. Wandera research shows that more than 20% of corporate Android devices allow third-party installations, so a significant number of devices are vulnerable to this threat.

It's also worth noting that Oreo, Google's latest OS version, makes it easier for users to detect apps with invasive permissions as they receive prompts when an app is attempting to gain escalated privileges. However, according to Google, almost half of Android devices are still running OS versions that predate Marshmallow – making it simple for RedDrop to bypass user scrutiny and be installed on devices. Organizations are strongly recommended to update their fleets to the latest version of Android to minimize their exposure to this new malware family.

> 
> *This multifaceted hybrid attack is entirely unique. The malicious actor cleverly uses a seemingly helpful app to front an incredibly complex operation with malicious intent. This is one of the more persistent malware variants we've seen. Dr Michael Covington, VP of Product Strategy at Wandera*

It's likely that RedDrop will continue to be employed by attackers even after these apps are flagged as malicious. As was seen in the case of SLocker last year, attackers are smart in creating variants of known malware in an attempt to bypass traditional security measures. We expect the same to be true of RedDrop in the coming months –

and much like with SLocker, future variants will be detected by MI:RIAM, the security intelligence engine powering Wandera's threat detection.

Wandera's threat research team will continue to investigate RedDrop variants and will update you on their findings.

General app safety tips

- Change your device settings to disallow third-party downloads
- Avoid rooting your device
- Check the permissions apps are requesting
- Deploy in a security solution that can monitor and block C&C traffic at the device level

Learn more about threat prevention

You might hear about the dangerous leaks and mobile attacks that make the news. But your organization might just be vulnerable to other threats right now.

FIND OUT MORE
