Unmasking State-Sponsored Mobile Surveillance Malware from Russia, China, and North Korea

Threat Actors, Tactics, and Defense Strategies

Kyle Schmittle
Alemdar Islamoglu
Kristina Balaam

black hat®
EUROPE 2024

Who We Are

Kyle Schmittle

Senior Security Intelligence Researcher

- Russia & Iran
- BouldSpy, GuardZoo
- Threat intelligence, reverse engineering

https://www.linkedin.com/in/kyle-s-b851ab151/

Kristina Balaam

Senior Staff Security Intelligence Researcher

- Campaigns initiated by Chinese threat actors.
- DragonEgg/WyrmSpy, MOONSHINE & Android BadBazaar
- Passion for uncovering threats that target marginalized populations within mainland China and abroad.

https://linkedin.com/in/kebalaam

Alemdar Islamoglu

Senior Staff Security Intelligence Researcher

- North Korea and Middle East.
- Hermit, BouldSpy and GuardZoo
- Reverse engineering, penetration testing, and security software development.

https://www.linkedin.com/in/alemdarh/

Agenda

- I – Overview of the Mobile APT Landscape
  - Russia, China, North Korea
- II – APTs and Their Tricks
  - Accessing Devices
  - Detection Countermeasures
  - Who’s Under Attack
  - How We Attribute Activity

Agenda

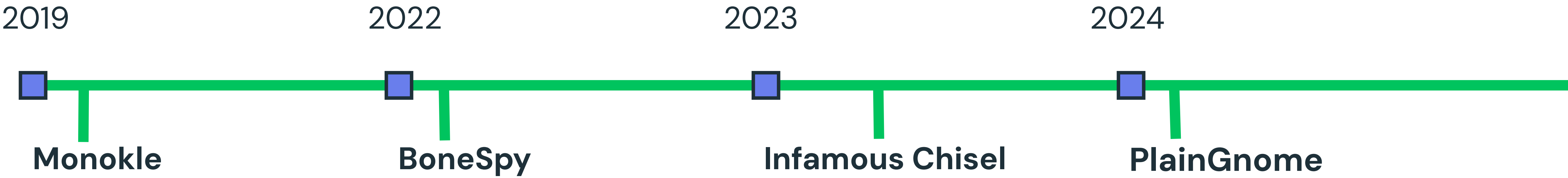
- III – Takeaways
  - Fingerprints of State-Backed Surveillance
  - Mitigation Techniques
  - Call to Action

I – Overview of the Mobile APT Landscape

Russia, China, North Korea

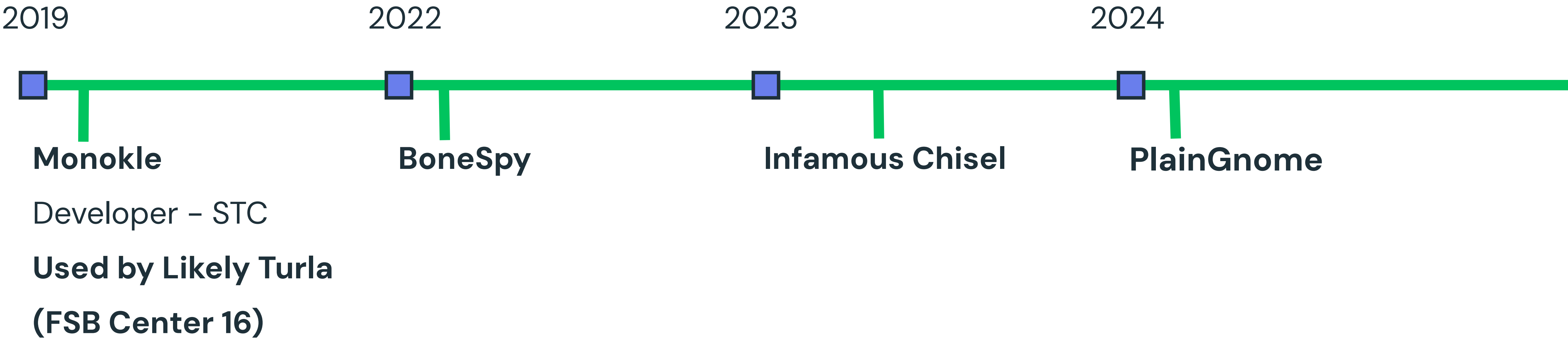
Mobile APT Groups: Russia

Mobile APT Groups: Russia



2019	2022	2023	2024
Monokle	BoneSpy	Infamous Chisel	PlainGnome

Mobile APT Groups: Russia



2019

Monokle

Developer – STC

Used by Likely Turla

(FSB Center 16)

2022

BoneSpy

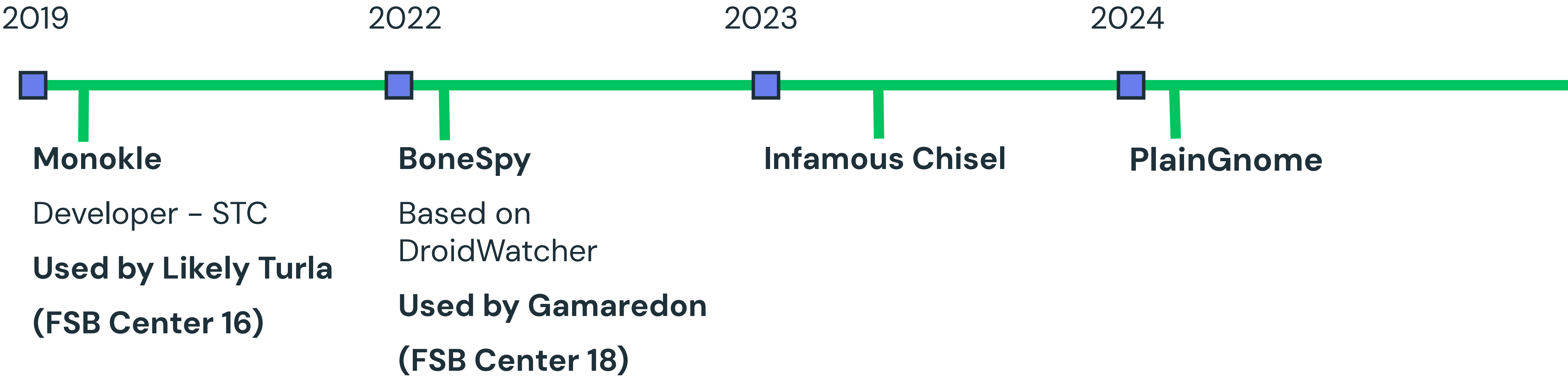
2023

Infamous Chisel

2024

PlainGnome

Mobile APT Groups: Russia



2019

Monokle

Developer – STC

Used by Likely Turla

(FSB Center 16)

2022

BoneSpy

Based on DroidWatcher

Used by Gamaredon

(FSB Center 18)

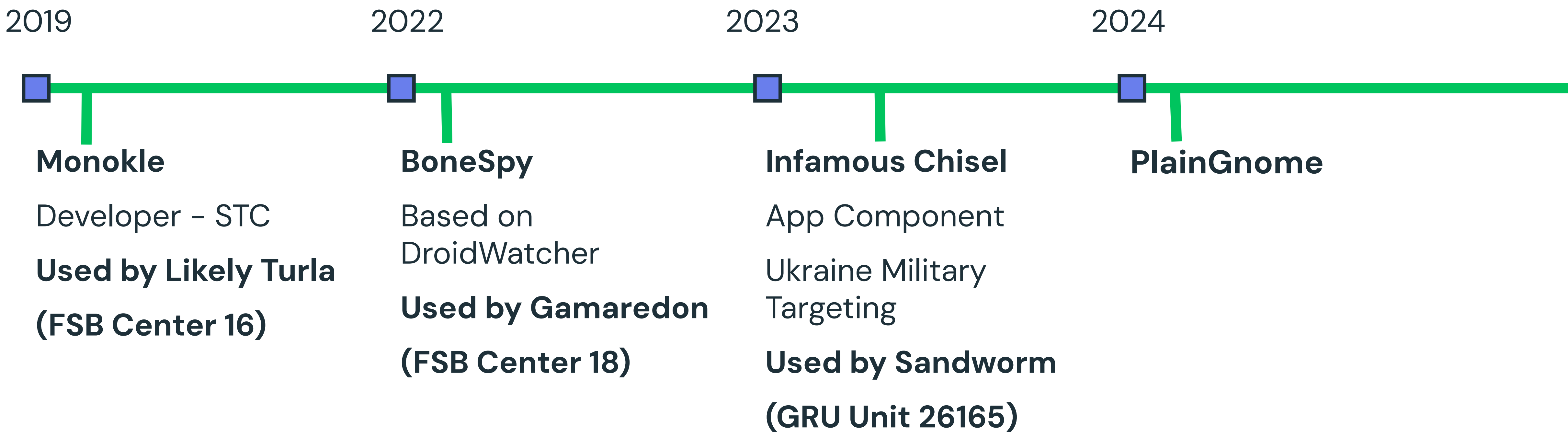
2023

Infamous Chisel

2024

PlainGnome

Mobile APT Groups: Russia



2019

Monokle

Developer – STC

Used by Likely Turla

(FSB Center 16)

2022

BoneSpy

Based on DroidWatcher

Used by Gamaredon

(FSB Center 18)

2023

Infamous Chisel

App Component

Ukraine Military Targeting

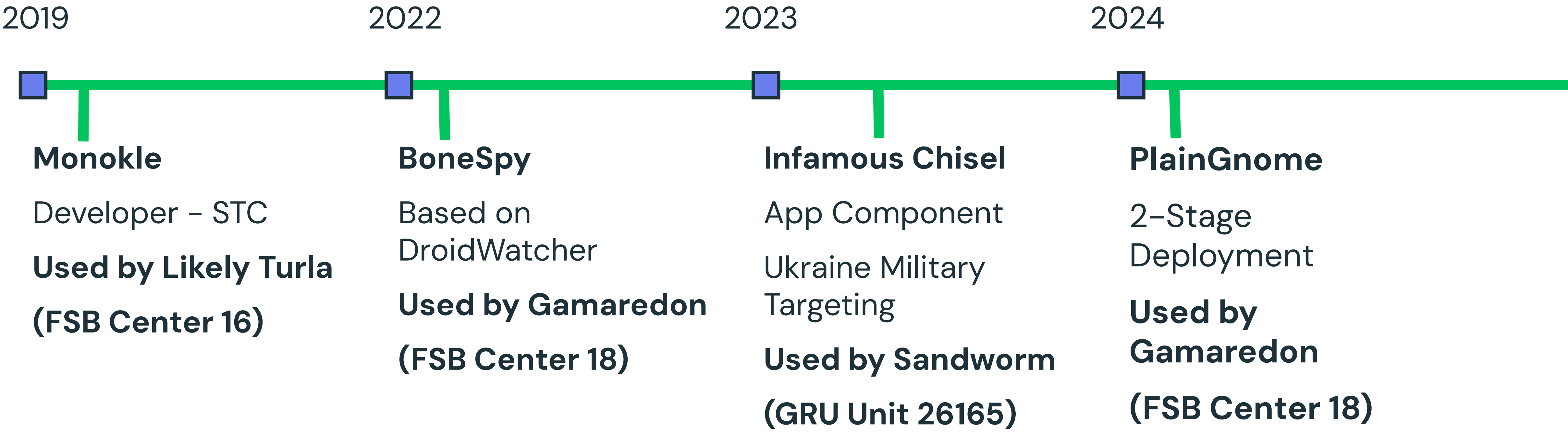
Used by Sandworm

(GRU Unit 26165)

2024

PlainGnome

Mobile APT Groups: Russia



2019

Monokle

Developer – STC

Used by Likely Turla

(FSB Center 16)

2022

BoneSpy

Based on DroidWatcher

Used by Gamaredon

(FSB Center 18)

2023

Infamous Chisel

App Component

Ukraine Military Targeting

Used by Sandworm

(GRU Unit 26165)

2024

PlainGnome

2-Stage Deployment

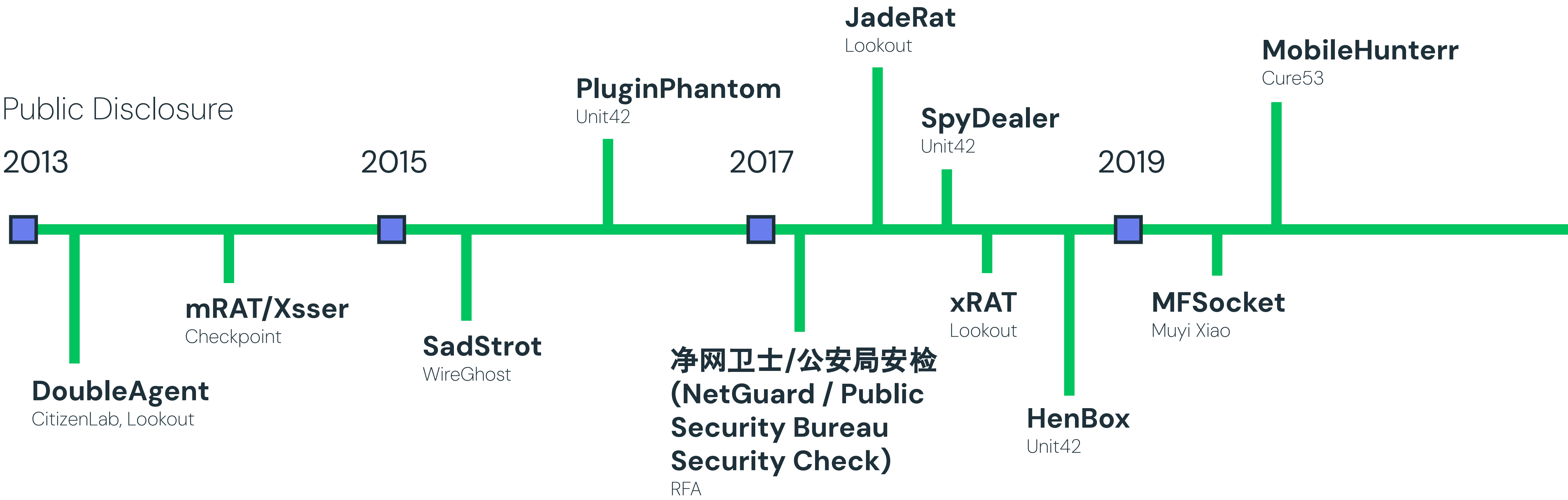
Used by Gamaredon

(FSB Center 18)

Mobile APT Groups: China

The Mobile Chinese Surveillance Landscape

Major Mobile Chinese Surveillance Campaigns



Public Disclosure

2013

DoubleAgent
CitizenLab, Lookout

mRAT/Xsser
Checkpoint

2015

SadStrot
WireGhost

PluginPhantom
Unit42

2017

净网卫士/公安局安检 (NetGuard / Public Security Bureau Security Check)
RFA

JadeRat
Lookout

SpyDealer
Unit42

xRAT
Lookout

HenBox
Unit42

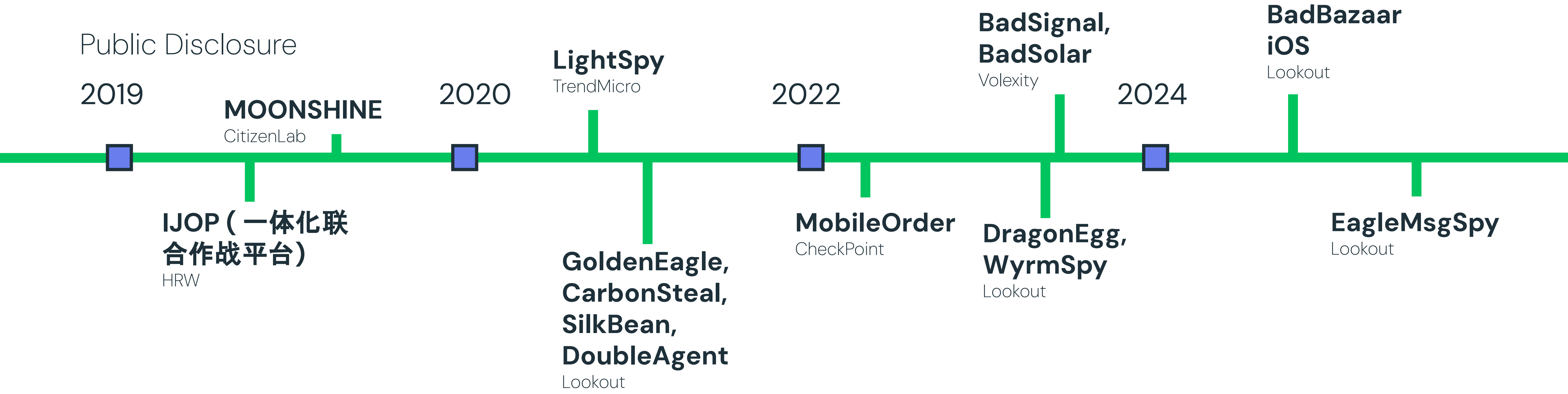
2019

MFSocket
Muyi Xiao

MobileHunterr
Cure53

The Mobile Chinese Surveillance Landscape

Major Mobile Chinese Surveillance Campaigns



Public Disclosure

2019

MOONSHINE
CitizenLab

IJOP (一体化联合作战平台)
HRW

2020

LightSpy
TrendMicro

GoldenEagle, CarbonSteal, SilkBean, DoubleAgent
Lookout

2022

MobileOrder
CheckPoint

BadSignal, BadSolar
Volexity

DragonEgg, WyrmSpy
Lookout

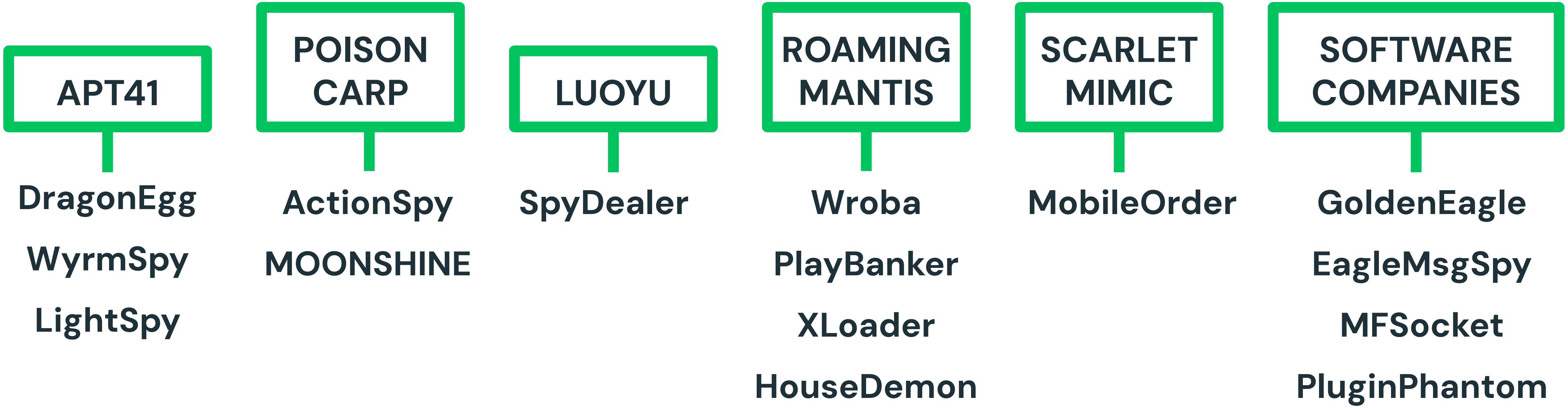
2024

BadBazaar iOS
Lookout

EagleMsgSpy
Lookout

Mobile APT Groups: China

Major Threat Actor – Malware Relationships



APT41
- DragonEgg
- WyrmSpy
- LightSpy

POISON CARP
- ActionSpy
- MOONSHINE

LUOYU
- SpyDealer

ROAMING MANTIS
- Wroba
- PlayBanker
- XLoader
- HouseDemon

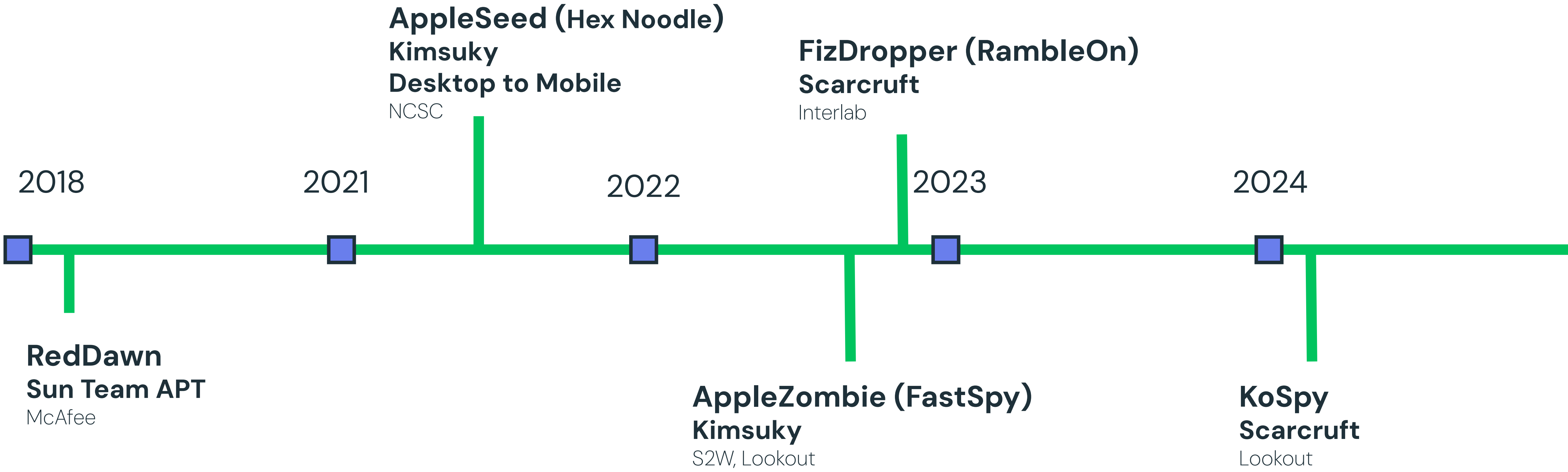
SCARLET MIMIC
- MobileOrder

SOFTWARE COMPANIES
- GoldenEagle
- EagleMsgSpy
- MFSocket
- PluginPhantom

Mobile APT Groups: North Korea

Mobile APT Campaigns: North Korea

Malware Families Timeline



2018

RedDawn
Sun Team APT
McAfee

2021

AppleSeed (Hex Noodle)
Kimsuky
Desktop to Mobile
NCSC

2022

AppleZombie (FastSpy)
Kimsuky
S2W, Lookout

FizDropper (RambleOn)
Scarcruft
Interlab

2023

2024

KoSpy
Scarcruft
Lookout

II – APTs and Their Tricks

Accessing Devices

Russia

Strong reliance on social engineering

Strong reliance on social engineering

Spearphishing

Strong reliance on social engineering

Spearphishing

Deception

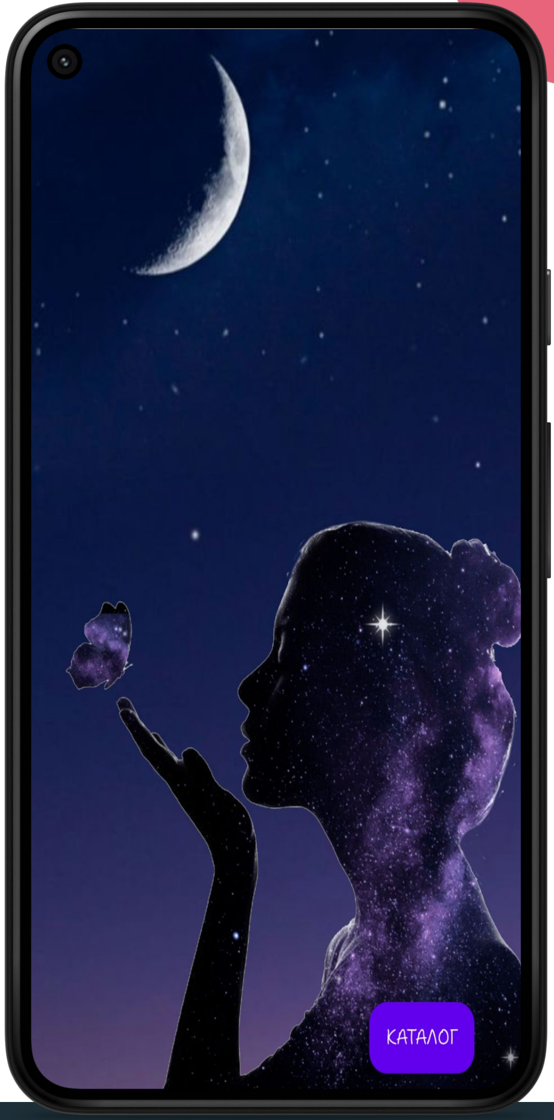
Strong reliance on social engineering

Spearphishing

Deception

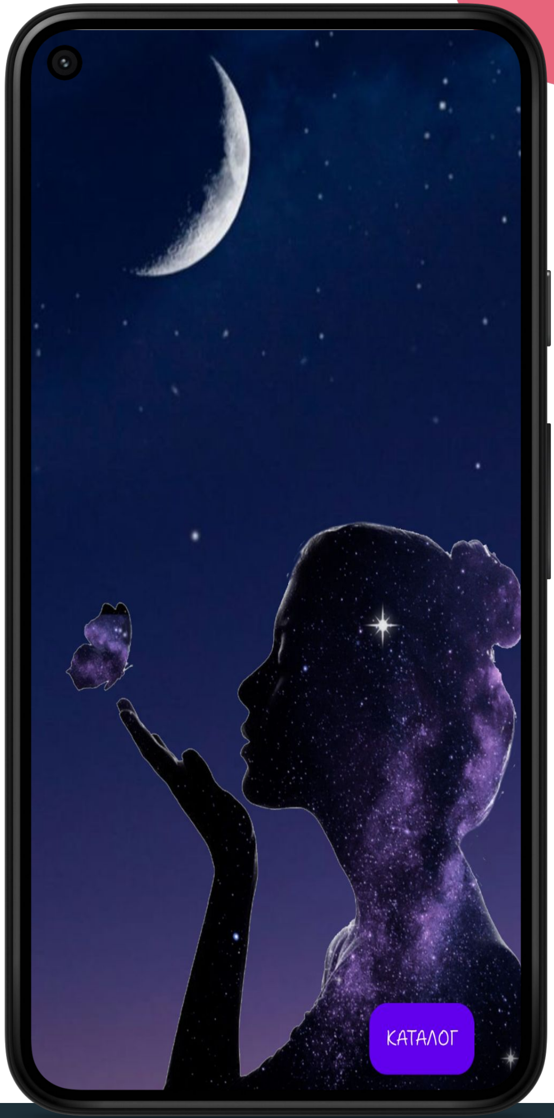
Physical Access

PlainGnome introduced 2024



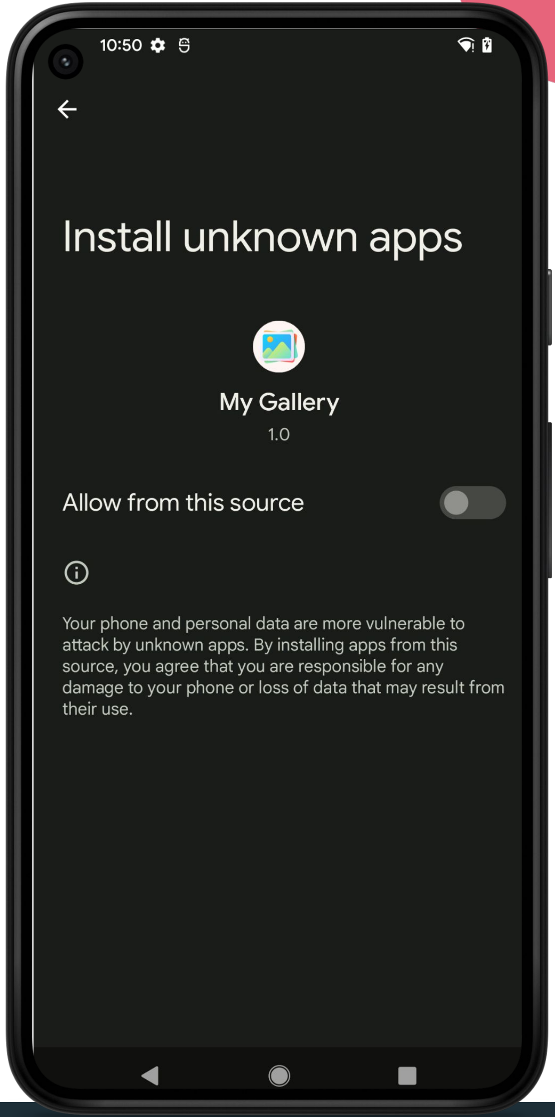
Two-Stage Deployment

Stage 1
MainActivity



Two-Stage Deployment

Stage 1
MainActivity



10:50

Install unknown apps

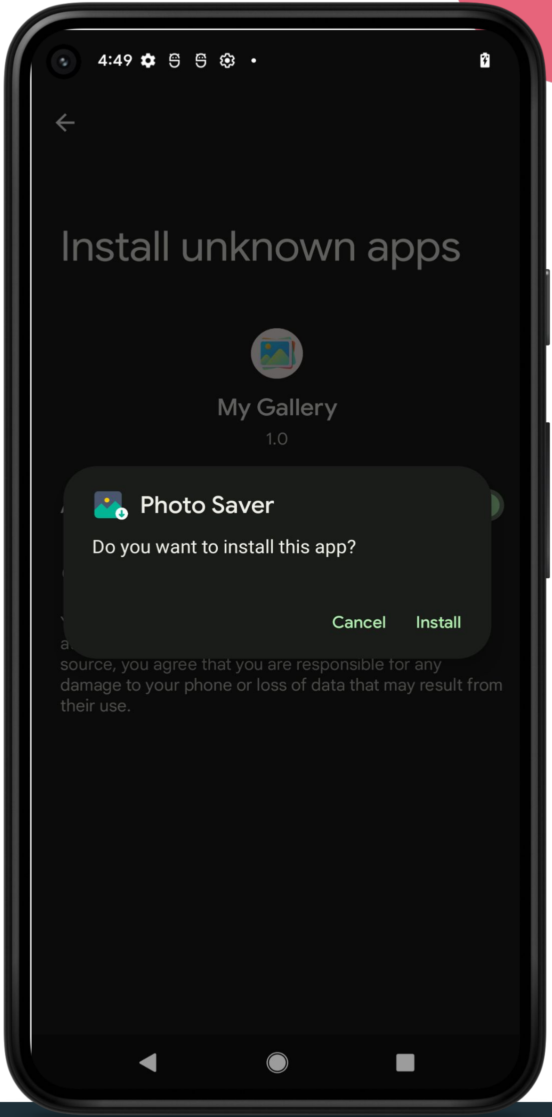
My Gallery
1.0

Allow from this source

Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

Two-Stage Deployment

Stage 1
MainActivity



4:49

Install unknown apps

My Gallery
1.0

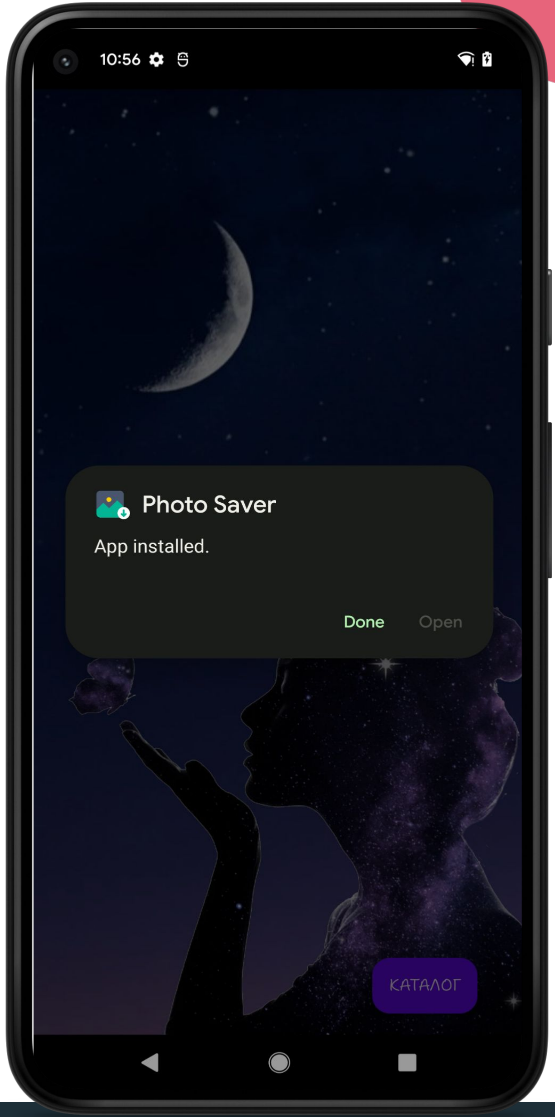
Photo Saver

Do you want to install this app?

source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

Two-Stage Deployment

Stage 1
MainActivity



10:56

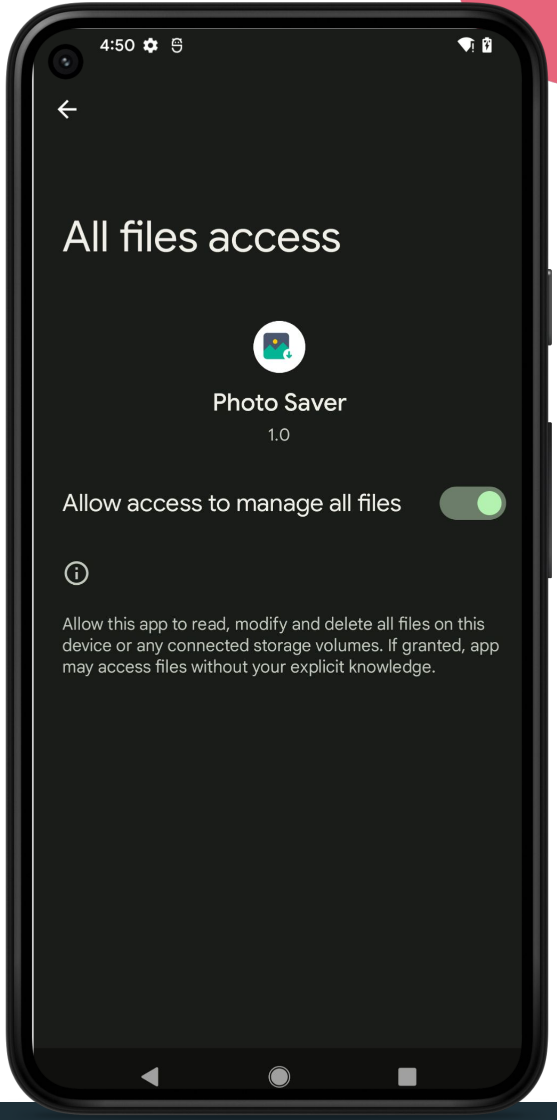
Photo Saver

App installed.

Two-Stage Deployment

Stage 1
MainActivity

Stage 2
MainActivity



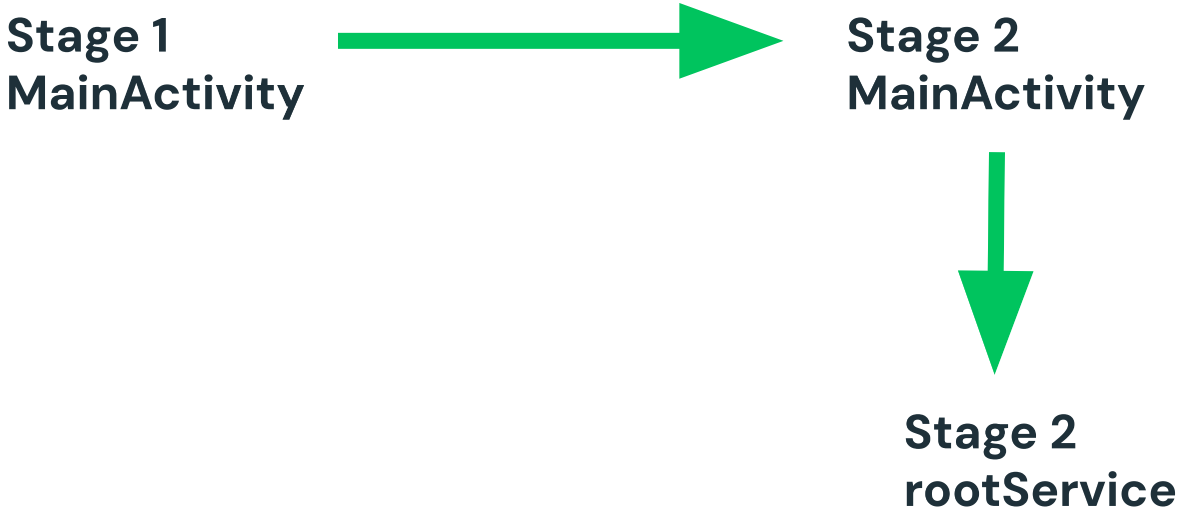
All files access

Photo Saver
1.0

Allow access to manage all files ●

Allow this app to read, modify and delete all files on this device or any connected storage volumes. If granted, app may access files without your explicit knowledge.

Two-Stage Deployment


Stage 1
MainActivity

Stage 2
MainActivity

Stage 2
rootService

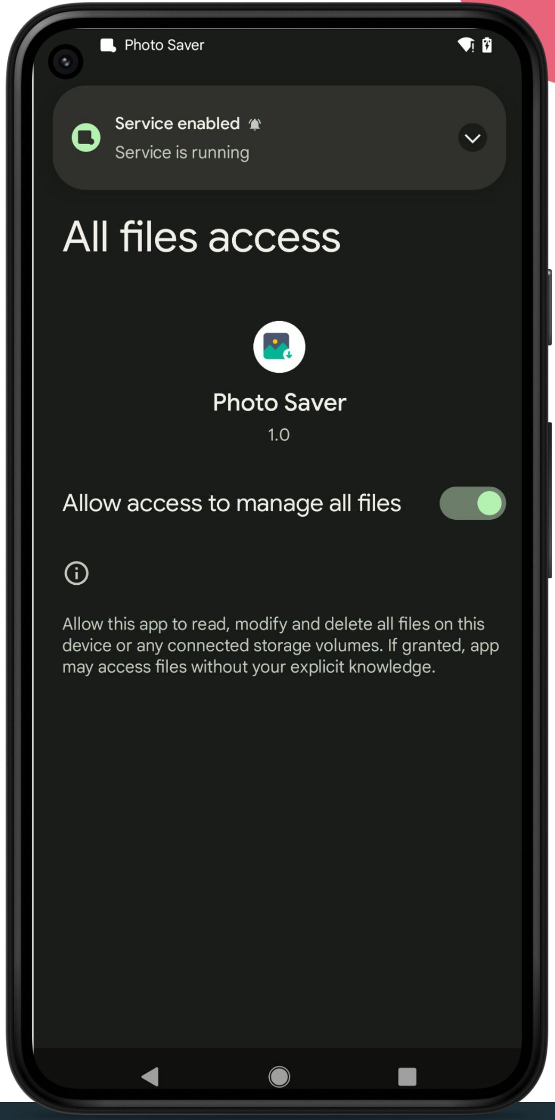


Photo Saver

Service enabled
Service is running

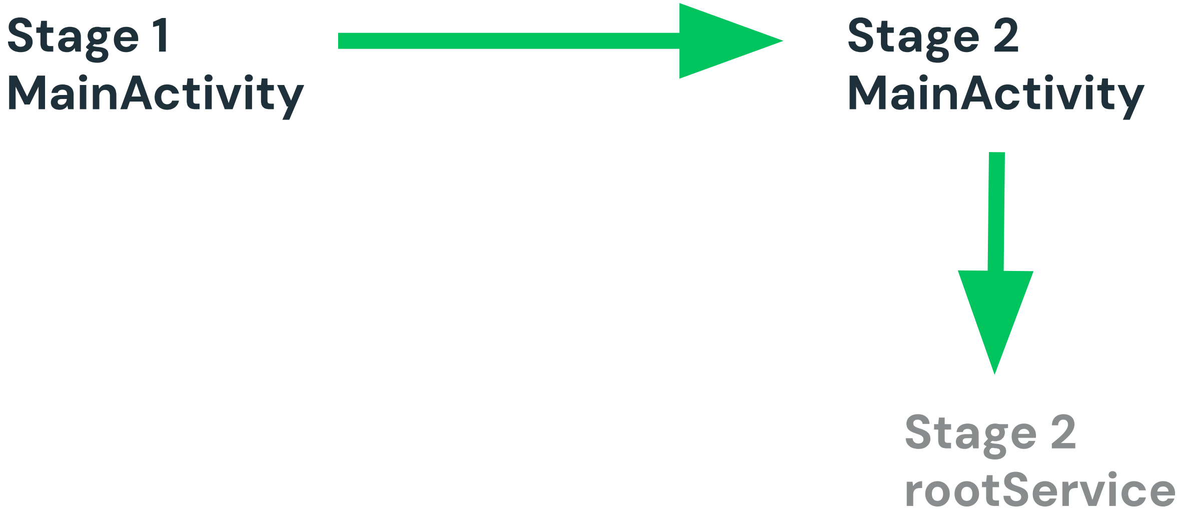
All files access

Photo Saver
1.0

Allow access to manage all files

Allow this app to read, modify and delete all files on this device or any connected storage volumes. If granted, app may access files without your explicit knowledge.

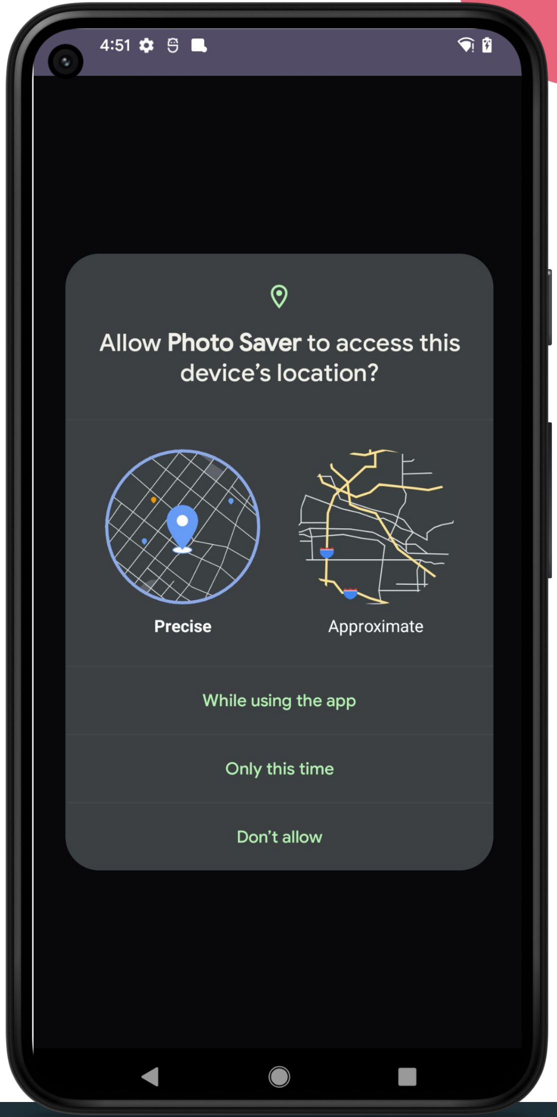
Two-Stage Deployment



Stage 1
MainActivity

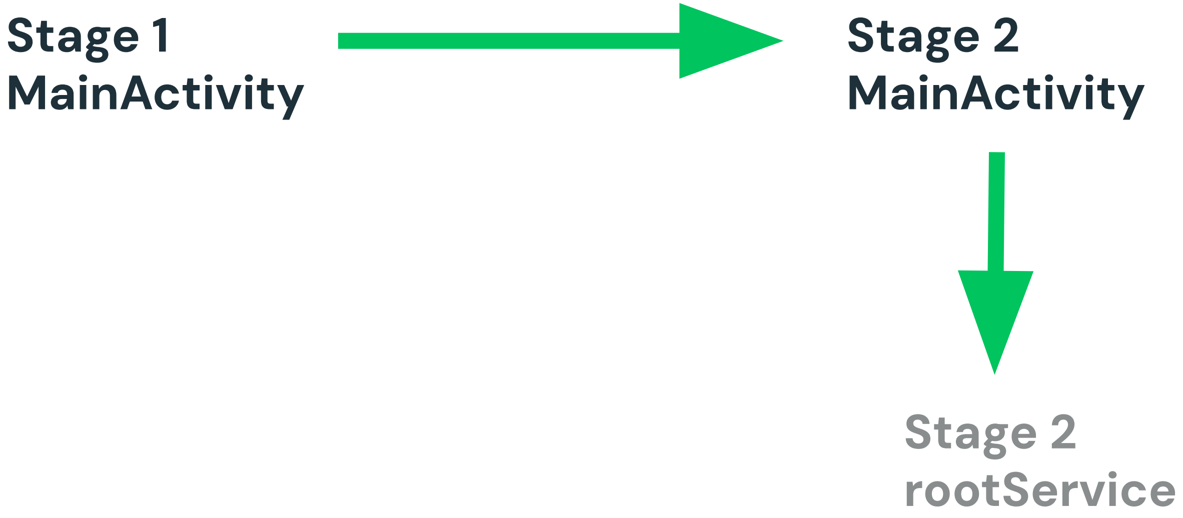
Stage 2
MainActivity

Stage 2
rootService



Allow **Photo Saver** to access this device's location?

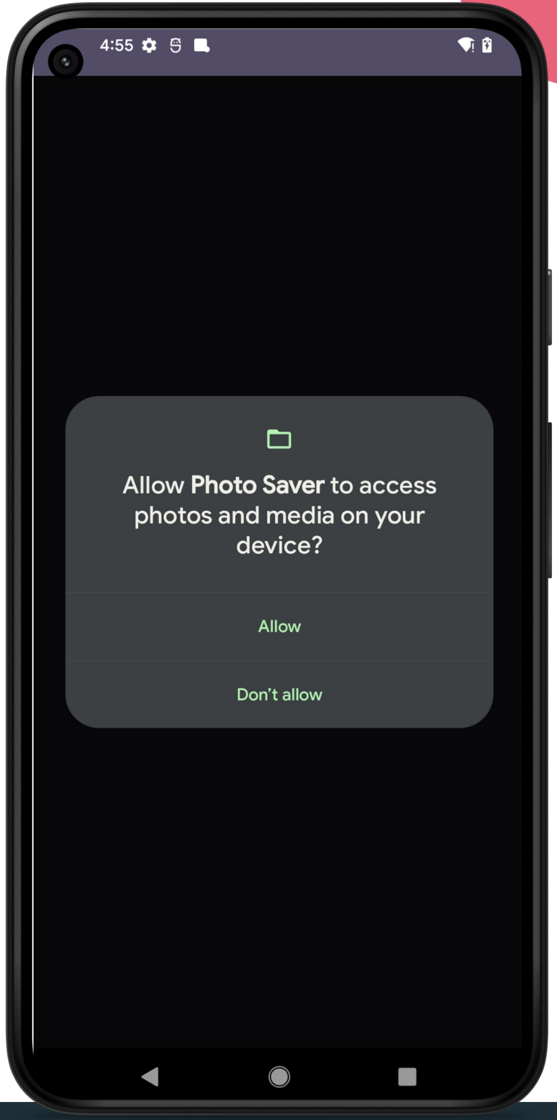
Two-Stage Deployment



Stage 1
MainActivity

Stage 2
MainActivity

Stage 2
rootService

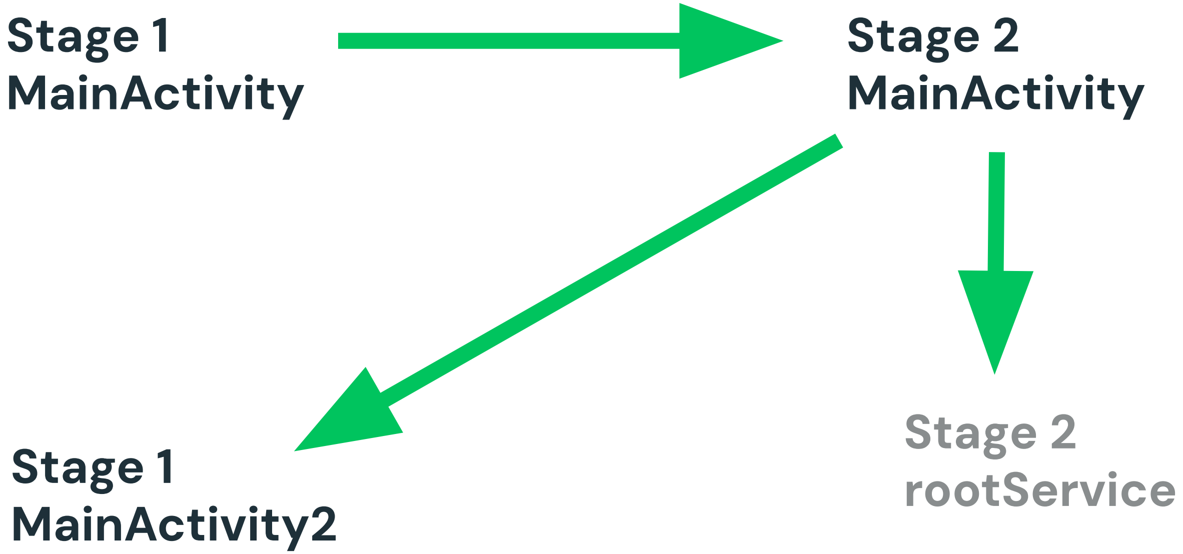


Allow **Photo Saver** to access photos and media on your device?

Allow

Don't allow

Two-Stage Deployment



Stage 1
MainActivity

Stage 2
MainActivity

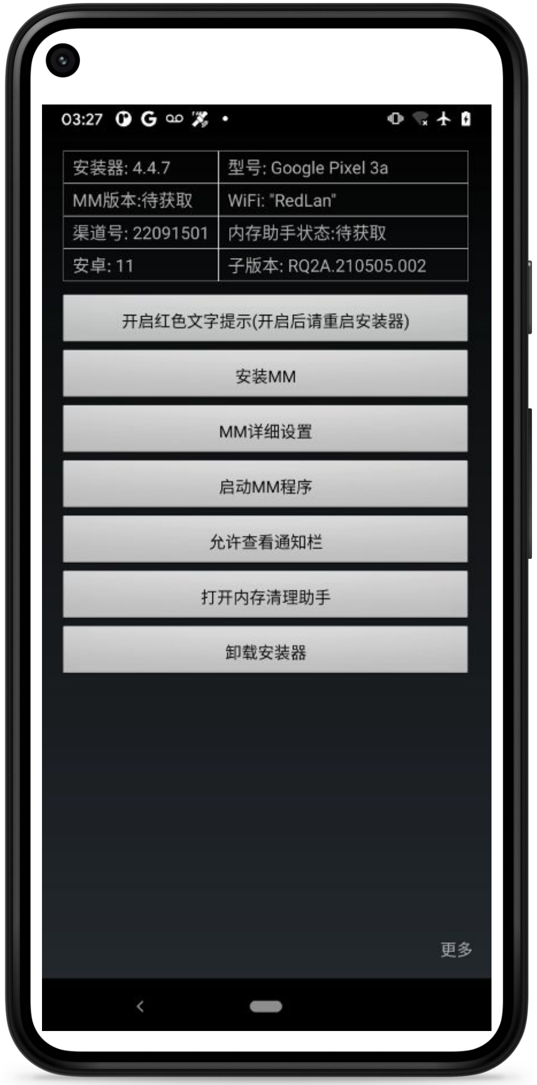
Stage 1
MainActivity2

Stage 2
rootService

China

Physical Access

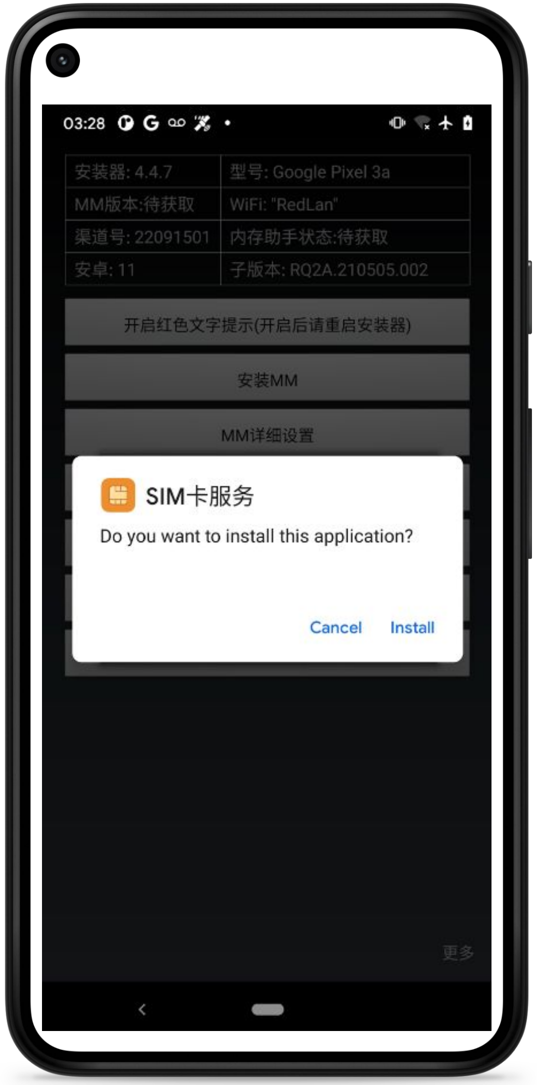
Reports of devices confiscated by law enforcement, at border checkpoints, by immigration officials.



安装器: 4.4.7	型号: Google Pixel 3a
MM版本:待获取	WiFi: "RedLan"
渠道号: 22091501	内存助手状态:待获取
安卓: 11	子版本: RQ2A.210505.002

Physical Access

Reports of devices confiscated by law enforcement, at border checkpoints, by immigration officials.



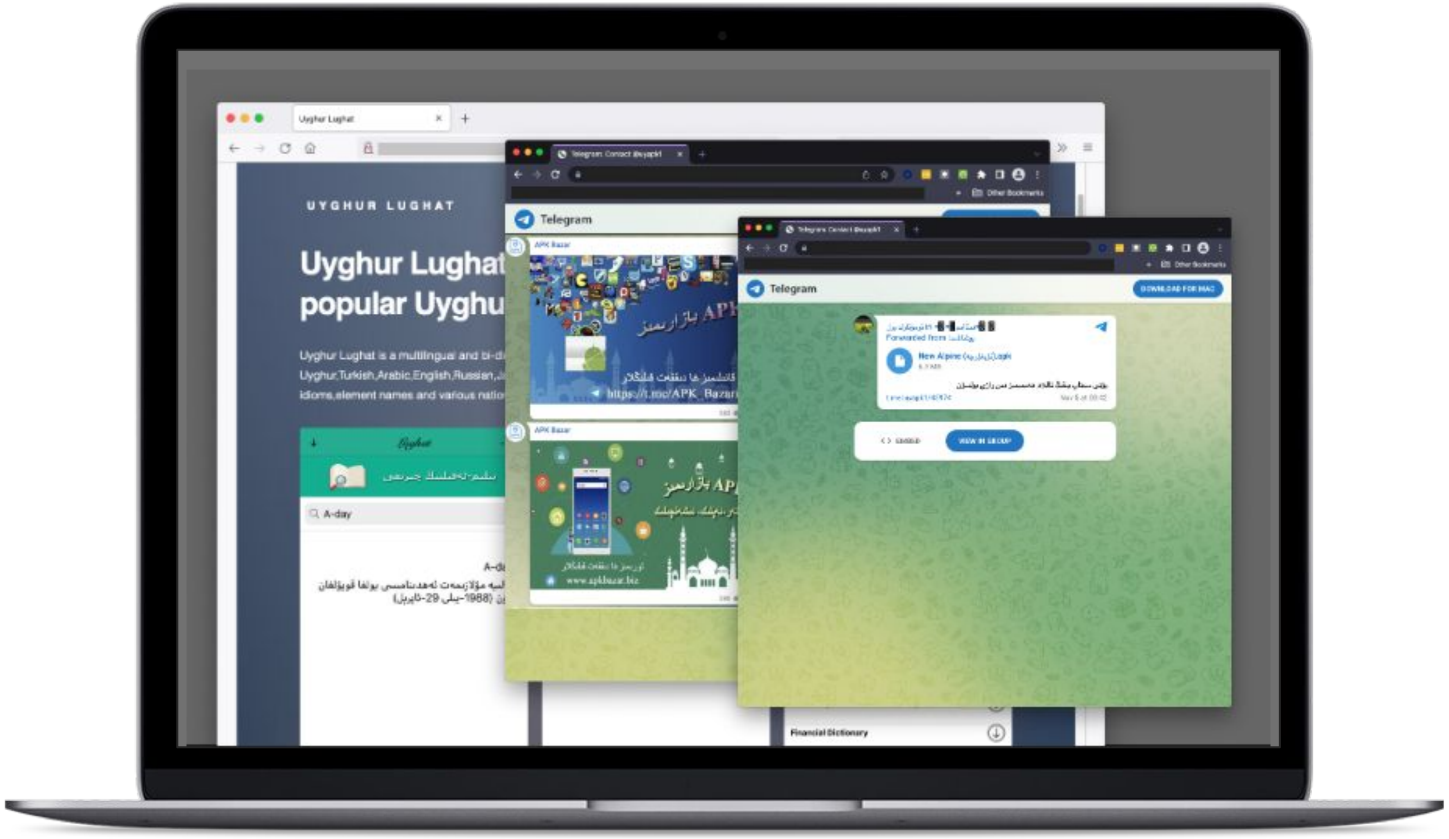
安装器: 4.4.7	型号: Google Pixel 3a
MM版本:待获取	WiFi: "RedLan"
渠道号: 22091501	内存助手状态:待获取
安卓: 11	子版本: RQ2A.210505.002

SIM卡服务

Do you want to install this application?

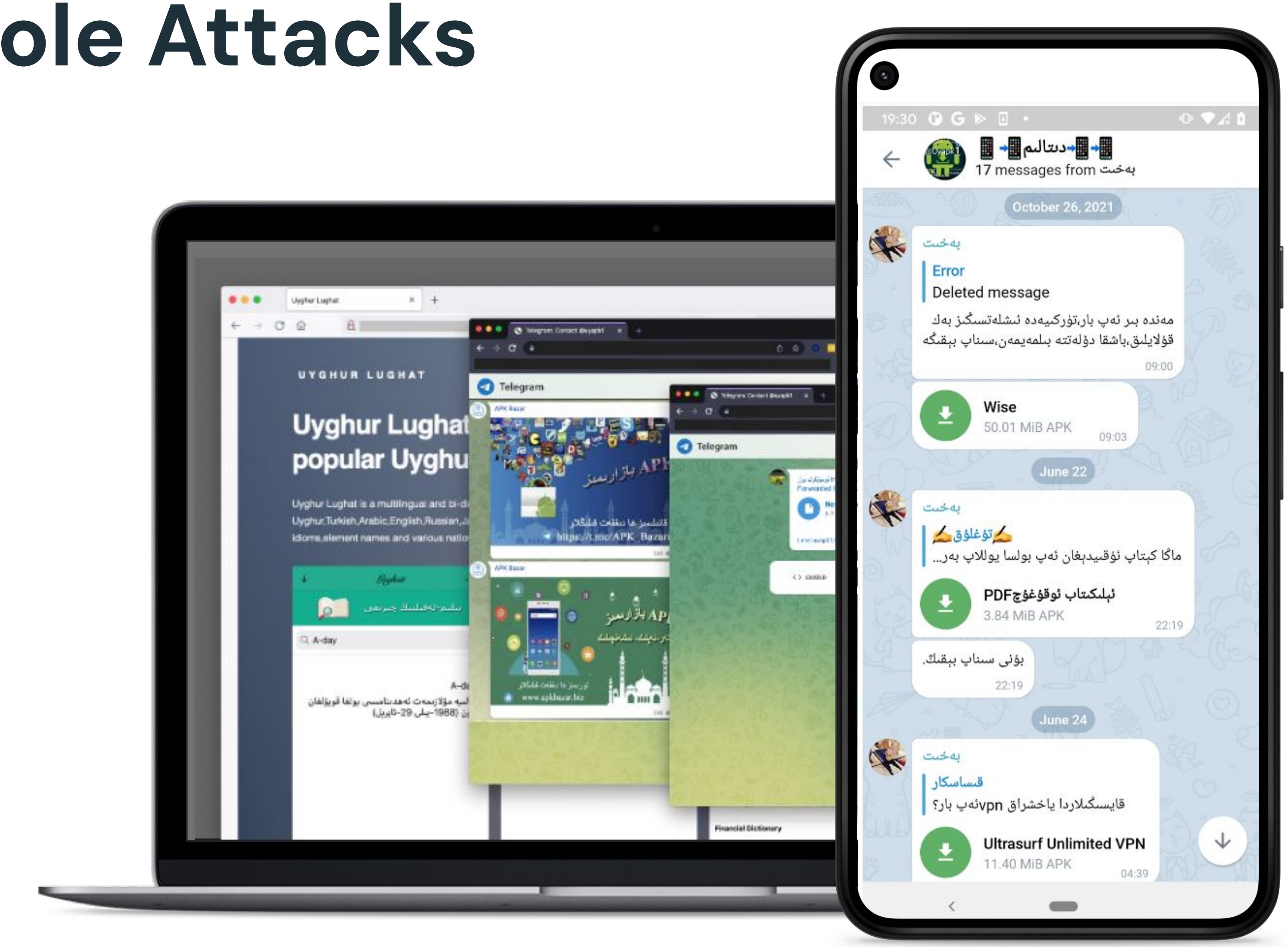
Watering Hole Attacks

Targeting of "Five Poisons" communities through fake app stores, social media, forums.



Watering Hole Attacks

Targeting of "Five Poisons" communities through fake app stores, social media, forums.



Uyghur Lughat
UYGHUR LUGHAT
Uyghur Lughat popular Uyghu
Uyghur Lughat is a multilingual and bi-di
Uyghur,Turkish,Arabic,English,Russian,
idioms,element names and various natio
A-day
Telegram
APK Bazar
https://t.me/APK_Bazar
www.apkbazar.biz
Financial Dictionary

📱➡📱دىتالىم➡📱➡📱

17 messages from بەخت

October 26, 2021

بەخت

Error

Deleted message

مەندە بىر ئەپ بار،تۈركىيەدە ئىشلەتسىگىز بەك قۇلايلىق،باشقا دۆلەتتە بىلمەيمەن،سىناپ بېقىڭە

09:00

Wise
50.01 MiB APK
09:03

June 22

بەخت

✍تۇغلۇق✍

ماگا كىتاپ ئوقىيدىغان ئەپ بولسا يوللاپ بەر...

ئېلكىتاب ئوقۇغۇچPDF
3.84 MiB APK
22:19

بۇنى سىناپ بېقىڭ.

22:19

June 24

بەخت

قىساسكار

قايىسىگىلاردا ياخشىراق vpnئەپ بار؟

Ultrasurf Unlimited VPN
11.40 MiB APK
04:39

Social Engineering / Spear-Phishing

Direct messages through social media, messaging apps.

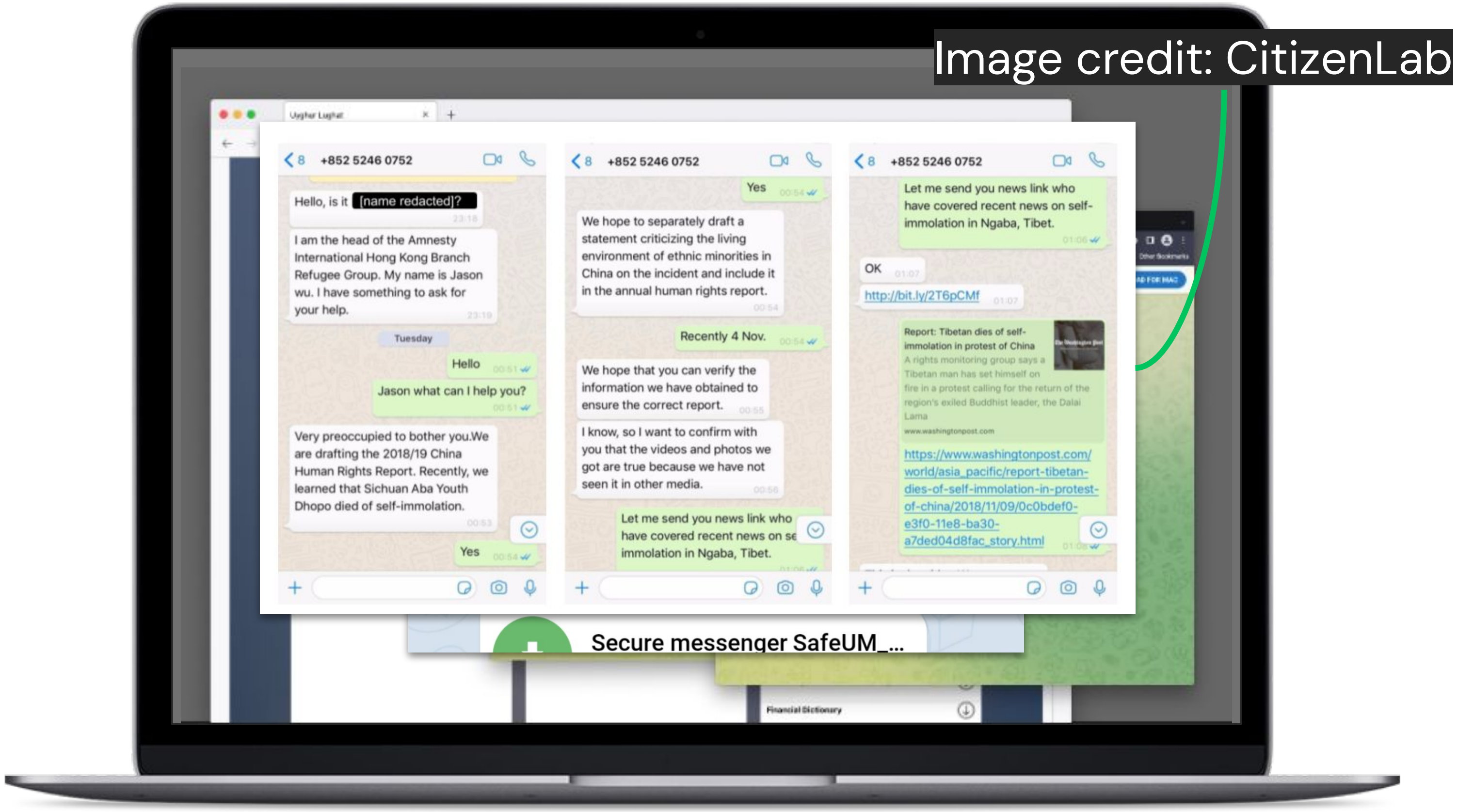


Image credit: CitizenLab

+852 5246 0752

Hello, is it [name redacted]? 23:18

I am the head of the Amnesty International Hong Kong Branch Refugee Group. My name is Jason wu. I have something to ask for your help. 23:19

Tuesday

Hello 00:51

Jason what can I help you? 00:51

Very preoccupied to bother you.We are drafting the 2018/19 China Human Rights Report. Recently, we learned that Sichuan Aba Youth Dhopo died of self-immolation. 00:53

Yes 00:54

+852 5246 0752

Yes 00:54

We hope to separately draft a statement criticizing the living environment of ethnic minorities in China on the incident and include it in the annual human rights report. 00:54

Recently 4 Nov. 00:54

We hope that you can verify the information we have obtained to ensure the correct report. 00:55

I know, so I want to confirm with you that the videos and photos we got are true because we have not seen it in other media. 00:56

Let me send you news link who have covered recent news on se immolation in Ngaba, Tibet.

+852 5246 0752

Let me send you news link who have covered recent news on self-immolation in Ngaba, Tibet. 01:06

OK 01:07

http://bit.ly/2T6pCMf 01:07

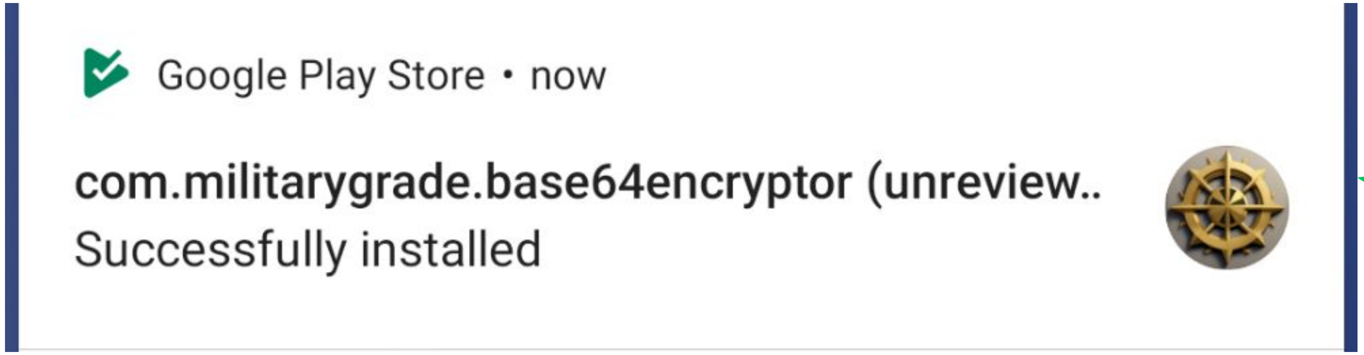
Report: Tibetan dies of self-immolation in protest of China
A rights monitoring group says a Tibetan man has set himself on fire in a protest calling for the return of the region's exiled Buddhist leader, the Dalai Lama
www.washingtonpost.com

https://www.washingtonpost.com/world/asia_pacific/report-tibetan-dies-of-self-immolation-in-protest-of-china/2018/11/09/0c0bdef0-e3f0-11e8-ba30-a7ded04d8fac_story.html 01:08

North Korea

Abusing Google Play Features

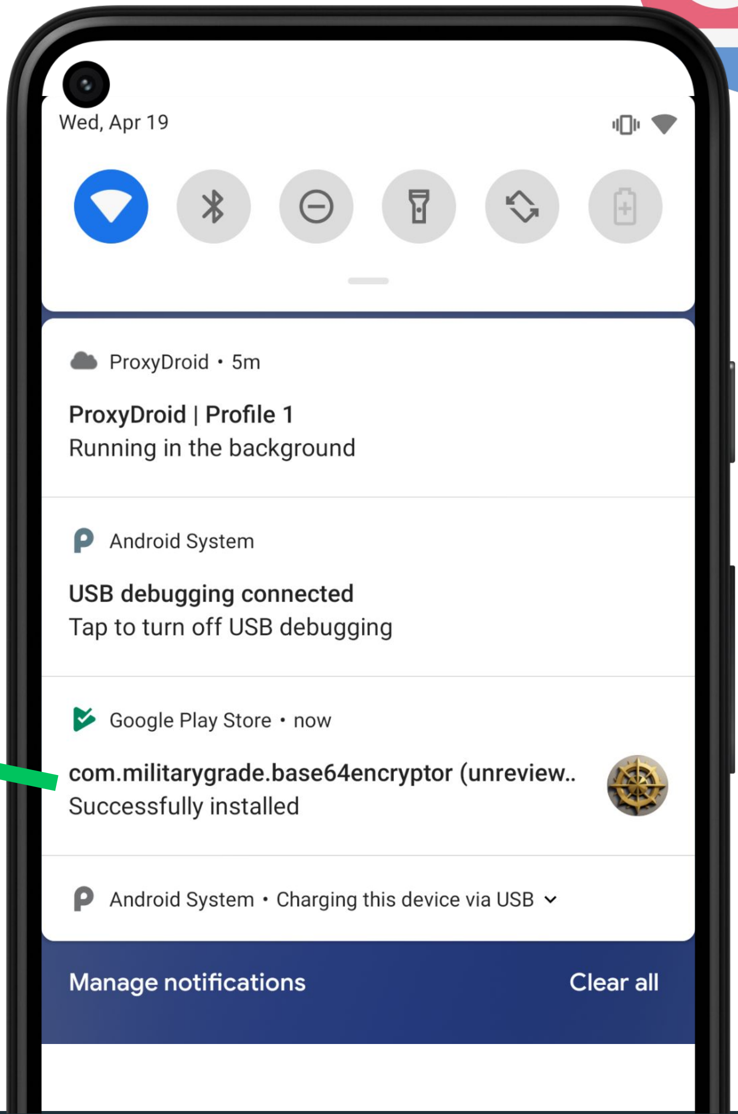
Uses Google Play's internal testing and app sync feature



Google Play Store • now

com.militarygrade.base64encryptor (unreview..

Successfully installed



Wed, Apr 19

ProxyDroid • 5m

ProxyDroid | Profile 1

Running in the background

Android System

USB debugging connected

Tap to turn off USB debugging

Google Play Store • now

com.militarygrade.base64encryptor (unreview..

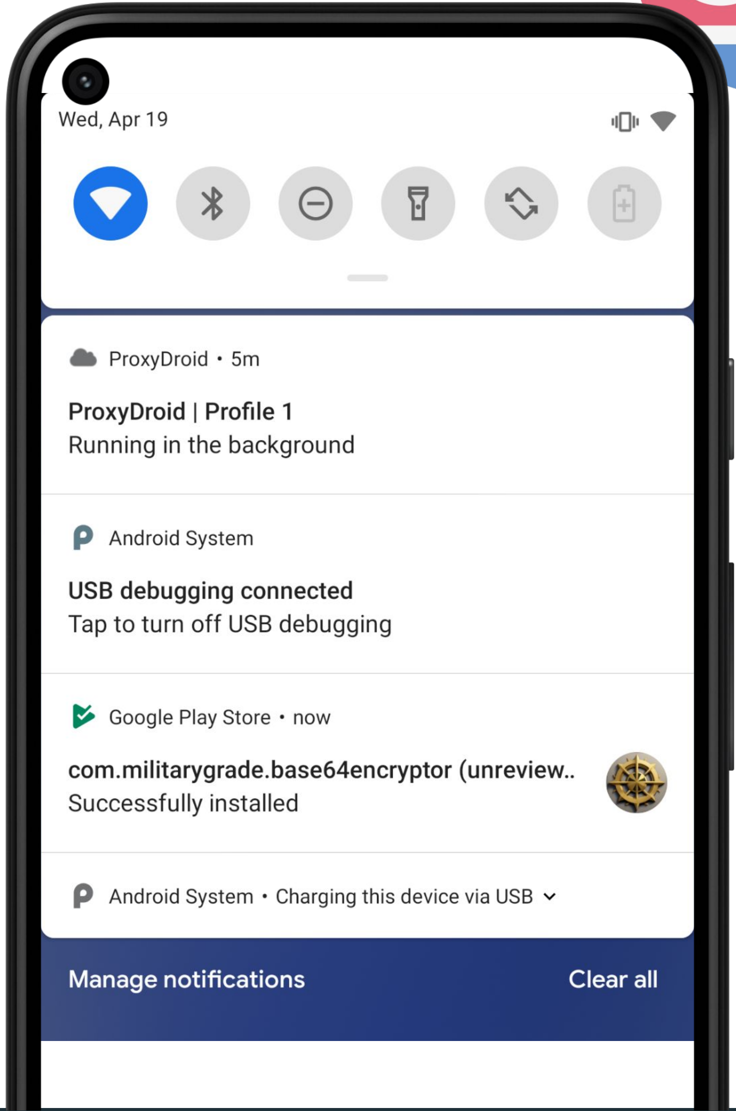
Successfully installed

Android System • Charging this device via USB

Abusing Google Play Features

Uses Google Play's internal testing and app sync feature

Used by Kimsuky to install AppleZombie



Wed, Apr 19

ProxyDroid • 5m

ProxyDroid | Profile 1

Running in the background

Android System

USB debugging connected

Tap to turn off USB debugging

Google Play Store • now

com.militarygrade.base64encryptor (unreview..

Successfully installed

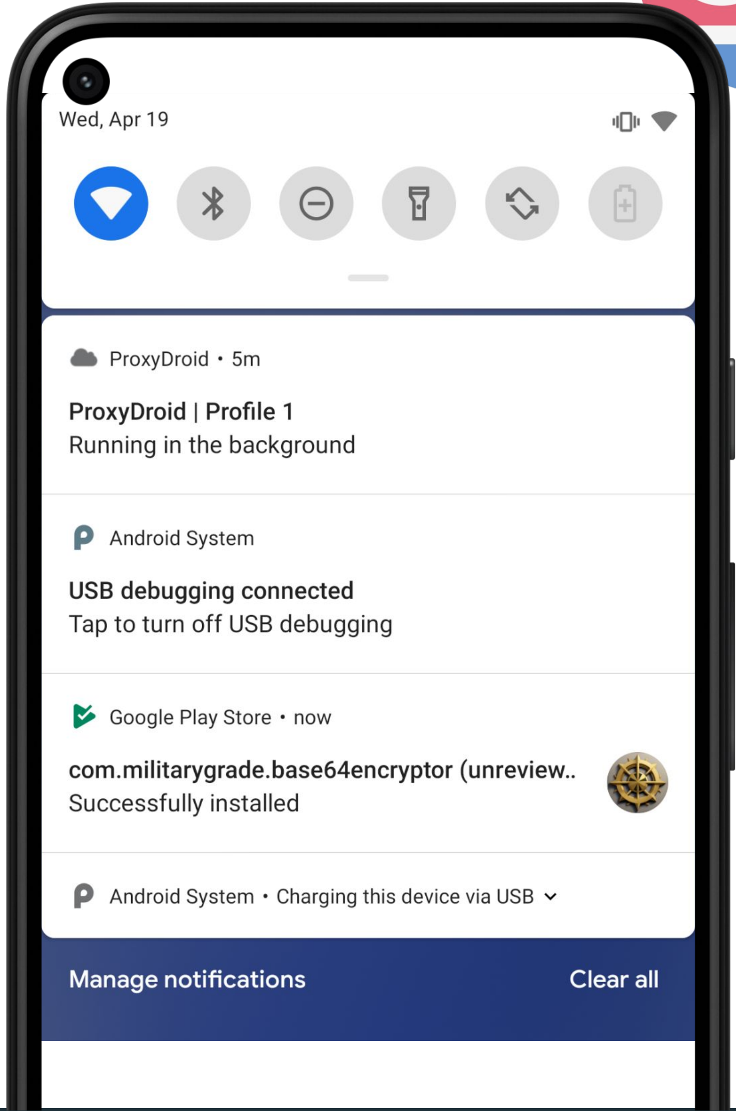
Android System • Charging this device via USB

Abusing Google Play Features

Uses Google Play's internal testing and app sync feature

Used by Kimsuky to install AppleZombie

Requires Google account compromise and more



Wed, Apr 19

ProxyDroid • 5m

ProxyDroid | Profile 1
Running in the background

Android System

USB debugging connected
Tap to turn off USB debugging

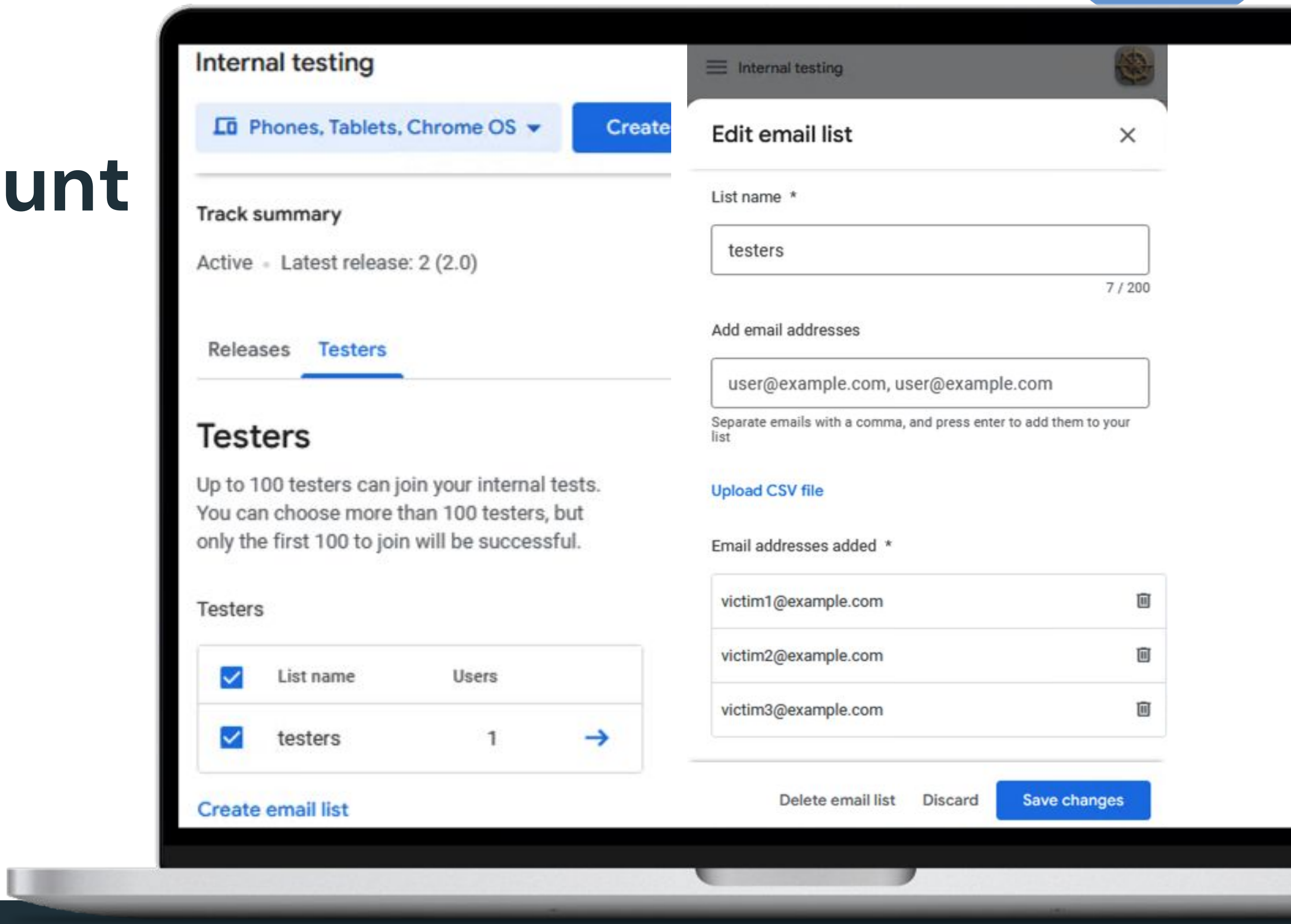
Google Play Store • now

com.militarygrade.base64encryptor (unreview..
Successfully installed

Android System • Charging this device via USB

Abusing Google Play Features

Attacker controls a Google developer account



Track summary

Active · Latest release: 2 (2.0)

Testers

Up to 100 testers can join your internal tests. You can choose more than 100 testers, but only the first 100 to join will be successful.

Testers

☑	List name	Users	
☑	testers	1	→

Edit email list ✕

List name *

testers

7 / 200

Add email addresses

user@example.com, user@example.com

Separate emails with a comma, and press enter to add them to your list

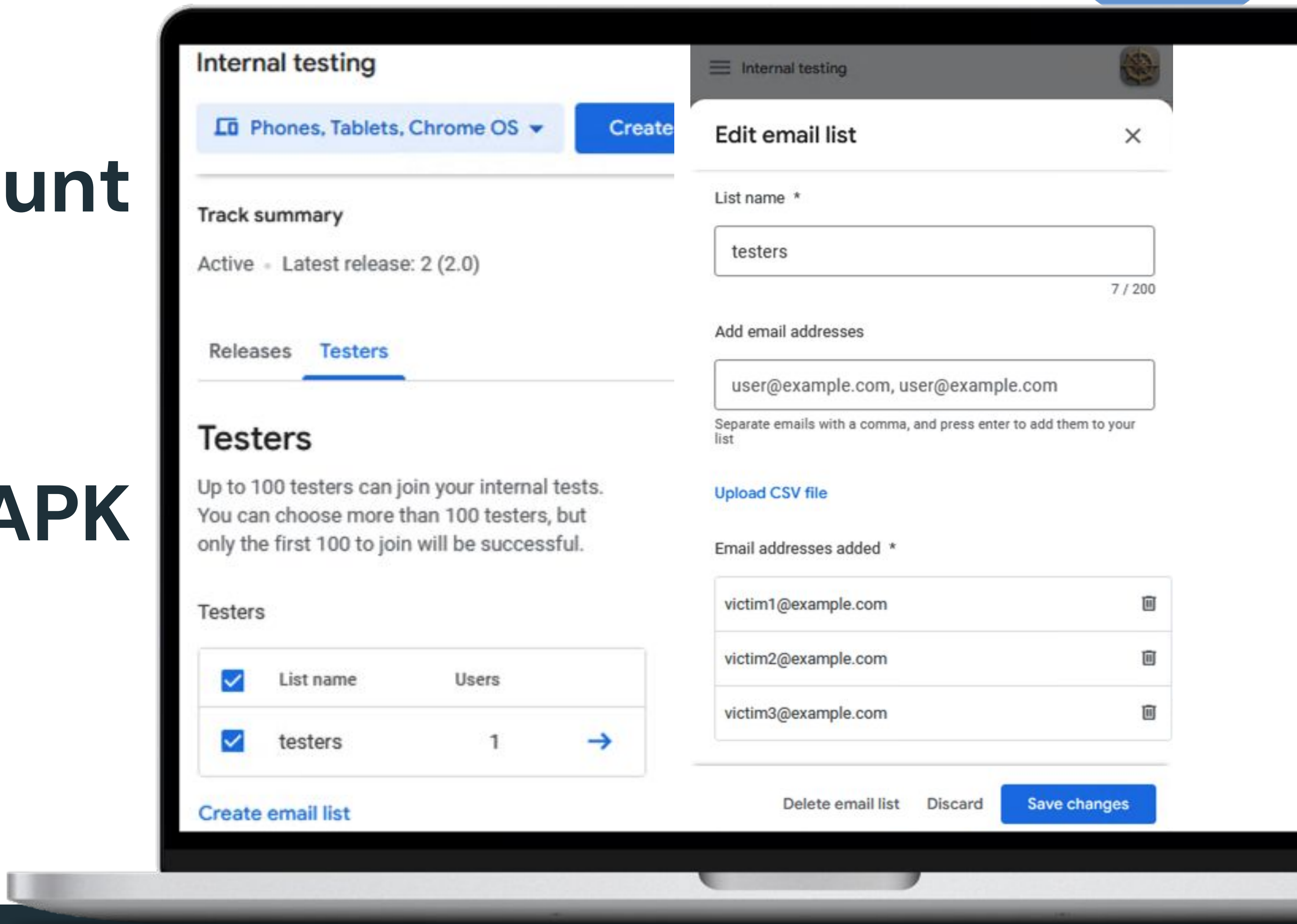
Email addresses added *

- victim1@example.com
- victim2@example.com
- victim3@example.com

Abusing Google Play Features

Attacker controls a Google developer account

Creates one or more releases by uploading APK files



Internal testing

Phones, Tablets, Chrome OS ▾ | Create

Track summary

Active · Latest release: 2 (2.0)

Releases | Testers

Testers

Up to 100 testers can join your internal tests. You can choose more than 100 testers, but only the first 100 to join will be successful.

Testers

☑	List name	Users	
☑	testers	1	→

Create email list

≡ Internal testing

Edit email list ✕

List name *

testers

7 / 200

Add email addresses

user@example.com, user@example.com

Separate emails with a comma, and press enter to add them to your list

Upload CSV file

Email addresses added *

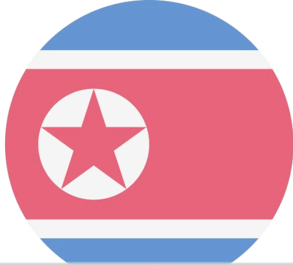
victim1@example.com

victim2@example.com

victim3@example.com

Delete email list | Discard | Save changes

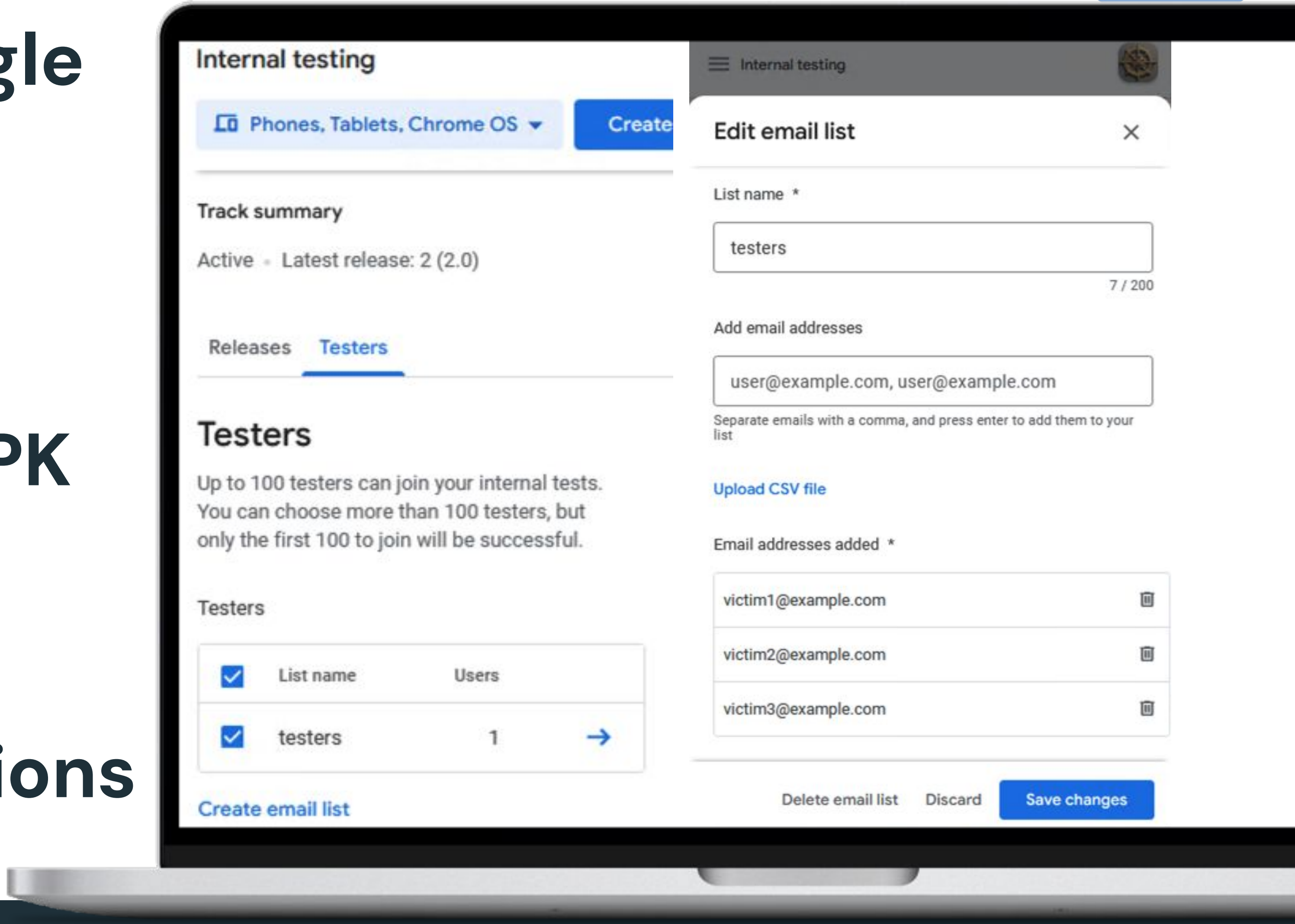
Abusing Google Play Features



Attacker controls a Google developer account

Creates one or more releases by uploading APK files

Can pick any of the versions as test release



Internal testing

Track summary

Active · Latest release: 2 (2.0)

Testers

Up to 100 testers can join your internal tests. You can choose more than 100 testers, but only the first 100 to join will be successful.

Testers

☑	List name	Users	
☑	testers	1	→

Edit email list ×

List name *

testers

7 / 200

Add email addresses

user@example.com, user@example.com

Separate emails with a comma, and press enter to add them to your list

Email addresses added *

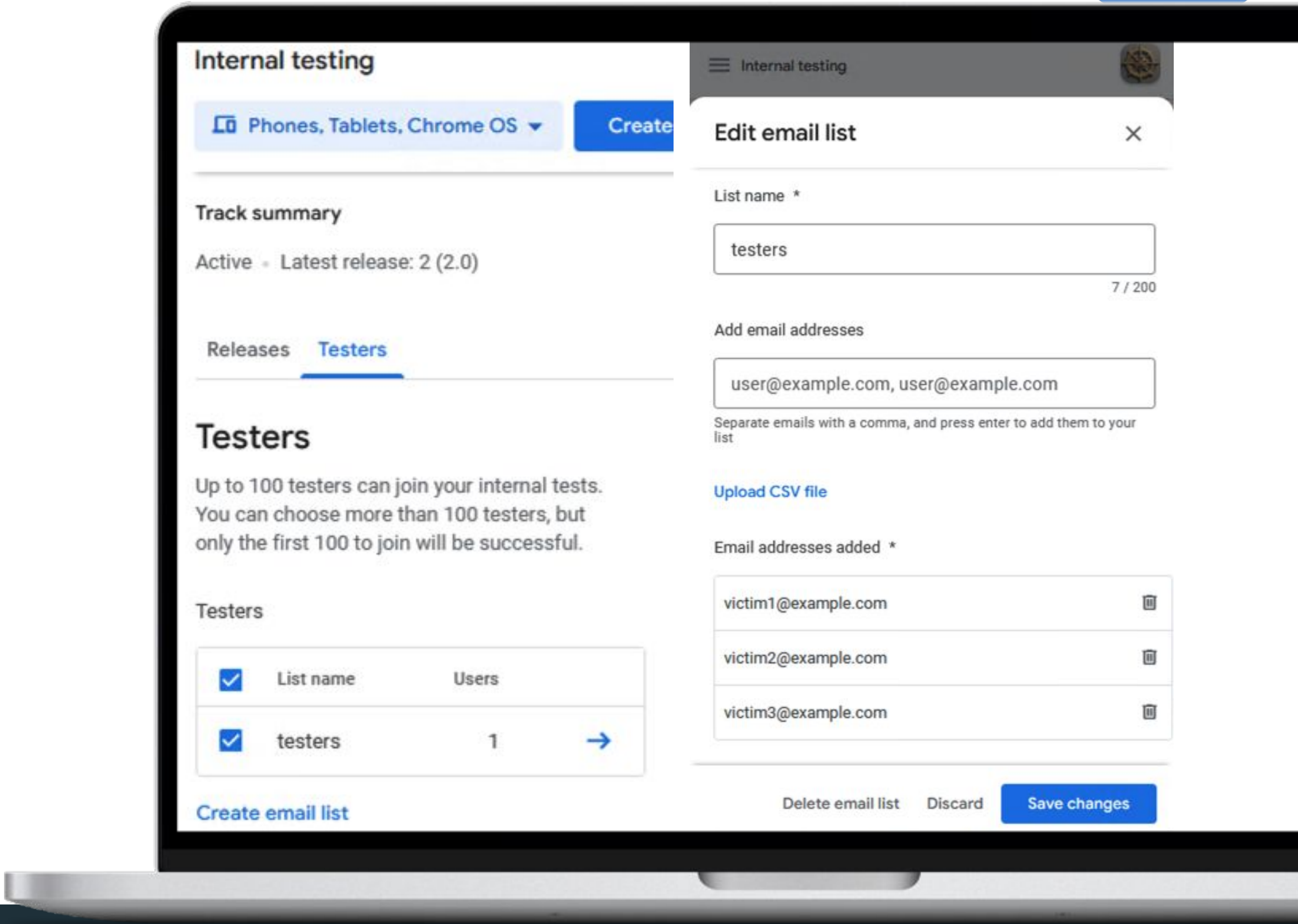
victim1@example.com

victim2@example.com

victim3@example.com

Abusing Google Play Features

Creates list with up to 100 emails



Internal testing

Track summary

Active · Latest release: 2 (2.0)

Testers

Up to 100 testers can join your internal tests. You can choose more than 100 testers, but only the first 100 to join will be successful.

Testers

☑	List name	Users
☑	testers	1

Edit email list

List name *

testers

7 / 200

Add email addresses

user@example.com, user@example.com

Separate emails with a comma, and press enter to add them to your list

Email addresses added *

victim1@example.com

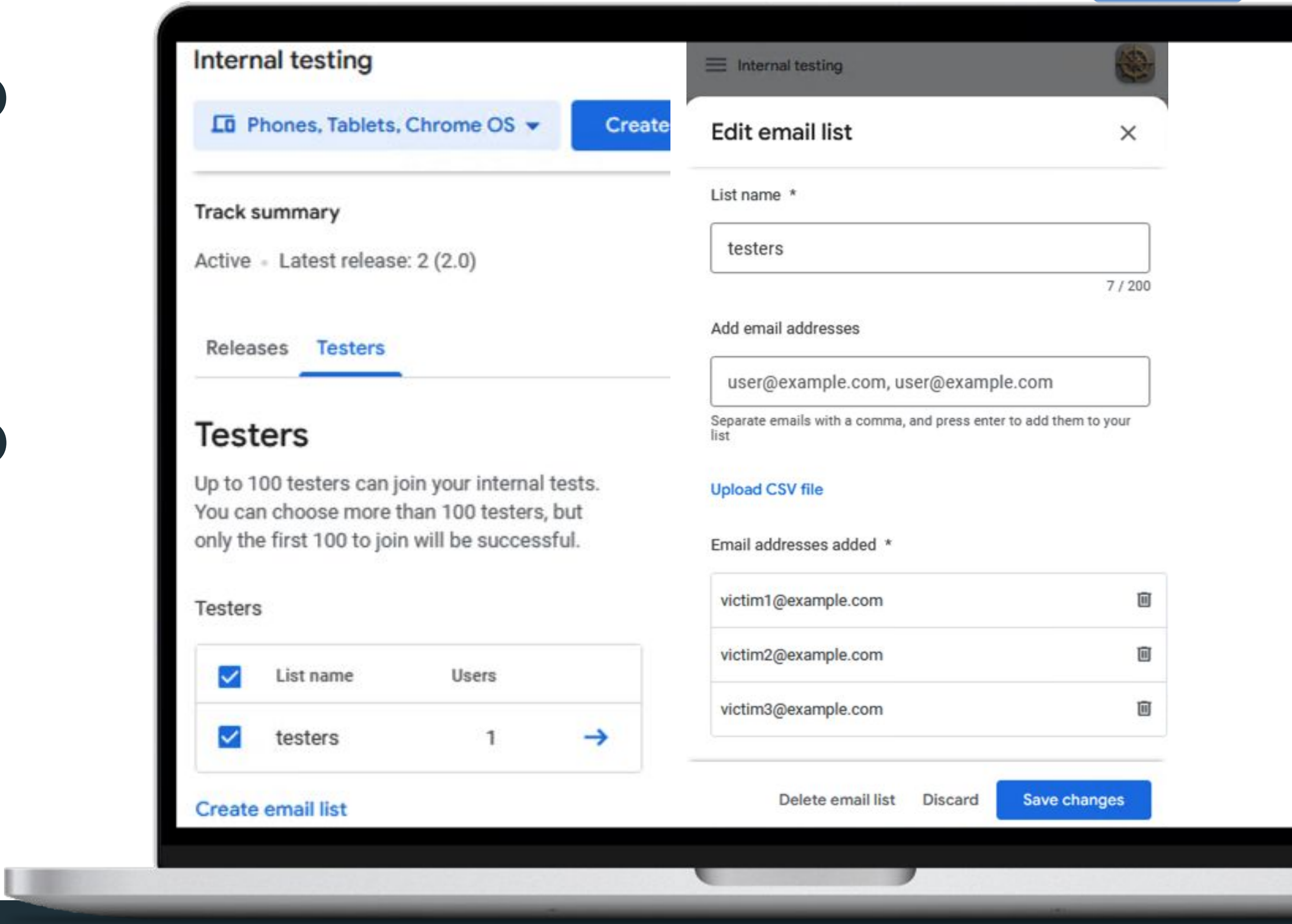
victim2@example.com

victim3@example.com

Abusing Google Play Features

Creates list with up to 100 emails

Adds victim's email to the list



Internal testing

Track summary

Active · Latest release: 2 (2.0)

Testers

Up to 100 testers can join your internal tests. You can choose more than 100 testers, but only the first 100 to join will be successful.

Testers

☑	List name	Users	
☑	testers	1	→

Edit email list

List name *

testers

7 / 200

Add email addresses

user@example.com, user@example.com

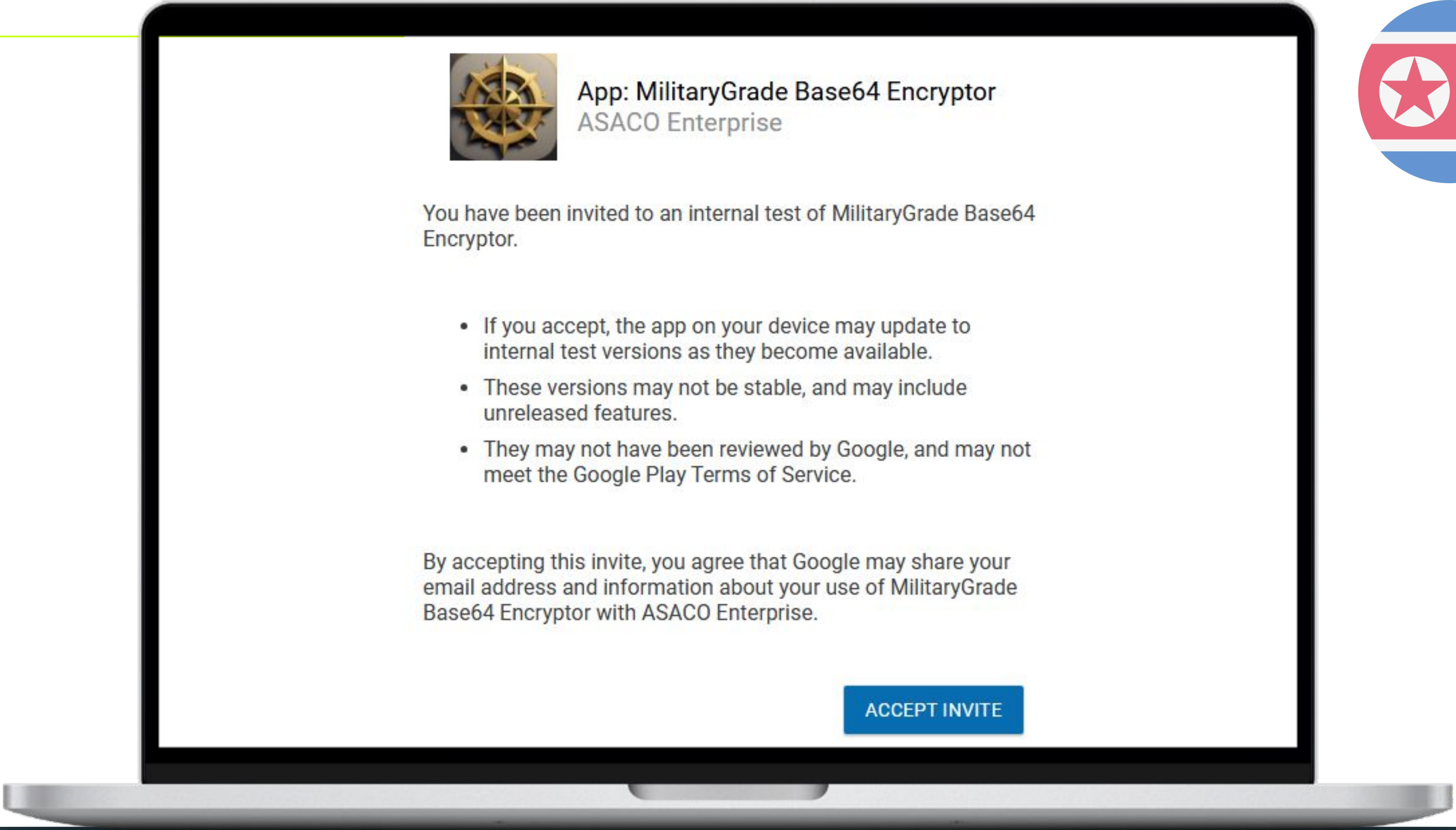
Separate emails with a comma, and press enter to add them to your list

Email addresses added *

victim1@example.com

victim2@example.com

victim3@example.com



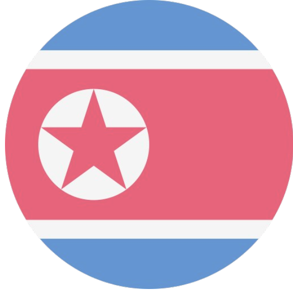
App: MilitaryGrade Base64 Encryptor

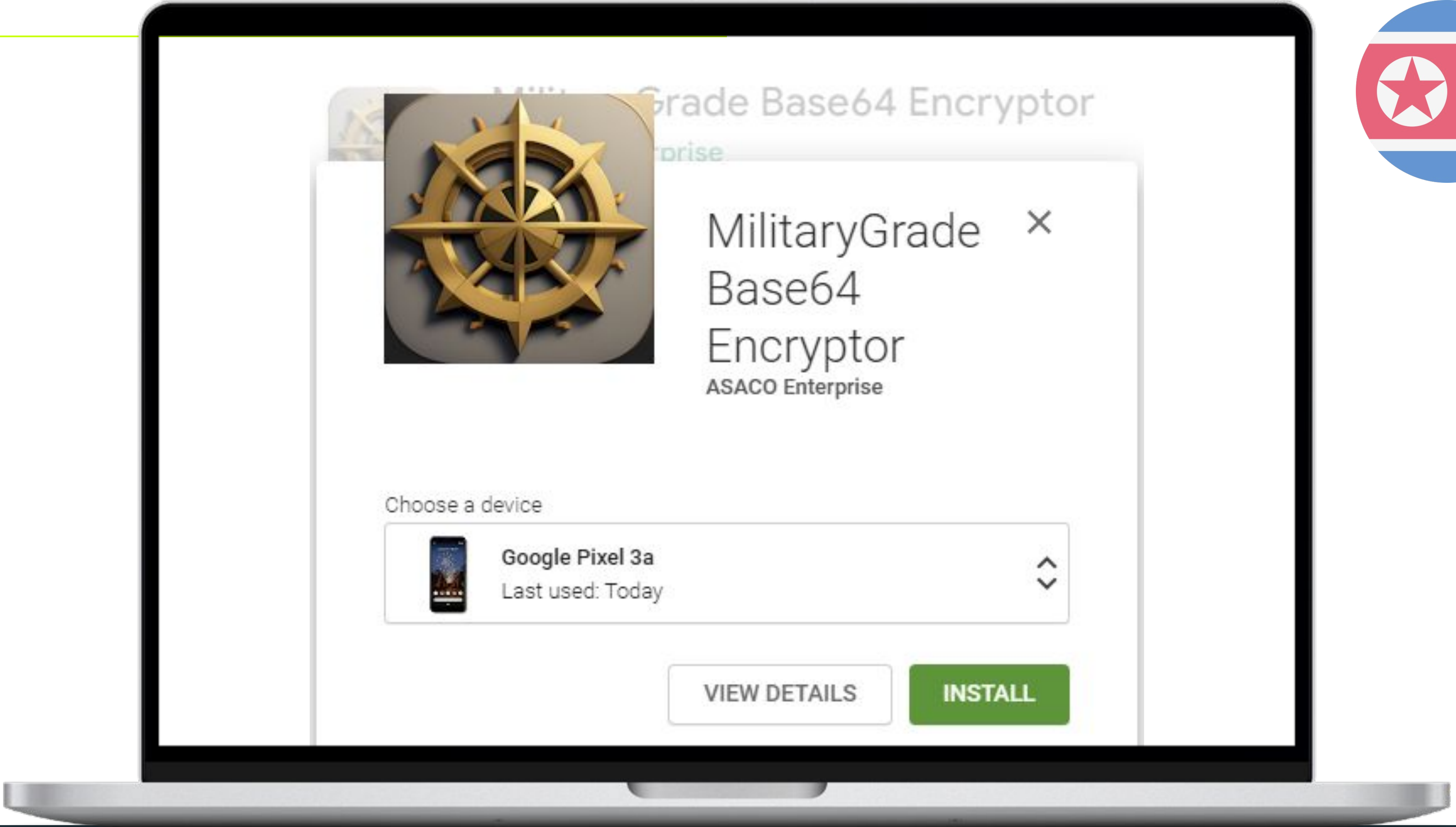
ASACO Enterprise

You have been invited to an internal test of MilitaryGrade Base64 Encryptor.

- If you accept, the app on your device may update to internal test versions as they become available.
- These versions may not be stable, and may include unreleased features.
- They may not have been reviewed by Google, and may not meet the Google Play Terms of Service.

By accepting this invite, you agree that Google may share your email address and information about your use of MilitaryGrade Base64 Encryptor with ASACO Enterprise.





Grade Base64 Encryptor

rprise

MilitaryGrade Base64 Encryptor

ASACO Enterprise

Choose a device

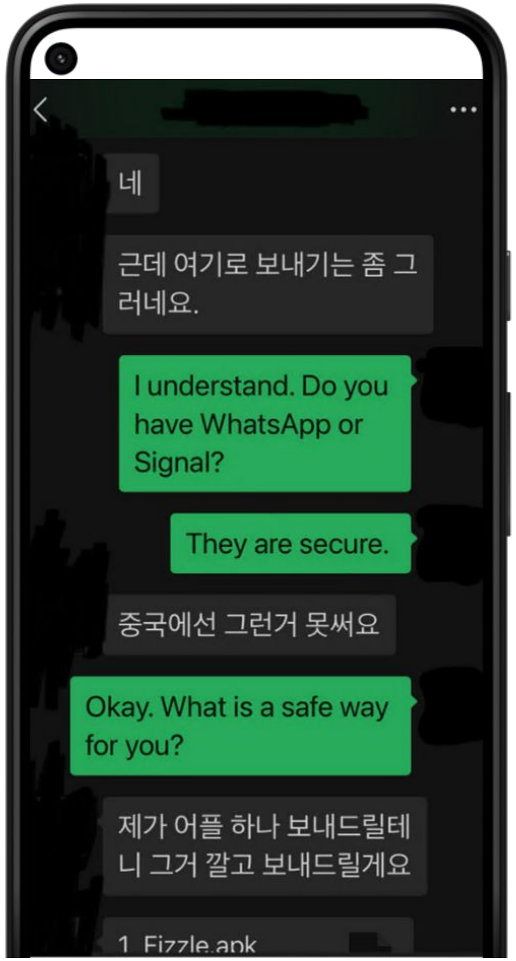
Google Pixel 3a

Last used: Today

Direct Message Spearphishing

ScarCruft APT direct messages over WeChat

Targeted Korean journalists



[redacted]

네

근데 여기로 보내기는 좀 그러네요.

I understand. Do you have WhatsApp or Signal?

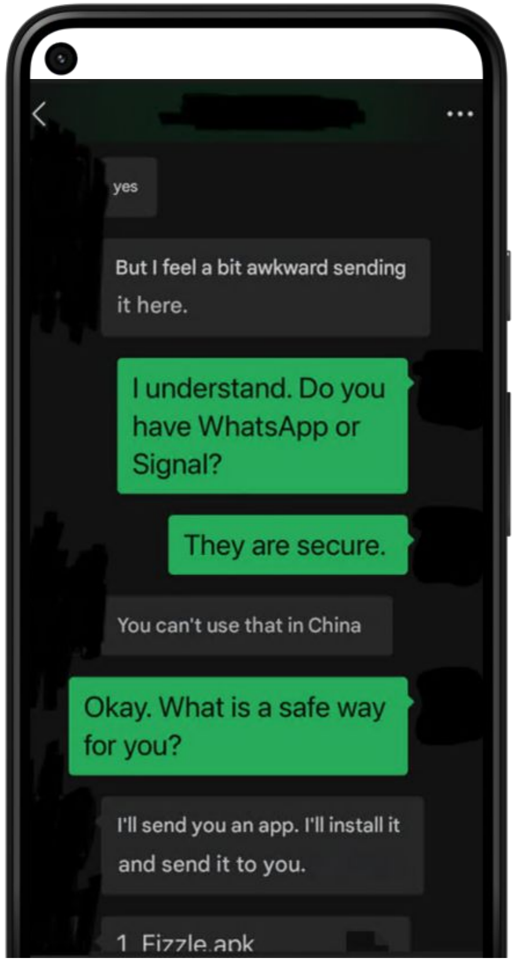
They are secure.

중국에선 그런거 못써요

Okay. What is a safe way for you?

제가 어플 하나 보내드릴테니 그거 깔고 보내드릴게요

1 Fizzle.apk



[redacted]

yes

But I feel a bit awkward sending it here.

I understand. Do you have WhatsApp or Signal?

They are secure.

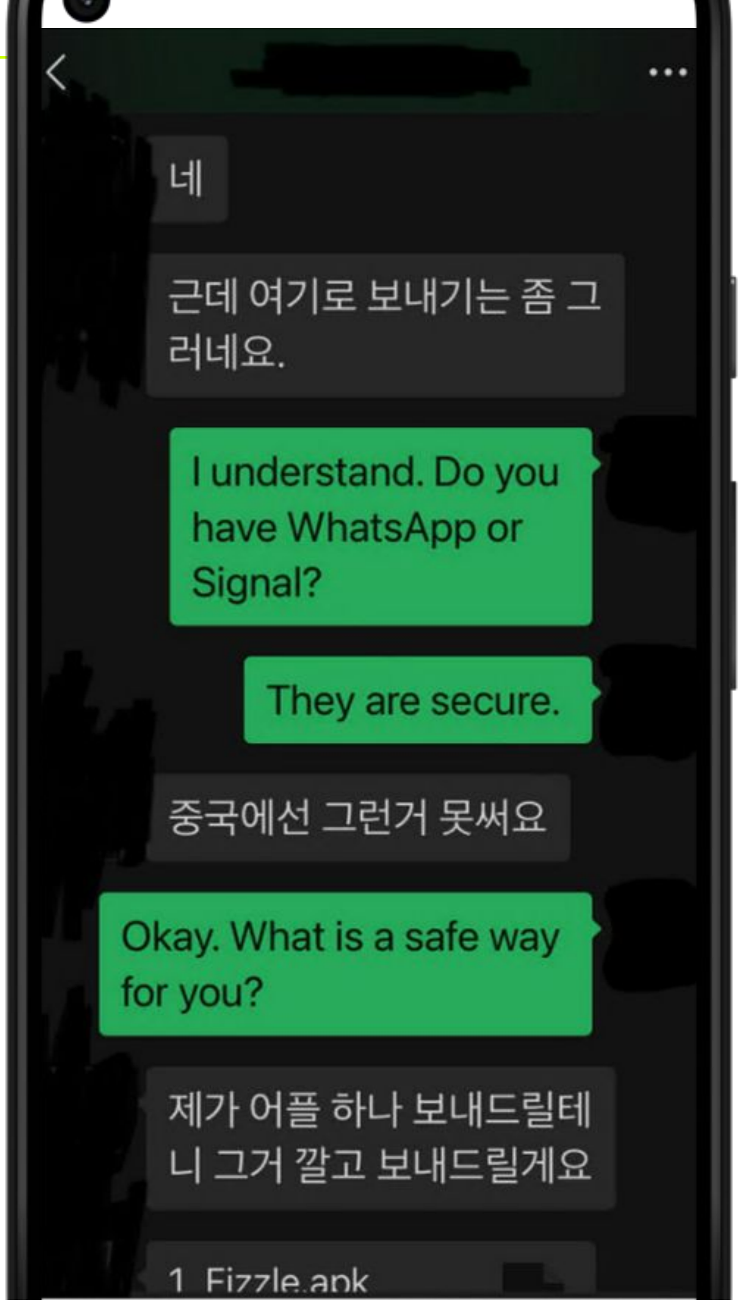
You can't use that in China

Okay. What is a safe way for you?

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

1 Fizzle.apk

Credit: https://interlab.or.kr/archives/2567



[redacted]

네

근데 여기로 보내기는 좀 그러네요.

I understand. Do you have WhatsApp or Signal?

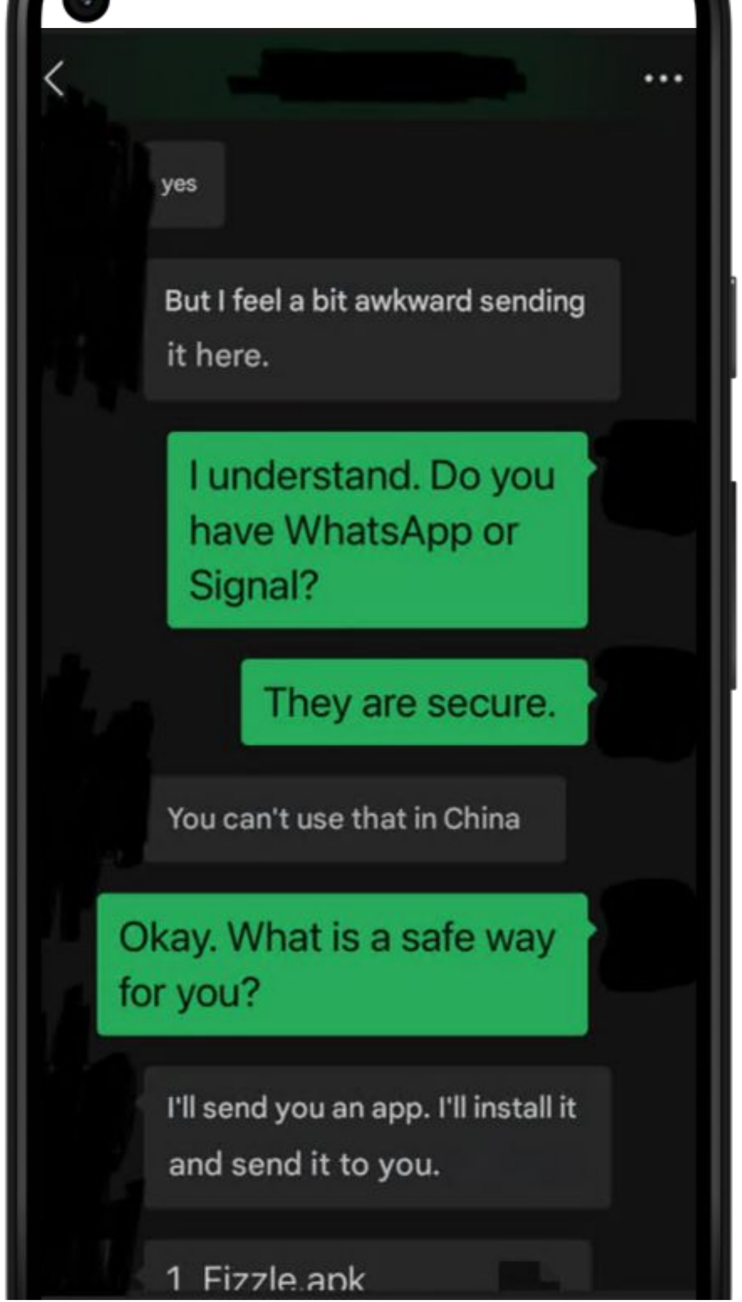
They are secure.

중국에선 그런거 못써요

Okay. What is a safe way for you?

제가 어플 하나 보내드릴테니 그거 깔고 보내드릴게요

1_Fizzle.apk



[redacted]

yes

But I feel a bit awkward sending it here.

I understand. Do you have WhatsApp or Signal?

They are secure.

You can't use that in China

Okay. What is a safe way for you?

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

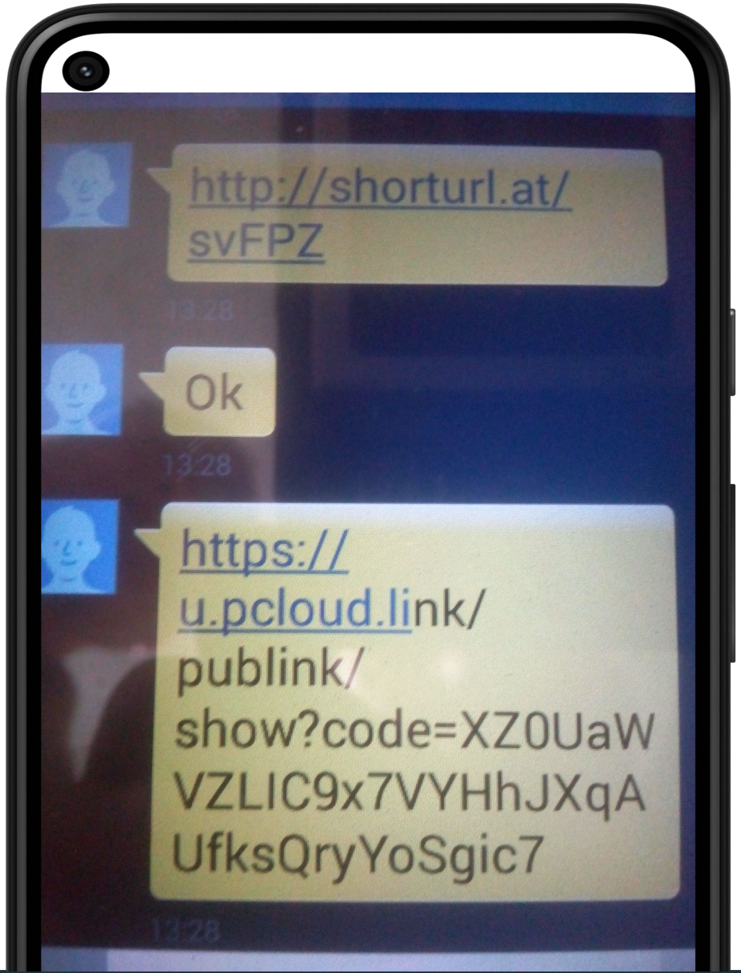
1_Fizzle.apk

Credit: https://interlab.or.kr/archives/2567

ScarCruft APT

Public cloud storage staging

Malware served over direct messages



http://shorturl.at/svFPZ

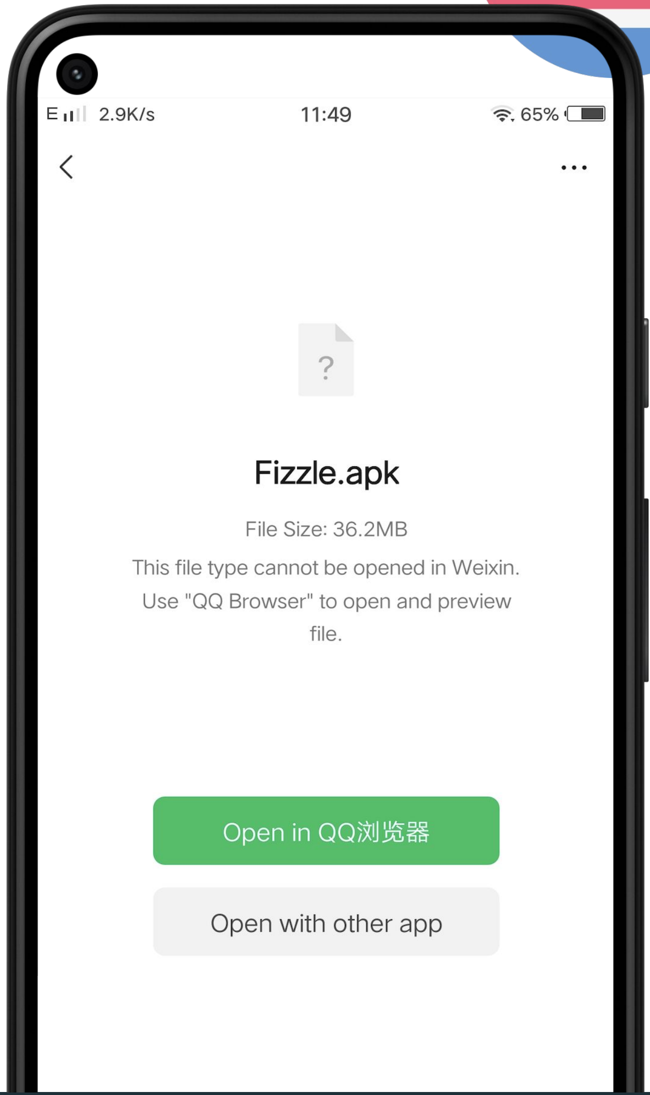
13:28

Ok

13:28

https://u.pcloud.link/publink/show?code=XZ0UaWVZLIC9x7VYHhJXqAUfksQryYoSgic7

13:28



Fizzle.apk

File Size: 36.2MB

This file type cannot be opened in Weixin. Use "QQ Browser" to open and preview file.

Countering Detection and Stealing Data

Russia

Deception Techniques:

Trojanized apps (Telegram)

Adult content (Photo gallery apps)

Trojanized system apps (Infamous Chisel)

Pretexts for trust subversion

Deception Techniques:

- Trojanized apps (Telegram)
- Adult content (Photo gallery apps)
- Trojanized system apps (Infamous Chisel)
- Fake system apps

Multi-stage deployment

Encryption for:

- Configuration files
- Payload encryption
- String encryption
- C2 traffic

China

Dynamic Code Loading

Application Versioning

Encrypted Exfiltration

Headless surveillance modules

Multi-stage deployments

Trojanized popular apps

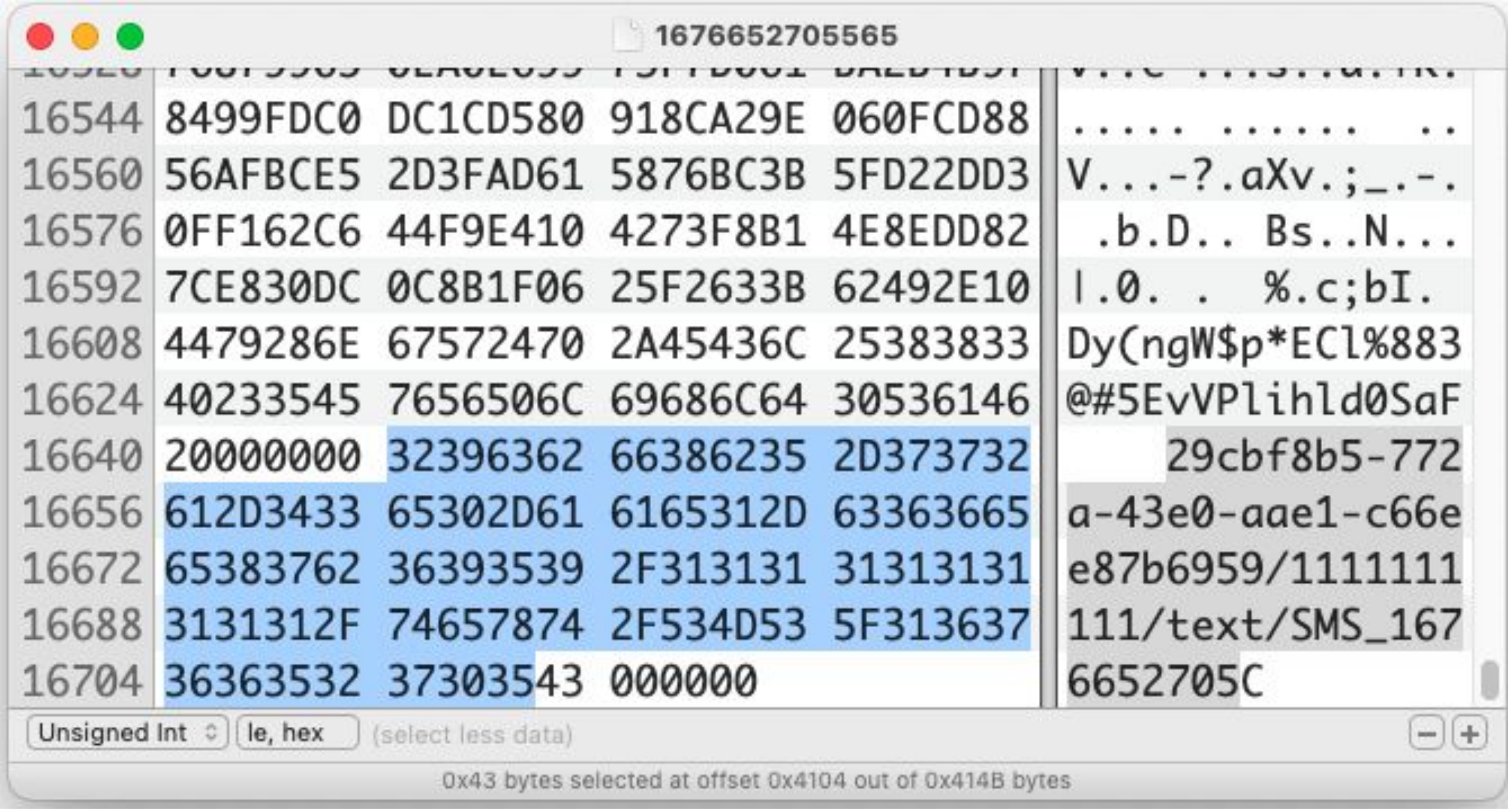
Hidden malware artifacts
(eg. hidden folders, files in /sdcard)

North Korea

Dynamic Code Loading – Kimsuky & ScarCruft

Limited Functionality in Initial Stages – Kimsuky

Encrypted Exfiltration



1676652705565

```
16544 8499FDC0 DC1CD580 918CA29E 060FCD88  ..... ......  ..
16560 56AFBCE5 2D3FAD61 5876BC3B 5FD22DD3  V...-?.aXv.;_.-.
16576 0FF162C6 44F9E410 4273F8B1 4E8EDD82   .b.D.. Bs..N...
16592 7CE830DC 0C8B1F06 25F2633B 62492E10  |.0.  .  %.c;bI.
16608 4479286E 67572470 2A45436C 25383833  Dy(ngW$p*ECl%883
16624 40233545 7656506C 69686C64 30536146  @#5EvVPlihld0SaF
16640 20000000 32396362 66386235 2D373732      29cbf8b5-772
16656 612D3433 65302D61 6165312D 63363665  a-43e0-aae1-c66e
16672 65383762 36393539 2F313131 31313131  e87b6959/1111111
16688 3131312F 74657874 2F534D53 5F313637  111/text/SMS_167
16704 36363532 37303543 000000             6652705C
```

Unsigned Int ⌃ | le, hex | (select less data)

0x43 bytes selected at offset 0x4104 out of 0x414B bytes

[<encrypted_data> + <aes_key> + <length_of_aes_key> + <file+path> + <length_of_path>]

System Utilities: Generic icons & names, like "Settings" and "Auth".

Trojanizing Popular Apps: Threema and other messaging apps

Exploiting Cultural Context:

Naver, KISA, Hancom Office

Who’s Under Attack

The Victims of State-Backed Surveillance

Russia

Domestic Victims

“High Risk” Events, Individuals

Supporting Military Operations

- Syria, 2016
- Ukraine, current
- Planning, Combat Operations, Forces Disposition

Ukrainian Government

Entities Operating in Ukraine (Allied NGOs)

Former Soviet Countries (Central Asia)

China

Who's Under Attack: China

Transnational and domestic repression of the "Five Poisons" – groups considered a threat to the CCP's stability.

- Practitioners of Falun Gong
- Uyghurs
- Tibetans
- Taiwanese
- Hong Kong pro-democracy advocates

Observed targeting of tourists & business travellers.

"the reason [the Five Poisons] pose a threat is that they operate inside and outside China"

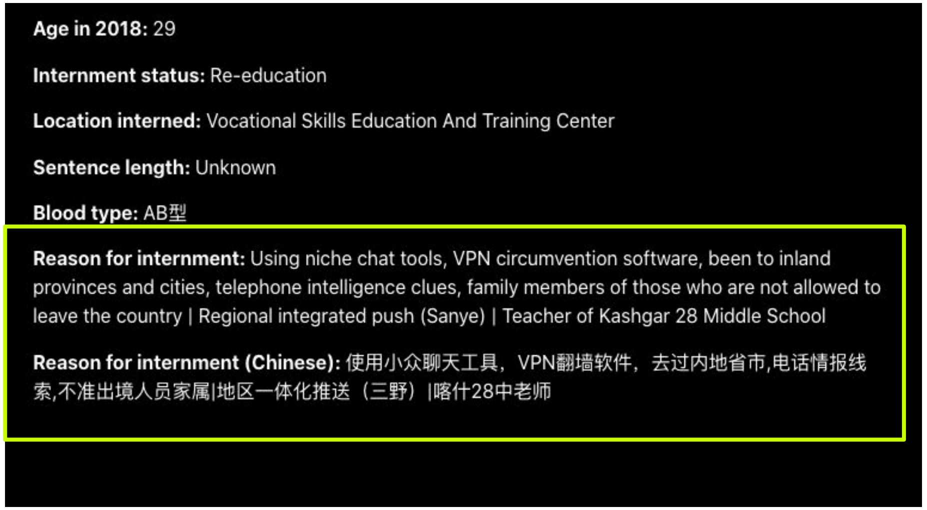
(Hoffman & Mattis, 2016)

Who’s Under Attack: China

Exfiltrated data presumed useful for laying criminal charges against individuals of interest.

Example “pre-criminal” activity:

- visiting a mosque “more than 200 times” (Byler, 2021)
- using a VPN (“violent and terrorist software”) (Lam, 2016)
- viewing religious texts or receiving religious texts via SMS or social media
- Accessing social media platforms after they had been blocked (eg. for users in Xinjiang)



Age in 2018: 29

Internment status: Re-education

Location interned: Vocational Skills Education And Training Center

Sentence length: Unknown

Blood type: AB型

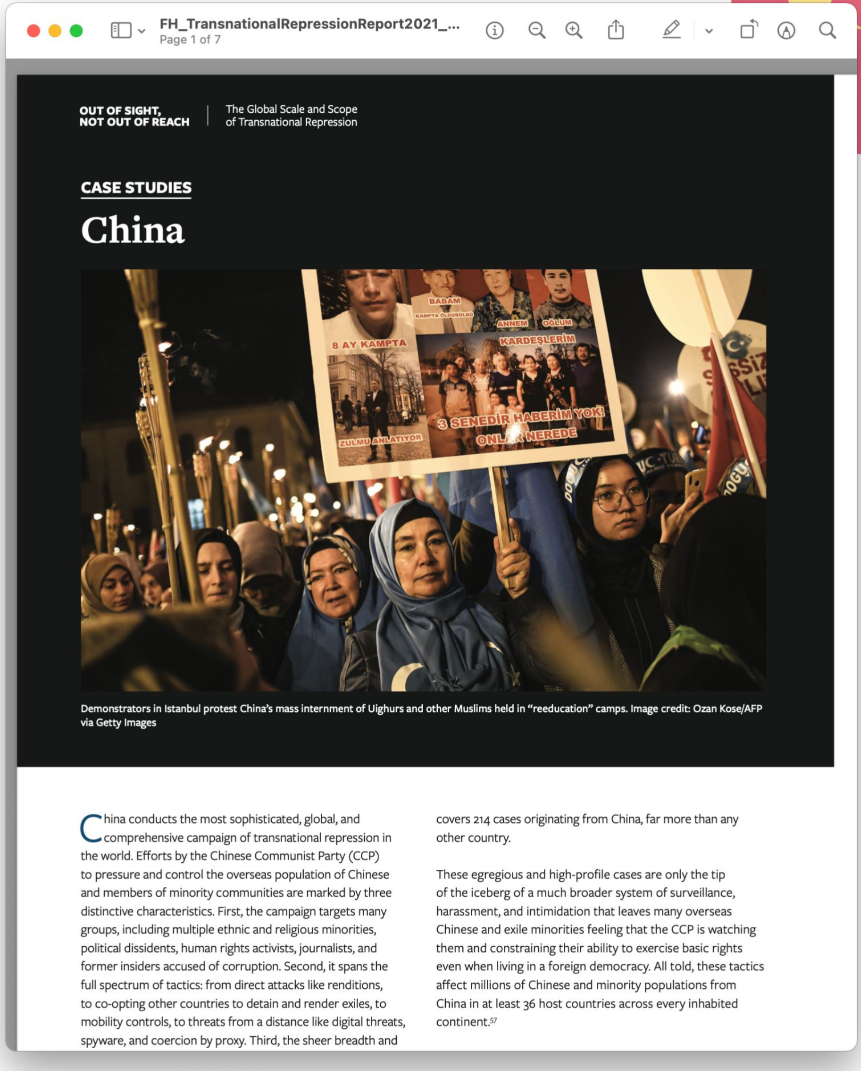
Reason for internment: Using niche chat tools, VPN circumvention software, been to inland provinces and cities, telephone intelligence clues, family members of those who are not allowed to leave the country | Regional integrated push (Sanye) | Teacher of Kashgar 28 Middle School

Reason for internment (Chinese): 使用小众聊天工具，VPN翻墙软件，去过内地省市,电话情报线索,不准出境人员家属|地区一体化推送（三野）|喀什28中老师

Xinjiang Police Files - VOC, 2022

Who’s Under Attack

> *“China conducts the most sophisticated, global, and comprehensive campaign of transnational repression in the world.”*
>
> *– FreedomHouse*



FH_TransnationalRepressionReport2021_...
Page 1 of 7

OUT OF SIGHT, NOT OUT OF REACH | The Global Scale and Scope of Transnational Repression

CASE STUDIES

China

Demonstrators in Istanbul protest China’s mass internment of Uighurs and other Muslims held in “reeducation” camps. Image credit: Ozan Kose/AFP via Getty Images

China conducts the most sophisticated, global, and comprehensive campaign of transnational repression in the world. Efforts by the Chinese Communist Party (CCP) to pressure and control the overseas population of Chinese and members of minority communities are marked by three distinctive characteristics. First, the campaign targets many groups, including multiple ethnic and religious minorities, political dissidents, human rights activists, journalists, and former insiders accused of corruption. Second, it spans the full spectrum of tactics: from direct attacks like renditions, to co-opting other countries to detain and render exiles, to mobility controls, to threats from a distance like digital threats, spyware, and coercion by proxy. Third, the sheer breadth and

covers 214 cases originating from China, far more than any other country.

These egregious and high-profile cases are only the tip of the iceberg of a much broader system of surveillance, harassment, and intimidation that leaves many overseas Chinese and exile minorities feeling that the CCP is watching them and constraining their ability to exercise basic rights even when living in a foreign democracy. All told, these tactics affect millions of Chinese and minority populations from China in at least 36 host countries across every inhabited continent.[57]

North Korea

Individuals and Organizations of Strategic Interest

- Politicians
  - Member of National Assembly
- Government and Political Organizations
  - Advisor to the Korean MoD
  - Civil servant at the MoD

- Academia and Research:
  - Researcher at Keimyung University
  - A translator
  - Professor of Political Science

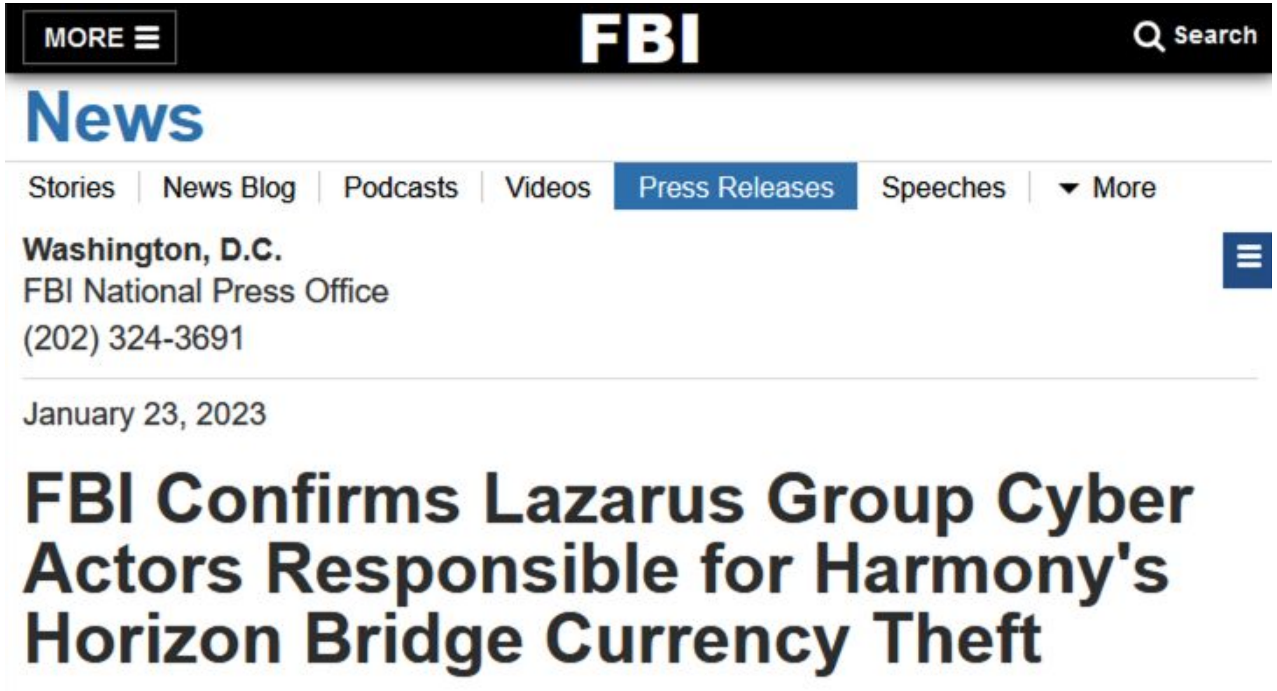
Individuals and Organizations of Strategic Interest

- North Korean defectors
- Journalists covering North Korean affairs

Recovered Victim File: Two North Korean friends successfully entered the United States

Financial and Opportunistic Targeting

- Generate revenue for the regime.
- Circumvent international sanctions
- Non-mobile targeting: APT38
- Mobile is opportunistic



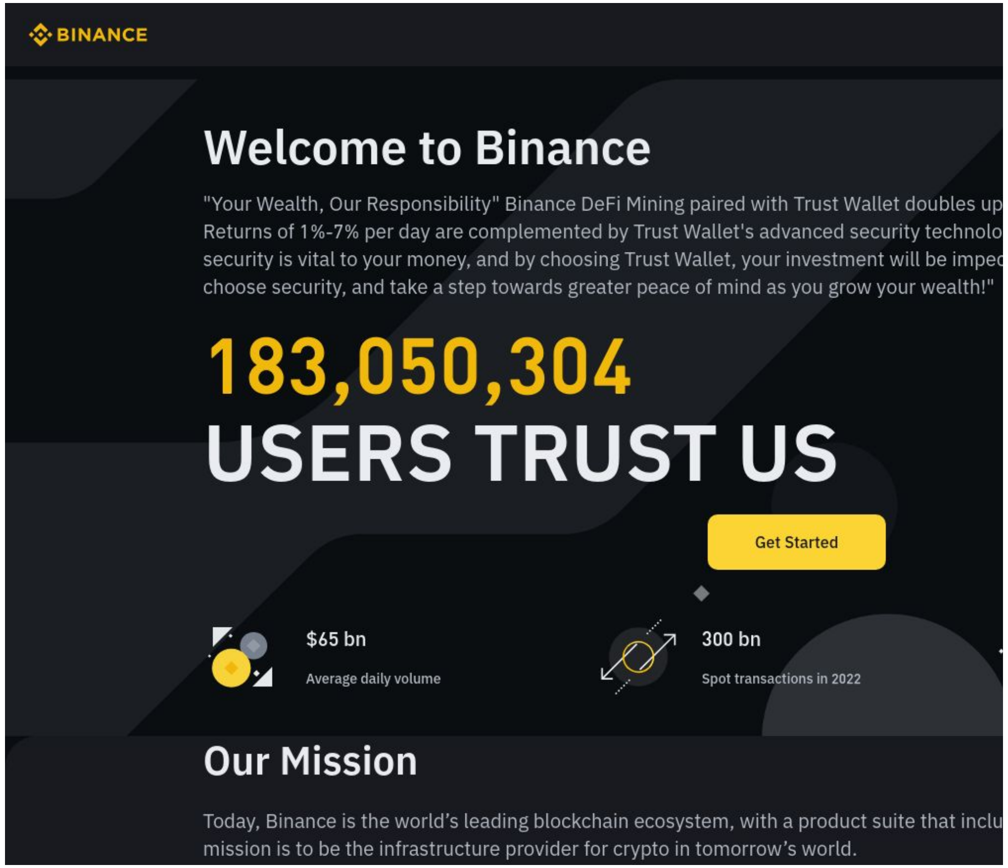
Washington, D.C.
FBI National Press Office
(202) 324-3691

January 23, 2023

FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft

Financial and Opportunistic Targeting

- Cryptocurrency phishing on the AppleZombie C2 servers.
  - binace[.]homes: Binance
  - secure-bdf[.]com
  - dsp2formulaire-bdf[.]net: Banco de Finanzas of Nicaragua.
  - secure-qonto-pro[.]com: Banking businesses in EU.



BINANCE

Welcome to Binance

"Your Wealth, Our Responsibility" Binance DeFi Mining paired with Trust Wallet doubles up
Returns of 1%-7% per day are complemented by Trust Wallet's advanced security technolo
security is vital to your money, and by choosing Trust Wallet, your investment will be impec
choose security, and take a step towards greater peace of mind as you grow your wealth!"

183,050,304
USERS TRUST US

Get Started

$65 bn
Average daily volume

300 bn
Spot transactions in 2022

Our Mission

Today, Binance is the world's leading blockchain ecosystem, with a product suite that inclu
mission is to be the infrastructure provider for crypto in tomorrow's world.

How We Attribute Activity

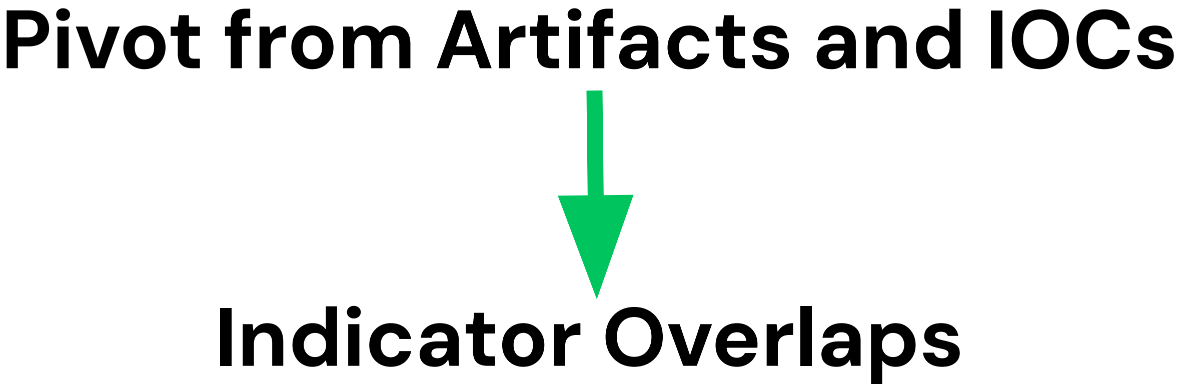
Finding the Groups Behind the Surveillance Operations

Analytical Techniques

How We Attribute Activity

Pivot from Artifacts and IOCs

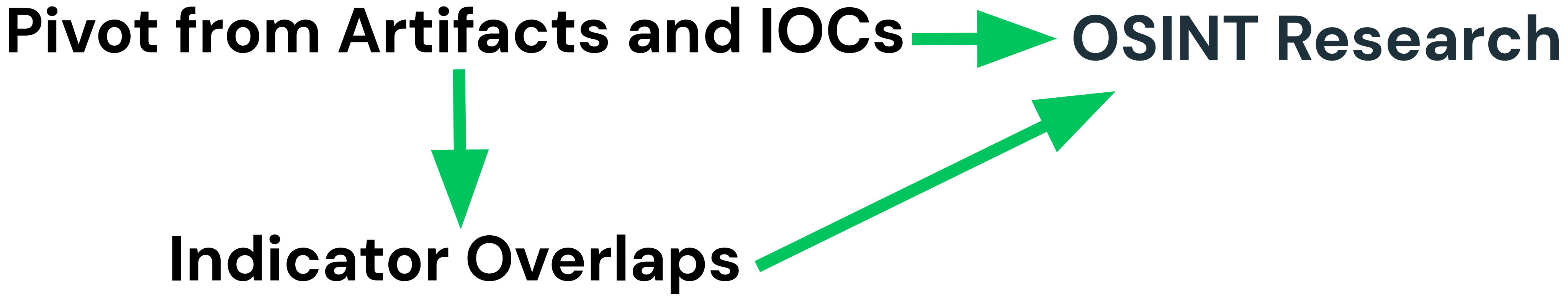
How We Attribute Activity



Pivot from Artifacts and IOCs

Indicator Overlaps

How We Attribute Activity

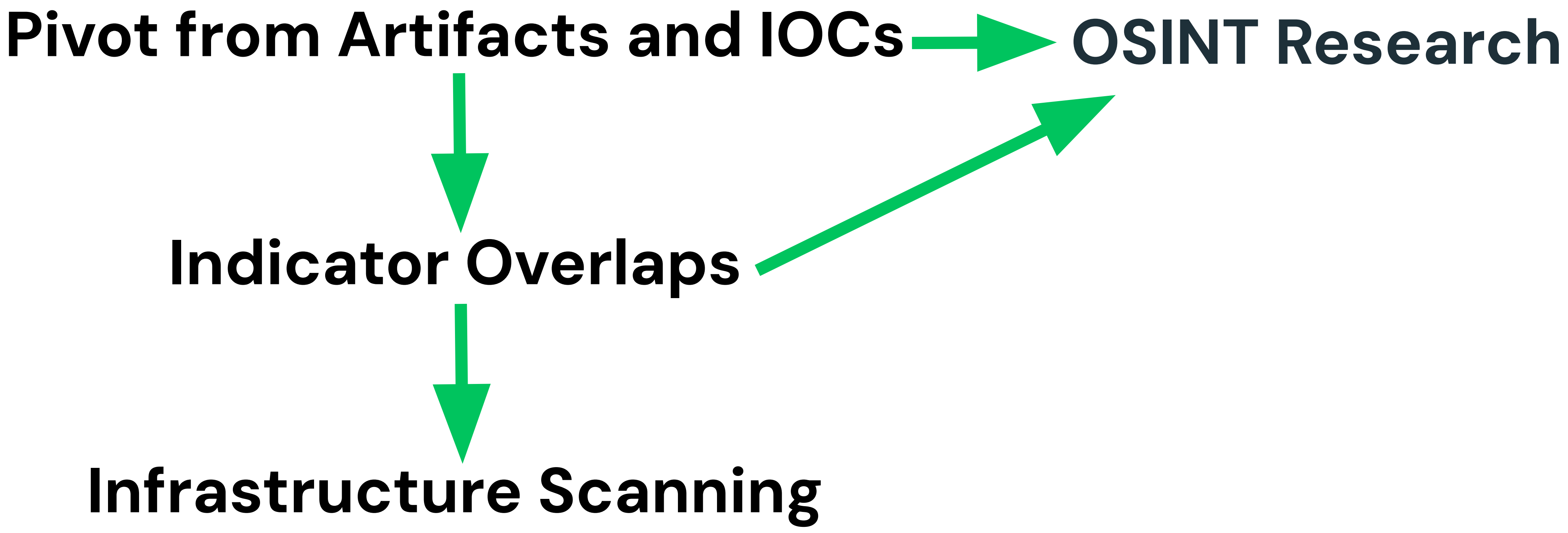


Pivot from Artifacts and IOCs

OSINT Research

Indicator Overlaps

How We Attribute Activity



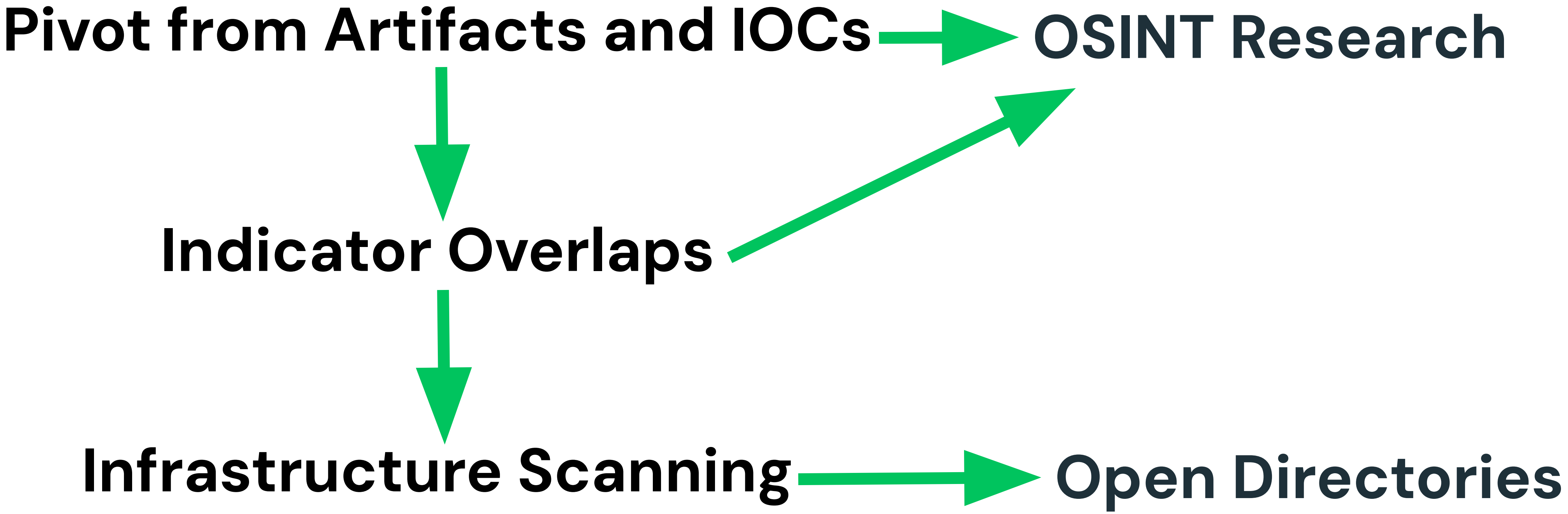
Pivot from Artifacts and IOCs

OSINT Research

Indicator Overlaps

Infrastructure Scanning

How We Attribute Activity



Pivot from Artifacts and IOCs

OSINT Research

Indicator Overlaps

Infrastructure Scanning

Open Directories

How We Attribute Activity

Judgments and Inferences

How We Attribute Activity

Judgments and Inferences

Evaluate Hypotheses

How We Attribute Activity

Judgments and Inferences

Evaluate Hypotheses

Quality of Information

How We Attribute Activity

Judgments and Inferences

Evaluate Hypotheses

Quality of Information

=

High–Moderate–Low Confidence

Attributions: Russia

Infrastructure Indicators

Gamaredon: C2 overlap with desktop-side campaigns

Infrastructure Indicators

Gamaredon: C2 overlap with desktop-side campaigns

llkeyvost.ddns[.]net

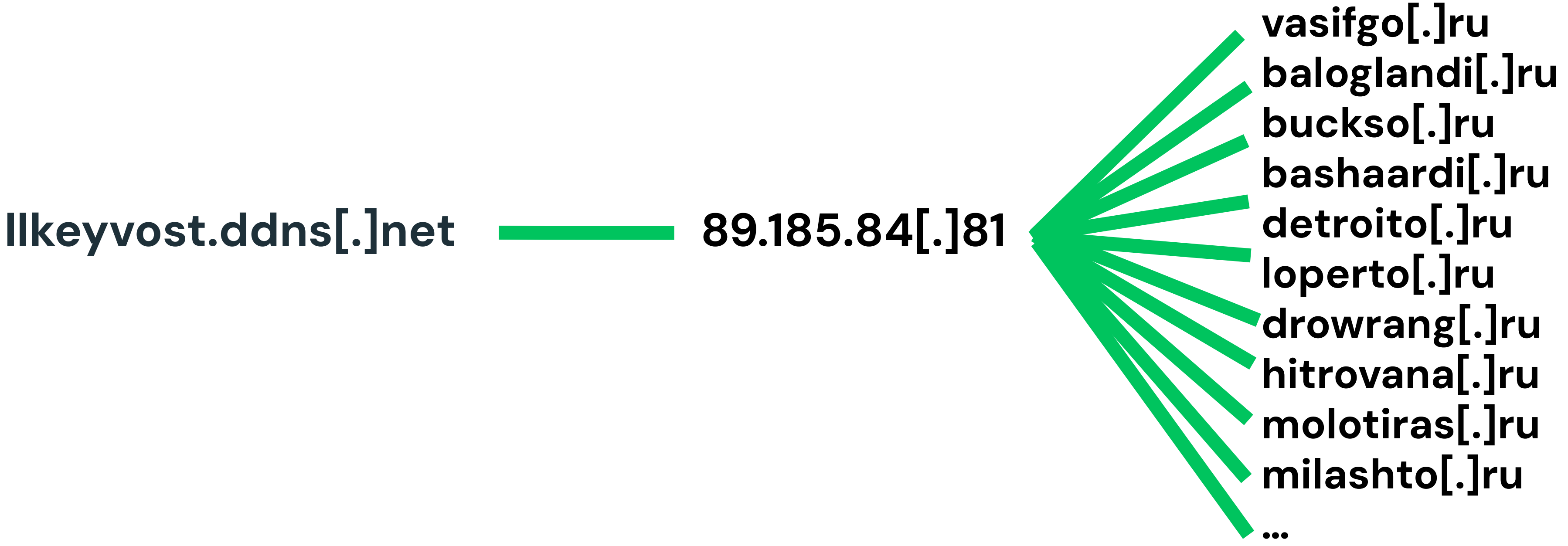
Infrastructure Indicators

Gamaredon: C2 overlap with desktop-side campaigns

llkeyvost.ddns[.]net — 89.185.84[.]81

Infrastructure Indicators

Gamaredon: C2 overlap with desktop-side campaigns



llkeyvost.ddns[.]net

89.185.84[.]81

vasifgo[.]ru
baloglandi[.]ru
buckso[.]ru
bashaardi[.]ru
detroito[.]ru
loperto[.]ru
drowrang[.]ru
hitrovana[.]ru
molotiras[.]ru
milashto[.]ru
…

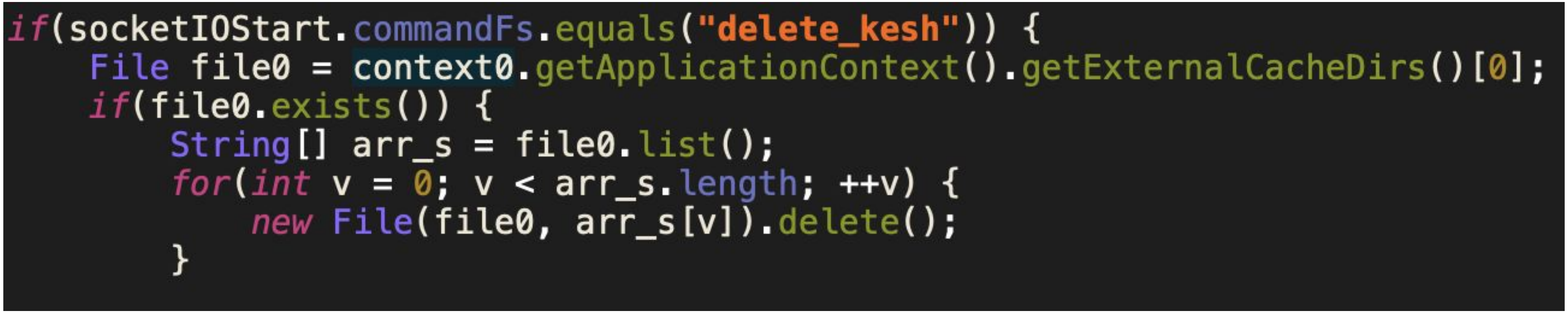
Filename Indicators

Russian-language Artifacts – Filenames, Strings…

galareya.apk	gallery
фотоальбом.apk	photo album
Альбом.apk	Album
Личный.apk	Personal

String Indicators

Russian-language Artifacts - Filenames, Strings…



```
if(socketIOStart.commandFs.equals("delete_kesh")) {
    File file0 = context0.getApplicationContext().getExternalCacheDirs()[0];
    if(file0.exists()) {
        String[] arr_s = file0.list();
        for(int v = 0; v < arr_s.length; ++v) {
            new File(file0, arr_s[v]).delete();
        }
```

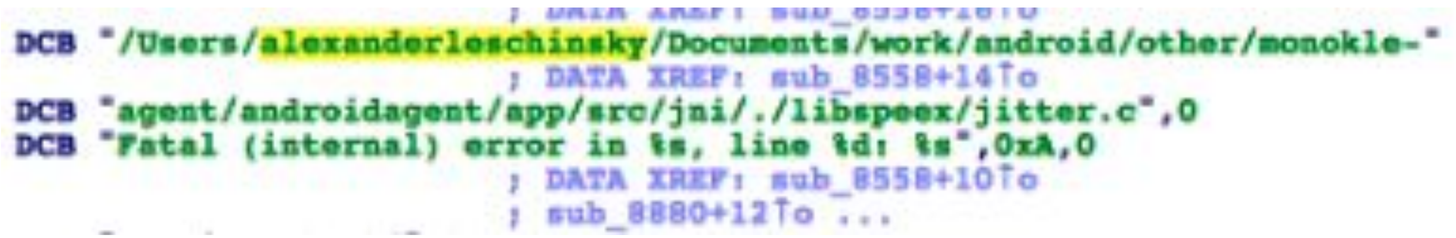
String Indicators

Russian-language Artifacts - Filenames, Strings…

cache -> кэш -> kesh

Monokle String Artifacts

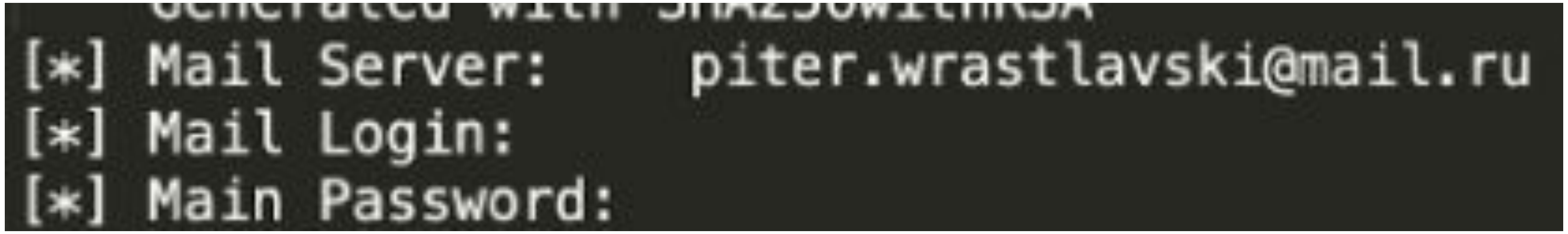
Developer Names in Code



```
                                ; DATA XREF: sub_8558+18↑o
DCB "/Users/alexanderleschinsky/Documents/work/android/other/monokle-"
                                ; DATA XREF: sub_8558+14↑o
DCB "agent/androidagent/app/src/jni/./libspeex/jitter.c",0
DCB "Fatal (internal) error in %s, line %d: %s",0xA,0
                                ; DATA XREF: sub_8558+10↑o
                                ; sub_8880+12↑o ...
```

Monokle String Artifacts

Developer Names in Config Files



```
    Generated with SHA256withRSA
[*] Mail Server:    piter.wrastlavski@mail.ru
[*] Mail Login:
[*] Main Password:
```

Pivoting on Indicators

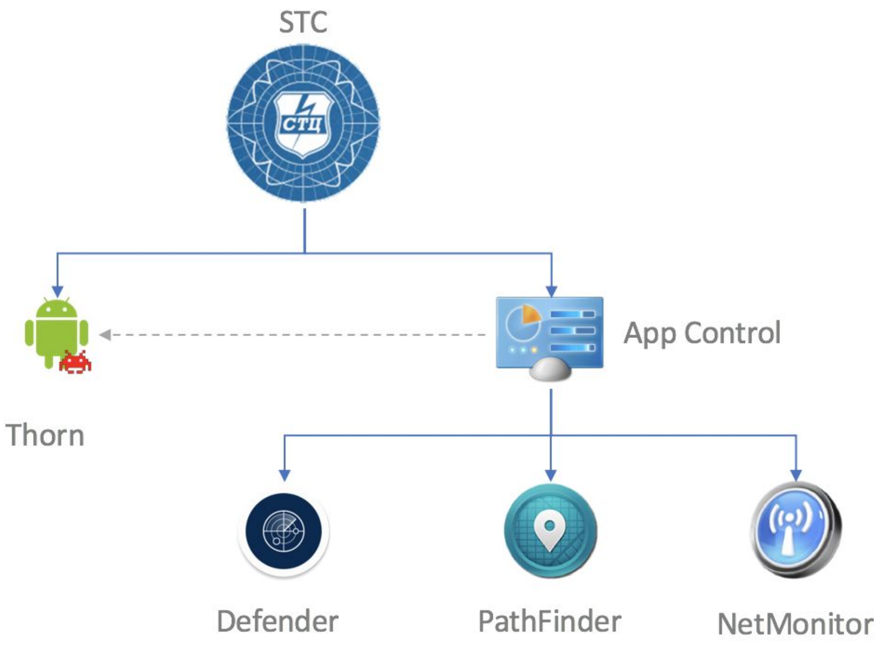
Monokle: Infrastructure Artifacts

СТЦ

СПЕЦИАЛЬНЫЙ
ТЕХНОЛОГИЧЕСКИЙ
ЦЕНТР

Pivoting on Indicators

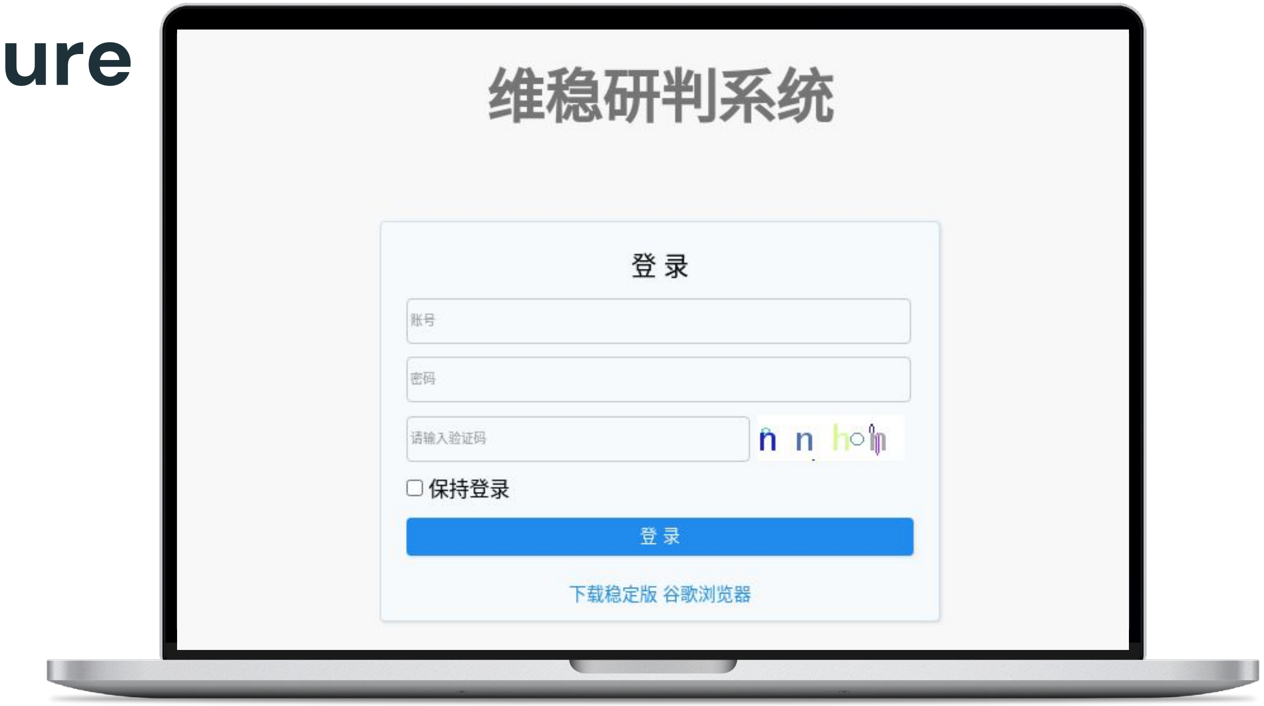
Monokle: Infrastructure Artifacts



Attributions: China

EagleMsgSpy Infrastructure

Old demo C2 infrastructure resolved to commercial subdomains



维稳研判系统

登 录

账号

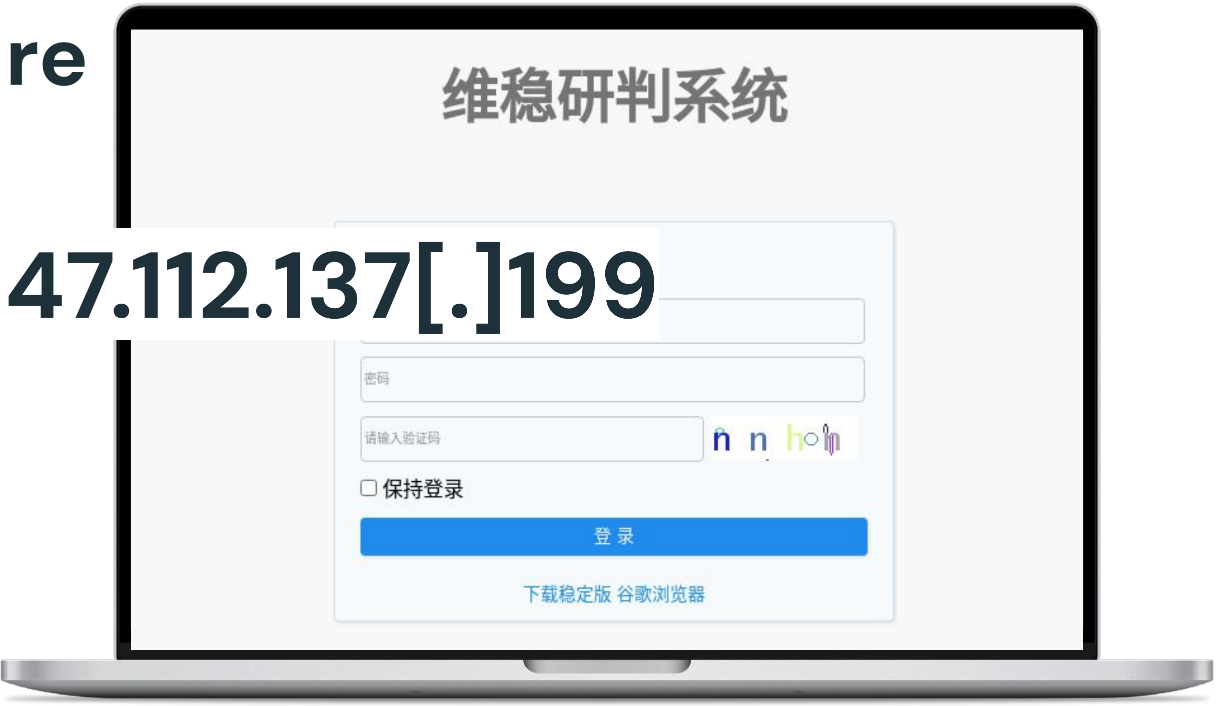
密码

请输入验证码

□ 保持登录

EagleMsgSpy Infrastructure

Old demo C2 infrastructure resolved to commercial subdomains



维稳研判系统

密码

请输入验证码

□ 保持登录

登 录

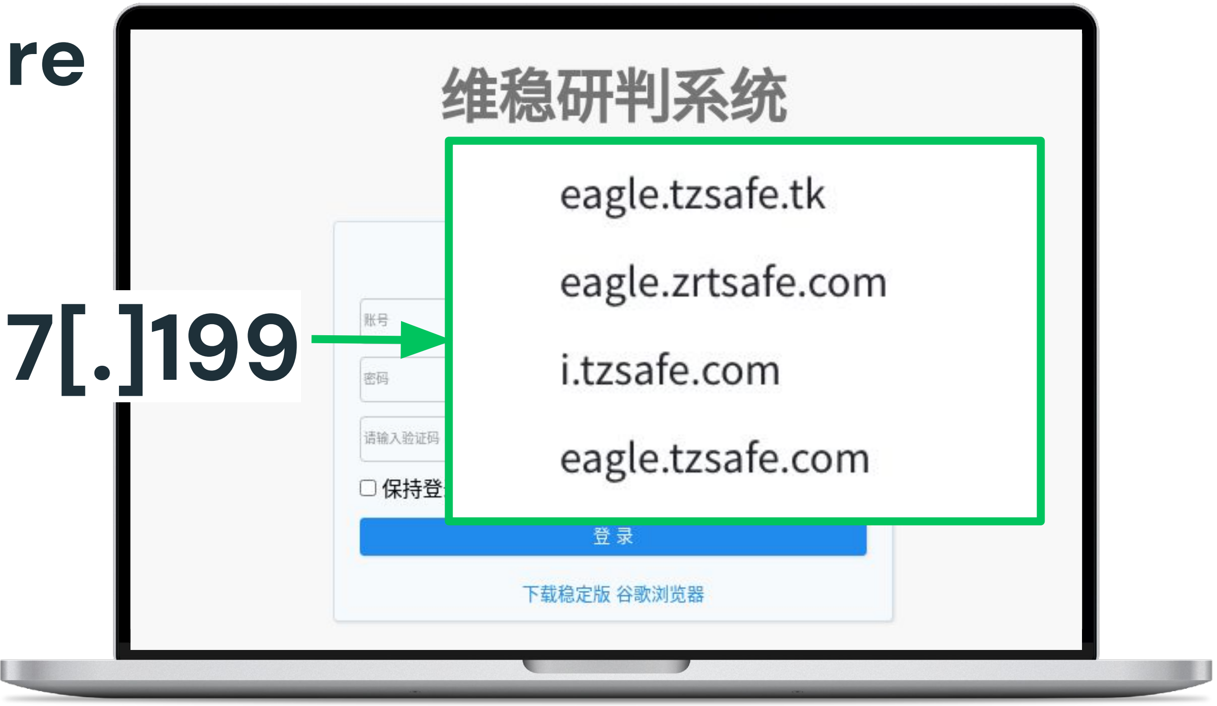
下载稳定版 谷歌浏览器

47.112.137[.]199

EagleMsgSpy Infrastructure

Old demo C2 infrastructure resolved to commercial subdomains

47.112.137[.]199



维稳研判系统

账号

密码

请输入验证码

□ 保持登

eagle.tzsafe.tk

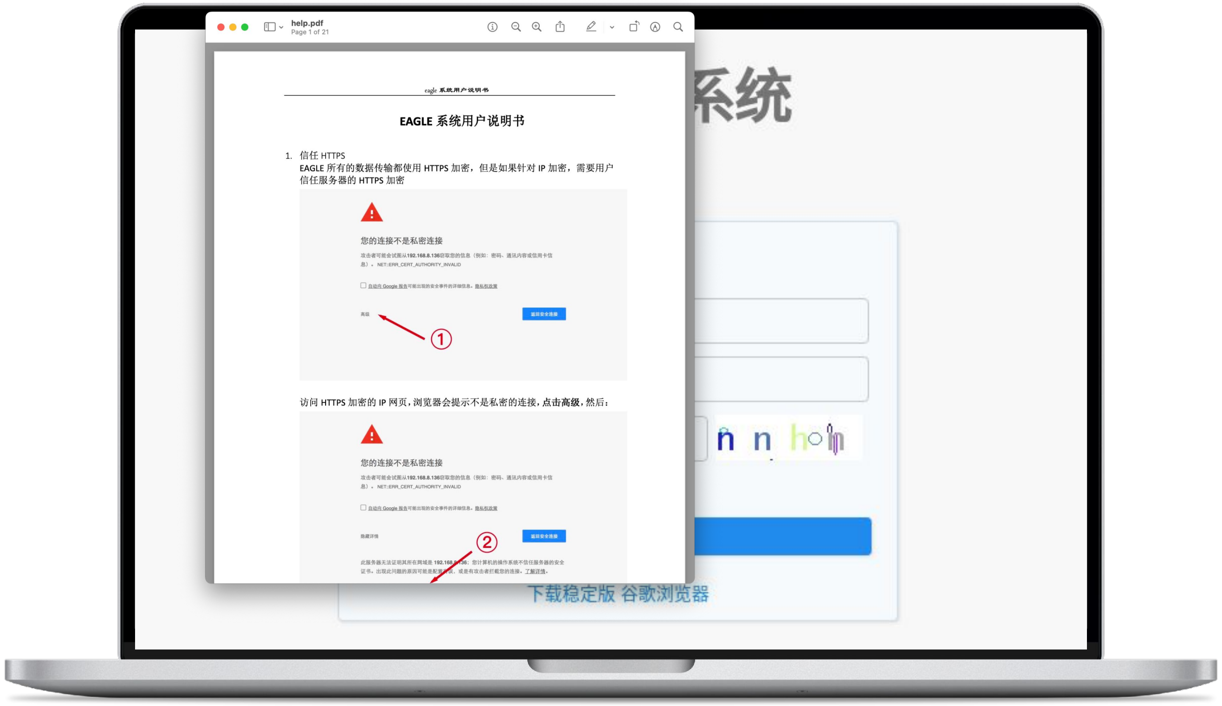
eagle.zrtsafe.com

i.tzsafe.com

eagle.tzsafe.com

Open Directories

Artifacts detail surveillance tool's use



help.pdf
Page 1 of 21

eagle 系统用户说明书

EAGLE 系统用户说明书

1. 信任 HTTPS
   EAGLE 所有的数据传输都使用 HTTPS 加密，但是如果针对 IP 加密，需要用户信任服务器的 HTTPS 加密

您的连接不是私密连接

攻击者可能会试图从192.168.8.136窃取您的信息（例如：密码、通讯内容或信用卡信息）。NET::ERR_CERT_AUTHORITY_INVALID

□ 自动向 Google 报告可能出现的安全事件的详细信息。隐私权政策

访问 HTTPS 加密的 IP 网页，浏览器会提示不是私密的连接，**点击高级**，然后：

您的连接不是私密连接

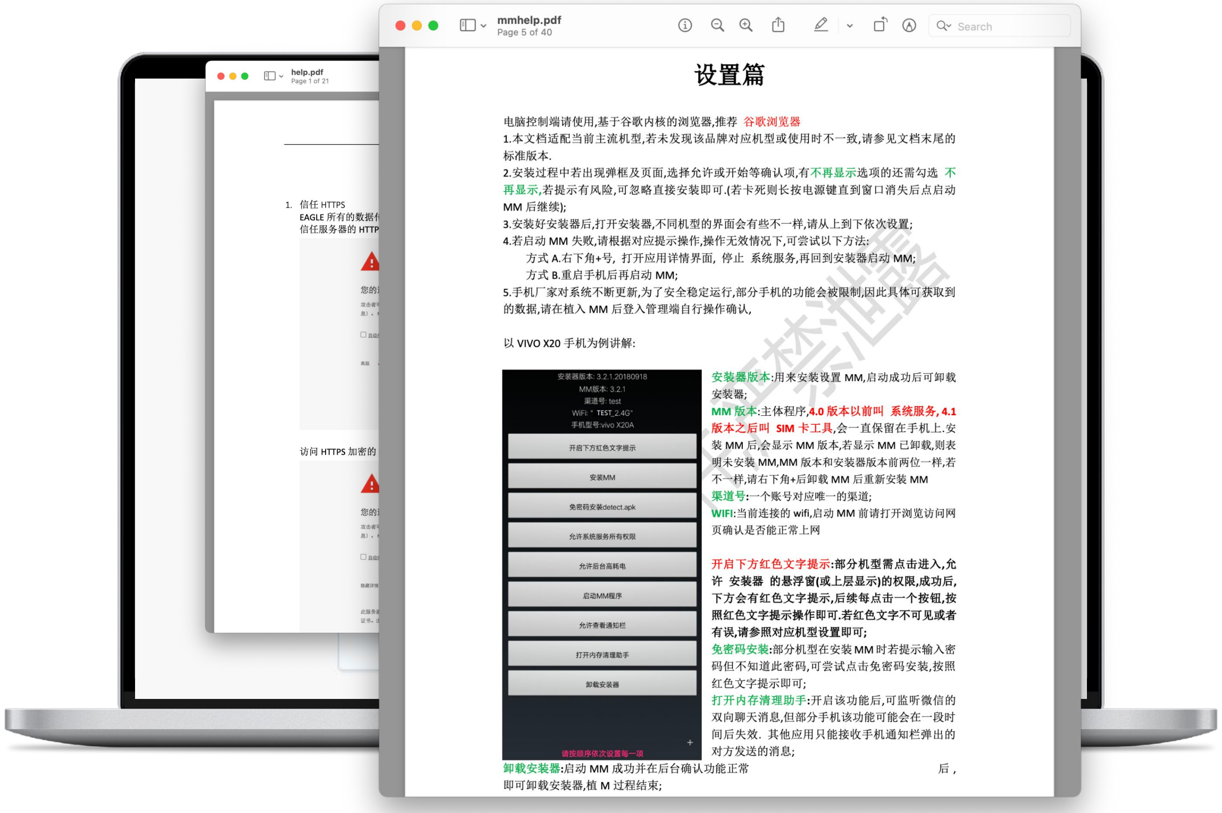
攻击者可能会试图从192.168.8.136窃取您的信息（例如：密码、通讯内容或信用卡信息）。NET::ERR_CERT_AUTHORITY_INVALID

□ 自动向 Google 报告可能出现的安全事件的详细信息。隐私权政策

此服务器无法证明其所在网域是 192.168.8.136；您计算机的操作系统不信任服务器的安全证书。出现此问题的原因可能是配置有误，或是有攻击者拦截您的连接。了解详情。

Open Directories

Artifacts detail surveillance tool’s use



help.pdf
Page 1 of 21

1. 信任 HTTPS
EAGLE 所有的数据传
信任服务器的 HTTP

访问 HTTPS 加密的

mmhelp.pdf
Page 5 of 40

设置篇

电脑控制端请使用,基于谷歌内核的浏览器,推荐 谷歌浏览器
1.本文档适配当前主流机型,若未发现该品牌对应机型或使用时不一致,请参见文档末尾的标准版本.
2.安装过程中若出现弹框及页面,选择允许或开始等确认项,有不再显示选项的还需勾选 不再显示,若提示有风险,可忽略直接安装即可.(若卡死则长按电源键直到窗口消失后点启动 MM 后继续);
3.安装好安装器后,打开安装器,不同机型的界面会有些不一样,请从上到下依次设置;
4.若启动 MM 失败,请根据对应提示操作,操作无效情况下,可尝试以下方法:
方式 A.右下角+号, 打开应用详情界面, 停止 系统服务,再回到安装器启动 MM;
方式 B.重启手机后再启动 MM;
5.手机厂家对系统不断更新,为了安全稳定运行,部分手机的功能会被限制,因此具体可获取到的数据,请在植入 MM 后登入管理端自行操作确认,

以 VIVO X20 手机为例讲解:

安装器版本: 3.2.1.20180918
MM版本: 3.2.1
渠道号: test
WiFi: " TEST_2.4G"
手机型号:vivo X20A

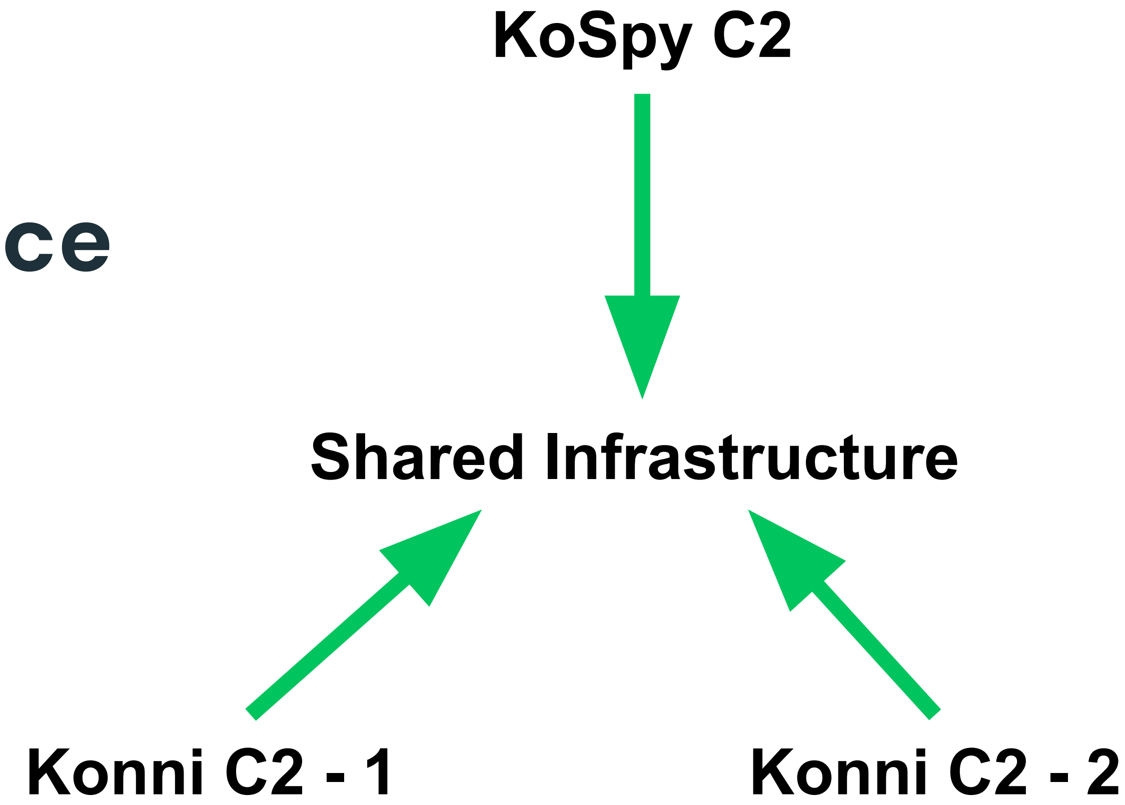
安装器版本:用来安装设置 MM,启动成功后可卸载安装器;
MM 版本:主体程序,4.0 版本以前叫 系统服务, 4.1 版本之后叫 SIM 卡工具,会一直保留在手机上.安装 MM 后,会显示 MM 版本,若显示 MM 已卸载,则表明未安装 MM,MM 版本和安装器版本前两位一样,若不一样,请右下角+后卸载 MM 后重新安装 MM
渠道号:一个账号对应唯一的渠道;
WIFI:当前连接的 wifi,启动 MM 前请打开浏览访问网页确认是否能正常上网

开启下方红色文字提示:部分机型需点击进入,允许 安装器 的悬浮窗(或上层显示)的权限,成功后,下方会有红色文字提示,后续每点击一个按钮,按照红色文字提示操作即可.若红色文字不可见或者有误,请参照对应机型设置即可;
免密码安装:部分机型在安装 MM 时若提示输入密码但不知道此密码,可尝试点击免密码安装,按照红色文字提示即可;
打开内存清理助手:开启该功能后,可监听微信的双向聊天消息,但部分手机该功能可能会在一段时间后失效. 其他应用只能接收手机通知栏弹出的对方发送的消息;
卸载安装器:启动 MM 成功并在后台确认功能正常 后，即可卸载安装器,植 M 过程结束;

Attributions:
North Korea

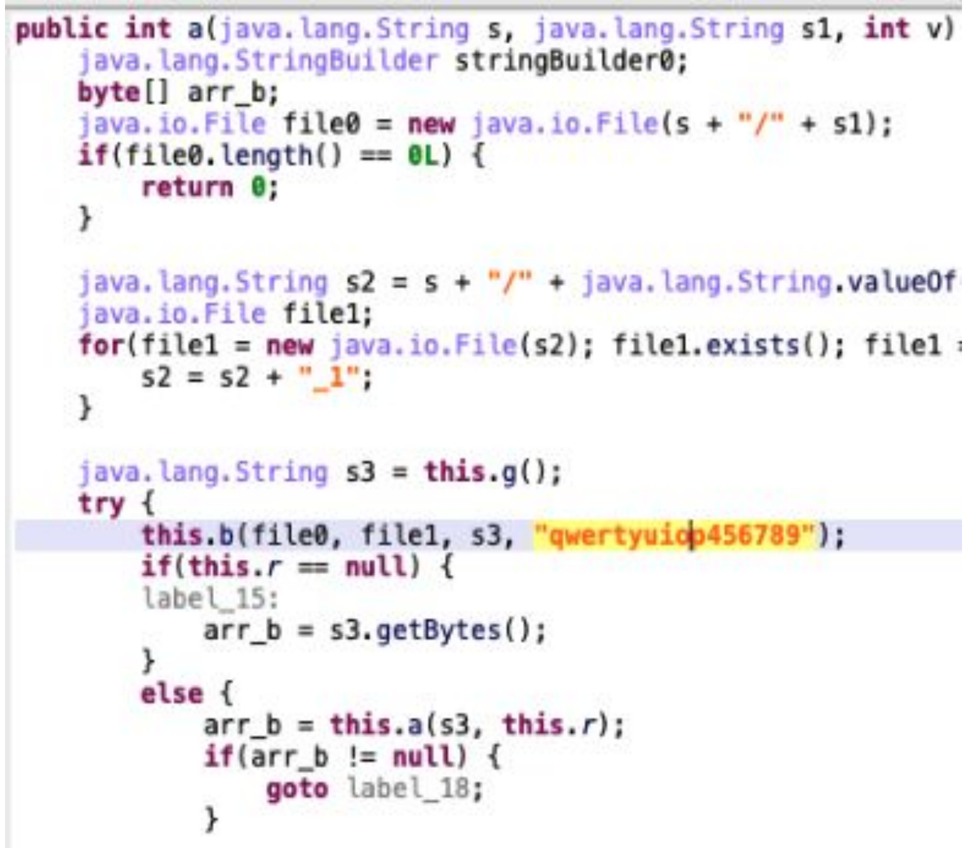
KoSpy Attribution to Scarcruft

C2 –> Konni APT IP space



Shared Code

RedDawn encryption (2018)

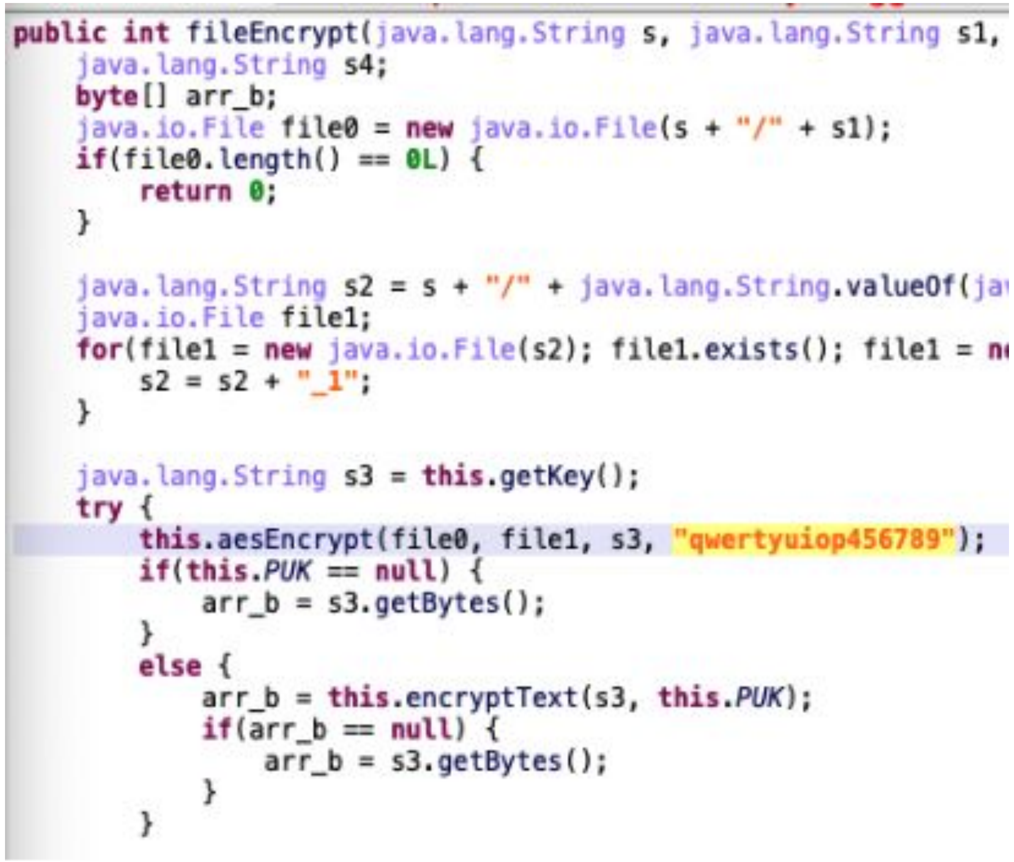


```
public int a(java.lang.String s, java.lang.String s1, int v)
    java.lang.StringBuilder stringBuilder0;
    byte[] arr_b;
    java.io.File file0 = new java.io.File(s + "/" + s1);
    if(file0.length() == 0L) {
        return 0;
    }

    java.lang.String s2 = s + "/" + java.lang.String.valueOf
    java.io.File file1;
    for(file1 = new java.io.File(s2); file1.exists(); file1
        s2 = s2 + "_1";
    }

    java.lang.String s3 = this.g();
    try {
        this.b(file0, file1, s3, "qwertyuiop456789");
        if(this.r == null) {
        label_15:
            arr_b = s3.getBytes();
        }
        else {
            arr_b = this.a(s3, this.r);
            if(arr_b != null) {
                goto label_18;
            }
```

FizDropper encryption (2022)



```
public int fileEncrypt(java.lang.String s, java.lang.String s1,
    java.lang.String s4;
    byte[] arr_b;
    java.io.File file0 = new java.io.File(s + "/" + s1);
    if(file0.length() == 0L) {
        return 0;
    }

    java.lang.String s2 = s + "/" + java.lang.String.valueOf(ja
    java.io.File file1;
    for(file1 = new java.io.File(s2); file1.exists(); file1 = ne
        s2 = s2 + "_1";
    }

    java.lang.String s3 = this.getKey();
    try {
        this.aesEncrypt(file0, file1, s3, "qwertyuiop456789");
        if(this.PUK == null) {
            arr_b = s3.getBytes();
        }
        else {
            arr_b = this.encryptText(s3, this.PUK);
            if(arr_b == null) {
                arr_b = s3.getBytes();
            }
        }
```

III – Takeaways

Fingerprints of State-Backed Surveillance

Fingerprints of State-Backed Surveillance

Heavy Reliance on Social Engineering

Often Highly Targeted Campaigns

OPSEC Varies by Threat Actor

Fingerprints of State-Backed Surveillance

Domestic Surveillance

Support for Military Operations

Syria (historically)
Ukraine currently

Fingerprints of State-Backed Surveillance

“Forensics” tool, vs. “spy” / “trojan” references

Calls for Proposal from government entities

Private, small-size software engineering companies

Fingerprints of State-Backed Surveillance

Abusing legitimate features in novel ways

Lateral movement from desktop and credential compromise to mobile

Granular targeting, hands-on, long-stretched campaigns.

Mitigation Techniques

Prevention & Detection – Individual

- Get Apps Only From Official Stores
- Do Not Follow Unsolicited Links
- Beware of Sensitive or Excessive Permissions
- Enable Native Security Features
- Adopt a Mobile Antivirus

Prevention & Detection – Enterprise

- Adopt & Deploy Mobile EDR
- Deploy EDR In Security Function – not IT
- Test & Audit Security Controls
- Adopt Relevant Policy for Mobile Security

Call to Action

- → Help us protect organizations and individuals at risk
- → Educate at-risk people about state surveillance
- → Employ threat mitigations including physical safety

Thank you!
Questions?

kyle.schmittle@lookout.com
alemdar.islamoglu@lookout.com
kristina.balaam@lookout.com

www.lookout.com/threat-intelligence