



APRIL 18-19, 2024

BRIEFINGS

Voice Phishing Syndicates Unmasked: An In-Depth Investigation and Exposure

Sojun Ryu(S2W Inc.), Yeongjae Shin(Ex-S2W Inc.)



APRIL 18-19, 2024

BRIEFINGS

Index

1. Background
2. Overview
3. Attack infrastructure provided as SaaS
4. SecretCalls
5. Automation

So-jun Ryu

Lead of Threat Analysis Team, @S2W

- Tracking major ransomware and APT attack groups and identifying their TTP
- Interested and passionate about reverse engineering, threat intelligence, and incident response

Career

- Oct, 2020 ~: Threat Analysis Team, S2W TALON
- Dec, 2013 ~ Oct, 2020: KrCERT/CC, KISA

Speaker of {FIRSTCON, FIRSTCTI, Virus Bulletin, ISCR, DCC}

Social

- hopen1117@gmail.com



Yeong-jae Shin

Researcher of SRE Squad, at Goorm

- Observability research and threat analysis on Cloud-native
- Analysis of threat actors on cloud-delivered infrastructure
- Compliance

Career

- Nov, 2023 ~: SRE Squad, at Goorm
- Mar, 2022 ~ Nov, 2023: Threat Analysis Team, S2W TALON

Speaker of {SIS, Virus Bulletin}

Social

- teaf1001@naver.com



[Facebook Profile](#)



[Linkedin Profile](#)

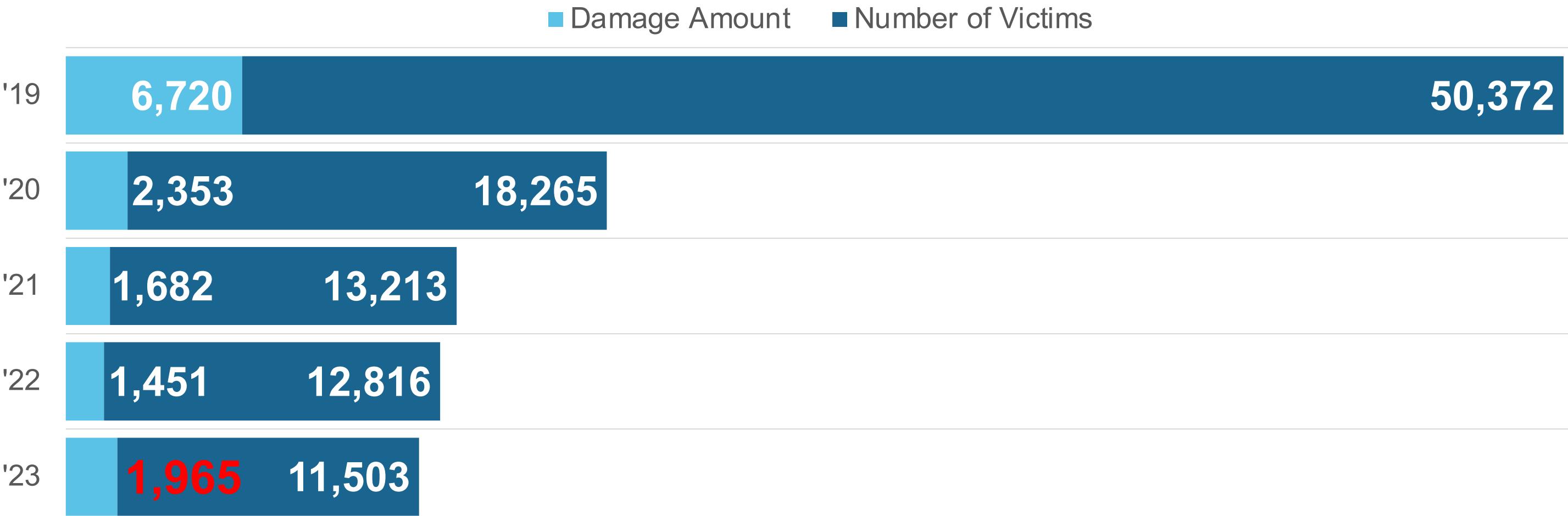
1. Background

1. Background

- An extension of "**When Voice Phishing met Malicious Android App**" at Black Hat Asia in 2019.
- Voice phishing is **social engineering attack over the phone**.
- Discovered in the 2000s, **since 2006 ~ Today** in South Korea
- Main goal is to **extort money from the victims**
- With **native South Koreans** now occupying key positions, attack scenarios becoming **sophisticated**.

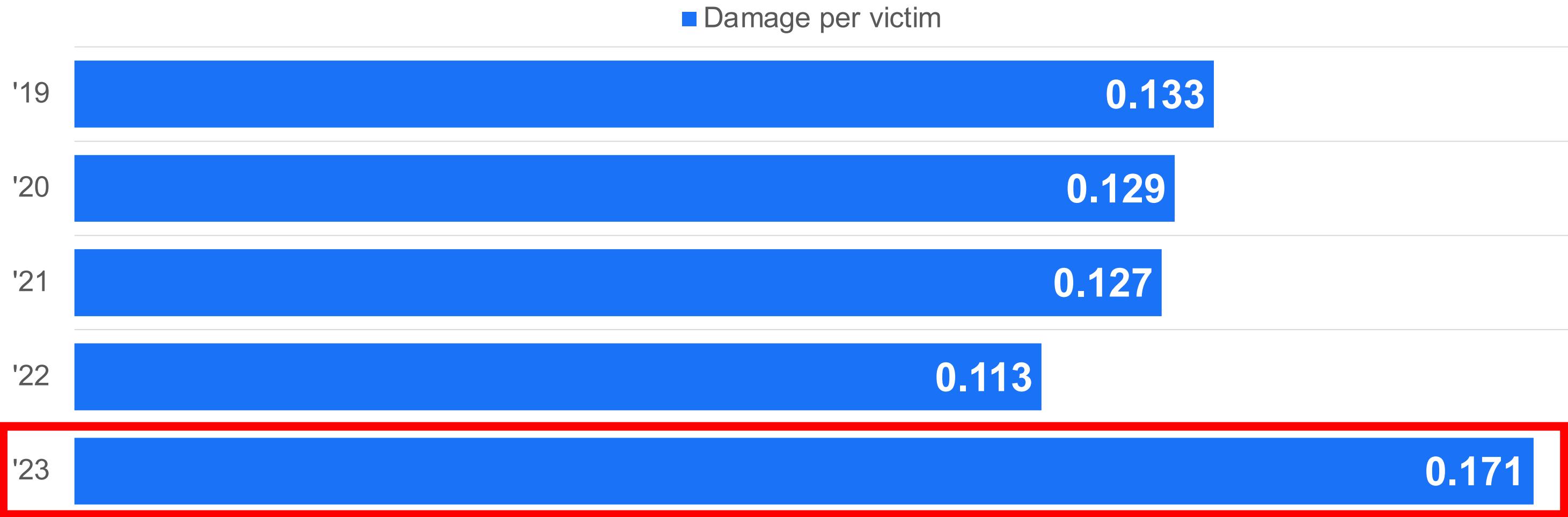
1. Background

Statistics for voice phishing victimization (Unit: 100M KRW, (= 75K USD))



1. Background

Statistics for voice phishing victimization (Unit: 100M KRW, (= 75K USD))

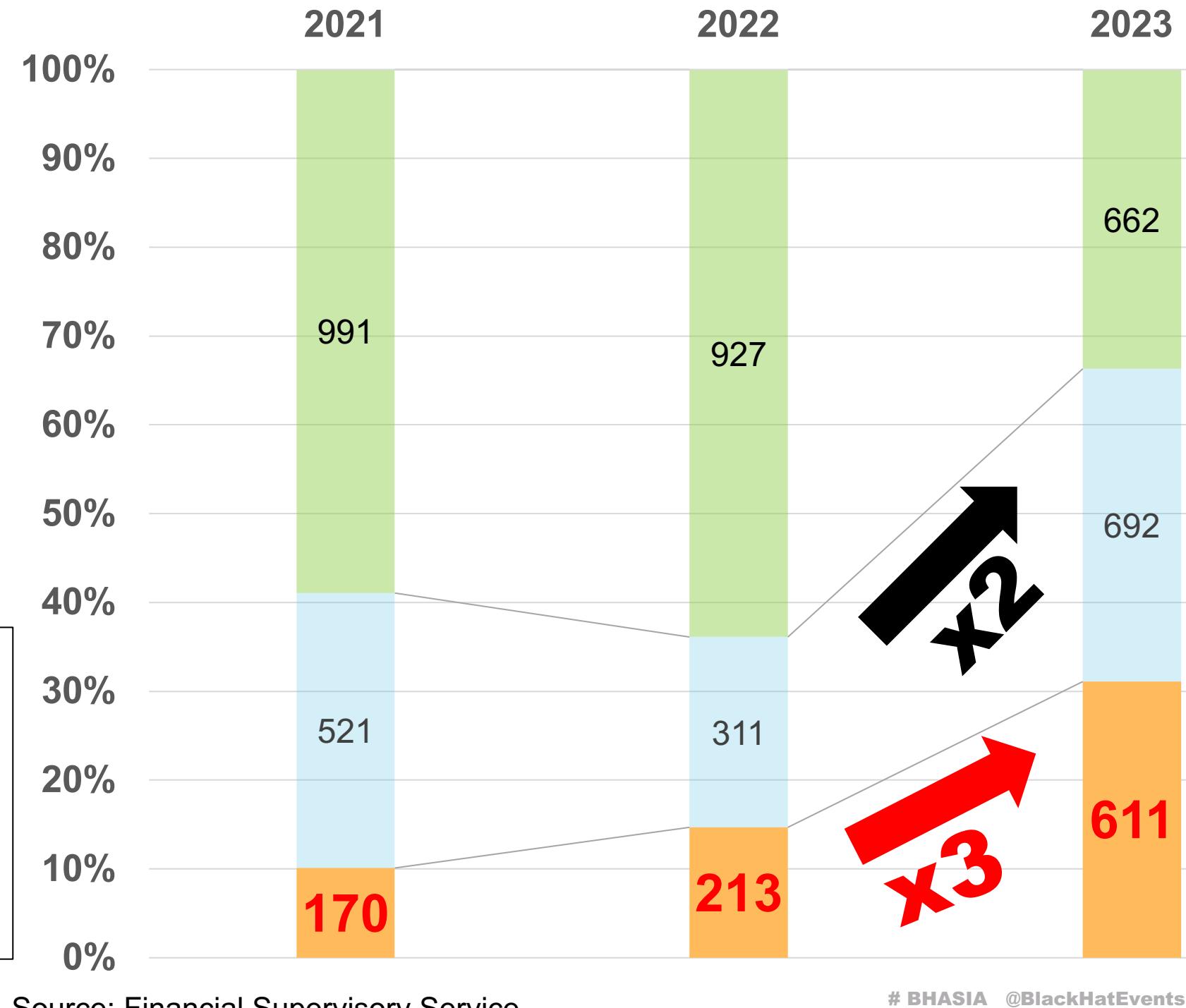
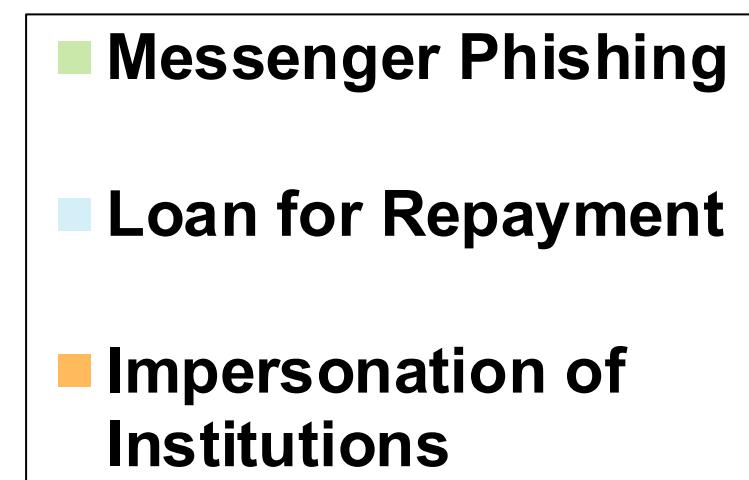


Fewer victims, but damage per victim has increased

1. Background

2023 type of voice-phishing

- The rate of **Loan for Repayment** has approximately **doubled**
- The rate of **Impersonation of Institutions** has approximately **tripled**

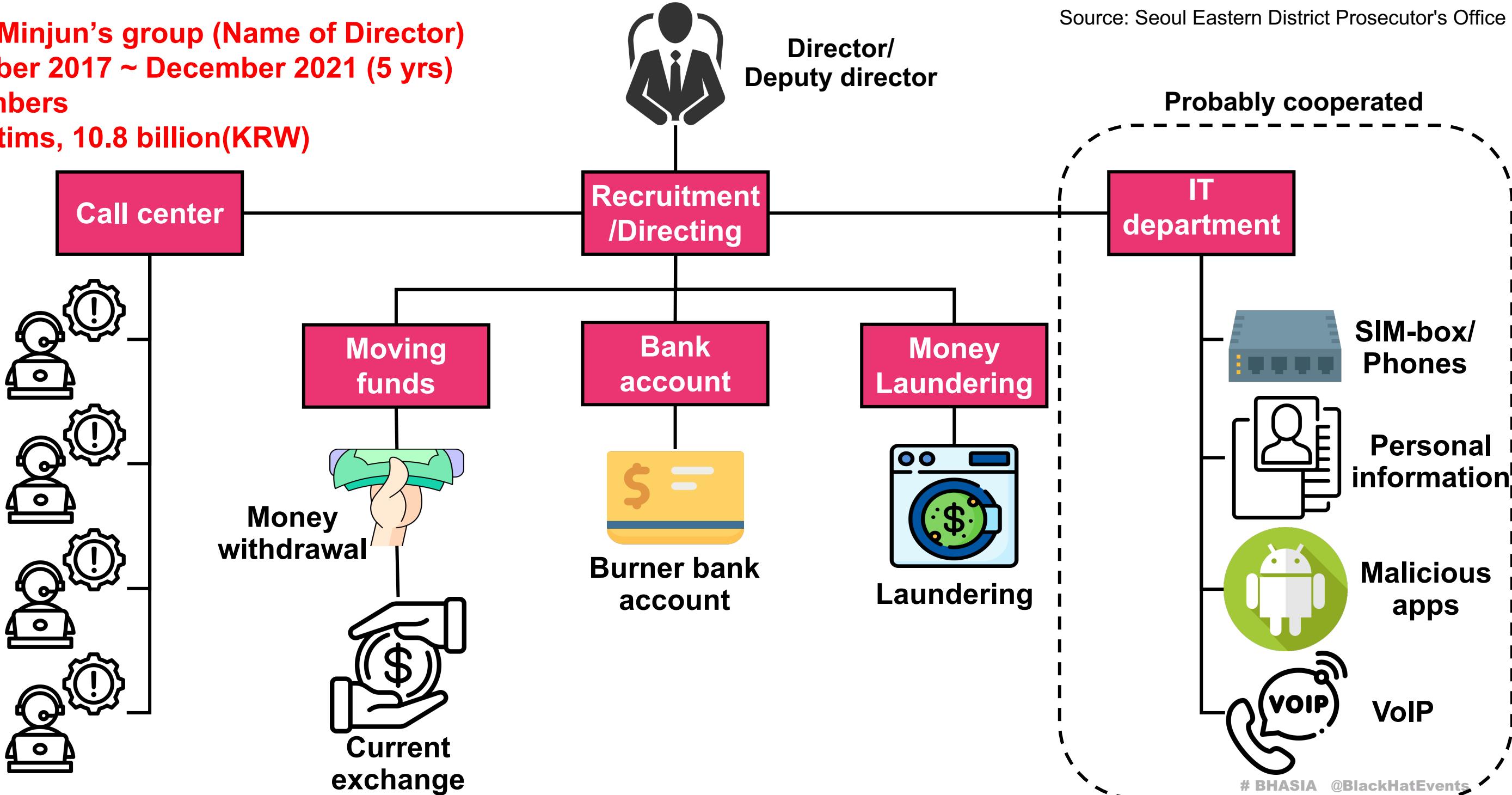


2. Overview

2. Overview – Group structure

- Name: Minjun's group (Name of Director)
- December 2017 ~ December 2021 (5 yrs)
- 60 members
- 560 victims, 10.8 billion(KRW)

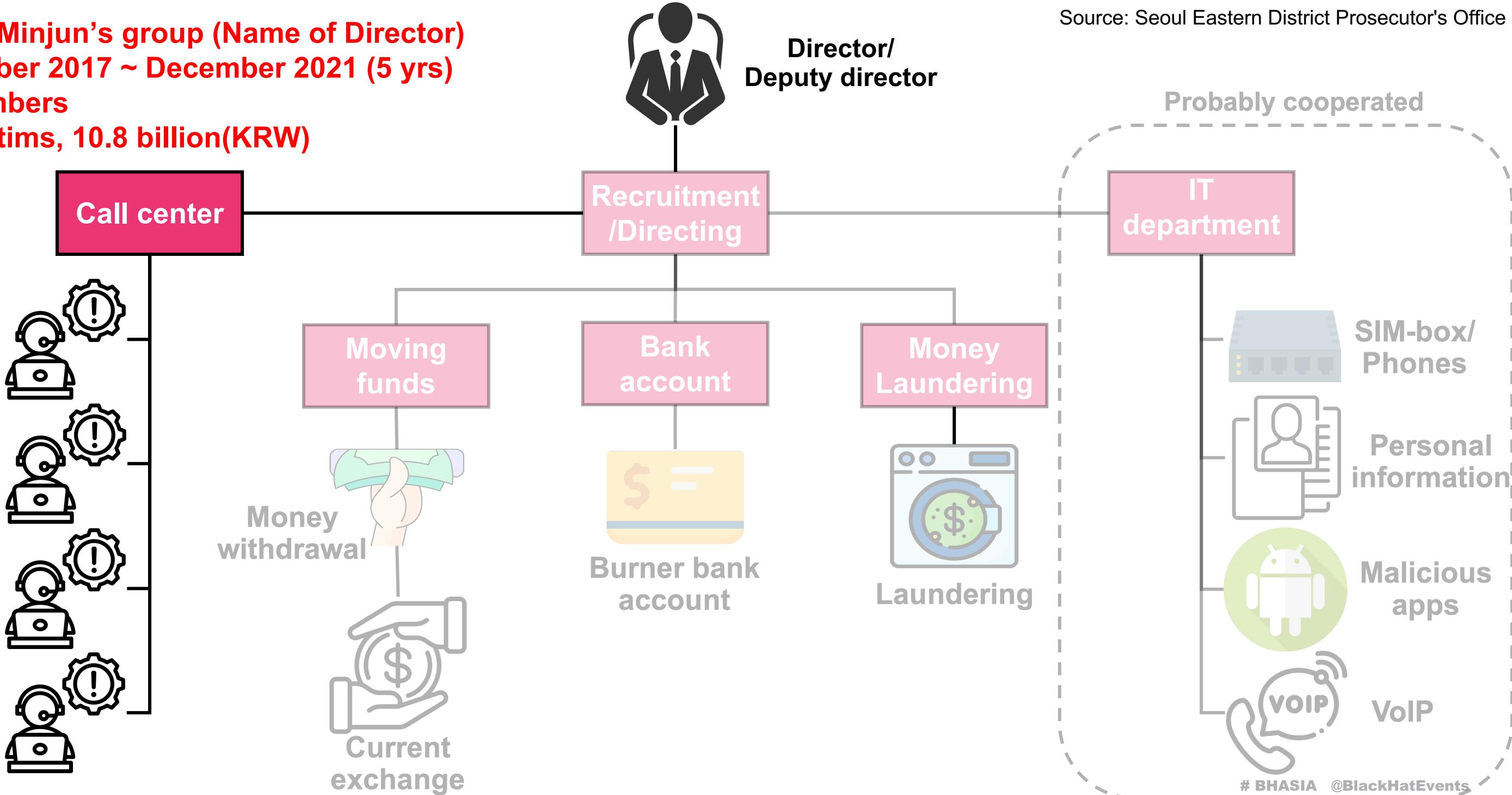
Call centers are in competition



2. Overview – Group structure

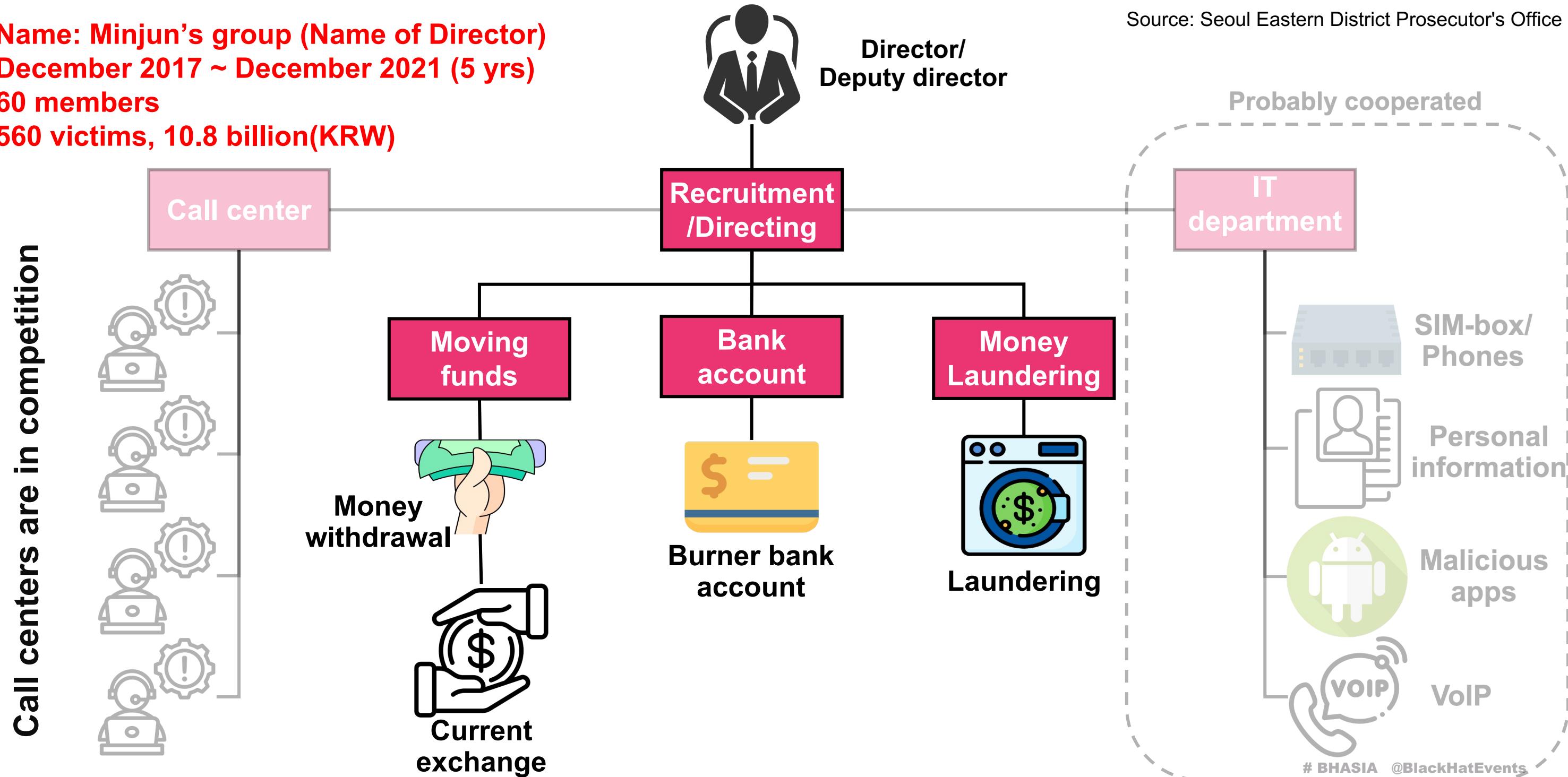
- Name: Minjun's group (Name of Director)
- December 2017 ~ December 2021 (5 yrs)
- 60 members
- 560 victims, 10.8 billion(KRW)

Call centers are in competition



2. Overview – Group structure

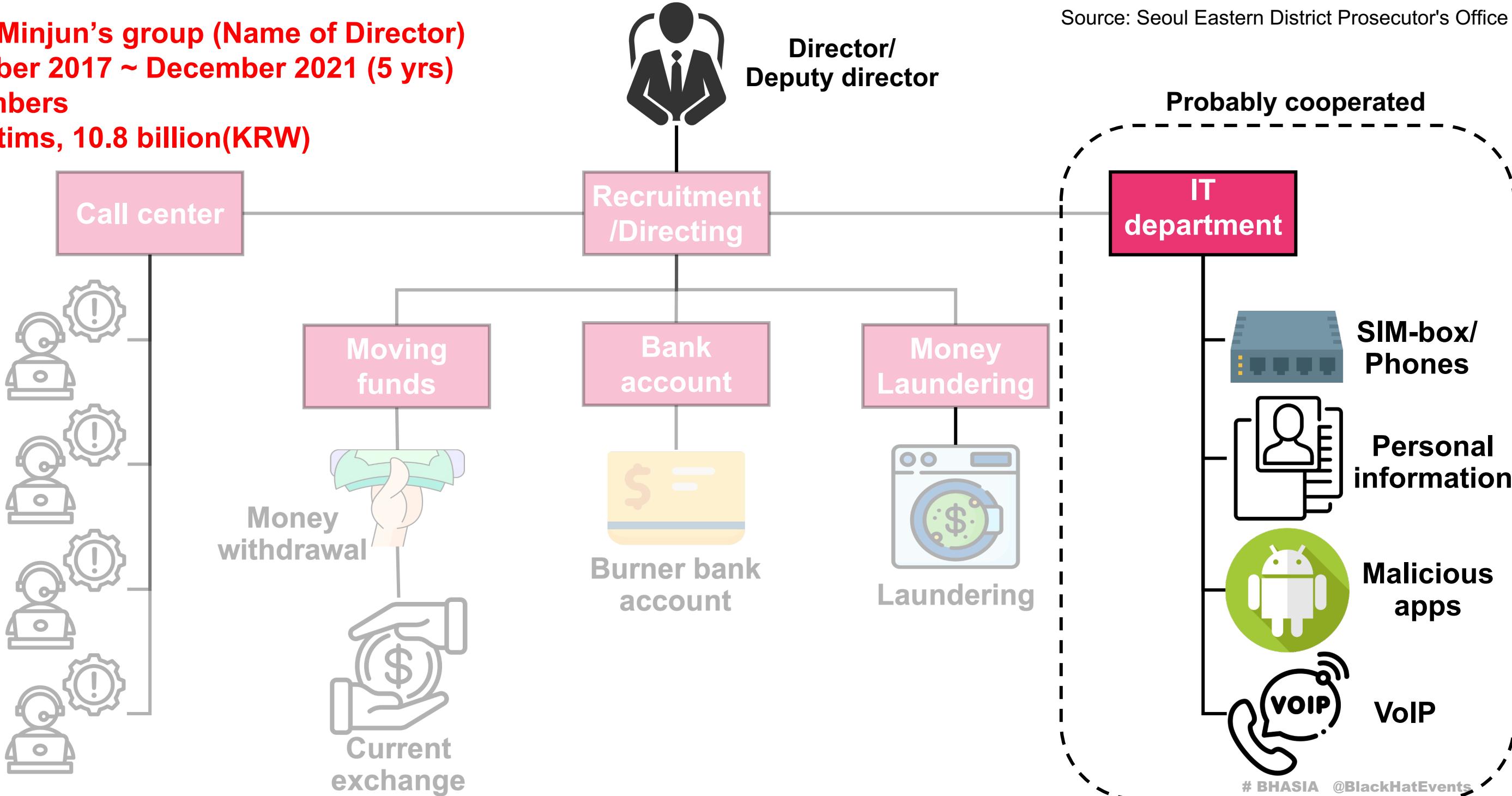
- **Name: Minjun's group (Name of Director)**
 - **December 2017 ~ December 2021 (5 yrs)**
 - **60 members**
 - **560 victims, 10.8 billion(KRW)**



2. Overview – Group structure

- Name: Minjun's group (Name of Director)
- December 2017 ~ December 2021 (5 yrs)
- 60 members
- 560 victims, 10.8 billion(KRW)

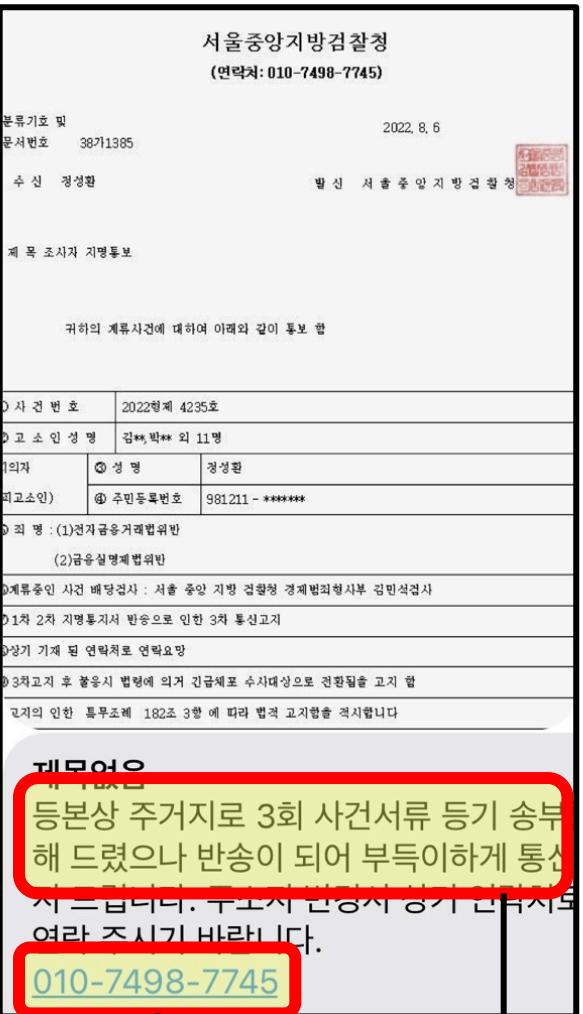
Call centers are in competition



2. Overview – Phishing theme

• Impersonation

- Impersonation-themed dispatch of case documents
- Send case documents by registered mail



Attacker's number

Case documents sent by registered mail
but returned

발행번호 2-210-2020-49785

서울중앙지방검찰청
(연락처: 010-7498-7745)

분류기호 및
문서번호 3

수신 [REDACTED]

제 목 조사자 지명통보

Seoul Central District
Prosecutors' Office

귀하의 계류사건에 대하여 아래와 같이 통보 함

① 사건 번호 2022형제 4235호

② 고소인 성명 김**, 박** 외 11명

피의자 ③ 성명 [REDACTED]

피고소인 ④ 주민등록번호 [REDACTED] - *****

⑤ 죄 명 : (1)전자 금융거래법위반

(2)금융실명제법위반

⑥ 계류중인 사건 배당검사 : 서울 중앙 지방 검찰청 경제범죄형사부 김민석검사

⑦ 1차 2차 지명통지서 반송으로 인한 3차 통신고지

⑧ 상기 기재 된 연락처로 연락

⑨ 3차고지 후 불응시 법령에 의거 긴급체포 수사대상으로 전환될을 고지 함

⑩ 고지의 인한 특무조례 182조 3항

Case number &
Plaintiff's name

Seoul Central District
Prosecutors' Office

2. Overview – Phishing theme

- **Loans for repayment**

- Emergency livelihood support
- Coronavirus-themed Government-backed low-interest refinancing

- **Deception Methods**

- Demanding money to boost credit rating via transactions
- Downloading loan app for contactless lending

Internet bank name

The last loan of 2021
for low-income

You've been selected
for a special offer.

FCFS

Limit: 10M ~ 200M (KRW),
Interest: 1.3% ~ 3.0%

Contact number &
operating hours for consultation

(광고) 카 카 오 뱅 크

고객님의 행복한 내일을 응원합니다.
2021년 마지막 서민신용대출 상품 안내
드립니다.

문자 수신 고객님께서는 당사승인 가능대
상자로 선정되어 특별안내 드립니다.

상품요약
접수마감: 2021년 9월 17일 **(선착순)**
대출기간: 12개월 - 120개월 이내 설정가
능
신청조건: 만 20세 이상 누구나

대출용도: 버팀목, 생활안정, 대환, 사업
등

승인한도: 최소 1000만원 - 최대 2억원
까지
(연)금리: 1.3 - 3.0 % 내외 (최초 1년간
이자 시역선풍모증재단 선액시원)
상환방법: 원(리)금분할상환, 만기 일시상
환

...

상담문의: [02-2647-9861](tel:02-2647-9861)
상담문의: [02-2647-9861](tel:02-2647-9861)

상담가능시간: 영업일 09:00 ~
18:00(주말, 공휴일 제외)

2. Overview – Phishing theme



INTEREST ON MY LOAN
AT THE TIME: 6.0%

Contact number &
g hours for consultation

Internet bank name

The last loan of 2021
for low-income

You've been selected
for a special offer.

FCFS

it: 10M ~ 200M (KRW),

Interest: 1.3% ~ 3.0%

(광고) 카 카 오 뱅 크

고객님의 행복한 내일을 응원합니다.

2021년 마지막 서민신용 대출 상품 안내
드립니다.

문자 수신 고객님께서는 당사승인 가능대
상자로 선정되어 특별안내 드립니다.

상품요약

접수마감: 2021년 9월 17일 **(선착순)**

대출기간: 12개월 - 120개월 이내 설정가
능

신청조건: 만 20세 이상 누구나

대출용도: 버팀목, 생활안정, 대환, 사업
등

승인한도: 최소 1000만원 - 최대 2억원
까지

(연)금리: 1.3 - 3.0 % 내외 (최초 1년간)

이사 시역선풍모증재단 선액시원)

상환방법: 원(리)금분할상환, 만기 일시상
환

...

상담문의: [02-2647-9861](tel:02-2647-9861)

상담문의: [02-2647-9861](tel:02-2647-9861)

상담가능시간: 영업일 09:00 ~

18:00(주말, 공휴일 제외)

2. Overview – Attack scenarios

Loans for repayment

Smishing / Call

Introduce a loan

Demand fine / fee

Impersonation

Smishing / Call

Threaten with involvement in a crime

Induce to access to **fake site**

Show fake official documents

Demand money for investigation / protection

Impersonation using APK (Case 1)

Smishing / Call

Disguise as investigator via 2nd Call / Messenger

Induce to install an **APK** via IP / Attachment

Using call forwarding, tricking a victim

Demand money for investigation / protection

Impersonation using APK (Case 2)

Smishing / Call

Threaten with involvement in a crime

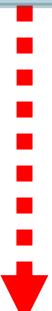
Induce access to **fake site**

Show fake official documents

Induce to install an **APK** via IP

Using call forwarding, tricking a victim

Demand money for investigation / protection



Scam / Extortion

2. Overview – Attack scenarios

Loans for repayment

Smishing / Call

Introduce a loan

Demand fine / fee

Impersonation

Smishing / Call

Threaten with involvement in a crime

Induce to access to **fake site**

Show fake official documents

Demand money for investigation / protection

Impersonation using APK (Case 1)

Smishing / Call

Disguise as investigator via 2nd Call / Messenger

Induce to install an **APK** via IP / Attachment

Using call forwarding, tricking a victim

Demand money for investigation / protection

Impersonation using APK (Case 2)

Smishing / Call

Threaten with involvement in a crime

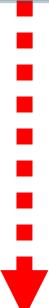
Induce access to **fake site**

Show fake official documents

Induce to install an **APK** via IP

Using call forwarding, tricking a victim

Demand money for investigation / protection



Scam / Extortion

2. Overview – Attack scenarios

Loans for repayment

Smishing / Call

Introduce a loan

Demand fine / fee

Impersonation

Smishing / Call

Threaten with involvement in a crime

Induce to access to **fake site**

Show fake official documents

Demand money for investigation / protection

Impersonation
using APK (Case 1)

Smishing / Call

Disguise as investigator via 2nd Call / Messenger

Induce to install an **APK** via IP / Attachment

Using call forwarding, tricking a victim

Demand money for investigation / protection

Impersonation
using APK (Case 2)

Smishing / Call

Threaten with involvement in a crime

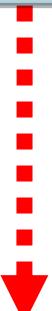
Induce access to **fake site**

Show fake official documents

Induce to install an **APK** via IP

Using call forwarding, tricking a victim

Demand money for investigation / protection



Scam / Extortion

2. Overview – Attack scenarios

Loans for repayment

Smishing / Call

Introduce a loan

Demand fine / fee

Impersonation

Smishing / Call

Threaten with involvement in a crime

Induce to access to **fake site**

Show fake official documents

Demand money for investigation / protection

Impersonation using APK (Case 1)

Smishing / Call

Disguise as investigator via 2nd Call / Messenger

Induce to install an **APK** via IP / Attachment

Using call forwarding, tricking a victim

Demand money for investigation / protection

Impersonation using APK (Case 2)

Smishing / Call

Threaten with involvement in a crime

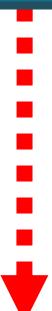
Induce access to **fake site**

Show fake official documents

Induce to install an **APK** via IP

Using call forwarding, tricking a victim

Demand money for investigation / protection



Scam / Extortion

2. Overview – Attack scenarios

Loans for repayment

Smishing / Call

Introduce a loan

Demand fine / fee

Impersonation

Smishing / Call

Threaten with involvement in a crime

Induce to access to **fake site**

Show fake official documents

Demand money for investigation / protection

Impersonation using APK (Case 1)

Smishing / Call

Disguise as investigator via 2nd Call / Messenger

Induce to install an **APK** via IP / Attachment

Using call forwarding, tricking a victim

Demand money for investigation / protection

Impersonation using APK (Case 2)

Smishing / Call

Threaten with involvement in a crime

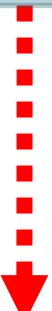
Induce access to **fake site**

Show fake official documents

Induce to install an **APK** via IP

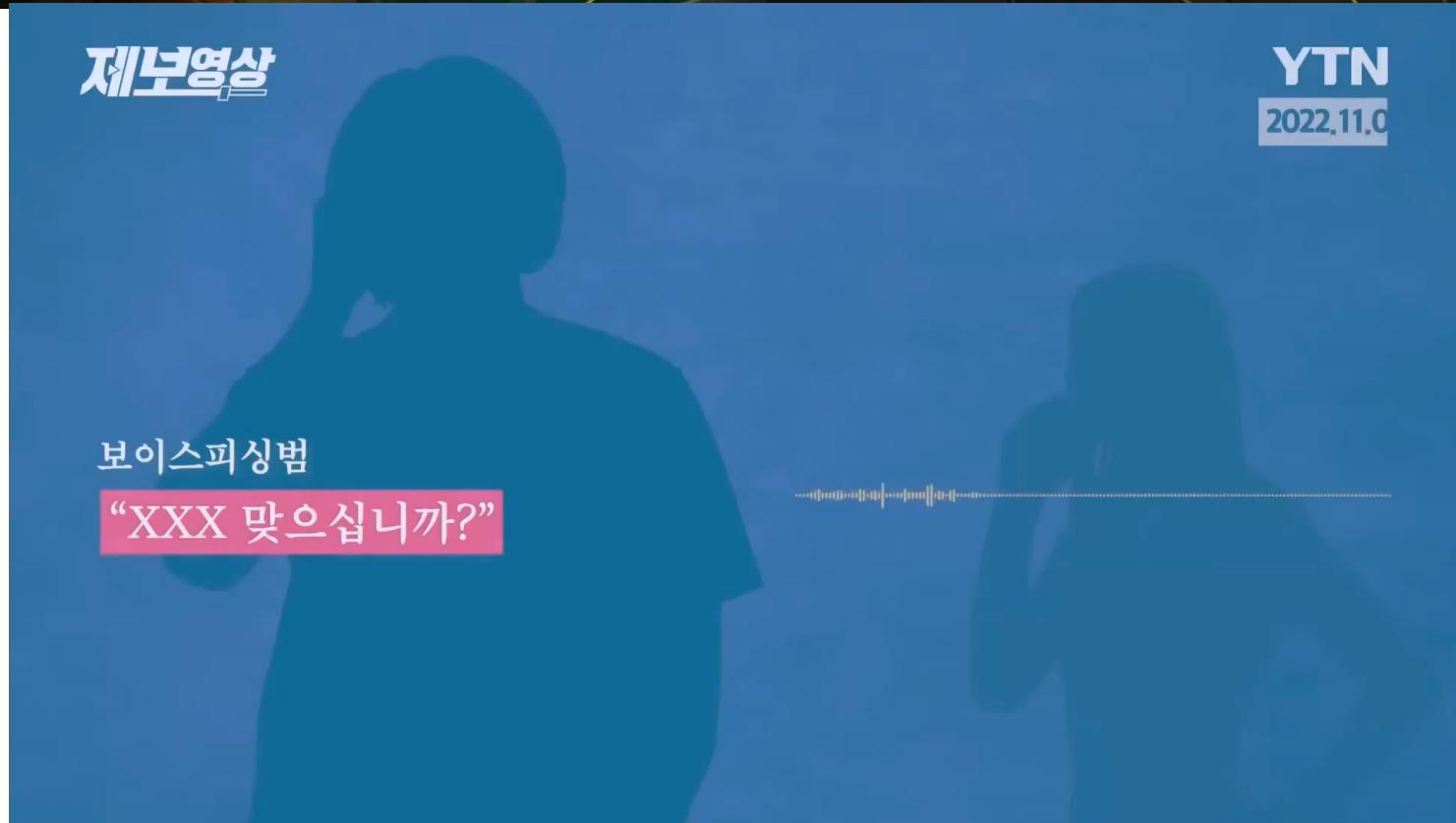
Using call forwarding, tricking a victim

Demand money for investigation / protection



Scam / Extortion

2. Overview – Attack scenarios



Source: Financial Supervisory Service,
YTN

1. Introduce as investigator



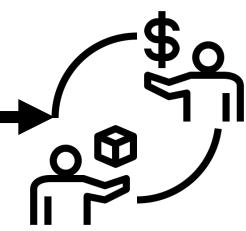
2. Disclose criminal arrests



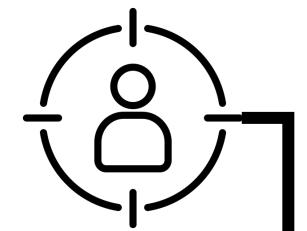
3. Obtain passbook/ID
in your name on site



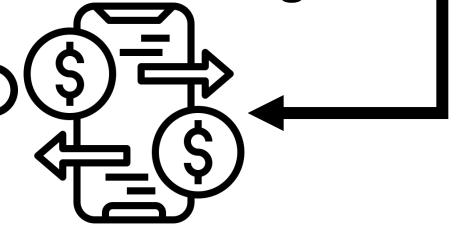
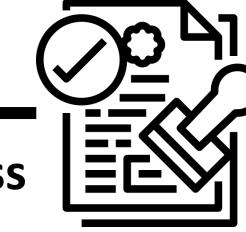
4. Ask if a victim
or accomplice



OR



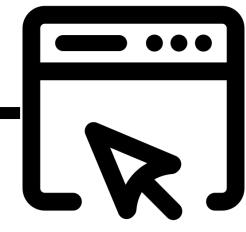
5. Request to verify
official docs for investigation



8. Encourage access to a
specific IP address



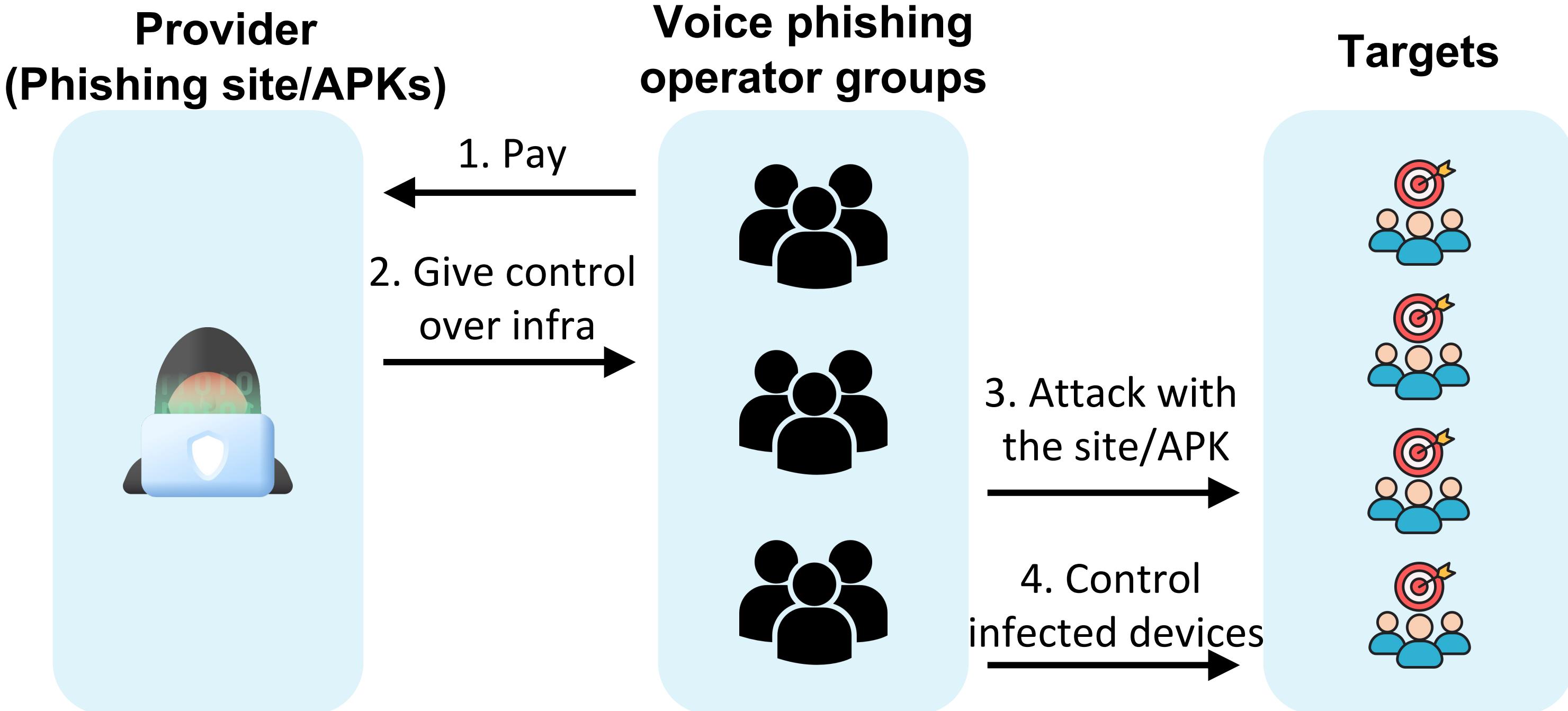
7. Mention about the
embargo



6. Request to access
a portal site

3. Attack infrastructure provided as SaaS

3. Infrastructure



3. Infrastructure

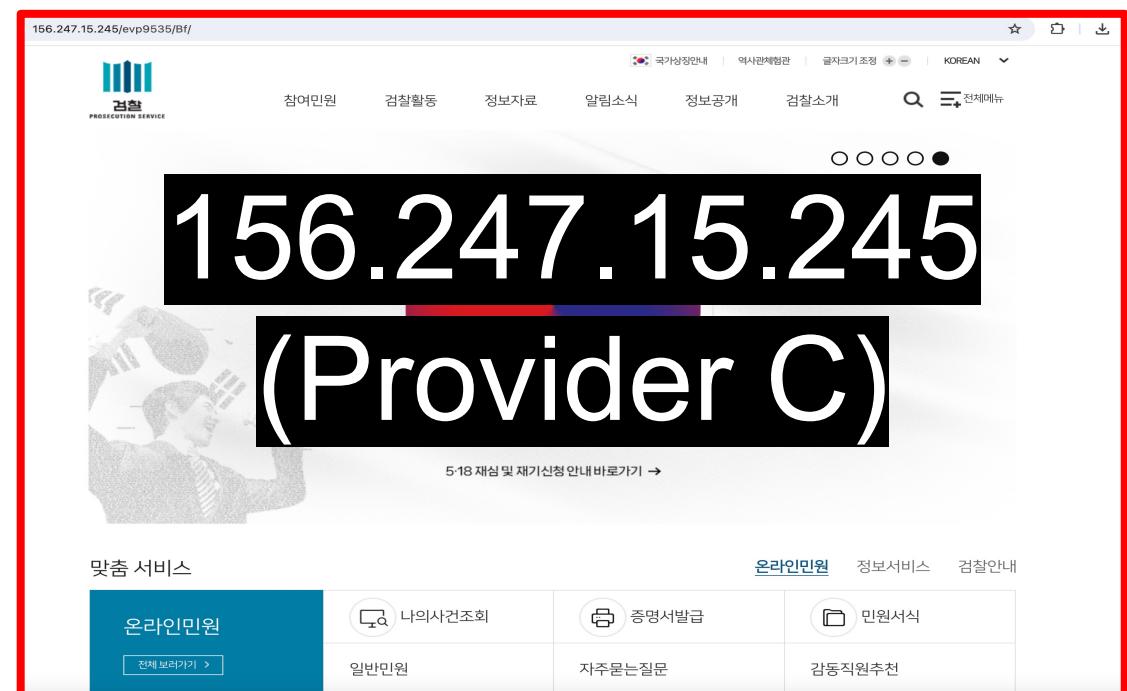
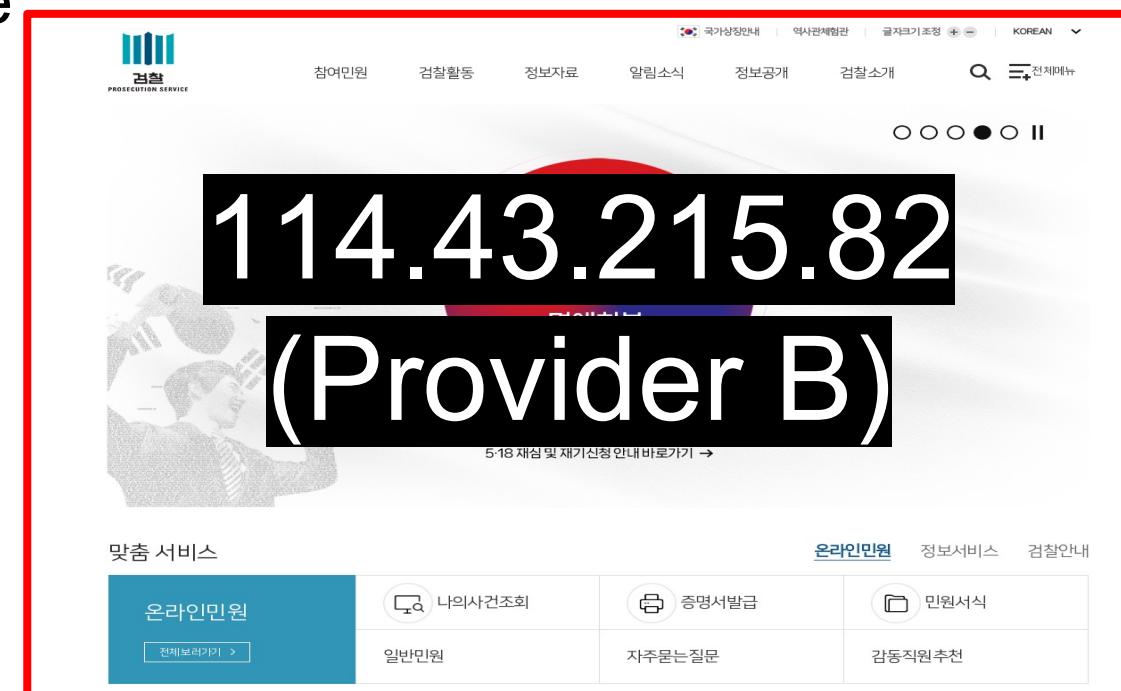
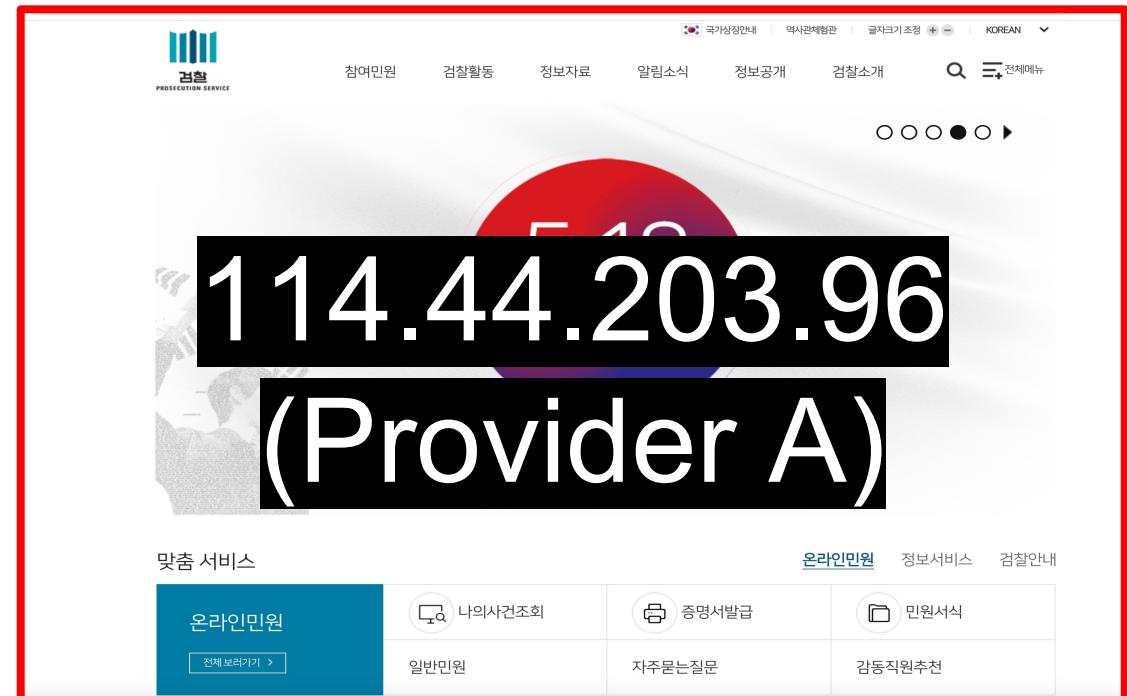
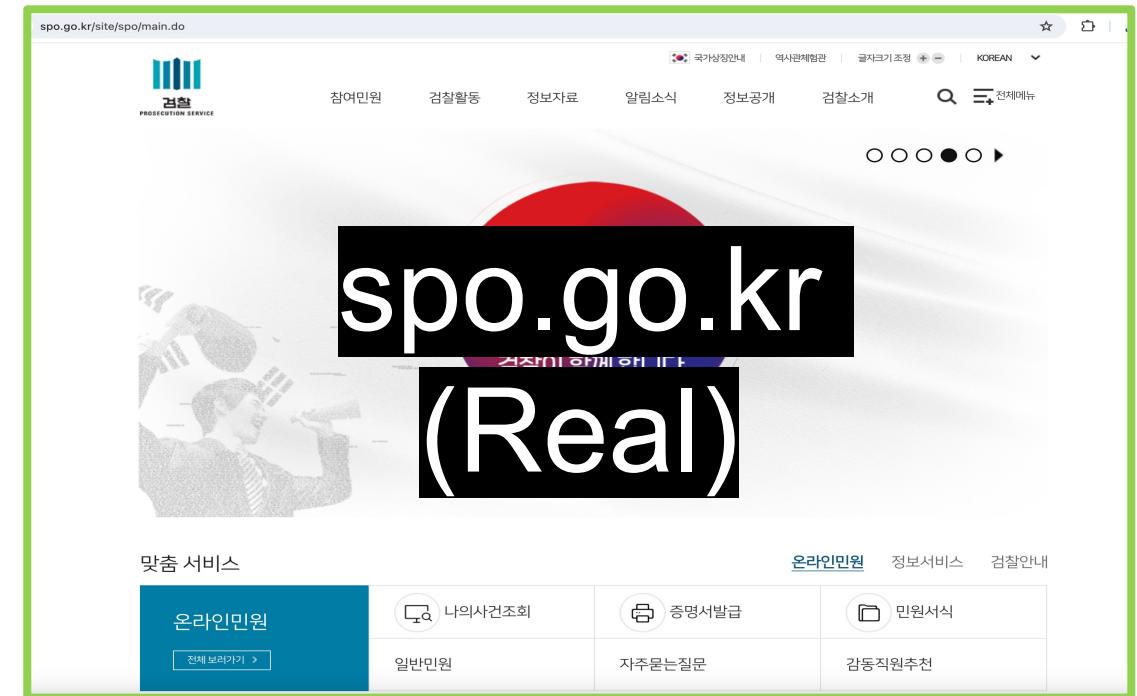
- **Disguised as Supreme Prosecutor's Office website**

- Built completely identical sites

- 3 providers supports this theme

- Redirects to fake page for querying incidents

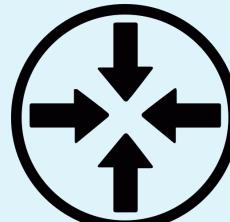
- Scenario:
Impersonation / Impersonation
(Case 2)



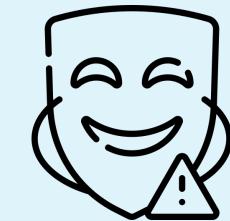
3. Infrastructure



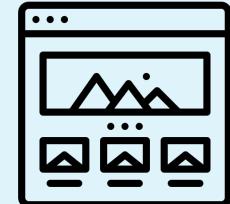
Provider A



AS 3462



(Supreme) (Seoul)
검찰 검찰
PROSECUTORS' OFFICE PROSECUTORS' OFFICE



Official letter, Seizure &
Search & Arrest Warrant



SecretCalls

The screenshot shows the homepage of the Korean Prosecution Service. At the top right, there are language and search options. The main content features a large red circle containing the date '5.10'. Below it, a large black rectangle displays the IP address '111.44.203.96' and the text '(Provider A)' in white. To the left of the IP address is a grayscale profile picture of a person. At the bottom, there are several navigation links and service icons.

국가상장안내 역사관체험관 글자크기 조정 KOREAN

검찰

참여민원 검찰활동 정보자료 알림소식 정보공개 검찰소개

00000

5.10
111.44.203.96
(Provider A)

5·18 재심 및 재기신청안내 바로가기 →

맞춤 서비스

온라인민원 나의사건조회 증명서발급 민원서식

온라인민원 전체보러가기 >

나의사건조회

증명서발급

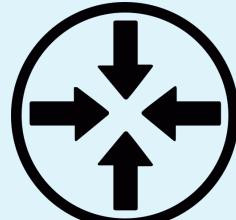
민원서식

일반민원 자주묻는질문 감동직원추천

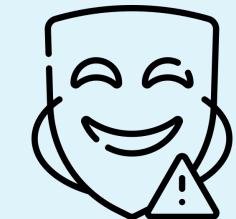
3. Infrastructure



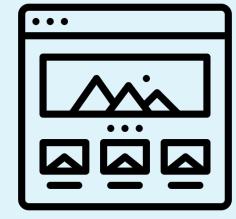
Provider B



AS 3462



(South)
검찰
PROSECUTORS' OFFICE



Official letter, Bank Statement,
Non-Disclosure Agreement,
Arrest Warrant



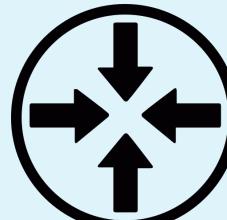
SyncCalls

The screenshot shows the official website of the South Korean Prosecution Service. At the top right, there are language and search options. The main content features a large red circular graphic with the number '518' and a large black rectangle containing the IP address '114.43.215.82' and the text '(Provider B)'. Below this, there is a stylized illustration of two people shaking hands. A link '5·18 재심 및 재기신청안내 바로가기' is visible. At the bottom, there is a navigation bar with tabs for '온라인민원' (Online Citizen Services), '정보서비스' (Information Services), and '검찰안내' (Prosecution Guide). There are also links for '맞춤 서비스' (Customized Services) and various service icons.

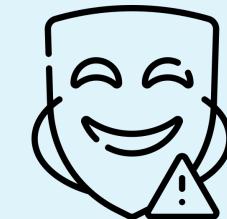
3. Infrastructure



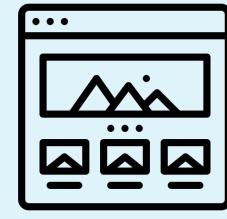
Provider C



AS 133199



(Supreme)
검찰
PROSECUTORS' OFFICE



Official letter, Arrest Warrant,
Bank Statement



MalCalls

156.247.15.245/evp9535/Bf/

국가상징안내 | 역사관체험관 | 글자크기 조정 + - | KOREAN

검찰
PROSECUTION SERVICE

참여민원 검찰활동 정보자료 알림소식 정보공개 검찰소개

전체메뉴

0 0 0 0 ●

156.247.15.245
(Provider C)

5·18 재심 및 재기신청 안내 바로가기 →

맞춤 서비스

온라인민원 나의사건조회 증명서발급 민원서식

전체보러가기 > 일반민원 자주묻는질문 감동직원추천

온라인민원 정보서비스 검찰안내

3. Infrastructure

(Provider A)

(Provider B)

(Provider C)

"피의자는 목비권을 행사할 수 있다." 피의자의 모든 발언은 법정에서 불리하게 적용할 수 있다. " 피의자는 변호인을 선임할 권리가 있다.

No 010567

중요 문서 무단 반출 시 법적 제재를 받을 수 있으며, 모든 출력본은 모니터링 됩니다.



검찰
PROSECUTION SERVICE

서울남부지방검찰청

(Supreme Prosecutors Office)



조사대상 :(-)

접수일자 : 2024년 03월 02일

사건번호 : 2023고합3047호

보안급수 : 특급

경찰비밀번호 : 0111

Case number, Target's name, Severity, Date, Registrant,

Former Official Prosecutor

General's seal

기 안 자: 황홍철 (인)

행정사무장: 김병현 (인)

서장: Wonseok

[주관기관: 서울남부지방검찰청 금융범죄조사부] [관계기관: 금융감독원 (금융위원회)]

COPYRIGHT (c) 2019 SUPREME PROSECUTORS' OFFICE. ALL RIGHTS RESERVED

 법무부 PROSECUTION SERVICE	사건번호: 2023조사 7403호	
접수인 : [REDACTED] 접수일자 : 2023년 06월 10일 사건번호 : 2023 조 사 7403호 금수 : 특급 부록 : 아래와같음		
형사 제 1부 검찰 법무관 : 박석삼 268		
<p>요지 : 단속접수자 윤인지 (980102-2352621) 2023 조 사 7403 특급 사건 김**등 전자금융거래법 위반 및 자금 세탁, 불법 명의도용 사건. 개인명의도용 침해신고 접수를 받음과 동시에 계좌양도 및 가해혐의거나 개인명의도용 피해자라는 것을 본인 스스로 해명해야함.</p> <p>1. 행정법규절차 14조 2항에 근거하여, 서울 중앙지검 수사과에서 행정집행사건을 담당, 단속접수자를 통보하여 반드시 본인의 계좌자금상증명 재산상황 혹은 기타 필요한 진술을 우선 해야함을 알려드립니다.</p> <p>2. 본 사건은 2021년 금융침행 (100001호~100286호) 단속접수자 관련 돈세탁방지법 사건, 단속접수자는 요지에 기록된 시간에 모든 재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득) 및 재산상황을 합법적인 재산임을 증명, 감독 받아야함.</p> <p>3. 금융법 39조 3항에 따라 합법절차에 따라 본인은 계좌추적조회를 통해서 금융실명제의 원칙에 따라서 본인 명의의 모든 합법적인 계좌에 대해 인적사항 자산이거나 모든 부당한 거래내역을 조회를 하여 투명성을 입증시켜야함.</p> <p>4. 단속접수자는 집행명령이 발표된 시간(여상)내에, 만일 본 사건의 조사, 집행내용을 제3자한테 전하였을 경우 (제3자 포함), 본처 및 관계기관(금융감독원)에서는 금융법 39조 17항 따라서 즉시 본인명의로된 재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득)를 동결처리하는 것입니다. 단속보호자는 다른 반대의견이 있어서는 안됩니다.</p> <p>5. 단속접수자는 수사진행과 동시에 휴대기기 검열조치를 의무적으로 시행 해야함. 시행 주요사항</p> <ol style="list-style-type: none"> 1. 사이버수사대 주관하에 검열을 진행할 것. 2. 개인정보 유출 확산방지 3. 범인도피 및 은닉 또는 증거인멸, 증거은닉에 대한 우려 등 4. 수사협조 기간내 조사자 신변보호에 관련한 이동경로 및 화면녹화 등 5. 수사협조 진행과 동시에 수사협조 관련 지출내역 발생시 수사협조 비용 지급 됨. 		
<div style="text-align: center; border: 2px solid red; padding: 10px; background-color: #ffffcc;">  </div> <div style="display: flex; justify-content: space-between; align-items: center;"> 대 검찰총장 검수증 기안자: <u>정난희</u> 과장: <u>김종만</u> 기증인: <u>이원석</u> </div> <div style="text-align: center; margin-top: 10px;"> 대 검찰청 총장 이원석 </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;"> 기안자 : 정난희 (인) <u>정 난 희</u> 사건과장 : 박종만 (인) <u>박 종 만</u> 검찰조사관 : 김재규 (인) <u>김 재 규</u> </div> <div style="text-align: center; margin-top: 10px;">  </div>		

3. Infrastructure

(Provider A)

P12_001A1		위변조 방지를 바코드입니다.	[집행부호] - 7794
			[구속영장번호]
대한민국 법원 Court of the Republic of Korea (압수수색 · 구속영장 허가서)			
집행대상	사건	전자금융사기, 전기통신금융사기 및 환급에 관한 금융범죄 사건사건	
	성명	[Redacted]	주민등록번호
금융계좌추적 및 압수수색 · 구속영장의 발부의 허가 사유			
<p>전자금융거래법 제 10 조(분실과도난책임 동부지법 2014.12.29 개정)에 근거 비록 집행대상자가 개인정보 분실과 도난으로 인하여 범죄행위에 적극적으로 가담하지 않았더라도 피고가 개인정보의 관리를 소홀히 하였다라는 점을 감안하여 사기를 방조했다고 할 것이므로, 민법 제 760 조 3 항에 따라 공동 불법행위자로써 그 손해를 배상할 책임이 있다고 인정하는 바 조사명령서 접행을 허가하였음을 알려드립니다.</p> <p>위의 집행대상에 대한 전기통신금융사기 및 환급에 관한 특별법 위반 건에 관하여 2022 형제 1357 호 사건에 관해 해외도피 및 증거인멸 요지가 있으므로, 해외출금금지 및 긴급체포명령 허가서가 발부되어 있음을 공지합니다.</p>			
〈공소사실의요지〉			
공무상 보안 누설죄 적용대상 (직계가족 포함.)			
수색, 검증 장소 신체, 물건	모든 재산 자료 (토지 , 주택 , 예금 , 적금 , 입출금 , 현금 및 기타 소득 · *가액수색*, *근무처*, *주변인물*, 입수·수색·검증 및 소환조사)		
적용 법령	전자금융거래법 제 49 조(범칙), 형법 제 309 조 제 2 항, 제 309 조 제 1 항, 제 307 조 제 2 항, 제 37 조, 제 38 조, 형법 제 70 조, 제 69 조 제 2 항 형사소송법 제 334 조 제 1 항, 민사소송법 제 741 조, 제 740 조 제 3 항		
인치구금할장소	서울동부구치소	인치구금기간	최초 48시간(연장 14일)
법원주사보	김철기	대법관인	박상우
조사담당검사	김현우 (인)	재판장판사	이수영 (인)
집행불능사유	•없음• 무혐의자 확정 전까지 위와 같이 처리하겠습니다.		
2024년 03월 03일			
법원행정처장 차한 			

(Provider B)

Arrest Warrant for Financial Crimes

Issued by a Korean Court with Target's Name & Registration number

Fake account number, Detention Center & Period

(Provider C)

NO 010567

 검찰
ADVISORY JUSTICE SERVICE REPUBLIC OF KOREA
법무부

서울지방법원 구속영장

352621
번호 : 2023형제 9821
사건번호 : 2023 조 사 7403호
사건명 : 전자금융거래법 위반 및 불법자금은닉, 전자금융거래법 위반

352621) 은 성매매 특별법, 불법자금은닉, 전자금융거래법 위반으로 자산이 불투명화되는 경우에 사용되는 계좌 (우리은행 1002-200-59****8)

위 내용을 인정하는 바 피고인의 모든 금융자산을 압수 함. 위 내용과 범죄사실이 일치하므로 구속조사를 명한다.

위 사건에 관하여 피고인을 구속한다.

조사자:

인치구금할 장소: 서울구치소

이 영장은 2024년 3월 10일까지 유효하다. 이 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다. 위와 같이 처리함

2024년 2월 25일

대검찰청 특수부

[처음으로](#) [다음으로](#)

3. Infrastructure

(Provider B)

Transaction History Inquiry Form

(Provider C)

거래내역 조회표							거래내역 조회표																																																																																																																																																																																																																																																																																																																																																																																																																
(조회일시 : 2023.11.08 15:32:27)							(조회일시 : 2023.06.14 15:27)																																																																																																																																																																																																																																																																																																																																																																																																																
계좌번호 : 우리은행 1002-200-599*** (지급정지) 조회기간 : 2022.02.09 ~ 2023.8.17							계좌번호 : 1002-200-59***8 (지급정지) 조회기간 : 2022. 02. 14 ~ 2023. 06. 14																																																																																																																																																																																																																																																																																																																																																																																																																
담당자 : 이은미 (인)							담당자 : 이은미 (인)																																																																																																																																																																																																																																																																																																																																																																																																																
<table border="1"> <thead> <tr> <th>거래일자</th> <th>상태</th> <th>거래구분</th> <th>거래금액</th> <th>표면잔액</th> <th>취급점</th> <th>입금의뢰인</th> <th>거래일자</th> <th>상태</th> <th>거래구분</th> <th>거래금액</th> <th>표면잔액</th> <th>취급점</th> <th>입금의뢰인</th> <th>거래시간</th> </tr> </thead> <tbody> <tr><td>20230502</td><td>입금</td><td>인터넷입금</td><td>150,000</td><td>150,000</td><td>2576</td><td>김도현</td><td></td><td></td><td></td><td>10,000</td><td>10,000</td><td>2576</td><td>김도현</td><td>165921</td></tr> <tr><td>20230502</td><td>출금</td><td>인터넷출금</td><td>150,000</td><td>0</td><td>201710</td><td>오종진</td><td></td><td></td><td></td><td>9,500</td><td>0</td><td>201710</td><td>오종진</td><td>200705</td></tr> <tr><td>20230504</td><td>입금</td><td>인터넷입금</td><td>2,300,000</td><td>2,300,000</td><td>3937</td><td>오미경</td><td></td><td></td><td></td><td>120,000</td><td>120,000</td><td>3937</td><td>오미경</td><td>110648</td></tr> <tr><td>20230504</td><td>출금</td><td>인터넷출금</td><td>2,300,000</td><td>0</td><td>1184</td><td>김종호</td><td></td><td></td><td></td><td>120,000</td><td>120,000</td><td>3937</td><td>농협 김종호</td><td>112238</td></tr> <tr><td>20230505</td><td>입금</td><td>인터넷입금</td><td>4,650,000</td><td>4,650,000</td><td>2576</td><td>20590880254</td><td></td><td></td><td></td><td>700,000</td><td>734,500</td><td>2576</td><td>20590880254</td><td>173404</td></tr> <tr><td>20230505</td><td>입금</td><td>인터넷입금</td><td>3,400,000</td><td>8,050,000</td><td>2576</td><td>20590880254</td><td></td><td></td><td></td><td>900,000</td><td>1,634,500</td><td>2576</td><td>20590880254</td><td>173911</td></tr> <tr><td>20230505</td><td>입금</td><td>인터넷입금</td><td>7,800,000</td><td>15,850,000</td><td>2576</td><td>20590880254</td><td></td><td></td><td></td><td>400,000</td><td>2,034,500</td><td>2576</td><td>20590880254</td><td>174627</td></tr> <tr><td>20230505</td><td>출금</td><td>인터넷출금</td><td>15,850,000</td><td>0</td><td>209600</td><td>김종호</td><td></td><td></td><td></td><td>2,000,000</td><td>34,000</td><td>209600</td><td>농협 김종호</td><td>105910</td></tr> <tr><td>20230507</td><td>입금</td><td>인터넷입금</td><td>23,000,000</td><td>23,000,000</td><td>263009</td><td>전재정</td><td></td><td></td><td></td><td>1,200,000</td><td>1,233,300</td><td>263009</td><td>제일 전재정</td><td>001415</td></tr> <tr><td>20230507</td><td>입금</td><td>인터넷입금</td><td>37,000,000</td><td>60,000,000</td><td>263009</td><td>전재정</td><td></td><td></td><td></td><td>500,000</td><td>1,732,800</td><td>263009</td><td>제일 전재정</td><td>001861</td></tr> <tr><td>20230607</td><td>출금</td><td>인터넷출금</td><td>60,000,000</td><td>0</td><td>030546</td><td>이명순</td><td></td><td></td><td></td><td>1,700,000</td><td>32,100</td><td>030546</td><td>농협 이명순</td><td>001749</td></tr> <tr><td>20230610</td><td>입금</td><td>인터넷입금</td><td>14,500,000</td><td>14,500,000</td><td>3990</td><td>이민호</td><td></td><td></td><td></td><td>3,000,000</td><td>3,031,500</td><td>3990</td><td>우리 이민호</td><td>171205</td></tr> <tr><td>20230610</td><td>출금</td><td>인터넷출금</td><td>14,500,000</td><td>0</td><td>9277</td><td>오미경</td><td></td><td></td><td></td><td>3,000,000</td><td>30,900</td><td>9277</td><td>오미경</td><td>094040</td></tr> <tr><td>20230726</td><td>입금</td><td>인터넷입금</td><td>34,000,000</td><td>34,000,000</td><td>205970</td><td>최태경</td><td></td><td></td><td></td><td>5,900,000</td><td>5,930,100</td><td>205970</td><td>모두 투어(주)</td><td>145222</td></tr> <tr><td>20230726</td><td>출금</td><td>인터넷출금</td><td>12,000,000</td><td>22,000,000</td><td>1754</td><td>20590890159</td><td></td><td></td><td></td><td>CD공동 출금</td><td>950,000</td><td>4,979,600</td><td>1754</td><td>205970890159</td><td>160349</td></tr> <tr><td>20230726</td><td>출금</td><td>인터넷출금</td><td>10,000,000</td><td>12,000,000</td><td>1754</td><td>20590890159</td><td></td><td></td><td></td><td>CD공동 출금</td><td>950,000</td><td>4,029,100</td><td>1754</td><td>205970890159</td><td>16702</td></tr> <tr><td>20230726</td><td>출금</td><td>인터넷출금</td><td>8,000,000</td><td>4,000,000</td><td>1754</td><td>20590890159</td><td></td><td></td><td></td><td>CD공동 출금</td><td>950,000</td><td>3,078,600</td><td>1754</td><td>205970890159</td><td>161859</td></tr> <tr><td>20230726</td><td>출금</td><td>인터넷출금</td><td>2,000,000</td><td>2,000,000</td><td>1754</td><td>20590890159</td><td></td><td></td><td></td><td>CD공동 출금</td><td>950,000</td><td>2,128,100</td><td>1754</td><td>205970890159</td><td>162238</td></tr> <tr><td>20230726</td><td>출금</td><td>인터넷출금</td><td>2,000,000</td><td>0</td><td>9277</td><td>오미경</td><td></td><td></td><td></td><td>인터넷출금</td><td>2,000,000</td><td>127,600</td><td>9277</td><td>오미경</td><td>163324</td></tr> <tr><td>20230812</td><td>입금</td><td>인터넷입금</td><td>56,000,000</td><td>56,000,000</td><td>263000</td><td>109511451</td><td></td><td></td><td></td><td>타행입금</td><td>16,000,000</td><td>16,127,100</td><td>263000</td><td>신한 01095154</td><td>093000</td></tr> <tr><td>20230812</td><td>출금</td><td>인터넷출금</td><td>56,000,000</td><td>0</td><td>1184</td><td>김종호</td><td></td><td></td><td></td><td>인터넷입금</td><td>16,100,000</td><td>25,900</td><td>1184</td><td>농협 김종호</td><td>110908</td></tr> <tr><td>20230827</td><td>입금</td><td>인터넷입금</td><td>12,000,000</td><td>12,000,000</td><td>013903</td><td>배현진</td><td></td><td></td><td></td><td>인터넷입금</td><td>1,500,000</td><td>1,525,200</td><td>013903</td><td>배현진</td><td>185027</td></tr> <tr><td>20230827</td><td>입금</td><td>인터넷입금</td><td>8,000,000</td><td>20,000,000</td><td>008644</td><td>박상준</td><td></td><td></td><td></td><td>인터넷입금</td><td>1,850,000</td><td>3,074,700</td><td>008644</td><td>박상준</td><td>105348</td></tr> <tr><td>20230827</td><td>입금</td><td>인터넷입금</td><td>27,000,000</td><td>47,000,000</td><td>004224</td><td>김정호</td><td></td><td></td><td></td><td>인터넷입금</td><td>270,000</td><td>3,344,200</td><td>004224</td><td>김정호</td><td>185240</td></tr> <tr><td>20230827</td><td>출금</td><td>인터넷출금</td><td>47,000,000</td><td>0</td><td>011090</td><td>KIMJINUO</td><td></td><td></td><td></td><td>인터넷출금</td><td>3,340,000</td><td>3,600</td><td>011090</td><td>KIMJINUO</td><td>201547</td></tr> </tbody> </table>							거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인	거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인	거래시간	20230502	입금	인터넷입금	150,000	150,000	2576	김도현				10,000	10,000	2576	김도현	165921	20230502	출금	인터넷출금	150,000	0	201710	오종진				9,500	0	201710	오종진	200705	20230504	입금	인터넷입금	2,300,000	2,300,000	3937	오미경				120,000	120,000	3937	오미경	110648	20230504	출금	인터넷출금	2,300,000	0	1184	김종호				120,000	120,000	3937	농협 김종호	112238	20230505	입금	인터넷입금	4,650,000	4,650,000	2576	20590880254				700,000	734,500	2576	20590880254	173404	20230505	입금	인터넷입금	3,400,000	8,050,000	2576	20590880254				900,000	1,634,500	2576	20590880254	173911	20230505	입금	인터넷입금	7,800,000	15,850,000	2576	20590880254				400,000	2,034,500	2576	20590880254	174627	20230505	출금	인터넷출금	15,850,000	0	209600	김종호				2,000,000	34,000	209600	농협 김종호	105910	20230507	입금	인터넷입금	23,000,000	23,000,000	263009	전재정				1,200,000	1,233,300	263009	제일 전재정	001415	20230507	입금	인터넷입금	37,000,000	60,000,000	263009	전재정				500,000	1,732,800	263009	제일 전재정	001861	20230607	출금	인터넷출금	60,000,000	0	030546	이명순				1,700,000	32,100	030546	농협 이명순	001749	20230610	입금	인터넷입금	14,500,000	14,500,000	3990	이민호				3,000,000	3,031,500	3990	우리 이민호	171205	20230610	출금	인터넷출금	14,500,000	0	9277	오미경				3,000,000	30,900	9277	오미경	094040	20230726	입금	인터넷입금	34,000,000	34,000,000	205970	최태경				5,900,000	5,930,100	205970	모두 투어(주)	145222	20230726	출금	인터넷출금	12,000,000	22,000,000	1754	20590890159				CD공동 출금	950,000	4,979,600	1754	205970890159	160349	20230726	출금	인터넷출금	10,000,000	12,000,000	1754	20590890159				CD공동 출금	950,000	4,029,100	1754	205970890159	16702	20230726	출금	인터넷출금	8,000,000	4,000,000	1754	20590890159				CD공동 출금	950,000	3,078,600	1754	205970890159	161859	20230726	출금	인터넷출금	2,000,000	2,000,000	1754	20590890159				CD공동 출금	950,000	2,128,100	1754	205970890159	162238	20230726	출금	인터넷출금	2,000,000	0	9277	오미경				인터넷출금	2,000,000	127,600	9277	오미경	163324	20230812	입금	인터넷입금	56,000,000	56,000,000	263000	109511451				타행입금	16,000,000	16,127,100	263000	신한 01095154	093000	20230812	출금	인터넷출금	56,000,000	0	1184	김종호				인터넷입금	16,100,000	25,900	1184	농협 김종호	110908	20230827	입금	인터넷입금	12,000,000	12,000,000	013903	배현진				인터넷입금	1,500,000	1,525,200	013903	배현진	185027	20230827	입금	인터넷입금	8,000,000	20,000,000	008644	박상준				인터넷입금	1,850,000	3,074,700	008644	박상준	105348	20230827	입금	인터넷입금	27,000,000	47,000,000	004224	김정호				인터넷입금	270,000	3,344,200	004224	김정호	185240	20230827	출금	인터넷출금	47,000,000	0	011090	KIMJINUO				인터넷출금	3,340,000	3,600	011090	KIMJINUO	201547
거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인	거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인	거래시간																																																																																																																																																																																																																																																																																																																																																																																																									
20230502	입금	인터넷입금	150,000	150,000	2576	김도현				10,000	10,000	2576	김도현	165921																																																																																																																																																																																																																																																																																																																																																																																																									
20230502	출금	인터넷출금	150,000	0	201710	오종진				9,500	0	201710	오종진	200705																																																																																																																																																																																																																																																																																																																																																																																																									
20230504	입금	인터넷입금	2,300,000	2,300,000	3937	오미경				120,000	120,000	3937	오미경	110648																																																																																																																																																																																																																																																																																																																																																																																																									
20230504	출금	인터넷출금	2,300,000	0	1184	김종호				120,000	120,000	3937	농협 김종호	112238																																																																																																																																																																																																																																																																																																																																																																																																									
20230505	입금	인터넷입금	4,650,000	4,650,000	2576	20590880254				700,000	734,500	2576	20590880254	173404																																																																																																																																																																																																																																																																																																																																																																																																									
20230505	입금	인터넷입금	3,400,000	8,050,000	2576	20590880254				900,000	1,634,500	2576	20590880254	173911																																																																																																																																																																																																																																																																																																																																																																																																									
20230505	입금	인터넷입금	7,800,000	15,850,000	2576	20590880254				400,000	2,034,500	2576	20590880254	174627																																																																																																																																																																																																																																																																																																																																																																																																									
20230505	출금	인터넷출금	15,850,000	0	209600	김종호				2,000,000	34,000	209600	농협 김종호	105910																																																																																																																																																																																																																																																																																																																																																																																																									
20230507	입금	인터넷입금	23,000,000	23,000,000	263009	전재정				1,200,000	1,233,300	263009	제일 전재정	001415																																																																																																																																																																																																																																																																																																																																																																																																									
20230507	입금	인터넷입금	37,000,000	60,000,000	263009	전재정				500,000	1,732,800	263009	제일 전재정	001861																																																																																																																																																																																																																																																																																																																																																																																																									
20230607	출금	인터넷출금	60,000,000	0	030546	이명순				1,700,000	32,100	030546	농협 이명순	001749																																																																																																																																																																																																																																																																																																																																																																																																									
20230610	입금	인터넷입금	14,500,000	14,500,000	3990	이민호				3,000,000	3,031,500	3990	우리 이민호	171205																																																																																																																																																																																																																																																																																																																																																																																																									
20230610	출금	인터넷출금	14,500,000	0	9277	오미경				3,000,000	30,900	9277	오미경	094040																																																																																																																																																																																																																																																																																																																																																																																																									
20230726	입금	인터넷입금	34,000,000	34,000,000	205970	최태경				5,900,000	5,930,100	205970	모두 투어(주)	145222																																																																																																																																																																																																																																																																																																																																																																																																									
20230726	출금	인터넷출금	12,000,000	22,000,000	1754	20590890159				CD공동 출금	950,000	4,979,600	1754	205970890159	160349																																																																																																																																																																																																																																																																																																																																																																																																								
20230726	출금	인터넷출금	10,000,000	12,000,000	1754	20590890159				CD공동 출금	950,000	4,029,100	1754	205970890159	16702																																																																																																																																																																																																																																																																																																																																																																																																								
20230726	출금	인터넷출금	8,000,000	4,000,000	1754	20590890159				CD공동 출금	950,000	3,078,600	1754	205970890159	161859																																																																																																																																																																																																																																																																																																																																																																																																								
20230726	출금	인터넷출금	2,000,000	2,000,000	1754	20590890159				CD공동 출금	950,000	2,128,100	1754	205970890159	162238																																																																																																																																																																																																																																																																																																																																																																																																								
20230726	출금	인터넷출금	2,000,000	0	9277	오미경				인터넷출금	2,000,000	127,600	9277	오미경	163324																																																																																																																																																																																																																																																																																																																																																																																																								
20230812	입금	인터넷입금	56,000,000	56,000,000	263000	109511451				타행입금	16,000,000	16,127,100	263000	신한 01095154	093000																																																																																																																																																																																																																																																																																																																																																																																																								
20230812	출금	인터넷출금	56,000,000	0	1184	김종호				인터넷입금	16,100,000	25,900	1184	농협 김종호	110908																																																																																																																																																																																																																																																																																																																																																																																																								
20230827	입금	인터넷입금	12,000,000	12,000,000	013903	배현진				인터넷입금	1,500,000	1,525,200	013903	배현진	185027																																																																																																																																																																																																																																																																																																																																																																																																								
20230827	입금	인터넷입금	8,000,000	20,000,000	008644	박상준				인터넷입금	1,850,000	3,074,700	008644	박상준	105348																																																																																																																																																																																																																																																																																																																																																																																																								
20230827	입금	인터넷입금	27,000,000	47,000,000	004224	김정호				인터넷입금	270,000	3,344,200	004224	김정호	185240																																																																																																																																																																																																																																																																																																																																																																																																								
20230827	출금	인터넷출금	47,000,000	0	011090	KIMJINUO				인터넷출금	3,340,000	3,600	011090	KIMJINUO	201547																																																																																																																																																																																																																																																																																																																																																																																																								

Inspector, Verifier, Recipient

3. Infrastructure

(Provider B)

Non-Disclosure Agreement

검찰
PROSECUTION SERVICE

비밀유지서약서

사건번호	2023고합3047호
작성일자	2024년 03월 02일

아래와 같이 비밀유지 서약서를 제출합니다.

이현석	박준만	박석삼	김정규
김철총장	시건과장	법무관	조사관

• 서약대상 : -
상기 본인은 서울남부지방검찰청에서 조사받음에 있어 아래의 사항을 준수할 것을 서약합니다.

- 서울남부지방검찰청에서 조사받은 사실과 사건 공문, 구속영장, 증거자료 등 수사 규정에 준하는 사항들에 대하여 허락 없이 공개 또는 누설하지 않을 것을 서약합니다.
- 본인이 알거나 지시받은 내용 진행 상황을 사건 담당자의 승낙 없이 부정하게 반출하지 않을 것을 서약합니다.
- 조사가 끝난 직후에도 3개월간 사건 내용을 이용하여 유출하거나 범인의 도주, 증거 인멸, 사건 유포 제3자를 위하여 사용하지 않을 것을 임명장을 서약합니다.
- 만일 본인이 상기 3개 항을 위반할 시에는 공무상 비밀 유지 조항에 관한 법규에 의거 엄중 처벌될 것을 인지하고 서약합니다.

단속접수자 귀하

대검찰청 총장 이원석
Lee Wonseok

기 안 자: 황충철 (인)
행정사무장: 김병현 (인)

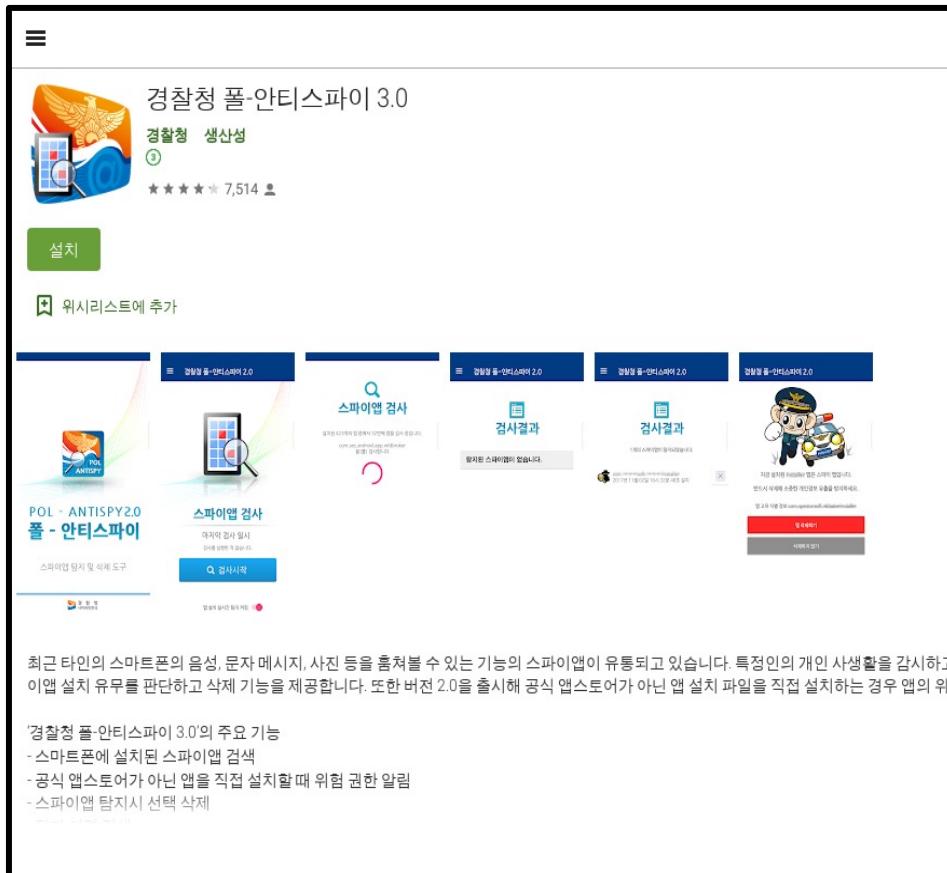
【 주관기관 : 서울남부지방검찰청 금융범죄조사부】 【 관계기관 : 금융감독원 (금융위원회) 】
COPYRIGHT (c) 2019 SUPREME PROSECUTORS' OFFICE. ALL RIGHTS RESERVED

처음으로 다음으로

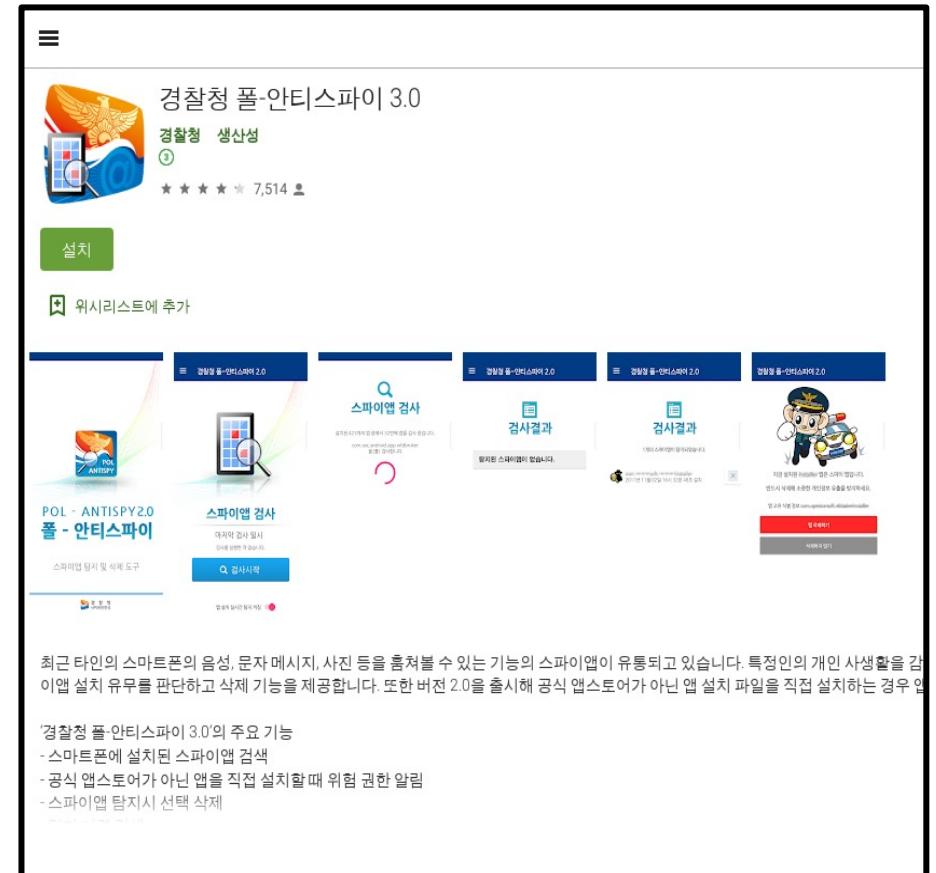
Attorney General, Case Director,
Legal Officer, Investigator's seal

3. Infrastructure – Pole-AntiSpy

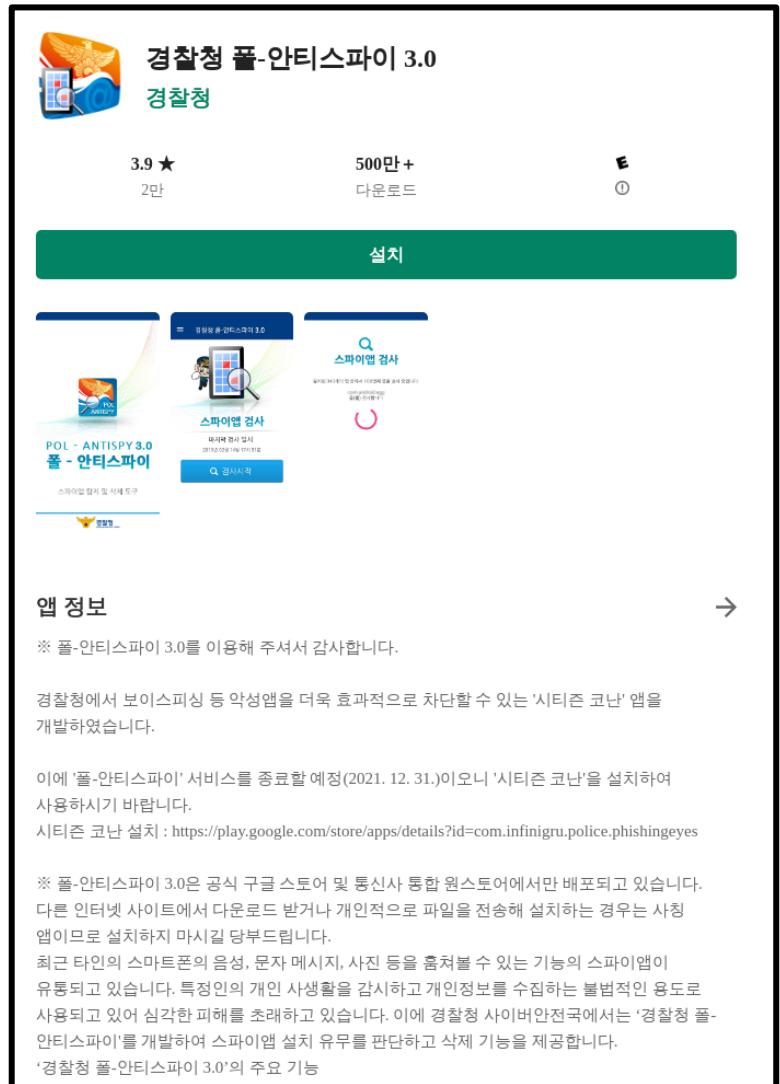
SecretCalls (Provider A)



MalCalls (Provider C)



SyncCalls (Provider B)



3. Infrastructure – Provider A

114.44.203.60 (FAKE)

play.google.com (REAL)

The screenshot shows a fake Google Play Store page for the app '경찰청 사이버캅'. The URL in the address bar is highlighted with a red box and shows '114.44.203.60'. The page content is identical to the real version but is served from a different IP address.

App Details:

- Rating: 3.6★
- Reviews: 3.15천 개
- Downloads: 50만+
- Age Rating: 3세 이상

Buttons:

- 설치 (Install)
- Play 스토어 앱에서 보기 (View on Play Store App)
- 공유 (Share)
- 위시리스트에 추가 (Add to Wish List)

App Screenshots: A red box highlights the first four screenshots, which show various interfaces of the app, including a home screen with a logo and a search interface.

App Information:

경찰청 사이버캅의 주요 기능:

- 악성 발신자, 스팸, 보이스피싱 등 위험 전화번호 확인
- 발신자 전화번호를 경찰청이 확보한 위험 전화번호와 대조하여 인터넷 사기 범죄에 이용된 번호인지 화면에 표출
- 인터넷으로 물품을 거래 할 때, 판매자의 계좌번호나 전화번호가 최근 3개월 동안 3회 이상 경찰에 인터넷...

업데이트 날짜: 2022. 6. 2.

라이프스타일 (LifeStyle) button.

The screenshot shows the real Google Play Store page for the app '경찰청 사이버캅'. The URL in the address bar is highlighted with a red box and shows 'play.google.com'. The page content is identical to the fake version but is served from the official Google Play Store.

App Details:

- Rating: 3.6★
- Reviews: 3.15천 개
- Downloads: 50만+
- Age Rating: 3세 이상

Buttons:

- 설치 (Install)
- 공유 (Share)
- 위시리스트에 추가 (Add to Wish List)

App Screenshots: A red box highlights the first five screenshots, which show various interfaces of the app, including a home screen with a logo and a search interface.

App Information:

경찰청 사이버캅의 주요 기능:

- 경찰청 사이버캅의 주요 기능
- 악성 발신자, 스팸, 보이스피싱 등 위험 전화번호 확인
- 발신자 전화번호를 경찰청이 확보한 위험 전화번호와 대조하여 인터넷 사기 범죄에 이용된 번호인지 화면에 표출
- 인터넷으로 물품을 거래 할 때, 판매자의 계좌번호나 전화번호가 최근 3개월 동안 3회 이상 경찰에 인터넷...

업데이트 날짜: 2022. 6. 2.

3. Infrastructure – Provider A

114.44.203.238 (FAKE)

피싱아이즈(라이트)
Infinigru Corporation

4.3★ 50만+ 3세 이상

설치 Play 스토어 앱에서 보기 공유 위시리스트에 추가

App 지원

Infinigru Corporation의 앱 더보기 →

- 교통민원24(이파인) Infinigru Corporation 2.4★
- 스마트국민제보 Infinigru Corporation 1.5★
- 안전Dream - 아동·여성·장애인경찰지원센터 Infinigru Corporation 3.3★
- 경찰 로스트112 Infinigru Corporation 2.9★
- 경찰 민원 모바일 Infinigru Corporation 1.5★
- 풀케어(PolCare2) Infinigru Corporation

앱 정보 →

- '피싱아이즈(라이트)' 의 주요 기능
 - 악성 발신자, 스팸, 보이스피싱 등 위험 전화번호 확인
 - 발신자 전화번호를 Infinigru Corporation이 확보한 위험 전화번호와 대조하여 인터넷 사기 범죄에 이용된 번호인지 확인
 - 인터넷으로 물품을 거래 할 때, 판매자의 계좌번호나 전화번호가 최근 3개월 동안 3회 이상 경찰에 인터넷...

업데이트 날짜
2022. 6. 2.

라이프스타일

play.google.com (REAL)

피싱아이즈 - 보이스피싱, 피싱차단, 스미싱, 시티즌코난
(주)인피니그루

3.5★ 100K+ 3+ Rated for 3+ Ⓜ

Install Share Add to wishlist

App support

- Website
- Phone number +82234534620
- Support email phishingeyes@gmail.com
- Privacy Policy

Similar apps →

- VIVA INNOVATION 4.7★
- V3 Mobile Security Anti-Virus AhnLab Inc. 4.6★
- NH은행 NH농협은행 4.1★

About this app →

피싱아이즈는 경찰청 및 제작된 금융사와 다양한 유형의 피싱에 대해 실시간으로 공동 대응함으로써, 피싱범의 4대 혐오 행위(악성 앱, 육체제어 앱, 문자, 카카오톡)와 5대 갈등 채널(APP, WEB, ARS, ATM, 청구)로부터 보이스피싱을 예방하는 국내 유일의 "보이스피싱 민관 공동 대응망 서비스"입니다.

피싱아이즈는 경찰대학 치안정책 연구소와 함께 운영하는 시티즌코난(=피싱아이즈 폴리스)과 함께 운영됩니다.

Updated on Jan 25, 2024

Tools

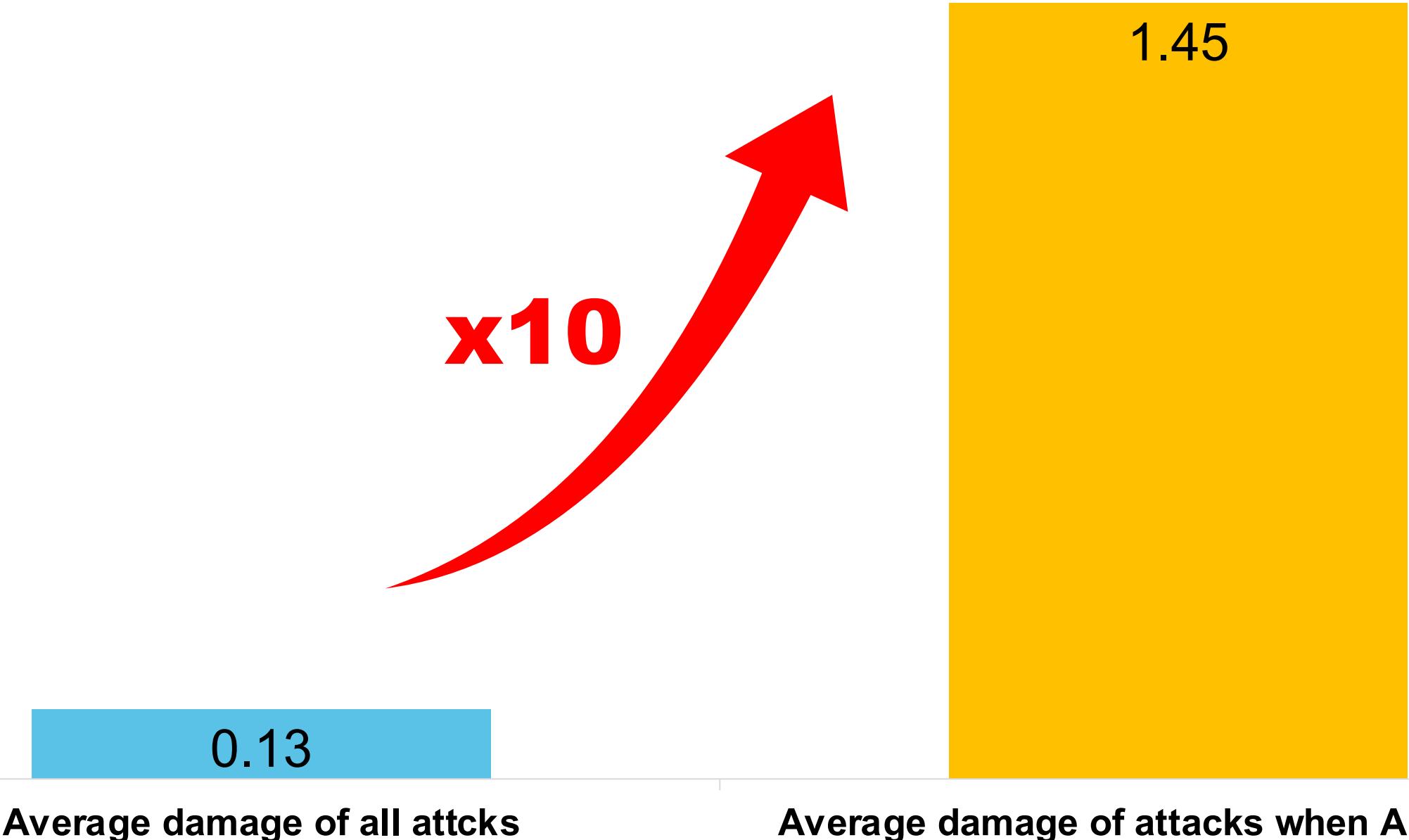
4. SecretCalls

4. SecretCalls

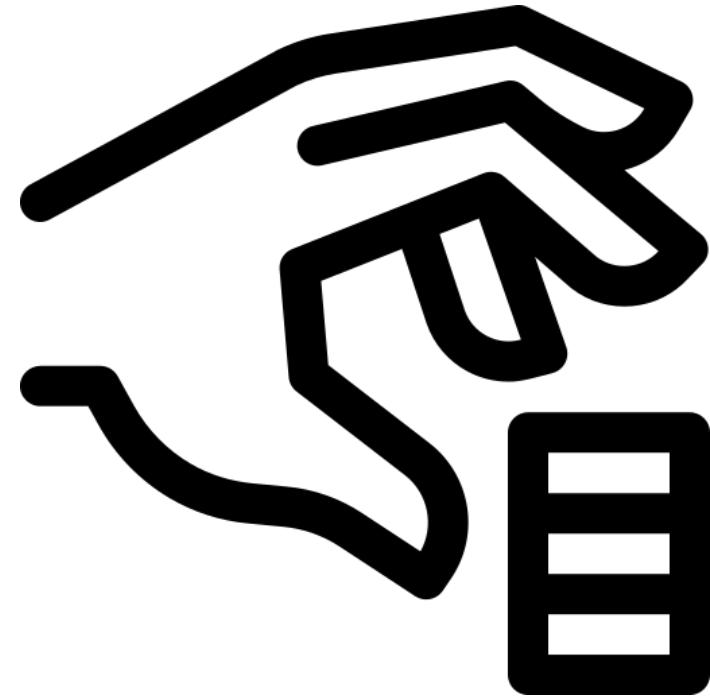
2019 Average damage per attack

(Unit: 100M KRW, (= 75K USD))

Source: Board of Audit and Inspection of Korea



4. SecretCalls – Common VP Actions



**Data theft
(photos, privacy)**

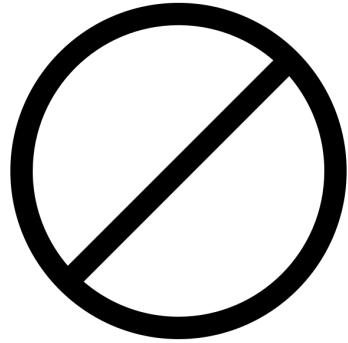


Surveillance



Call redirect

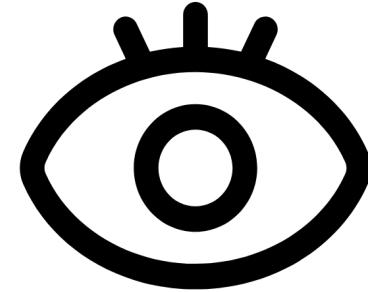
4. SecretCalls – Overview



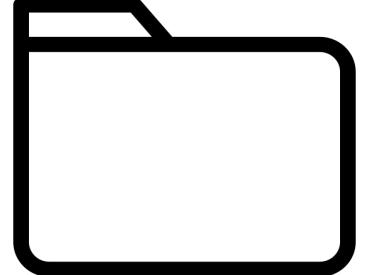
Anti
Decompile



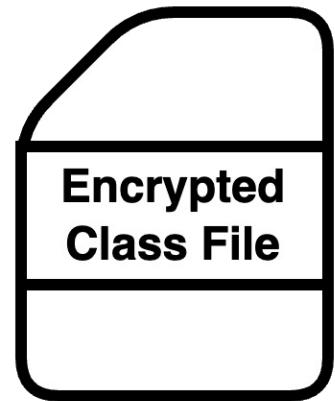
Call
Forwarding



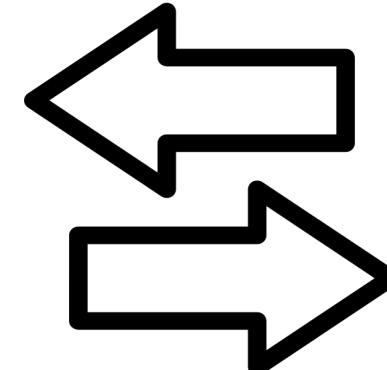
Surveillance



File
Structure



Encrypted
Class File



Network
Behavior



Reddit
Profile



C&C
with FCM

4. SecretCalls – Overview VP groups

Num	Family	Disguised as	DEX filename	Library(.SO) filename	DEX Decryption Method	C&C address location	C&C Endpoint OR Query
1	SecretCalls	Police, Anti-virus, Banking	secret-classes[Num].dex kill-classes[Num].dex black-classes[Num].dex	libdn_ssl.so libbbbed.so libset.so	AES-128-ECB	Hardcoded in DEX, Hardcoded in Lib, Get from Reddit	- postVal={data} - a{timestamp}={data}
2	MalCalls	Banking, Police, Anti-virus, Agency, E-commerce	obfdex[Num].dex obk[Num].dex	libbaiduprotec t_sec_jni.so	AES-256-ECB	Google Drive	- /api/user/ping_server - /api/user/get_extra_message -/api/user/get_limit_phone_number
3	SyncCalls	Police, Prosecutor's office	sclasses.dex yclasses.dex	libdex1.so libdevaxfo.so	AES-128-ECB	Hardcoded in DEX	- /spy/Sync?imei= - /spy/SyncConfig?imei=
4	RcCalls	Banking	classes1.dex	libopenssl.so	AES-128-ECB	Hardcoded in DEX	- {WebSocket}
5	KKvoice	Banking, Anti-virus	lpt[Num].obfdex	-	Base64+XOR	Hardcoded in DEX	- /api/[random]/signal/[random] - {WebSocket}

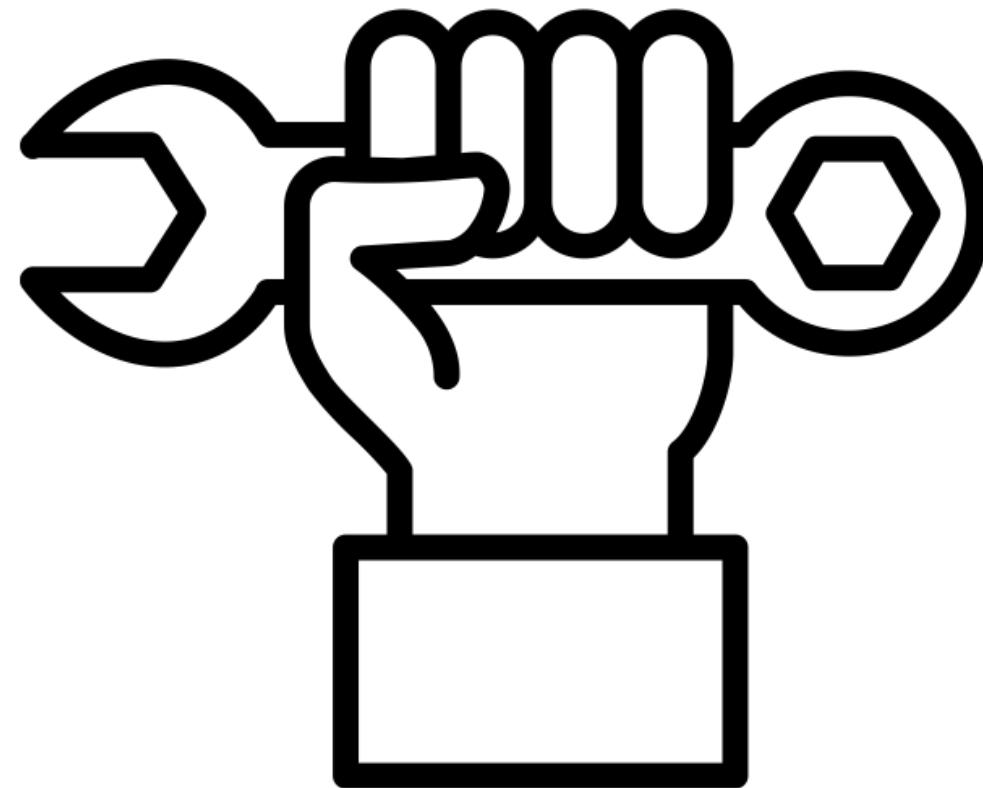
4. SecretCalls – Anti decompile

record[0]	droidManifest.xml	0h	BBCh	struct ZIPFILE...
> frSignature[4]	PK	0h	4h	char
frVersion	20	4h	2h	ushort
0	0	6h	2h	ushort
frCompression	17185	8h	8(Deflate)	enum COMPTYPE...
frFileTime	10:03:54	Ah	2h	DOSTIME
frFileDialog	07/04/2048	Ch	07/04/2024	DOSDATE
frCompressedSize	B8BE7ADh	Eh	4h	uint
frUncompressedSize	827850752	12h	4h	uint
frFileNameLength	1245184	16h	4h	uint
frExtraFieldLength	0	1Ah	2h	ushort
	28225	1Ch	2h	ushort

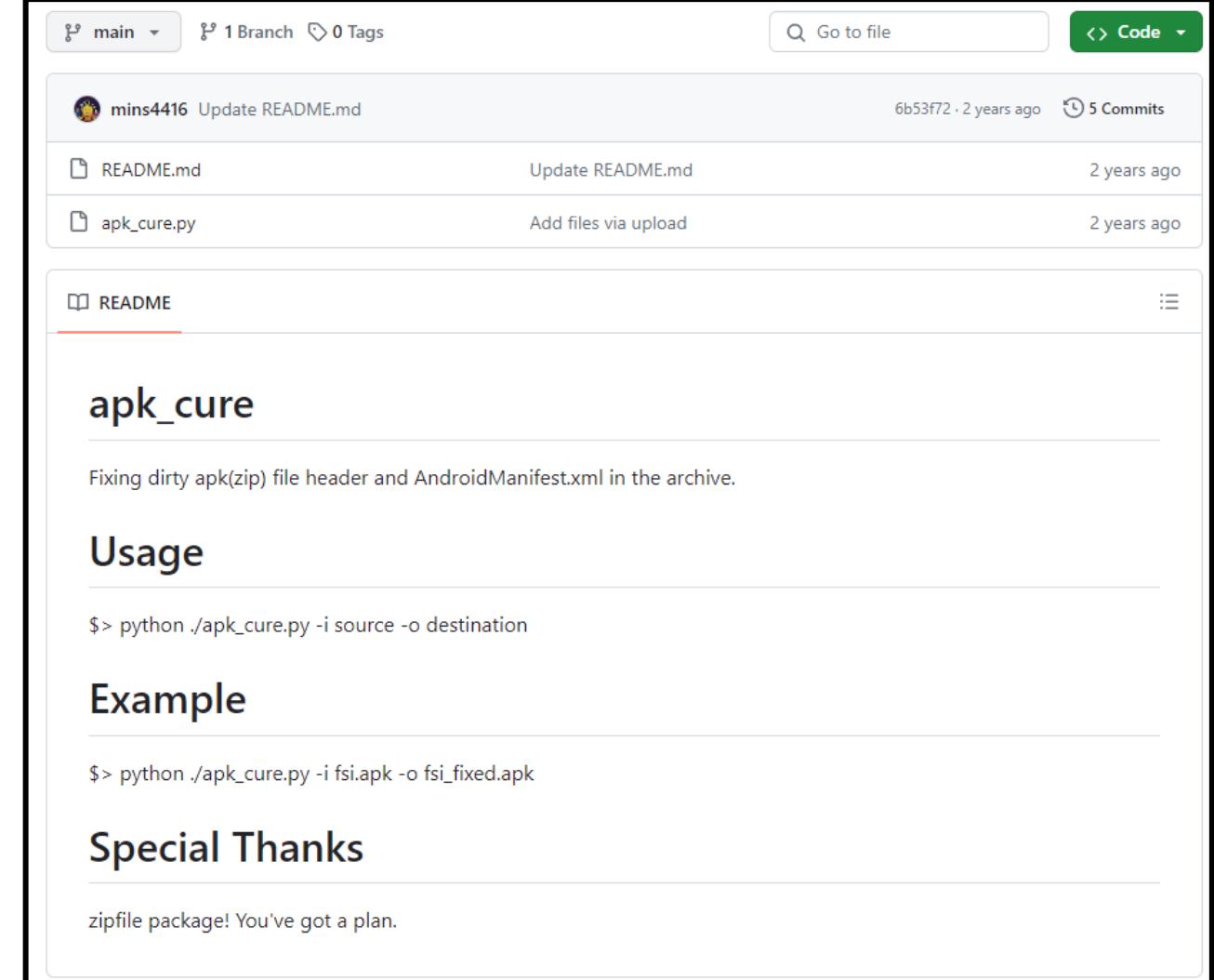
frCompression: 17185 is not valid, we can fix it to 8(Deflate)

frFileDialog: Not so far from now

4. SecretCalls – Anti decompile



Fix header manually



mins4416 · Update README.md · 6b53f72 · 2 years ago · 5 Commits

README.md · Update README.md · 2 years ago

apk_cure.py · Add files via upload · 2 years ago

apk_cure

Fixing dirty apk(zip) file header and AndroidManifest.xml in the archive.

Usage

```
$> python ./apk_cure.py -i source -o destination
```

Example

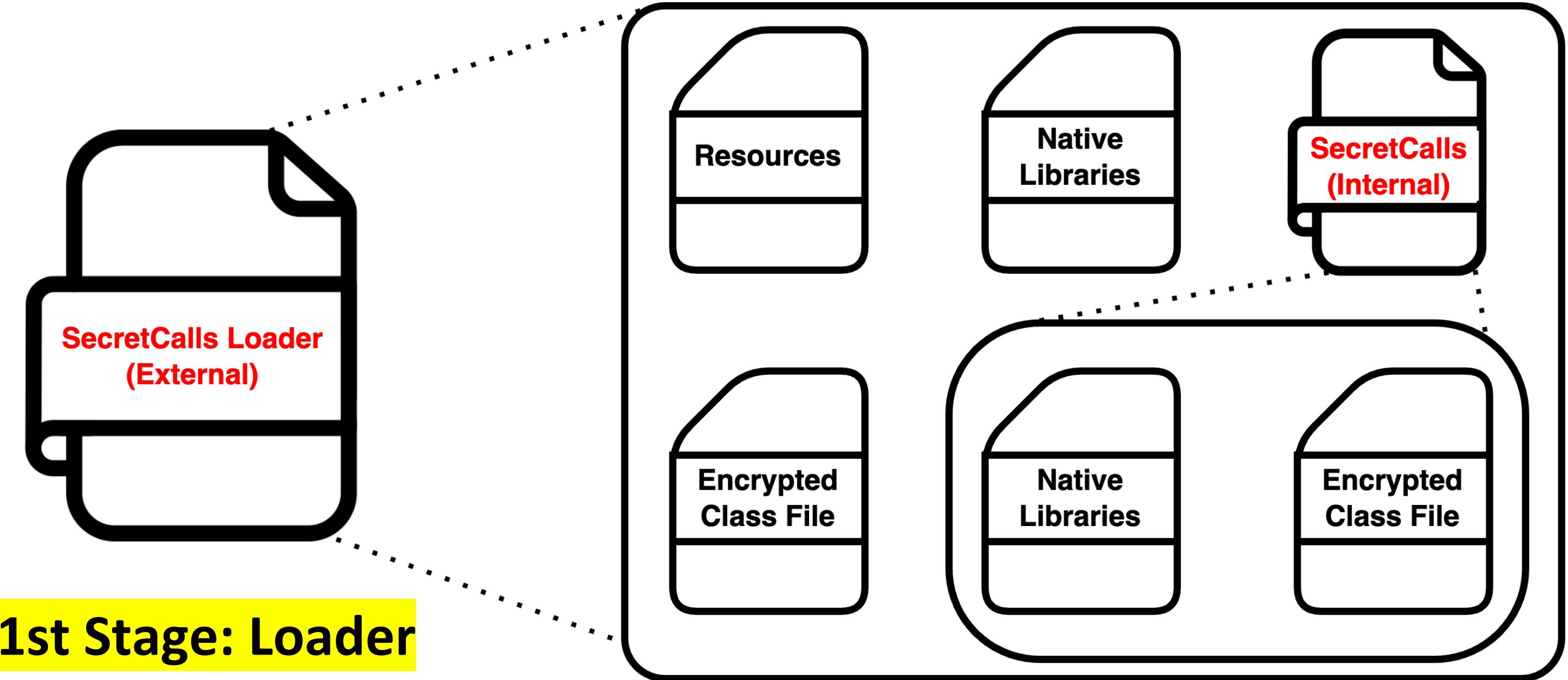
```
$> python ./apk_cure.py -i fsi.apk -o fsi_fixed.apk
```

Special Thanks

zipfile package! You've got a plan.

Use open Source
 mins4416

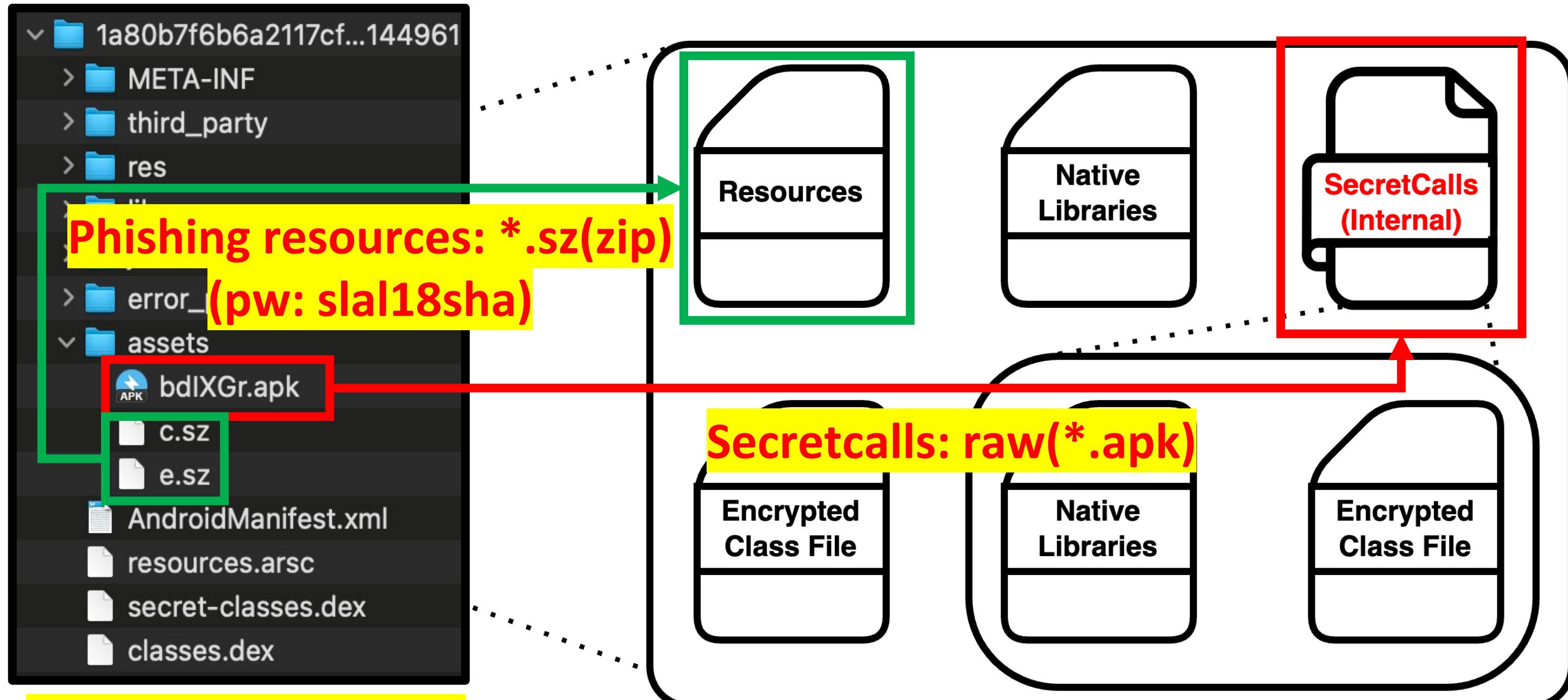
4. SecretCalls – File Structure



1st Stage: Loader

2nd Stage: SecretCalls

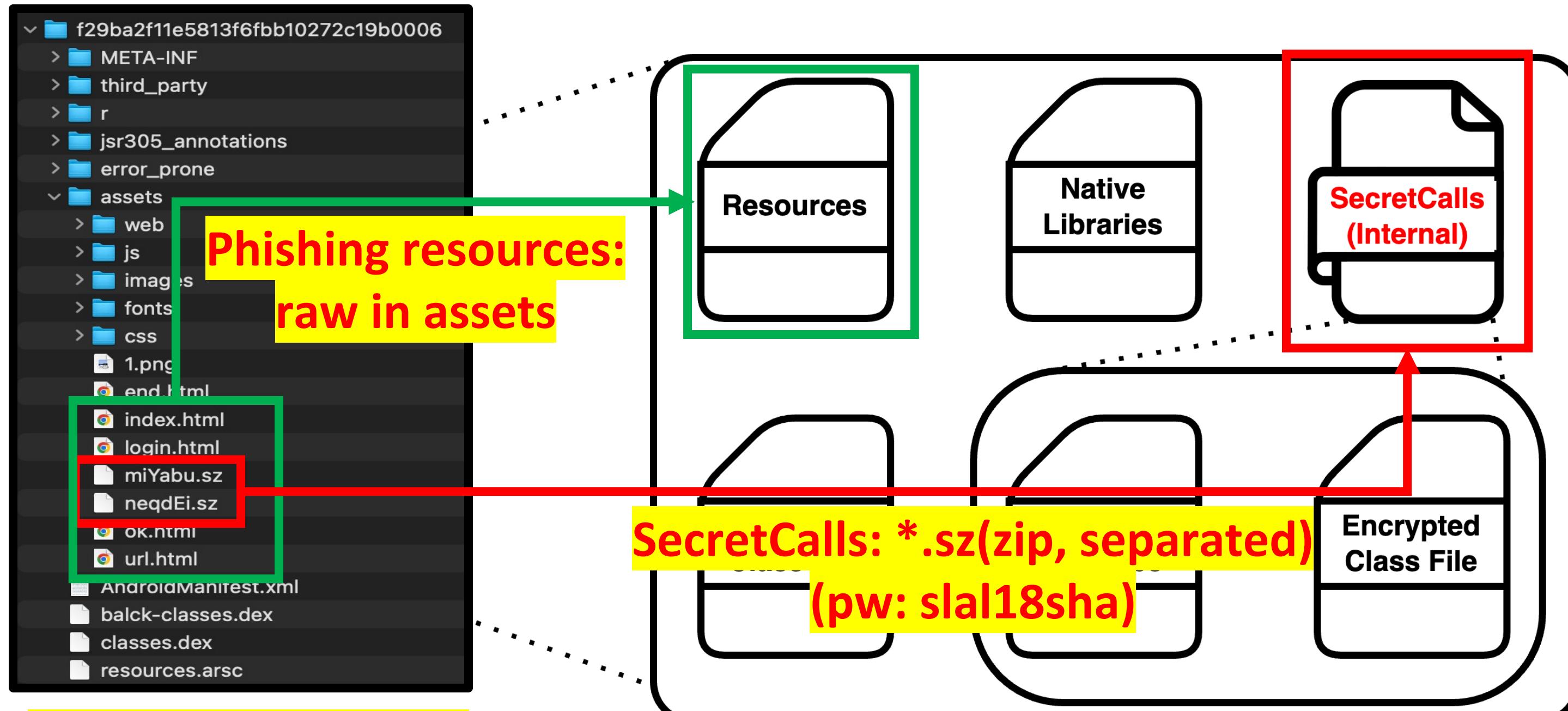
4. SecretCalls – File Structure (1)



SecretCalls Loader

*slal18sha: Korean profanity(moxxer fxxxer)

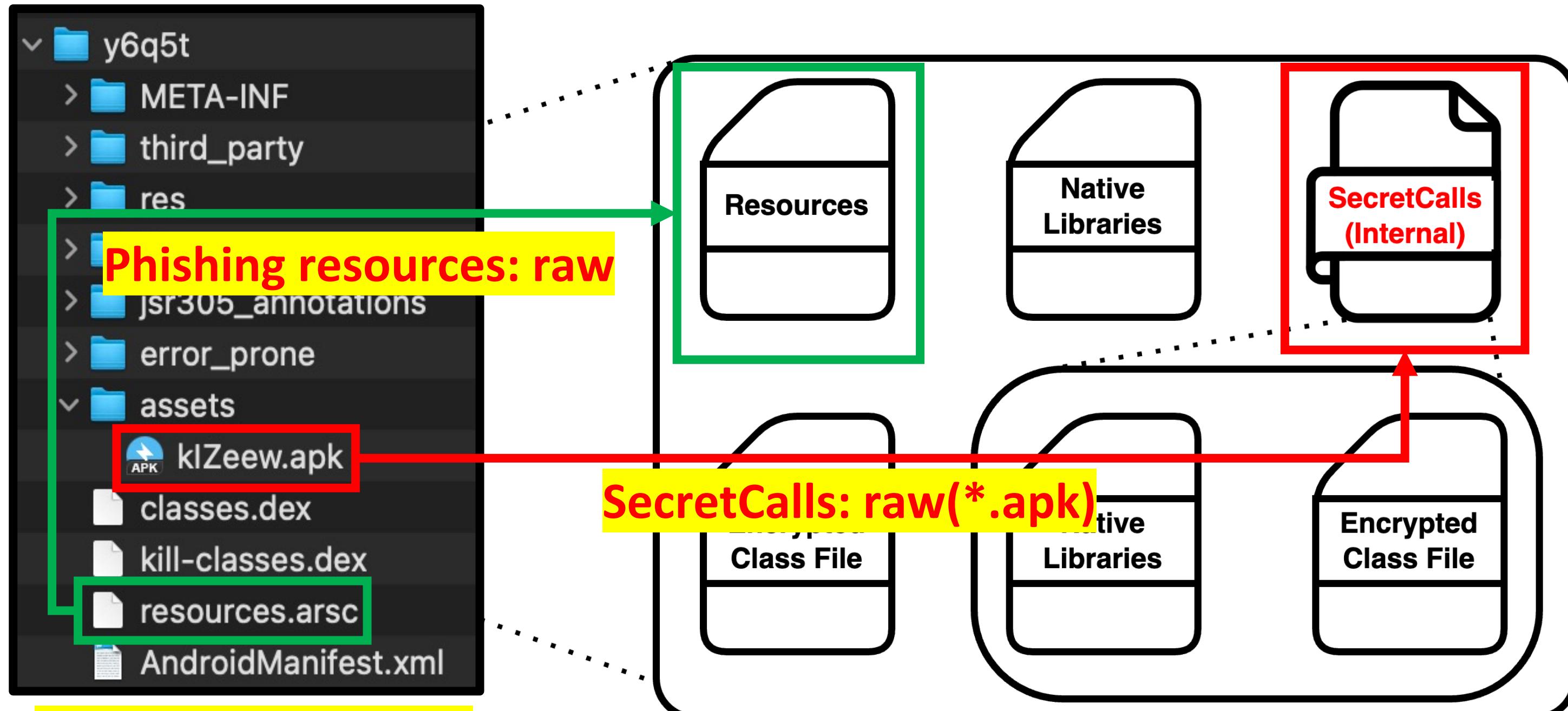
4. SecretCalls – File Structure (2)



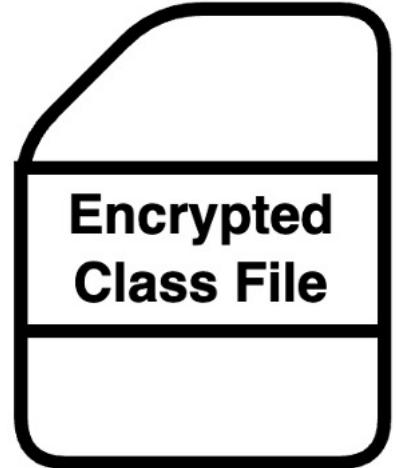
SecretCalls Loader

*slal18sha: Korean profanity(moxxer fxxxer)

4. SecretCalls – File Structure (3)



4. SecretCalls – Encrypted Class file



- Components of Each apps(Loader/SecretCalls)
- Key elements for malicious activity
- Decrypted / Loaded on memory in runtime
- Has changed to **three different names**

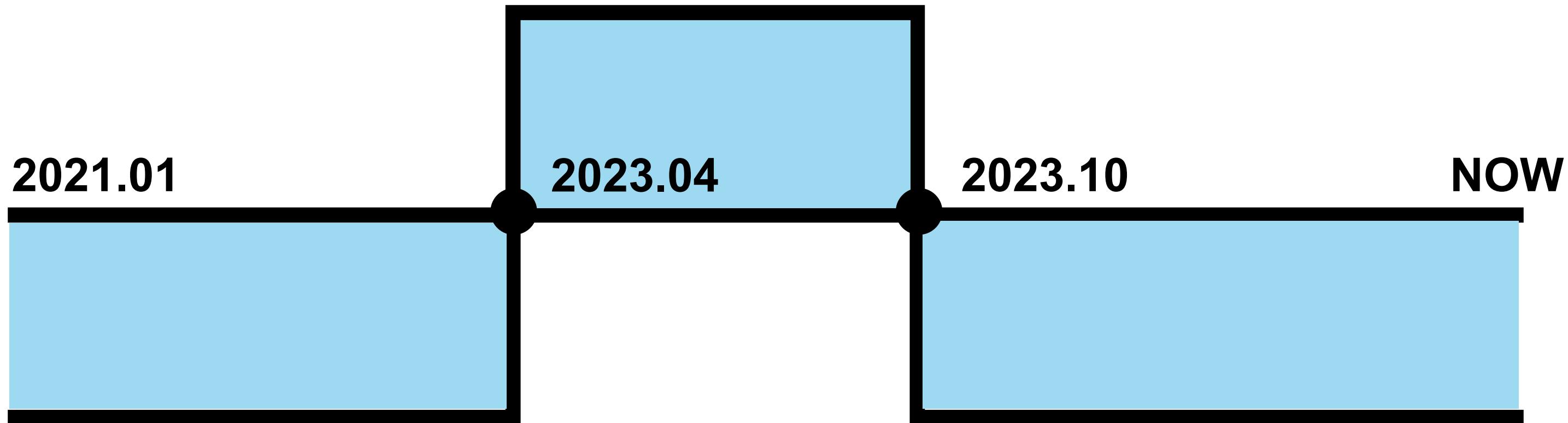
secret-
classes.dex

kill-
classes.dex

balck-
classes.dex

4. SecretCalls – Encrypted Class file

kill-classes.dex



1st secret-classes.dex

Balck-classes.dex
2nd Secret-classes.dex

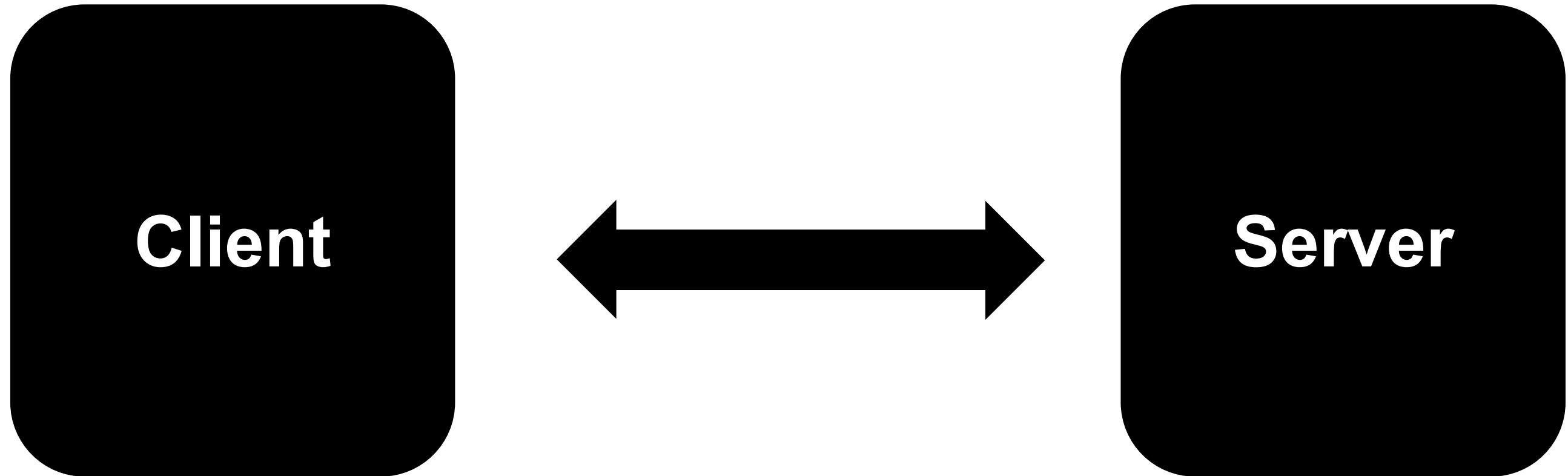
4. SecretCalls – Encrypted Class file

Encrypted class file	Decryption key stored in	Native library(.so) name
1 st Secret	Native Library AndroidManifest.xml	libfirebase.so
Kill	Native Library	libset.so libbbes.so
Balck	AndroidManifest.xml	No use library
2 nd Secret	Native Library	libdn_ssl.so libbbed.so

4. SecretCalls – Encrypted Class file

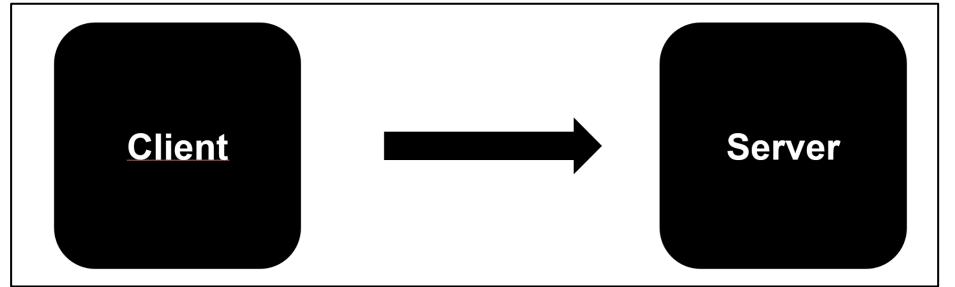
Encrypted class file	Key to decrypt class file (AES-128/ECB only)	key to decrypt extra C&C (AES-128/CBC only)
1st Secret Kill	dbcdfghijklmaop	rb!nBwXv4C%Gr^84(KEY) 1234567812345678(IV)
Balck	xxxxefgaxxdecccc dasdefvvvxxyyyy	
2nd Secret	dbcdfghijklmaop	PY06RguZ68k2as6v(KEY) 1862971933292829(IV)

4. SecretCalls – Network Behavior(Protocol)



Websocket + HTTP

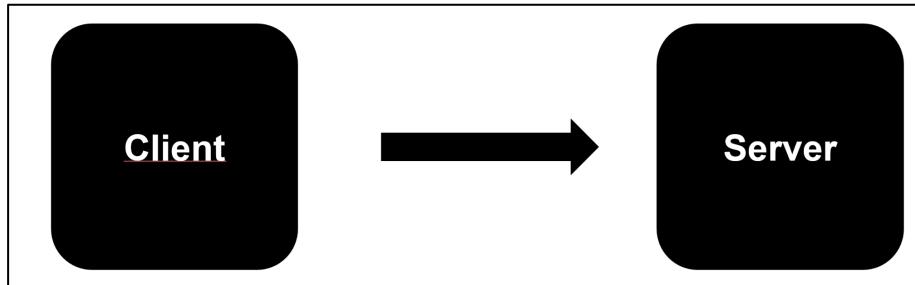
4. SecretCalls – Network Behavior(Requests)



App ID(key value)
Device's Information

```
appid: "11",
gg: "cs6IYfvD5d8:APA91bG85inRHPUnSXPj32dWAbCzccvSIIIfVh0kLU8ZvHGY-g0UCoTT2uphGJpzv4_ymEmmvlx-
h23Rx8bLgTRoJ4QxJzC-bEGARLaDggdRNNGFpIxj9UIQsYGiMC6clxj0wsUXXWeTT",
rid: "60884692-0c48-4422-9fdc-ad14d06f2f62-11",
rinfo: "
{\"blue\": \"1\", \"mes\": \"1\", \"def\": \"0\", \"wifi\": \"1\", \"acs\": \"0\", \"chatid\": \"82010545844
24\", \"scr\": \"1\", \"adds\": \"\", \"bat\": \"100%\", \"map\": \"\", \"sys\": \"0\", \"chat\": \"0\", \"nu
m\": \"+8201054584424\", \"oper\": \"KT\", \"rec\": \"0\", \"acc\": \"8201054584424\", \"ver\": \"7.1.2\",
\"model\": \"SM-N950N\"}",
rno: "+8201054584424",
sys: "0"
```

4. SecretCalls – Network Behavior(Requests)



a[timestamp]=[payload with encryption]
(old)postVal=[payload with encryption]

a1676531268344=JXwH71%2F9kzN%2B3ZvgG1PvbiFaZ
nzQ474Kp1942YFtXFKYFzN4gXohPv%2Fe4zLUCJ6qYEa
nG9VlUp%2FZVvhvIX9ZyfPx5fGC060L9oJp5mrvt
e6JUt6EmLNIDx0prJLhJ3DKCaTsDq3efD2V%2BCZjExsQKBI
KYaemBT97K80AshBJjWaZEnHmvloa5b2RwcT2bUats1B
b5Nc2hW5r5NQ87irUVxBEcX7kL69qNXcfkxv%2Bj0fwD

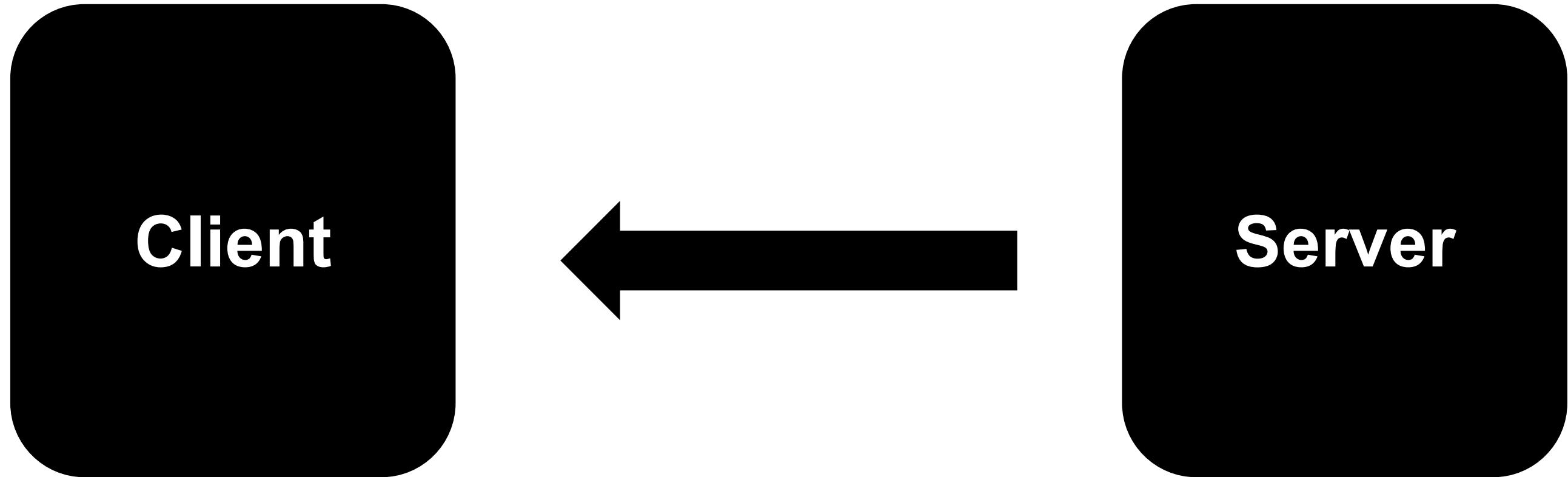
4. SecretCalls – Network Behavior(Requests)

Type	behavior	Endpoint
2	Send device status	http://{C&C ip}/A3bh3/Vdc5
3	Extort new message	http://{C&C ip}/bC4d/v8N/Sop40
...
13	Send audio, image files	http://{C&C ip}/a/bcF4c/Bdcm/.../vvbg

Type 3 => **http://{C&C ip}/bC4d/v8N/Sop40**

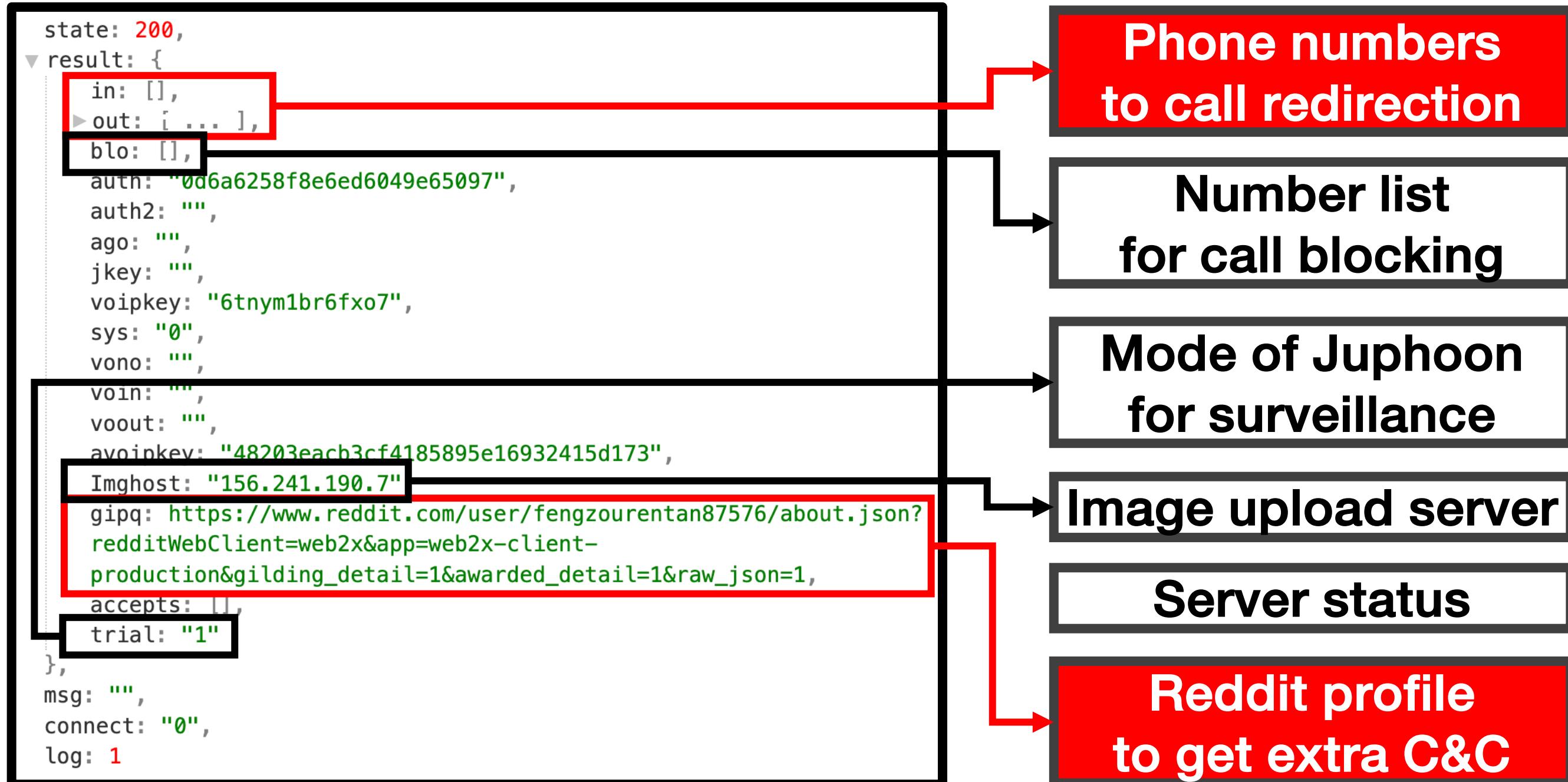
[a-zA-Z0-9]{1,5} * 3

4. SecretCalls – Network Behavior(Response)



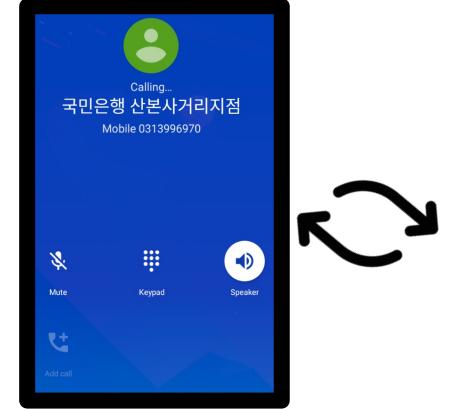
Config for malicious Behavior
(e.g. call forwarding)

4. SecretCalls – Network Behavior(Response)

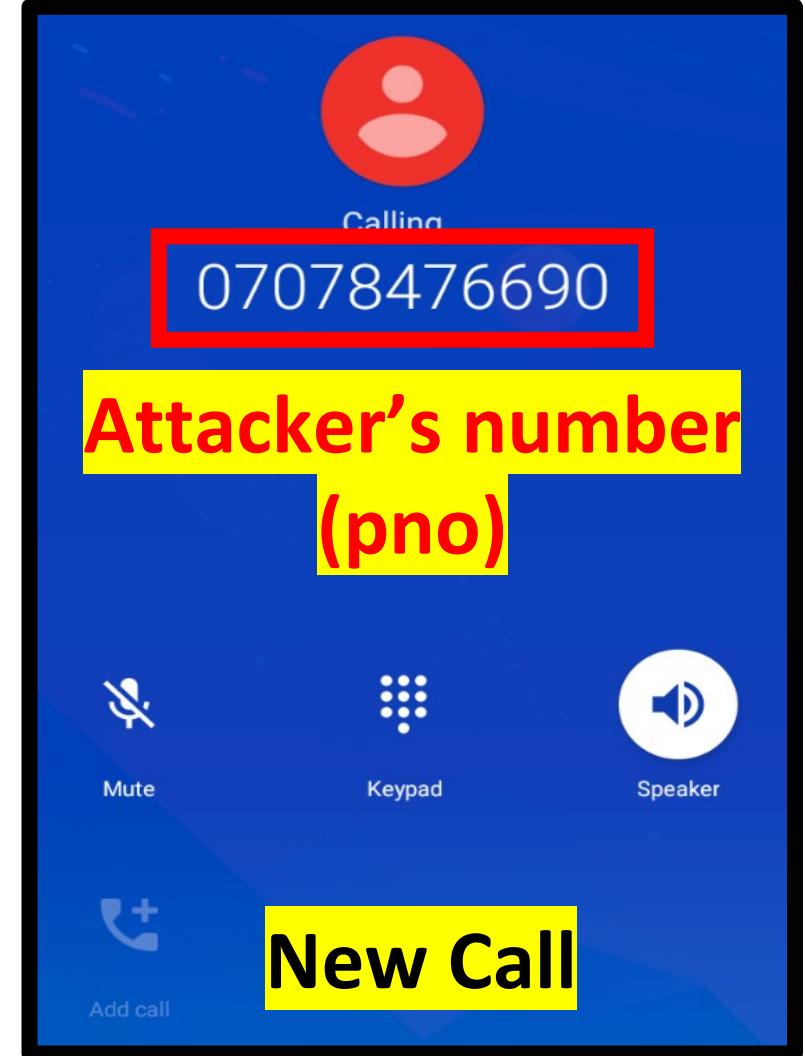


4. SecretCalls – Call Redirection

```
state: 200
▼ result: {
    ▶ in: []
    ▶ out: [
        ▶ {
            name: "국민은행 산본사거리지점",
            fno: "0313996970",
            pno: "07078476690"
        },
        ▶ {
            name: "국민은행 호계동종합센터",
            fno: "0314577134",
            pno: "07078476690"
        },
        ▶ {
            name: "국민은행 당정동지점",
            fno: "0314777485",
            pno: "07078476690"
        },
        ▶ {
            name: "국민은행 호계남지점",
            fno: "0314278361",
            pno: "07078476690"
        }
    ],
    ▶ auth: null
    ▶ auth2: null
    ▶ ago: null
    ▶ jkey: null
    ▶ voipkey: null
    ▶ sys: null
    ▶ vono: null
    ▶ voin: null
    ▶ voout: null
    ▶ avoipkey: null
    ▶ Imghost: null
    ▶ gipq: http://redditWebClient
    ▶ production: true
    ▶ accepts: [],
    ▶ trial: "1"
}
  ▶ oout.json?
  ▶ 1,
```



Original Call



Attacker's number
(pno)

New Call

The original call will be canceled, and a new call will be created.

connect: "0",
log: 1

It may be difficult to notice

4. SecretCalls – Call Redirection

```
state: 200
▼ result: {
    in: []
    ▶ out
    blo: |
    auth: 
    auth2: 
    ago: 
    jkey: 
    voipke
    sys: 
    vono: 
    voin: "
    voout: "
    avoipkey:
    Imghost:
    gipq: http://
    redditWebC
    production&
    accepts: [],
    trial: "1"
},
msg: "",
connect: "0",
log: 1
```

out: [

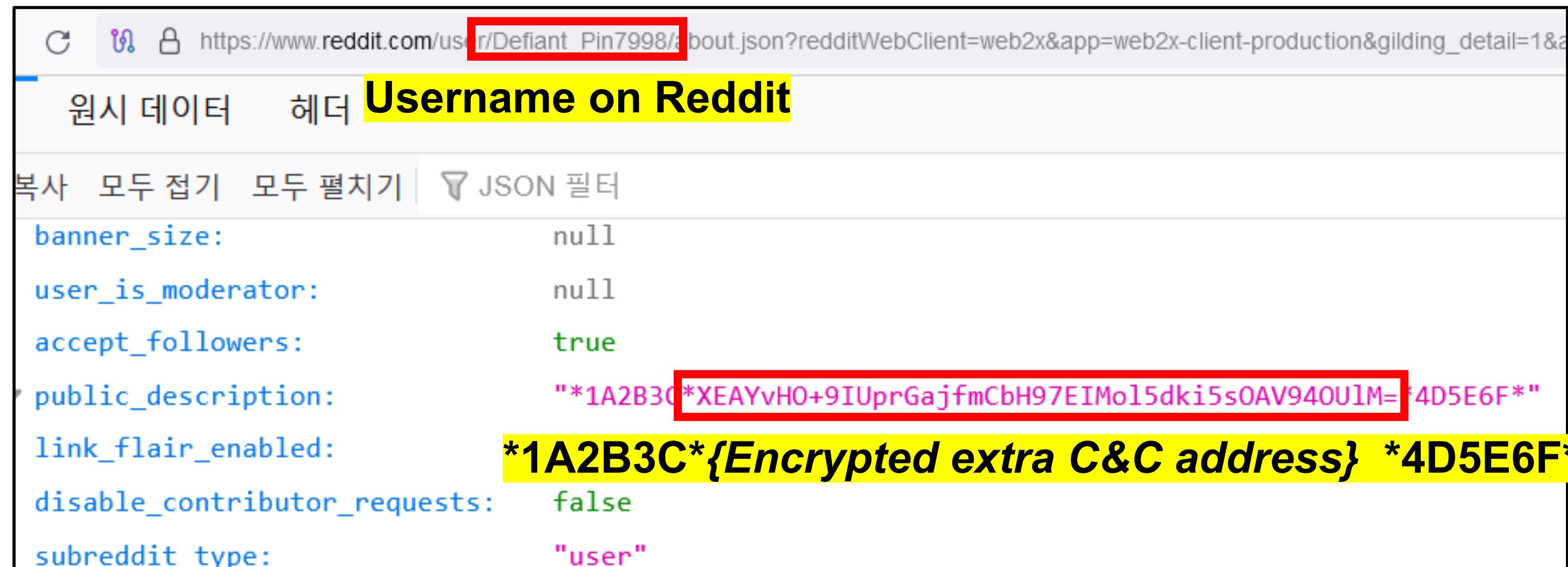
- {
name: "국민은행 산본사거리지점",
fno: "0313996970",
pno: "07078476690"
- {
name: "국민은행 호계동종합센터",
fno: "0314577134",
pno: "07078476690"
- {
name: "국민은행 당정동지점",
fno: "0314777485",
pno: "07078476690"
- {
name: "국민은행 호계남지점",
fno: "0314278361",
pno: "07078476690"

out.json?
1,

User sees a fake screen
overlaid on top of the new call screen.



4. SecretCalls – Extra C&C



https://www.reddit.com/user/r/Defiant_Pin7998/about.json?redditWebClient=web2x&app=web2x-client-production&gilding_detail=1&a

Username on Reddit

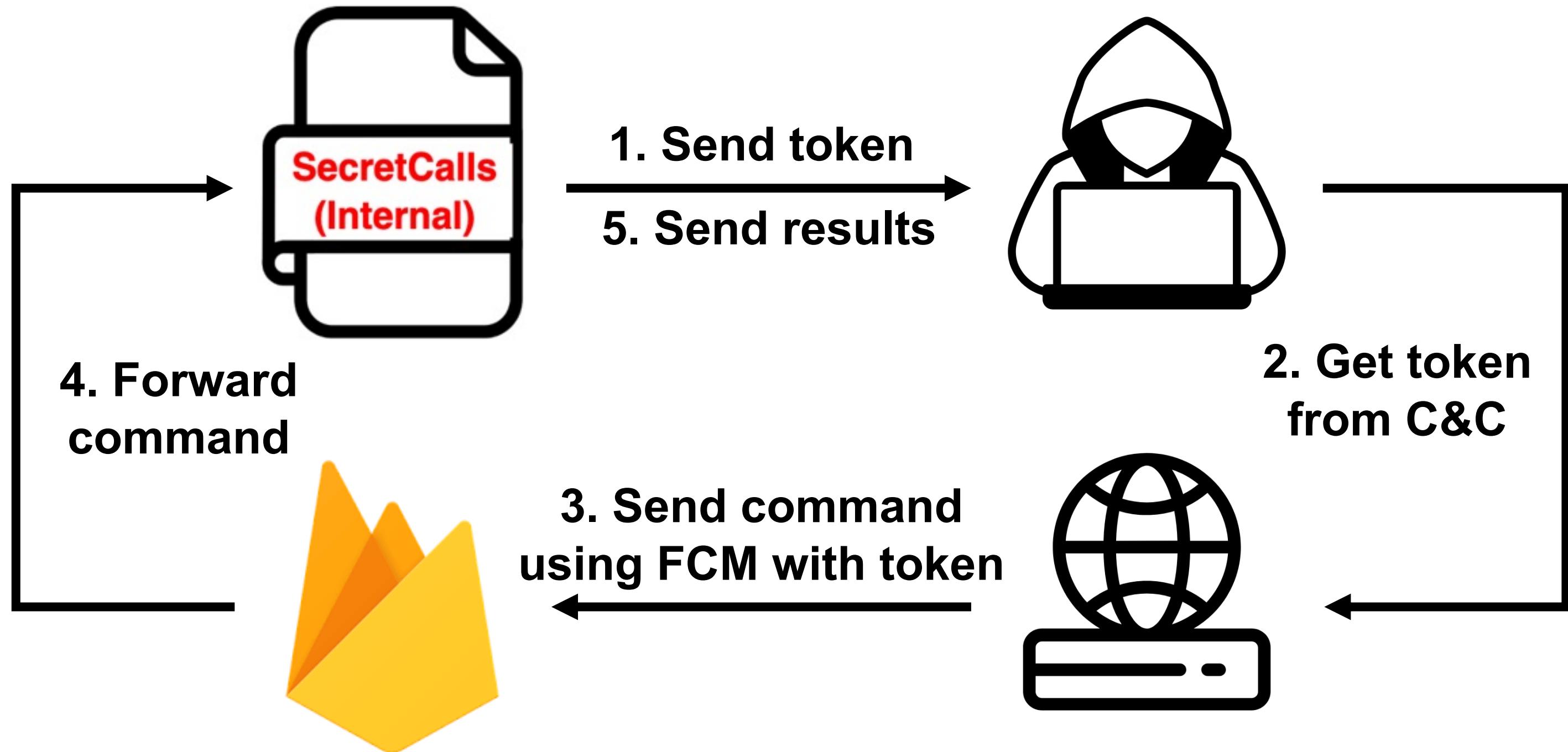
원시 데이터 헤더

복사 모두 접기 모두 펼치기 JSON 필터

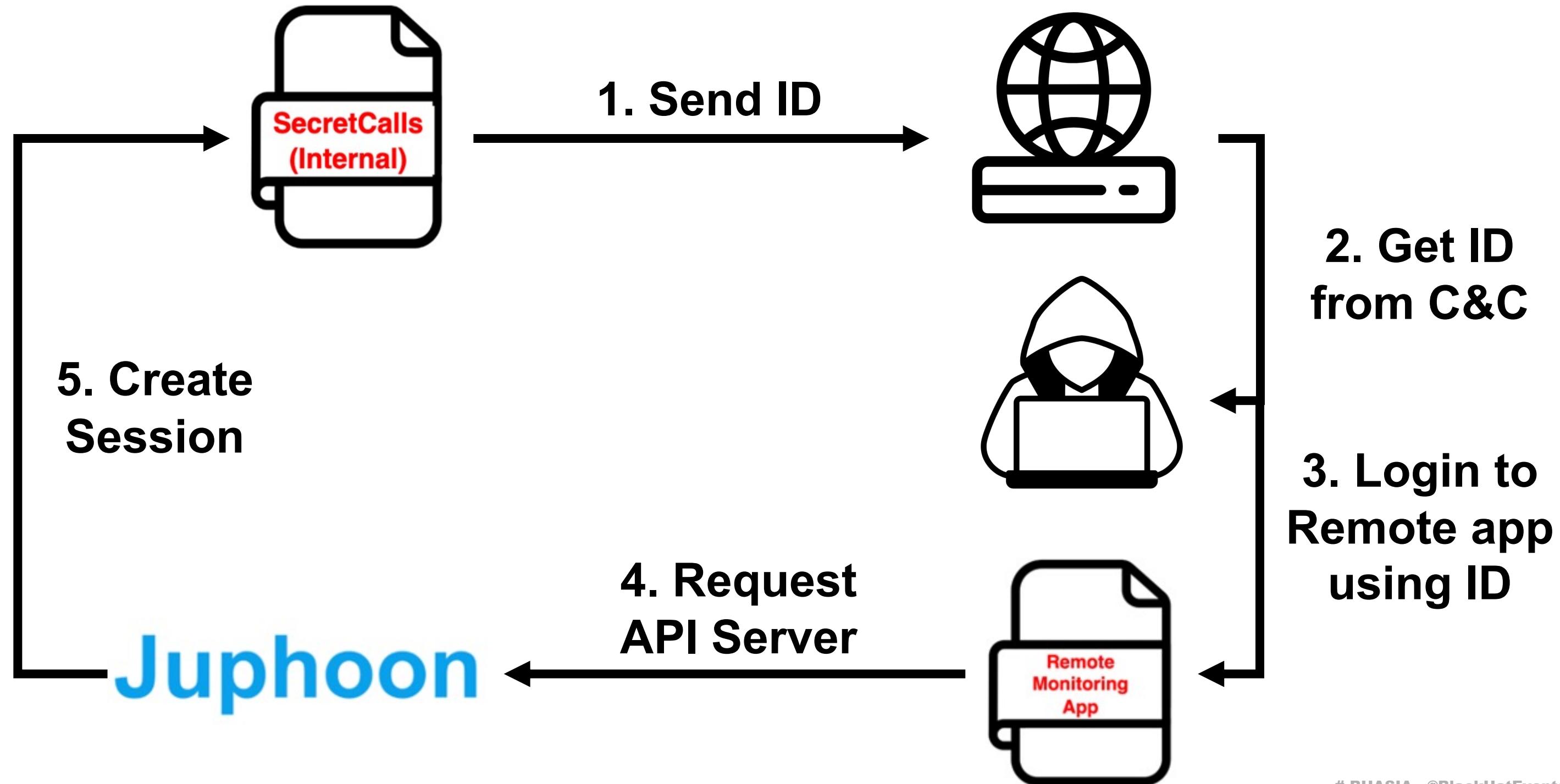
banner_size:	null
user_is_moderator:	null
accept_followers:	true
public_description:	*1A2B3C*XEAYvH0+9IUprGajfmCbH97EIMo15dk15s0AV940U1M=*4D5E6F*
link_flair_enabled:	*1A2B3C*{Encrypted extra C&C address} *4D5E6F*
disable_contributor_requests:	false
subreddit_type:	"user"

C&C on Reddit profile changes irregularly

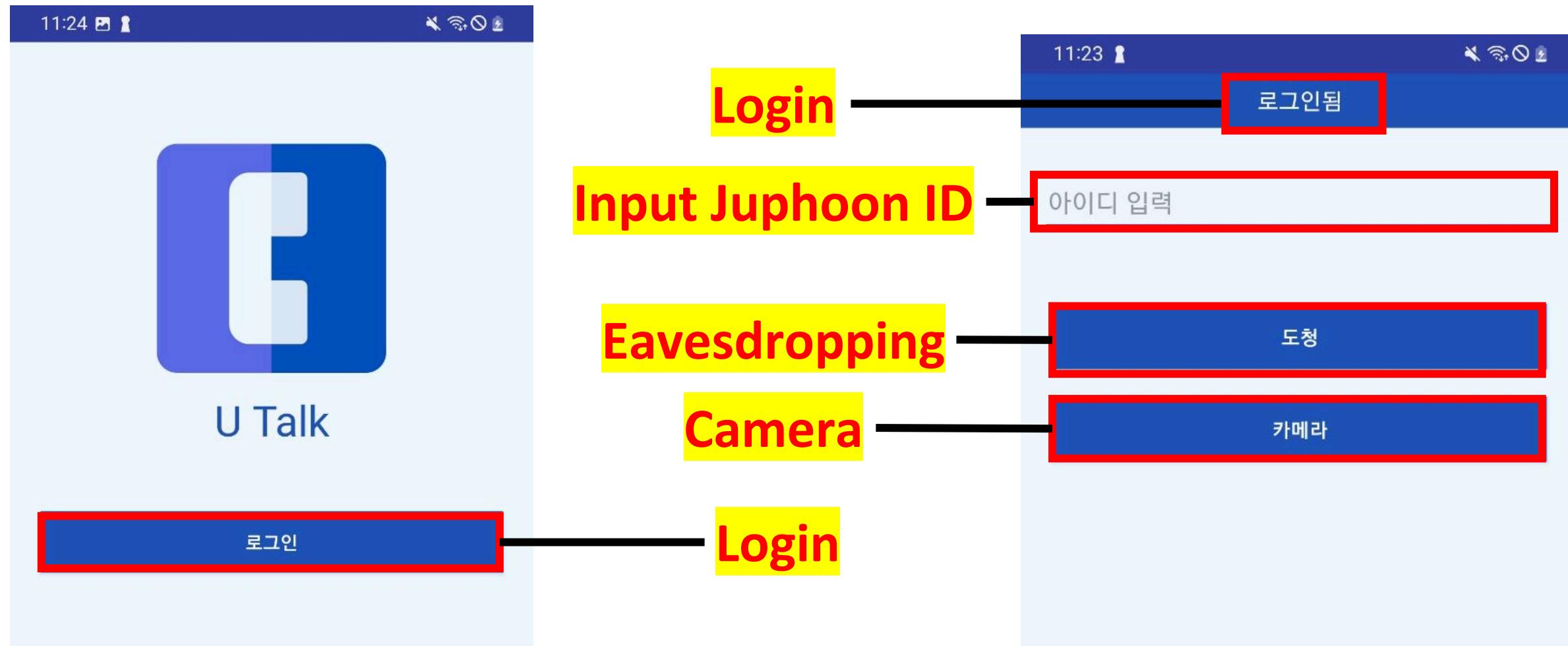
4. SecretCalls – FCM



4. SecretCalls - Surveillance



4. SecretCalls – Custom App for Surveillance



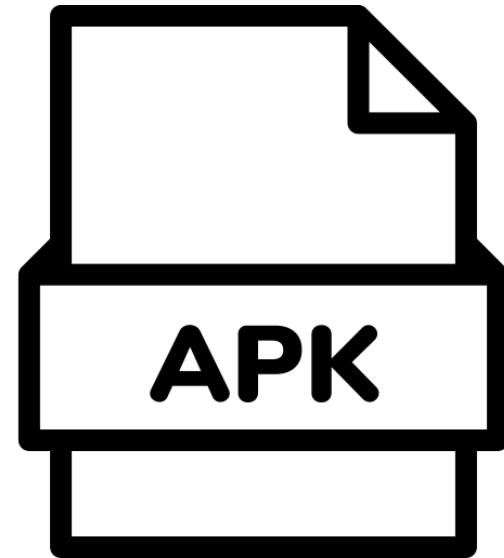
```
<string name="error_field_required">아이디 입력하세요</string>
<string name="error_voice_cam_connection!>도청실패! 아이디확인해주세요</string>
```

(error) input user ID

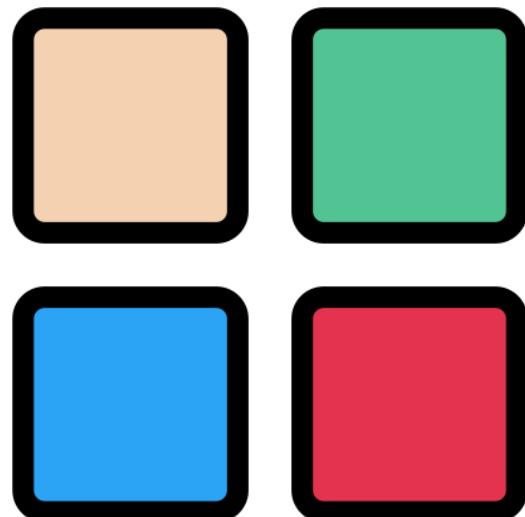
(error) Eavesdropping fail!
Check your ID

5. Automation

5. Automation - Statistics

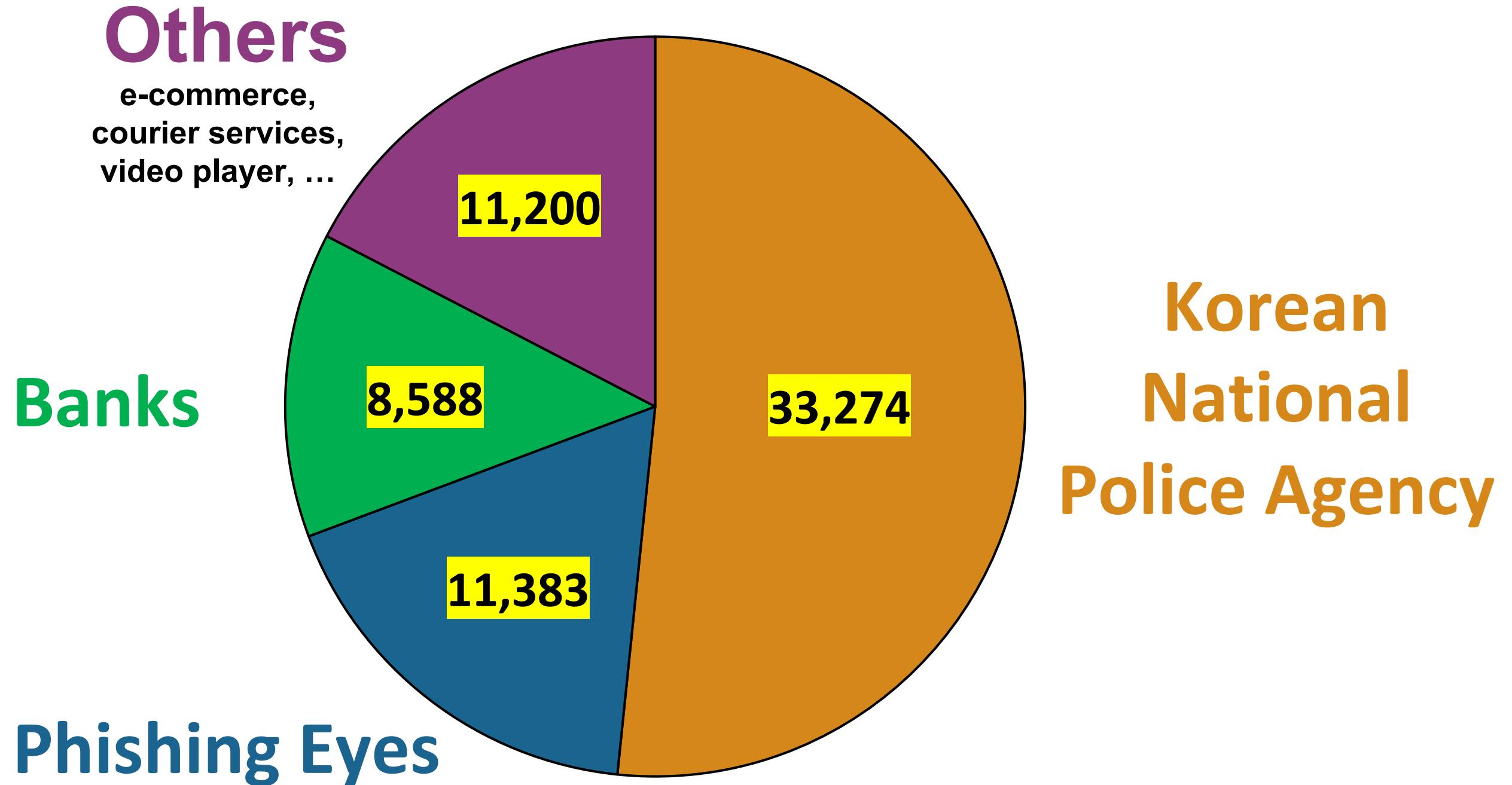


Collect Loader **64,000+**
(including Secretcalls, it doubles)



Classified into **15+**
target (theme)

5. Automation - Statistics



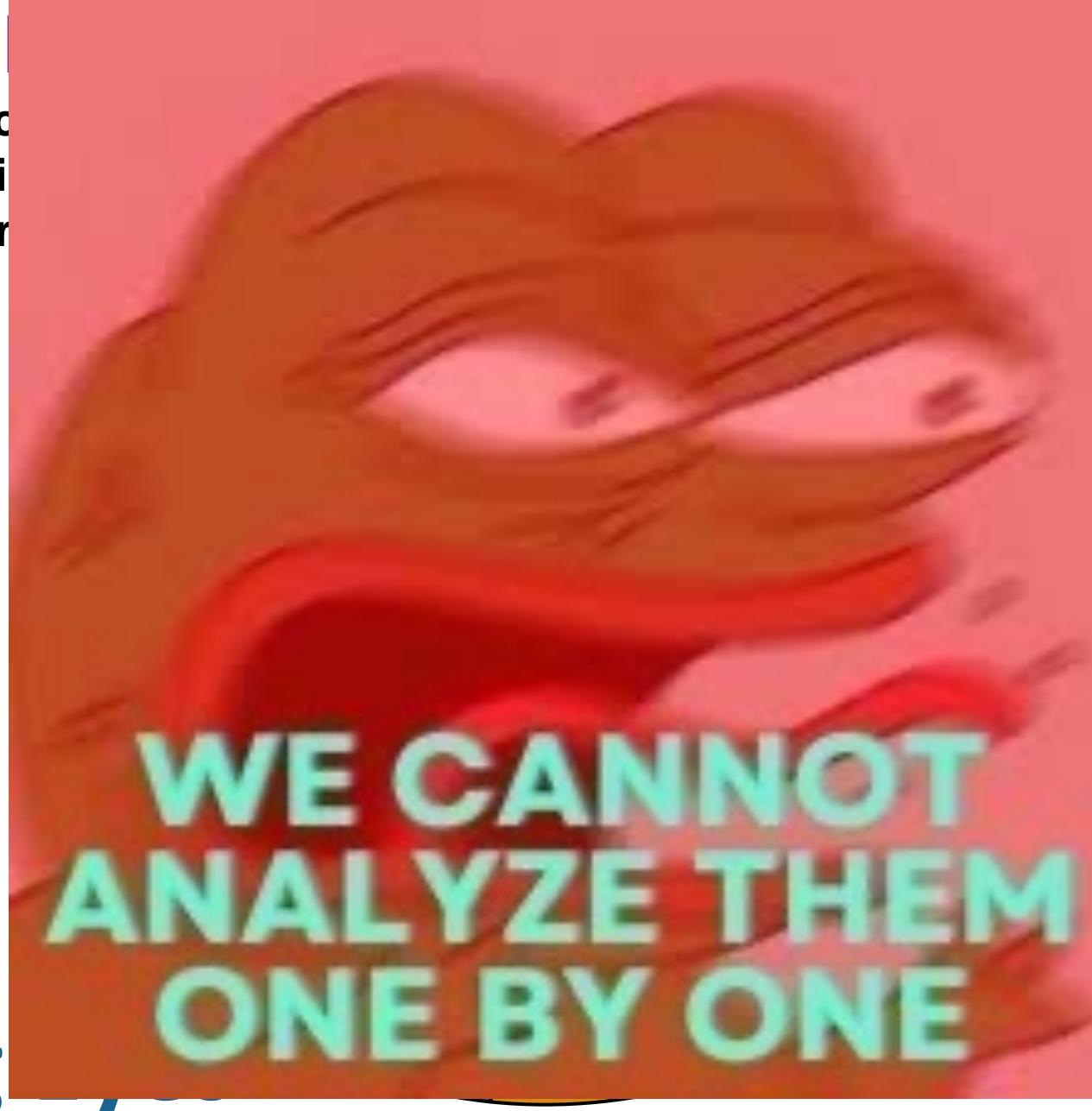
5. Automation - Statistics

Other

e-commerce
courier service
video player

Banks

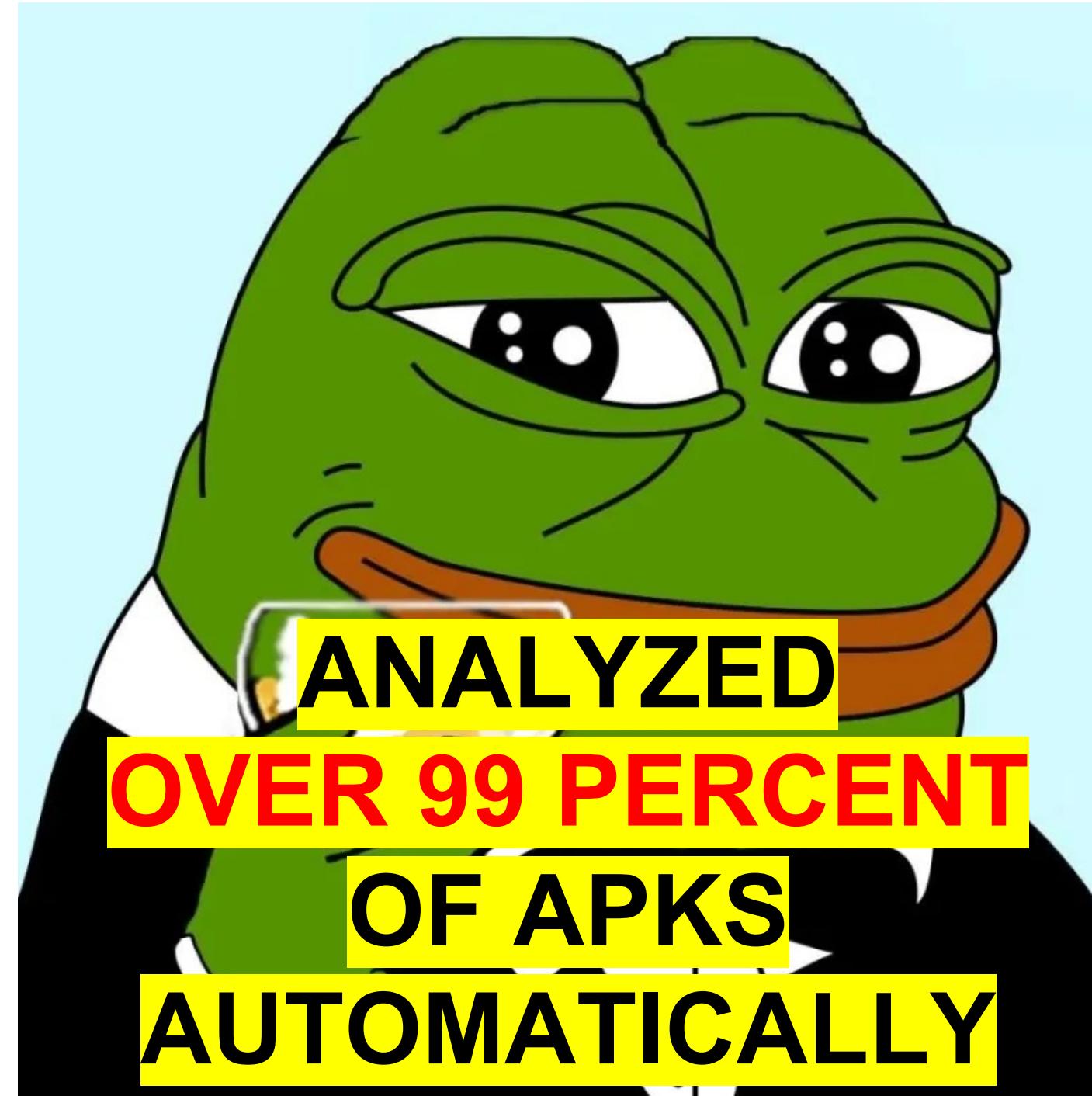
Phishing



Korean
National
Police Agency

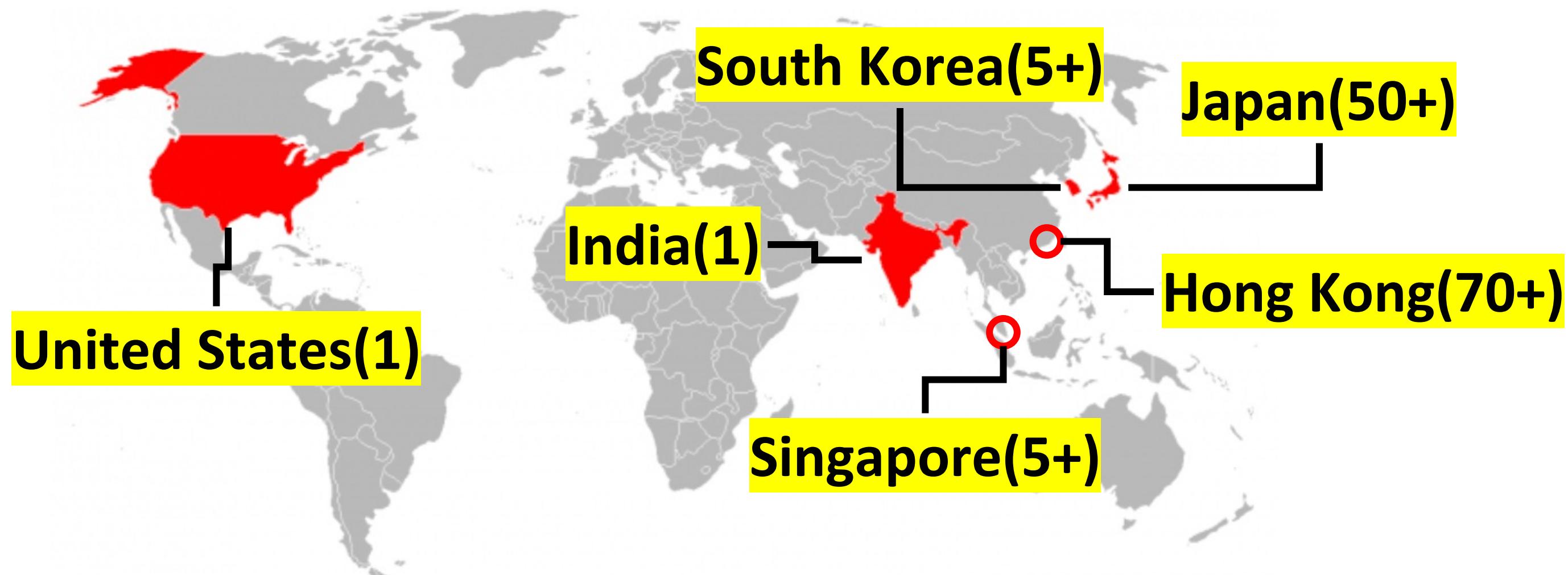
5. Automation - Conclusion

So, we...



5. Automation - Conclusion

- C&C server 130+
- Most are placed in **HK > JP > KR > SG > others**



5. Automation - Conclusion

- malicious phone number 15+
- About 10% of them(2) were **Chinese**, not Korean

15610
13074
7078
7078
7078
7078



130, 156: China Unicom

- With cases of impersonation of institutions on the rise, it's important to **monitor and block their phishing sites**.
- IoCs alone may not be enough, their attack scenarios need to be **understood and disseminated**.
- Need to track their infrastructure by extracting key information immediately **through automation**

Phishing site		
Provider A	Provider B	Provider C
114.44.203.96	114.44.215.128	156.247.15.245
114.41.74.75	114.44.215.163	208.87.202.44
111.253.228.97	114.43.215.82	45.207.51.254
111.253.207.49	114.43.215.197	45.207.51.229
61.223.147.45	114.43.212.118	45.207.54.115
61.223.140.235	114.43.195.191	45.207.54.114

Provider A - Phishing site		
Phishing Eyes	Supreme Prosecutor	Consumer Agency
114.41.64.218	111.253.216.161	111.253.215.49
111.253.198.50	111.253.220.43	61.223.157.84
111.253.200.198	111.253.246.44	114.41.75.234
111.253.238.95	111.253.247.9	114.41.79.203
61.223.143.191	61.223.129.229	114.41.80.221
61.223.139.252	114.41.76.156	114.47.71.228

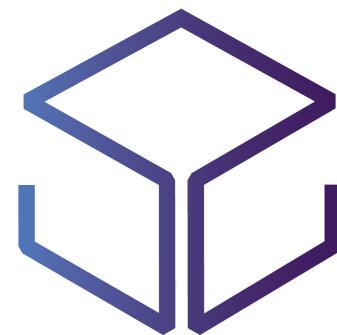
Provider A - SecretCalls		
Hash	Reddit profile	C&C
99dbb222c7096c3bd759bbd49799523e	Free-Breakfast-9220	43.202.65.81
0096dbf7aae99f71adaed0a05fd50bb8	WesternMastodon5235	154.19.69.67
d459471e7e64ba61e6592557f8d190e3	No_Double2876	38.181.2.17
305148cf2598d04ec3afe84271e49f8	Legitimate_Peanut139	27.56.36.70
29d371239a57796983ce1dc639c3e40e	CourseComfortable340	103.73.161.210
fd52ae1f3164deb1c9e1439b479c6bb5	Then-Lie-3539	103.97.178.69

Provider A		
SecretCalls' C&C		
27.124.36.74	38.181.2.49	137.220.245.14
149.104.49.43	38.181.2.83	137.220.245.18
149.104.49.44	154.19.69.75	137.220.245.26
149.104.49.46	198.176.60.87	137.220.245.37
149.104.49.49	103.186.215.103	137.220.245.38
13.124.202.35	137.220.245.13	137.220.245.45



Any question?
@

Contact
Sojun: hypen@s2w.inc
Yeongjae: teaf1001@naver.com



S2W
Safe and Secure World



About S2W

S2W is a big data intelligence company specialized in hidden channels and cryptocurrencies.

Contact

For any queries, please contact

info@s2w.inc

www.s2w.inc