



**blackhat**<sup>®</sup>

ASIA 2024

APRIL 18-19, 2024

BRIEFINGS

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

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



**blackhat**<sup>®</sup>  
ASIA 2024

**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

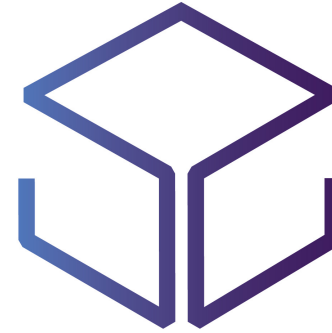
## Career

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

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

## Social

- [hypen1117@gmail.com](mailto:hypen1117@gmail.com)



# S2W

Safe and Secure World



@hypen1117

# 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](mailto:teaf1001@naver.com)



[Facebook Profile](#)

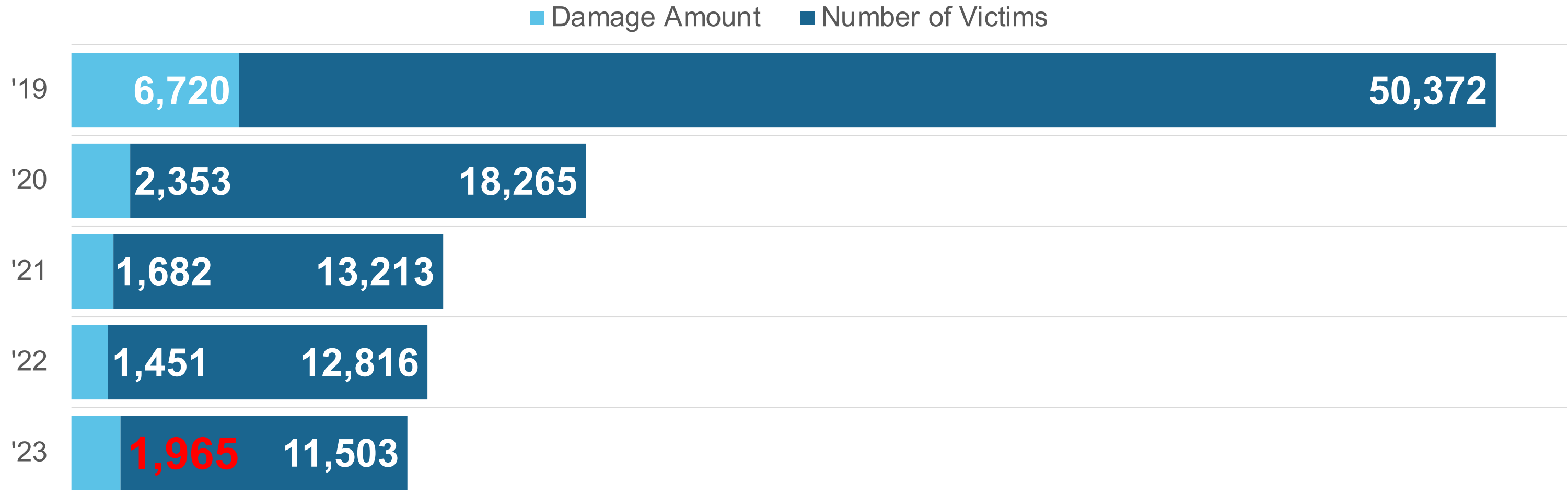


[Linkedin Profile](#)

# 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**.

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



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

■ Damage per victim

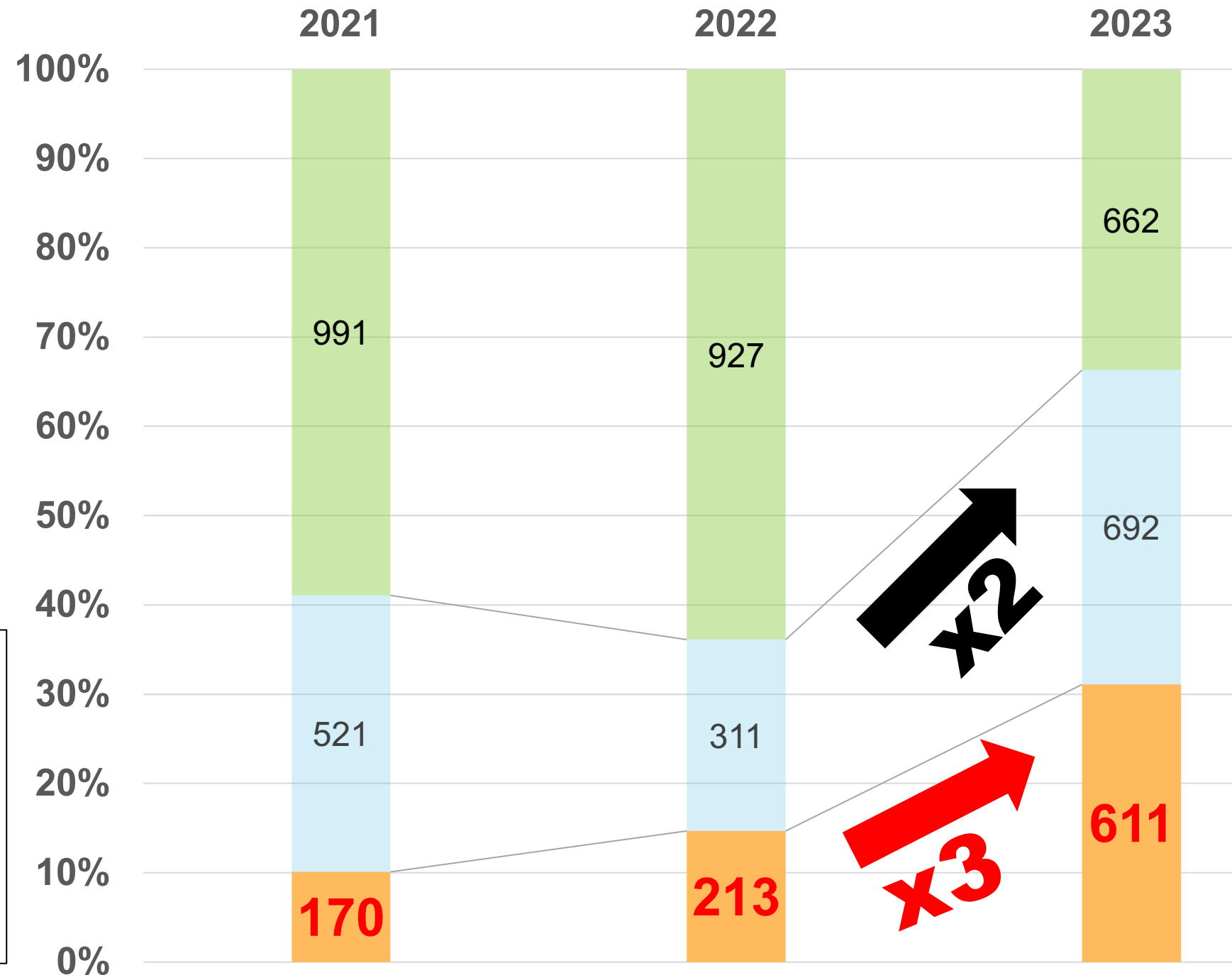
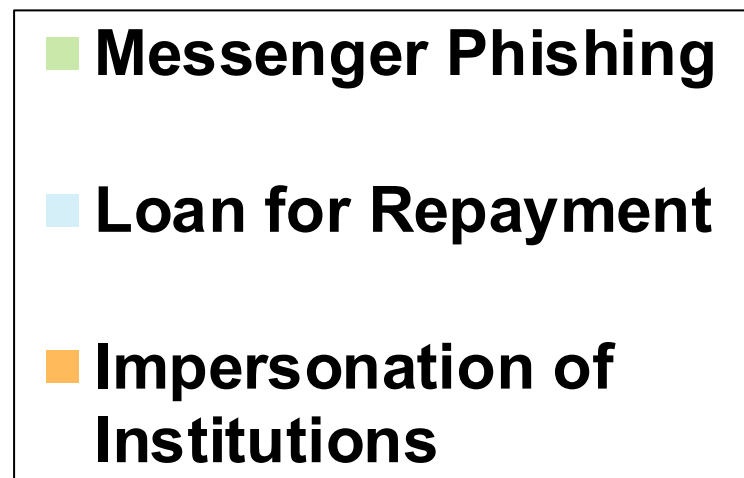


**Fewer victims, but damage per victim has increased**



## 2023 type of voice-phishing

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

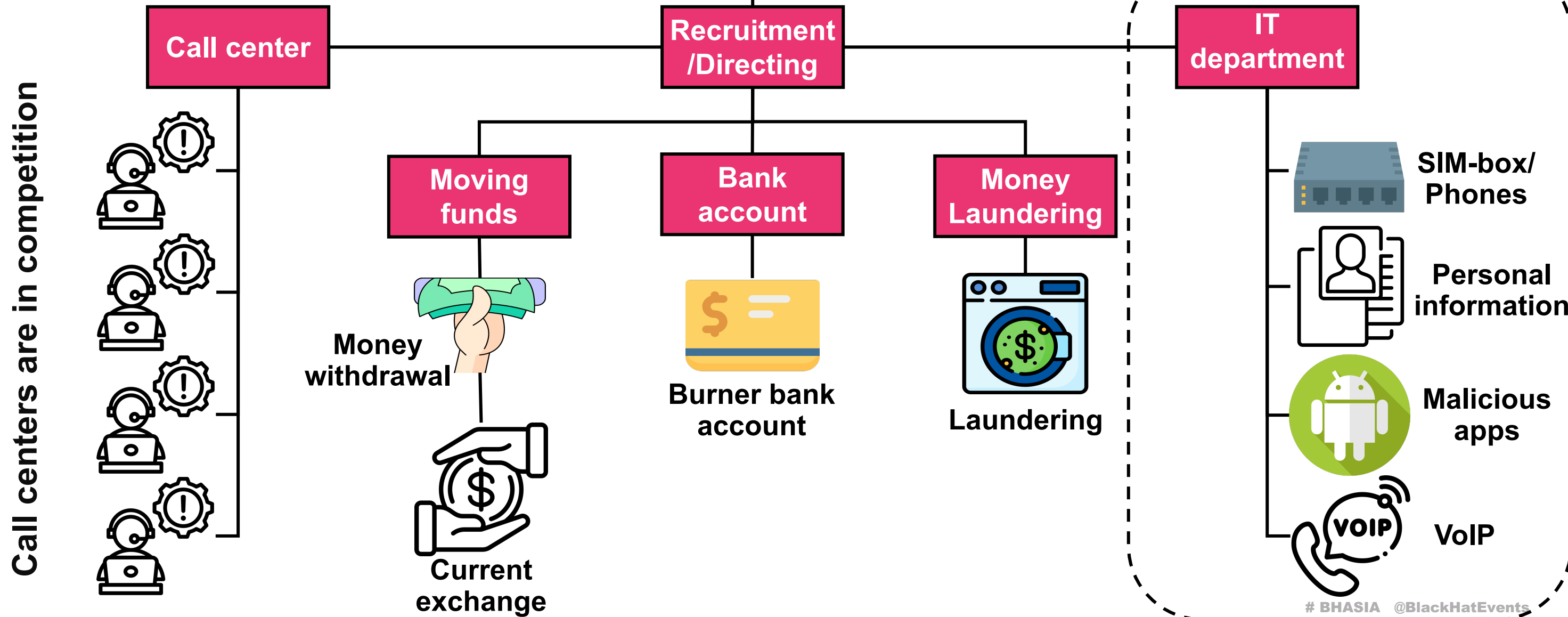


# 2. Overview

# 2. Overview – Group structure

Source: Seoul Eastern District Prosecutor's Office

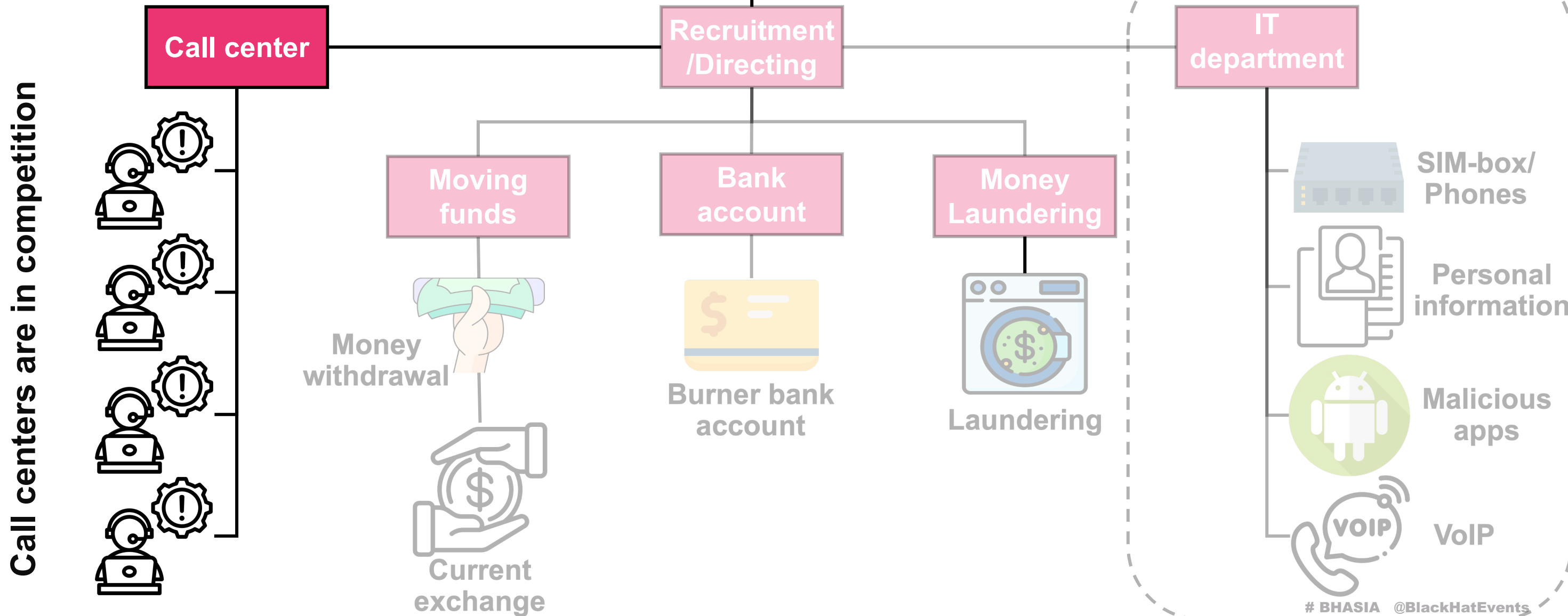
- **Name: Minjun's group (Name of Director)**
- **December 2017 ~ December 2021 (5 yrs)**
- **60 members**
- **560 victims, 10.8 billion(KRW)**



# 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)**

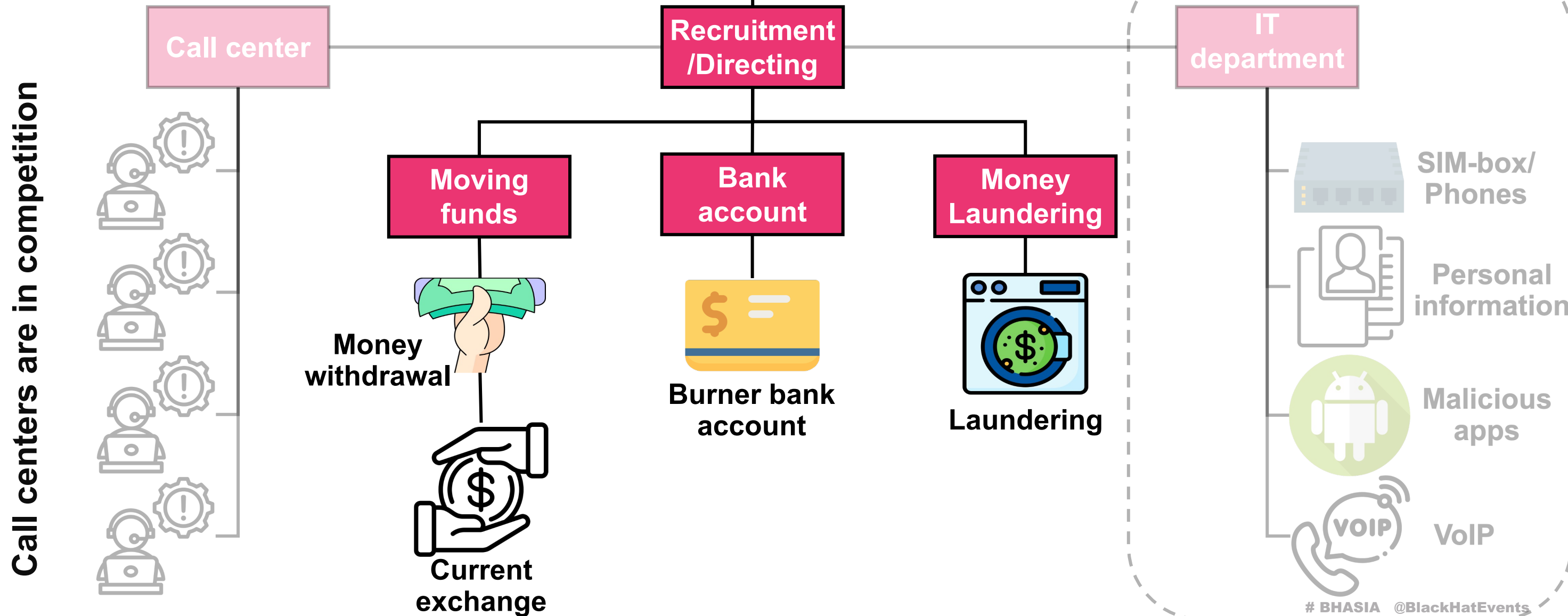
Source: Seoul Eastern District Prosecutor's Office



# 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)**

Source: Seoul Eastern District Prosecutor's Office

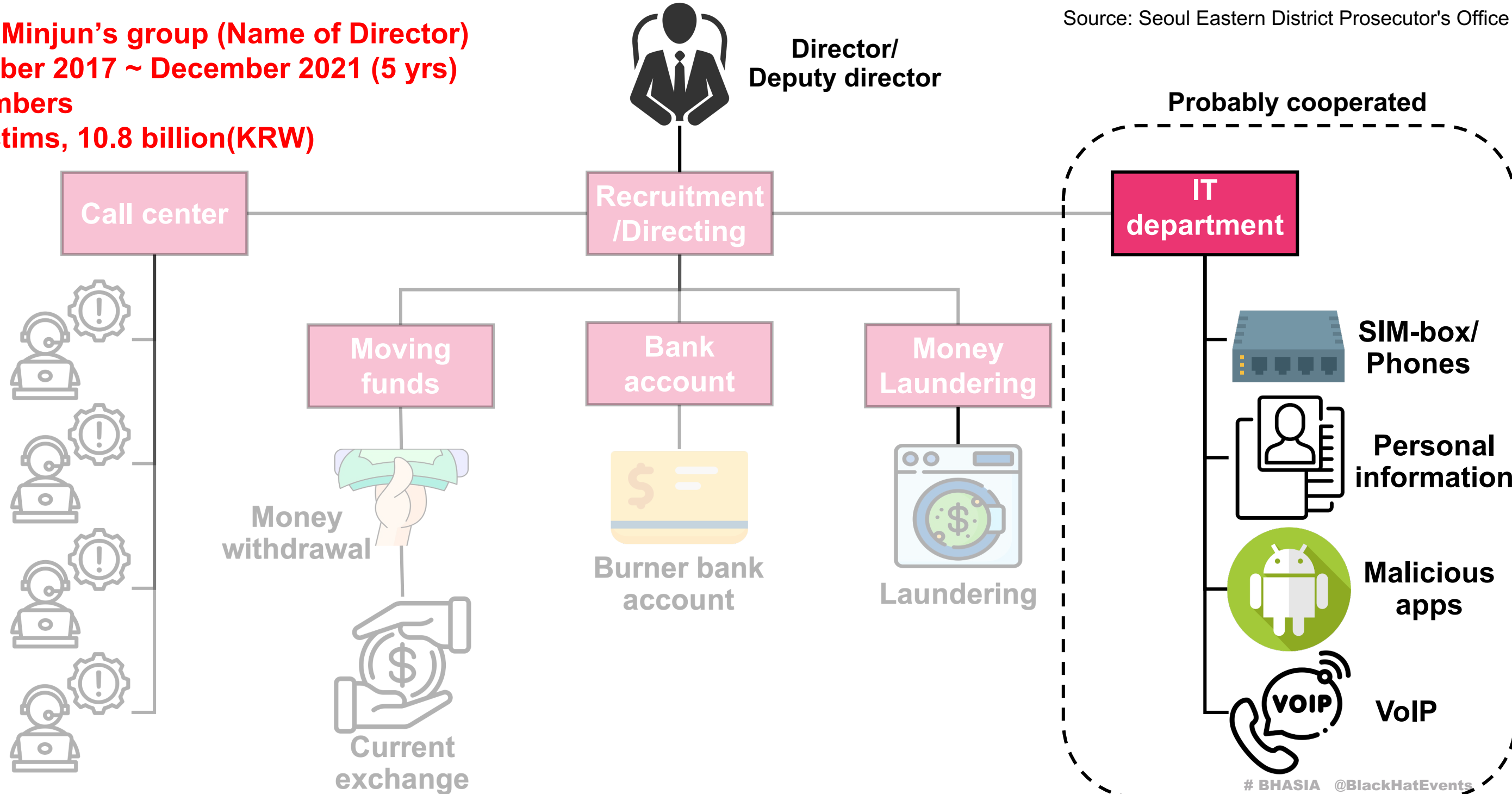


# 2. Overview – Group structure

Source: Seoul Eastern District Prosecutor's Office

- **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

## • Deception Methods

- Account used for criminal activities, investigation required
- Downloading app for proceeding with investigation procedures

Attacker's number

Case documents sent by registered mail but returned

서울중앙지방법검찰청  
(연락처: 010-7498-7745)

분류기호 및 문서번호 3871385 2022. 8. 6

수신 정성환 발신 서울중앙지방법검찰청

제 목 조사자 지명통보

귀하의 계류사건에 대하여 아래와 같이 통보 함

① 사건 번호	2022형제 4235호	
② 고 소 인 성 명	김**박** 외 11명	
피의자	③ 성 명	정성환
(피고소인)	④ 주민등록번호	981211 - *****

⑤ 죄 명 : (1)전자금융거래법위반  
(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 연락요망

⑨ 3차고지 후 불응시 법령에 의거 긴급체포 수시대상으로 전환될수 고지 함

⑩ 고지의 인한 특무조제 182조 3항 에 따라 법적 고지함을 명시합니다

제 무 엇 은

등본상 주거지로 3회 사건서류 등기 송부 해 드렸으나 반송이 되어 부득이하게 통신 고지합니다. 무도자 반송사 항기 관청서도 여라 주시기 바랍니다.

010-7498-7745

발행번호 2-210-2020-49785

서울중앙지방법검찰청  
(연락처: 010-7498-7745)

분류기호 및 문서번호 3871385

수신 [Redacted] 청

제 목 조사자 지명통보

귀하의 계류사건에 대하여 아래와 같이 통보 함

① 사건 번호	2022형제 4235호	
② 고 소 인 성 명	김**박** 외 11명	
피의자	③ 성 명	[Redacted]
(피고소인)	④ 주민등록번호	[Redacted] - *****

⑤ 죄 명 : (1)전자금융거래법위반  
(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 연락요망

⑨ 3차고지 후 불응시 법령에 의거 긴급체포 수시대상으로 전환될수 고지 함

⑩ 고지의 인한 특무조제 182조 3항 에 따라 법적 고지함을 명시합니다

Seoul Central District Prosecutors' Office

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) 카카오뱅크

고객님의 행복한 내일을 응원합니다.  
2021년 마지막 서민신용 대출 상품 안내 드립니다.

문자 수신 고객님께서서는 당사승인 가능대 상자로 선정되어 특별안내 드립니다.

상품요약  
접수마감: 2021년 9월 17일 (선착순)  
대출기간: 12개월 - 120개월 이내 설정가 능  
신청조건: 만 20세 이상 누구나  
대출용도: 머팀목, 생활안정, 대환, 사업 등

승인한도: 최소 1000만원 - 최대 2억원 까지

(연)금리: 1.3 - 3.0 % 내외( 최초 1년간 이자 지역신용보증재단 선택지원)  
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%**

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 &  
opening hours for consultation

(광고) 카카오뱅크

고객님의 행복한 내일을 응원합니다.  
2021년 마지막 서민신용 대출 상품 안내  
드립니다.

문자 수신 고객님께서서는 당사승인 가능대  
상자로 선정되어 특별안내 드립니다.

상품요약  
접수마감: 2021년 9월 17일 (선착순)  
대출기간: 12개월 - 120개월 이내 설정가  
능  
신청조건: 만 20세 이상 누구나  
대출용도: 머팀목, 생활안정, 대환, 사업  
등

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

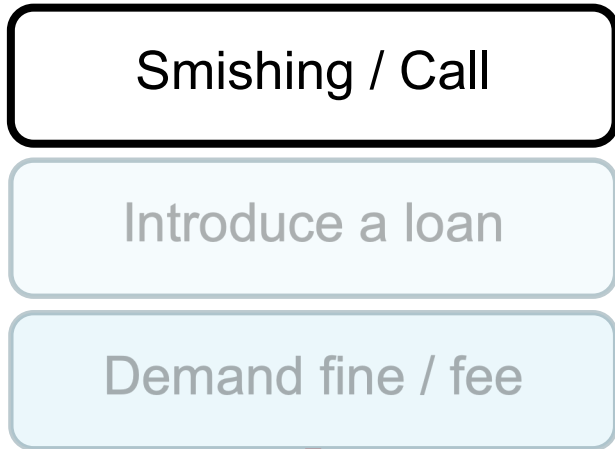
...

상담문의: 02-2647-9861  
상담문의: 02-2647-9861

상담가능시간: 영업일 09:00 ~  
18:00(주말, 공휴일 제외)

# 2. Overview – Attack scenarios

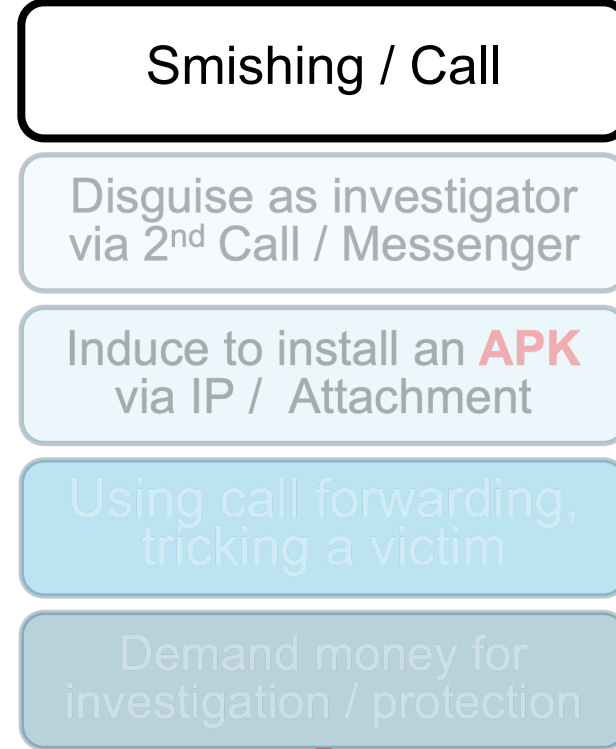
## Loans for repayment



## Impersonation



## Impersonation using APK (Case 1)



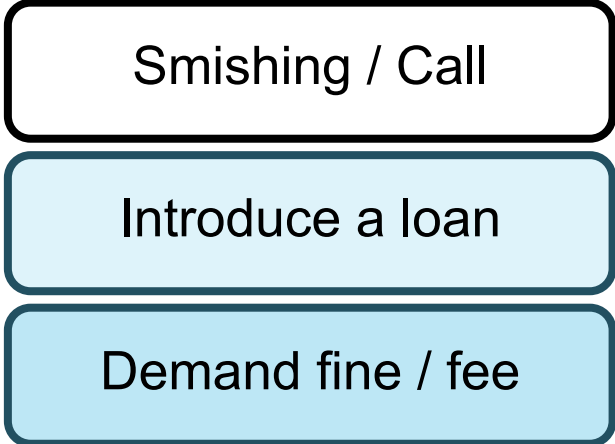
## Impersonation using APK (Case 2)



**Scam / Extortion**

# 2. Overview – Attack scenarios

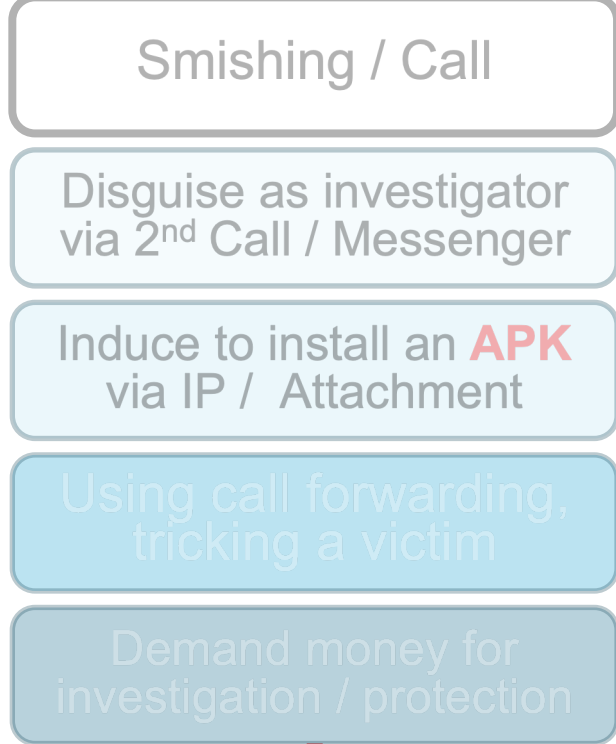
## Loans for repayment



## Impersonation



## Impersonation using APK (Case 1)

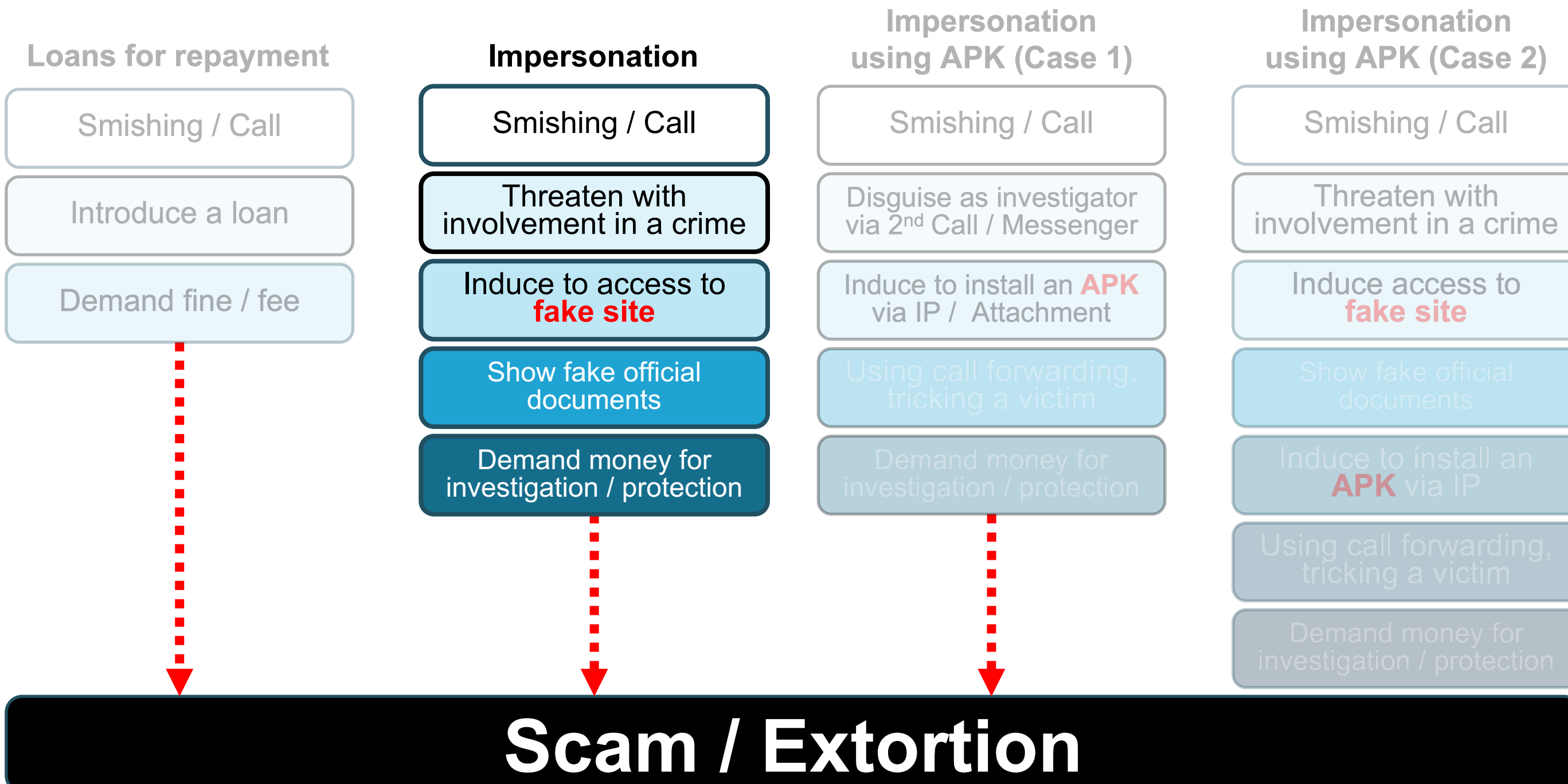


## Impersonation using APK (Case 2)

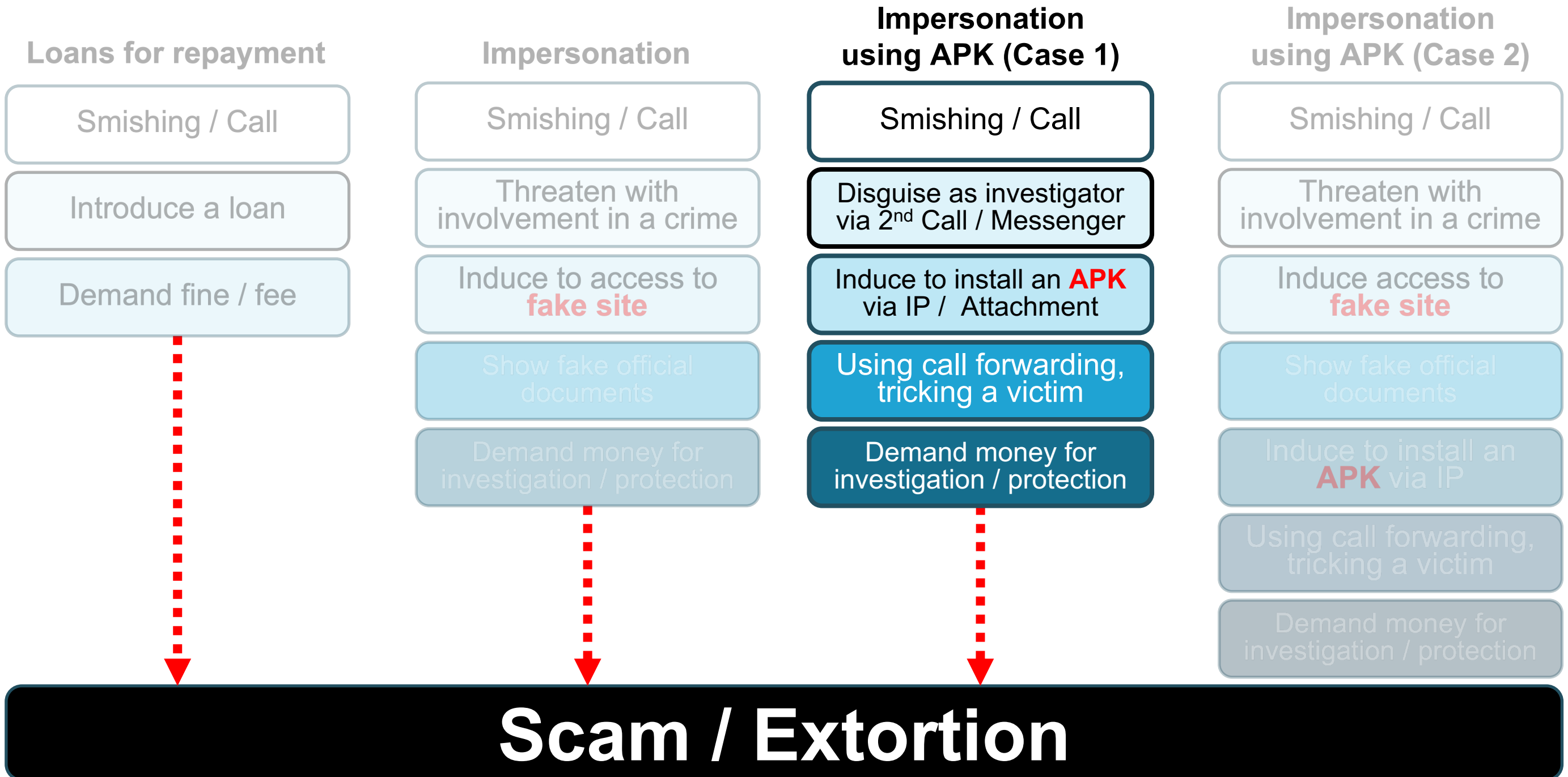


**Scam / Extortion**

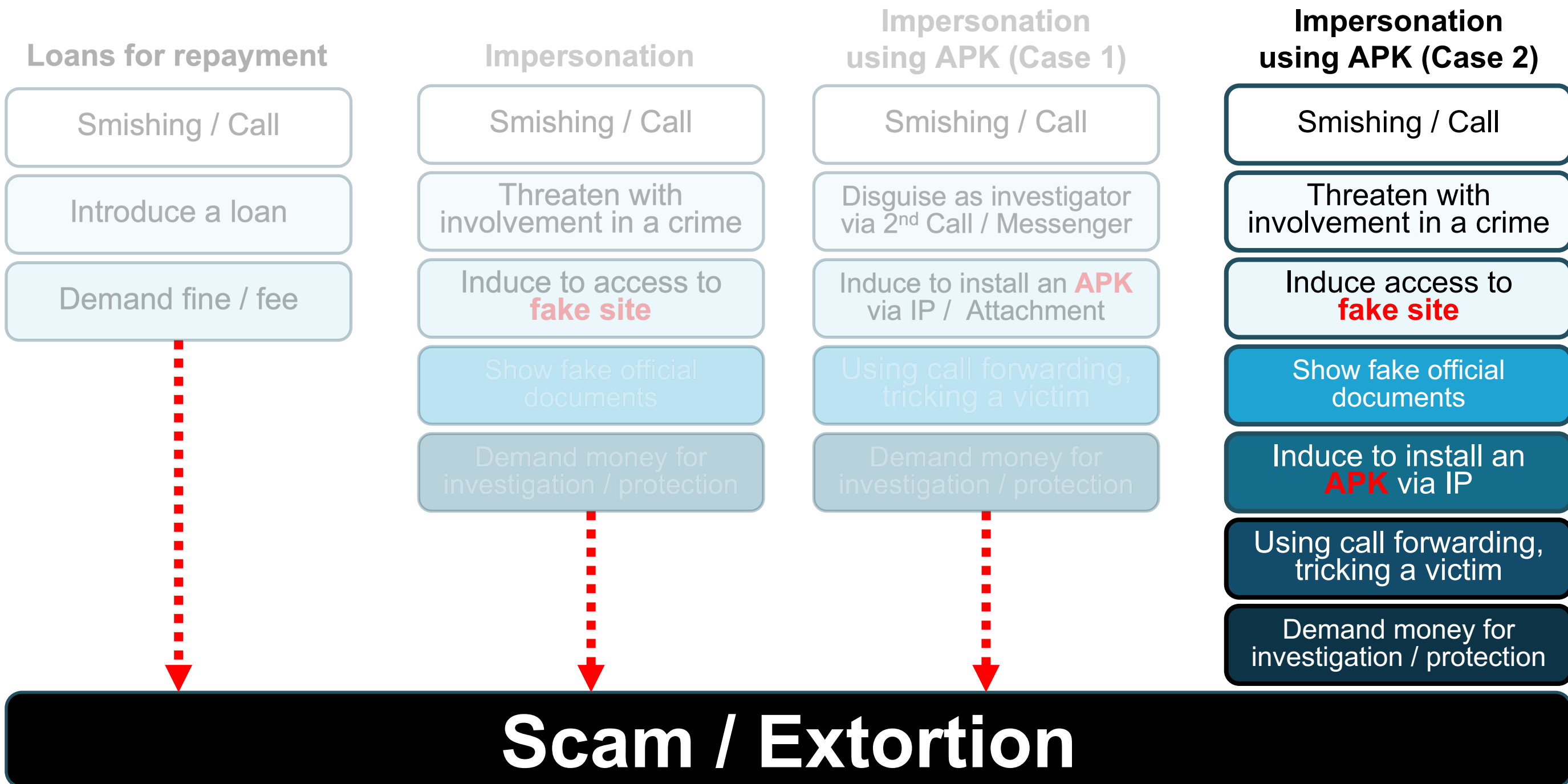
# 2. Overview – Attack scenarios



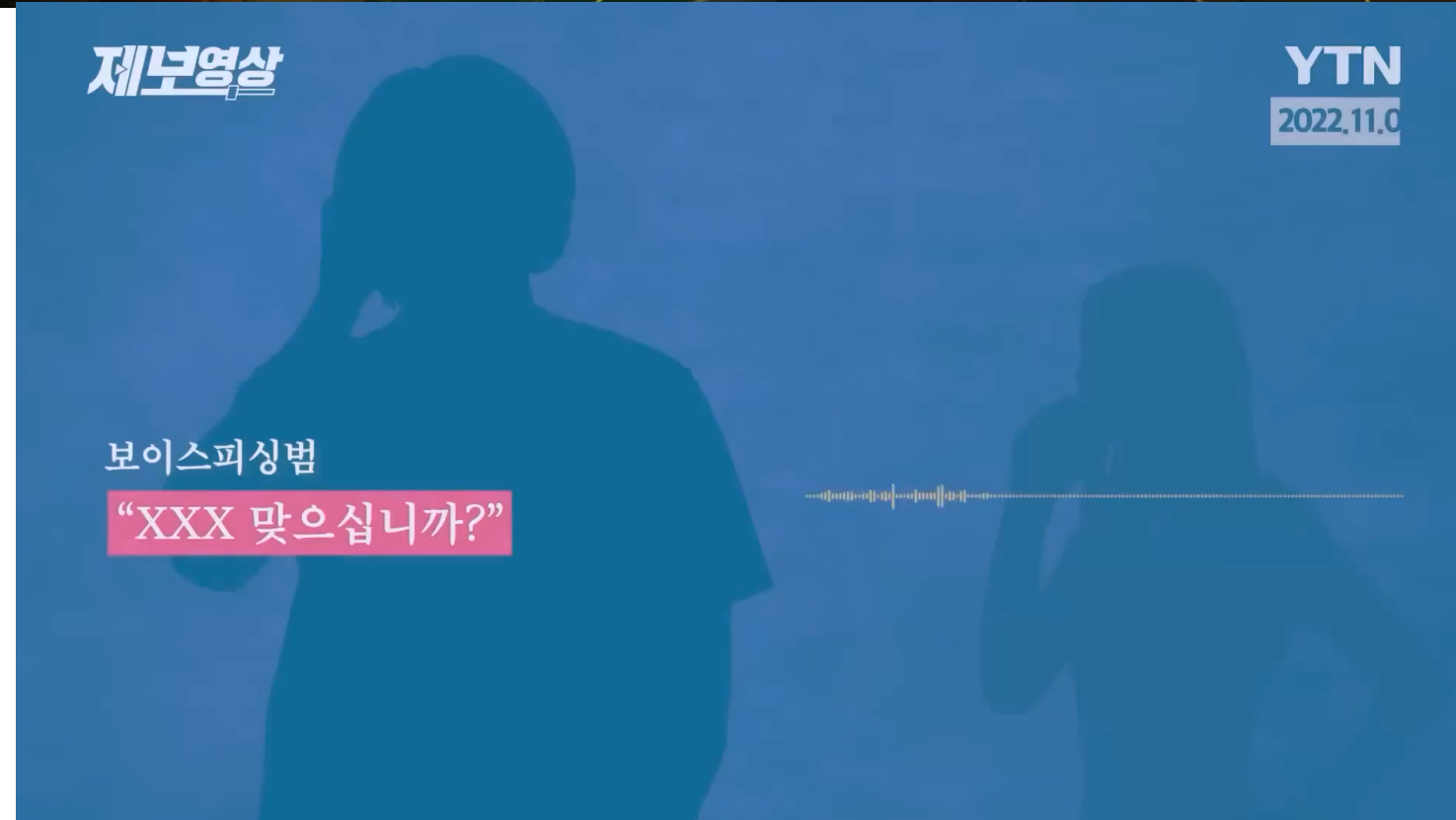
# 2. Overview – Attack scenarios



# 2. Overview – Attack scenarios

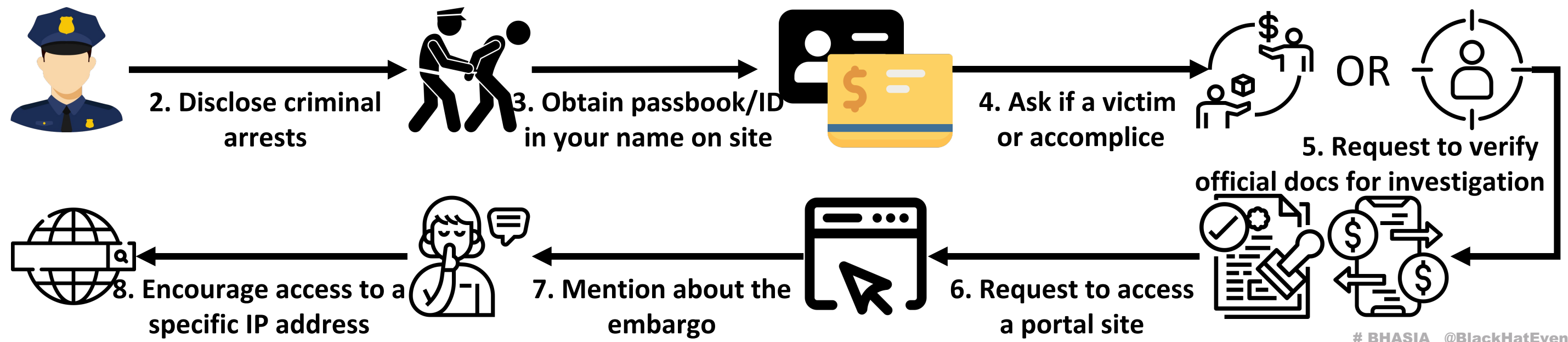


# 2. Overview – Attack scenarios



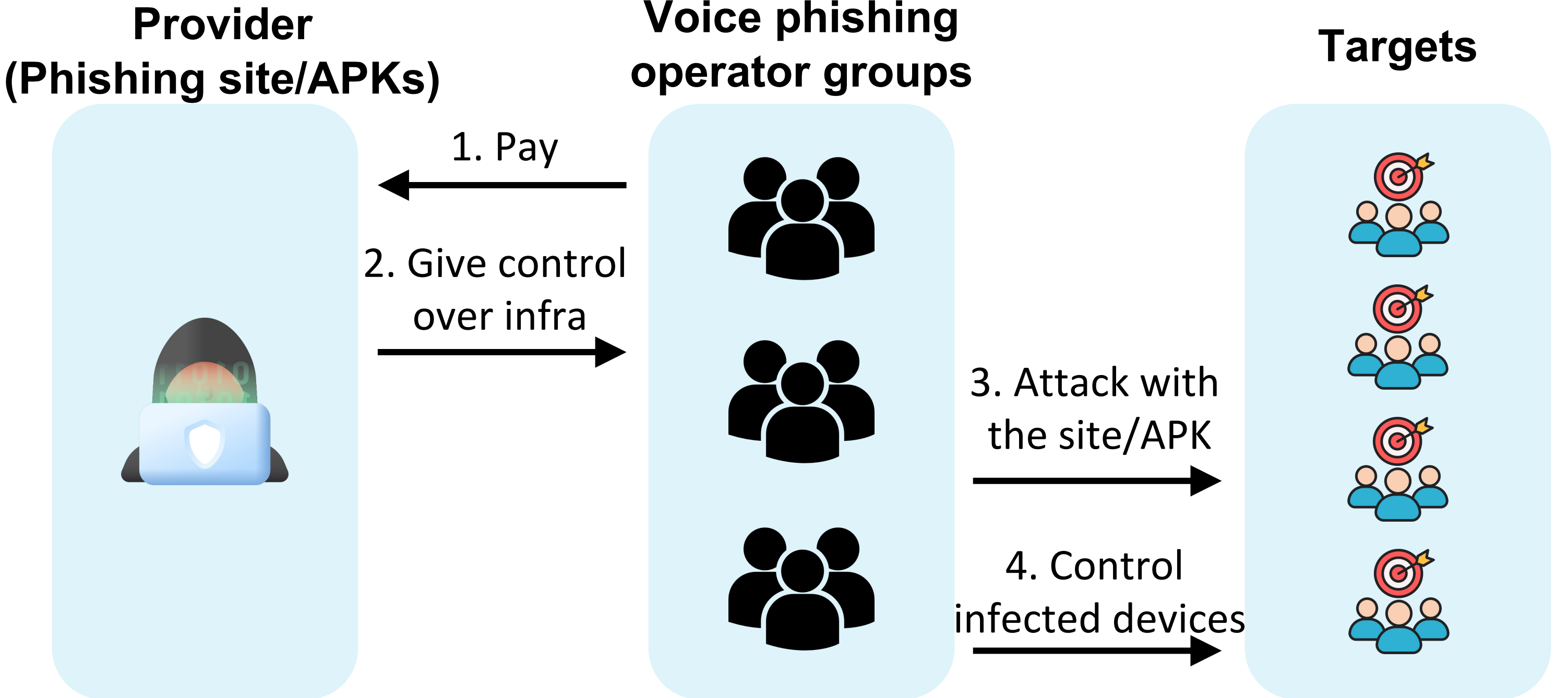
Source: Financial Supervisory Service, YTN

## 1. Introduce as investigator

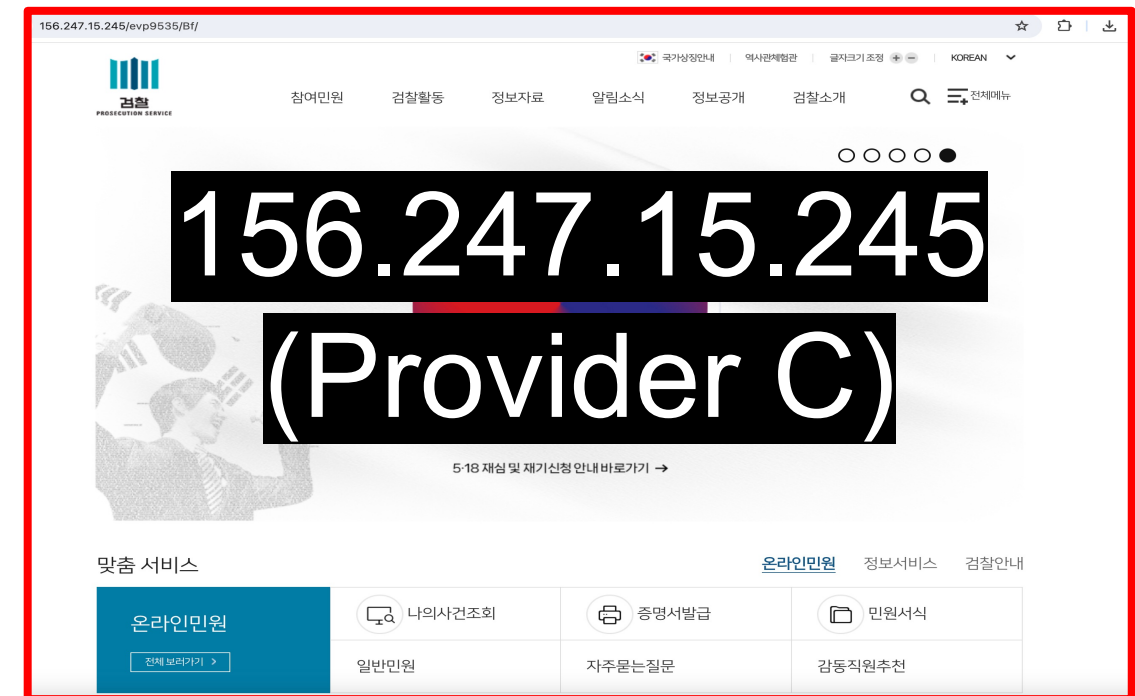
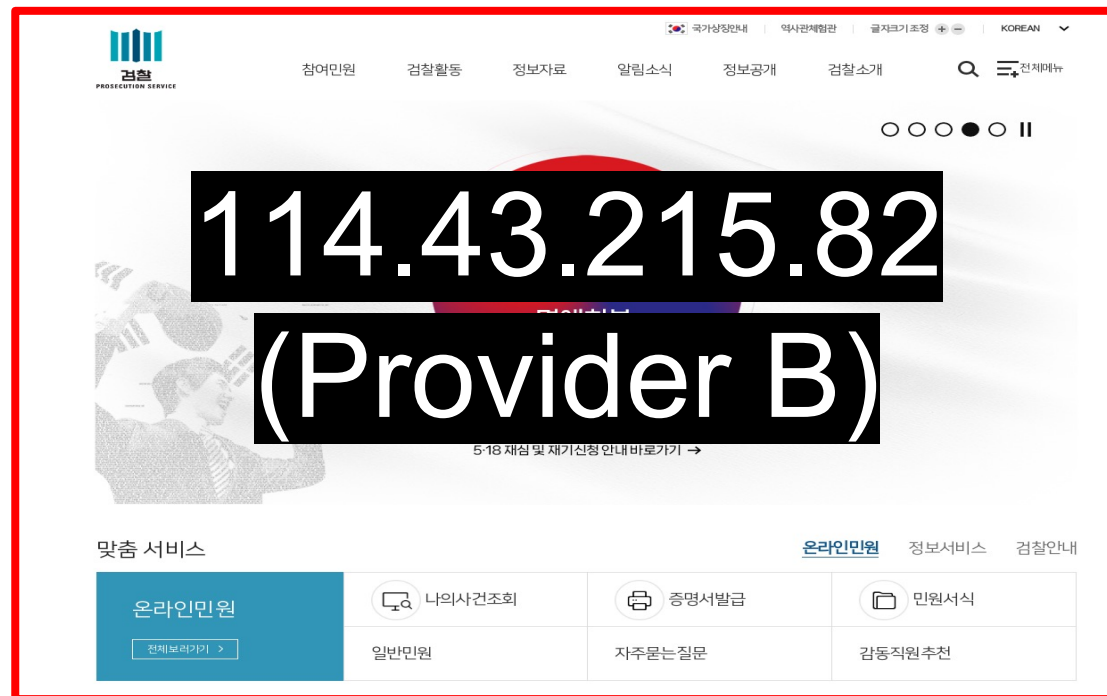
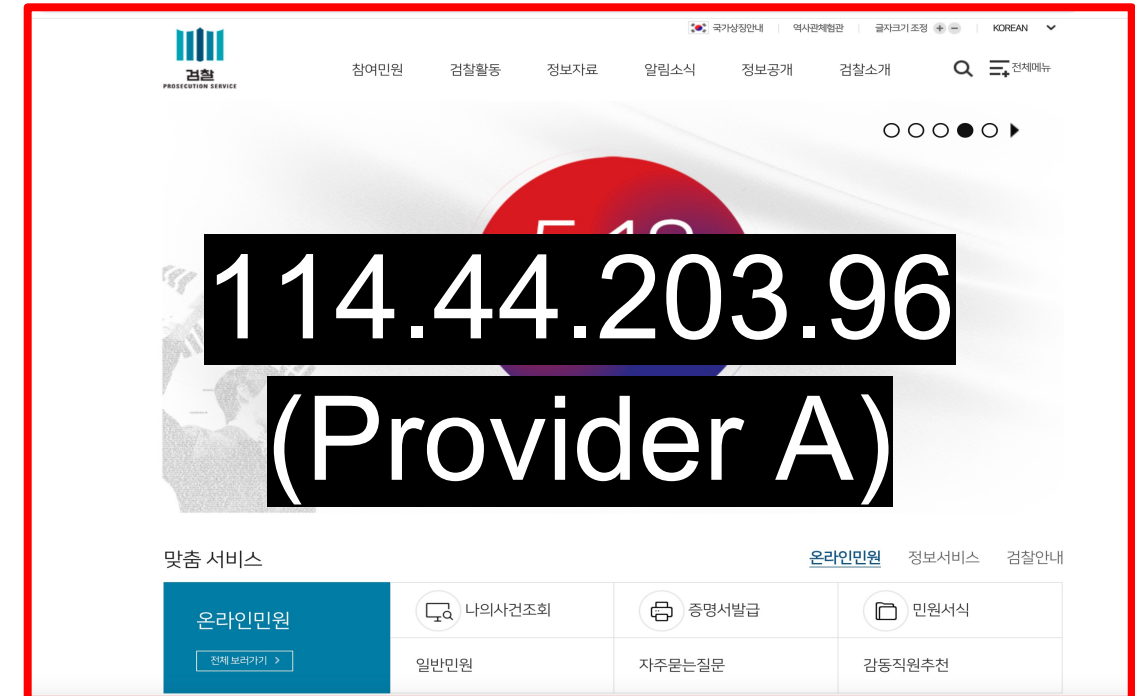


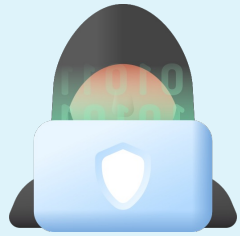
# 3. Attack infrastructure provided as SaaS





- **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)

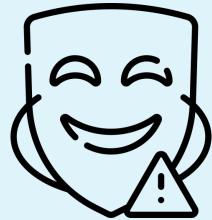




Provider A



AS 3462



(Supreme)



PROSECUTORS' OFFICE

(Seoul)



PROSECUTORS' OFFICE



Official letter, Seizure & Search & Arrest Warrant



SecretCalls

국가장정안내 | 역사관체험관 | 글자크기 조정 + - | KOREAN

참여민원 | 검찰활동 | 정보자료 | 알림소식 | 정보공개 | 검찰소개 | 전체메뉴

000●0▶

5.10

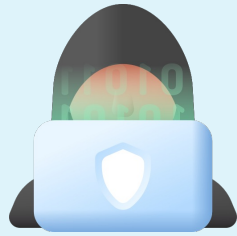
**111.44.203.96**  
**(Provider A)**

5.18 재심 및 재기신청 안내 바로가기 →

맞춤 서비스

온라인민원 | 정보서비스 | 검찰안내

온라인민원 전체 보러가기 >	나의사건조회	증명서발급	민원서식
일반민원	자주묻는질문	감동직원추천	



Provider B



AS 3462



(South)



검찰

PROSECUTORS' OFFICE



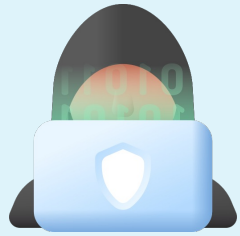
Official letter, Bank Statement,  
Non-Disclosure Agreement,  
Arrest Warrant



SyncCalls

The screenshot shows the homepage of the South Korean Prosecution Service (검찰 PROSECUTION SERVICE). The page features a navigation menu with links for '참여민원' (Participation in Civil Affairs), '검찰활동' (Prosecution Activities), '정보자료' (Information and Materials), '알림소식' (News and Notices), '정보공개' (Information Disclosure), and '검찰소개' (Introduction to Prosecution). A search bar and a '전체메뉴' (Full Menu) button are also present. The main content area displays a large red and blue circular graphic with the IP address '114.43.215.82' and '(Provider B)' overlaid in a black box. Below this, there is a link for '5-18 재심 및 재기신청 안내 바로가기' (Direct Link to 5-18 Re-examination and Re-application Guidance). At the bottom, there is a '맞춤 서비스' (Customized Services) section with a table of services.

맞춤 서비스	온라인민원	나의사건조회	증명서발급	민원서식
	전체보러가기 >	일반민원	자주묻는질문	감동직원추천



Provider C



AS 133199



(Supreme)



Official letter, Arrest Warrant,  
Bank Statement



MalCalls

## (Provider A)

## (Provider B)

## (Provider C)

A-A-FPS-1499587294-000624

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

**대검찰청**  
(Prosecutors'office 2024 no.1357 research)

사건번호 : 제 2023 형제 1357 호  
접수인 : [Redacted]  
안건담당 : 합동수사본부 특별수사팀  
접수일자 : 2024년 03월 03일  
발행일련번호 : 2024-009-1428-349-11-201-01  
협조자법무관 : **박석상**  
급수 : 특급안건

No 010567

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

**서울남부지방검찰청**  
(Supreme Prosecutors' Office)

조사대상 : (-)  
접수일자 : 2024년 03월 02일  
사건번호 : 2023고합3047호  
보안급수 : 특급

No 010567

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

**사건번호:2023조사 7403호**

접수인 : [Redacted]  
접수일자 : 2023년06월10일  
사건번호 : 2023 조사 7403호  
급수 : 특급  
부록 : 아래와같음

형사 제 1부 - 268  
검찰법무관 : **박석상**

**Name of Prosecutor's office with Case number, Target's name, Severity, Date, Registrant,**

**Former Official Prosecutor General's seal**

요지 : 단속 접수인은 2023 형제 1357 호 마약류 관리에 관한 법률 제 10 조 마약 밀반입 및 통관물류 사기 사건에 관련성이 있다는 정황을 확인하였기 때문에 위사건과 사실관계 여부에 대한 거래 추적조사 · 범죄 수익금 환수수사를 받음과 동시에 접수인은 마약 밀반입 또는 통관번호 양도 혐의이거나 명의 도용 피해자라는 것을 본인 스스로 해명 해야 함.

- 행정법규 절차 14 조 2 항에 근거하여 대검수사과에서 행정집행사건을 담당, 단속 접수자를 통보하여 반드시 본인의 계좌 자금상 증명재산 상황 혹은 기타 필요한 진술을 우선 해야 함.
- 본 사건(법률 제 6516 호, 제 7336 호)돈세탁방지법사건, 접수인의 집행명령 시간에 기록된 모든 재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득) 및 재산상황을 국유재산법 제 3 조 제 1 항 및 동법시행령 제 1 조에 의거하여 행정재산으로 분류, 합법적인 재산임을 반드시 증명, 감독 받아야 함.
- 금융법 39 조 3 항에 근거한 합법절차에 의하여 접수인은 계좌추적조치를 통해서 금융실명제의 원칙에 의거하여 본인명의로 모든 합법적인 계좌에 대해 인적 사항 자산이거나 모든 부당한 거래내역을 조회를 하여 투명성을 입증 시켜야 함.
- 단속접수자는 집행명령이 발표된 시간(여상)내에, 만일 본사건의 조사, 집행내용을 제 3 자에게 전하였을 경우(가족, 배우자, 직장동료, 지인 일체포함) 본처에서는 금융법 39 조 17 항 따라서 즉시 본인 명의로 된 재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득) 동결처리(압수수색) 하는 것입니다. 단속보호자는 다른 반대의견이 있어서는 안됩니다.

주무관 **양희진** 행정사무관 **김병현** 합동수사본부 **이원석** 전결 2024.03.03  
시행 합동수사본부-719 접수 입법정책관-317

3. 단속 접수자는 비밀유지 서약서에 따라 본 사건의 조사, 집행 내용을 제3자에게 전하였을 경우 분처 및 관계 기관에서는 공무상 비밀유지 조항에 관한 법규에 의거 구속영장이 집행이 될 수 있음

4. 김\*\* 등 불법자금 은닉 및 업무상 횡령 관련하여 귀하께 다음 자료를 요청하니 다른 반대 의견이 있어서는 안 됨

- 위 대상자에 대한 담당자 지시하에 금융감독원 계좌 추적 관련하여 금융권 방문해야 함
- 위 대상자에 대한 지폐 일련번호, 온라인 화폐 및 국가 안전 코드를 등록해야 함
- 위 대상자에 대한 행정재산으로 분류된 예금, 주식, 현금 및 가상화폐 환수, 검수 조사에 협조해야 함
- 위 대상자에 대한 휴대전화 검열 조치를 의무적으로 시행해야 함 (사이버수사대 주관하에 검열 진행, 개인 정보 유출 확산 방지, 번인도피 및 은닉 또는 증거인멸에 대한 우려)

기안자: 황홍철 (인)  
행정사무장: 김병현 (인)

**이원석** Wonseok

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

요지 : 단속접수자 윤인석 (980102-2352621) 2023 조사 7403 특급 사건 김\*\* 등 전자금융거래법 위반 및 자금 세탁, 불법 명의도용 사건. 개인명의도용 침해신고접수를 받음과 동시에 계좌양도 및 가해혐의거나 개인명의도용 피해자라는 것을 본인 스스로 해명해야함.

- 행정법규절차14조2항에 근거하여, 서울 중앙지검 수사과에서 행정집행사건을담당, 단속접수자를 통보하여 반드시 본인의 계좌자금상증명,재산상황 혹은 기타 필요한 진술을 우선 해야함을 알려드립니다.
- 본사건은 2021년.금융집행 (100001호~100286호) 단속접수자관련돈세탁방지법사건, 단속접수자는 요지에 기록된 시간에 모든재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득) 및 재산상황을 합법적인 재산임을 증명,감독 받아야함.
- 금융법 39조3항에 따라 합법절차에 따라 본인은 계좌추적조치를 통해서 금융실명제의 원칙에 따라서 본인명의로 모든 합법적인 계좌에 대해 인적사항 자산이거나 모든 부당한 거래내역을 조회를 하여 투명성을 입증시켜야함.
- 단속접수자는 집행명령이 발표된시간(여상)내에, 만일 본 사건의 조사, 집행내용을 제3자에게 전하였을 경우(제3자 포함), 본처 및 관계기관(금융감독원)에서는 금융법39조 17항 따라서 즉시 본인명의로된 재산자료(포함한 토지, 주택, 예금, 투자, 입금 및 기타 소득)를 동결처리하는것입니다. 단속보호자는 다른 반대의견이 있어서는 안됩니다.
- 단속접수자는 수사진행과 동시에 휴대기기 검열조치를 의무적으로 시행 해야함. 시행 주요사항)
  - 사이버수사대 주관하에 검열을 진행할 것.
  - 개인정보 유출 확산방지
  - 번인도피 및 은닉 또는 증거인멸, 증거은닉에 대한 우려 등
  - 수사협조 기간내 조사자 신변보호에 관련한 이동경로 및 화면녹화 등
  - 수사협조 진행과 동시에 수사협조 관련 지출내역 발생시 수사협조 비용 지급 됨.

대검찰청총장 **김오수**  
기안자 **황홍철** 과장 **김병현** 대검찰청총장 **이원석**

대검찰청총장 **이원석**

기안자 : 정난희 (인) **정난희**  
사건과장 : 박종만 (인) **박종만**  
검찰조사관 : 김정규 (인) **김정규**



## (Provider A)

## (Provider B)

## (Provider C)

위변조 방지를 바코드입니다.

[집행허가번호 - 77946]

[구속영장번호 - 7946]

대한민국 법원  
Court of the Republic of Korea  
(압수수색 · 구속영장 허가서)

집행대상	사건	전자금융사기, 전기통신금융사기 및 환급에 관한 금융범죄 사기사건	
	성명	[REDACTED]	주민등록번호 [REDACTED]

금융계좌추적 및 압수수색 · 구속영장의 발부의 허가 사유

전자금융거래법 제 10 조(본질과도난책임 동부지법 2014.12.29 개경)에 근거 비록 집행대상자가 개인정보 분실과도난으로 인하여 범죄행위에 적극적으로 가담하지 않았더라도 피고가 개인정보의 관리를 소홀히 하였다 라는 점을 감안하여 사기를 방조했다고 할 것이므로, 민법 제 760 조 3 항에 따라 공동 불법행위자로써 그 손해를 배상할 책임이 있다고 인정하는 바 조사명령서 집행은 허가 하였음을 알려드립니다.

위의 집행대상에 대한 전기통신금융사기 및 환급에 관한 특별법 위반 건에 관하여 2022 형제 1357 호 사건에 관해해외도피 및 증거인멸 요지가 있으므로, 해외출금금지 및 긴급제포명령 허가서가 발부되어 있음을 공지합니다.

<공소사실의요지>

공무상 보안 누설죄 적용대상 (직계가족 포함)

수색, 검증장소	모든 재산 자료 (토지, 주택, 예금, 적금, 입출금, 현금 및 기타소득, 가택수색, 근무처, 주변인물, 압수·수색·검증 및 소환조사)		
적용법령	전자금융거래법 제 49 조(벌칙), 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 48 시간(연장 14 일)

법원주사보	김철기 (인)	대법관인	박상욱 (인)
조사담당검사	김현우 (인)	재판장판사	이수영 (인)

집행불능사유: 없음 • 무혐의자 확정 전까지 위와 같이 처리 하겠습니다.

2024년 03월 03일

법원행정처장 차 한

법원 1/A AA 집행 5-9 /PAGA-77946-KIKE BB02-BE55303310030068SS

주: 일부기각의 경우에는 해당란에 "v" 표시를 한다

Arrest Warrant for Financial Crimes  
Issued by a Korean Court with  
Target's Name & Registration number

Fake account number,  
Detention Center & Period

서울중앙지방법원  
Seoul Central District Court

[拘束令狀]

피고인 ( )은 업무상 횡령 방조, 불법자금 은닉, 전자금융거래법 위반으로 자금이 불투명해져, 사건 유보 가능성이 있으며 도주 가능성이 있다. 위 사건에 관하여 범행에 사용된 계좌(우리은행 1002-200-599\*\*\*\*)에 대하여 인정한 바 피고인의 모든 금융자산을 압수함. 위 내용과 범죄 사실이 일치하므로 구속조사를 명한다.

인치구금할 장소: 서울구치소

발부기관: 서울 서초구 서초중앙로 157 서울중앙지방법원

<집행불능 사유>

위와 같이 처리 하겠습니다

처음으로 다음으로

서울지방법원 구속영장

번호: 2023형제 9821  
사건번호: 2023 조 사 7403호  
사건명: 전자금융거래법 위반및, 불법자금 은닉, 전자금융거래법 위반

[REDACTED] 352621) 은 성매매 특별법, 불법자금 은닉, 전자금융거래법 위반으로 자금이 불투명해져, 사건 유보 가능성이 있으며, 도주 가능성이 있다

[REDACTED] 352621) 은 [REDACTED] 계좌 (우리은행 1002-200-59\*\*\*8)

위 내용을 인정하는바 피고인의 모든 금융자산을 압수 함. 위 내용과 범죄 사실이 일치하므로 구속조사를 명한다.

위 사건에 관하여 피고인을 구속한다.

조사자: [REDACTED]

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

## Transaction History Inquiry Form

(Provider B)

(Provider C)

**거래내역 의뢰 조회표**  
(조회일시 : 2023.11.08 15:32:27)

계좌번호 : 우리은행 1002-200-599\*\*\* (지급정지)  
조회기간 : 2022.02.09 ~ 2023.8.17

담당자 : 이은미 (인)

거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인성명	거래시간
20230502	입금	인터넷입금	150,000	150,000	2576	김도현	165921
20230502	출금	인터넷출금	150,000	0	201710	오종진	200705
20230504	입금	인터넷입금	2,300,000	2,300,000	3937	오미경	110648
20230504	출금	인터넷출금	2,300,000	0	1184	김종호	112238
20230505	입금	인터넷입금	4,650,000	4,650,000	2576	20590880254	173404
20230505	입금	인터넷입금	3,400,000	8,050,000	2576	20590880254	173911
20230505	입금	인터넷입금	7,800,000	15,850,000	2576	20590880254	174627
20230505	출금	인터넷출금	15,850,000	0	209600	김종호	105910
20230507	입금	인터넷입금	23,000,000	23,000,000	263009	전재정	001415
20230507	입금	인터넷입금	37,000,000	60,000,000	263009	전재정	001850
20230607	출금	인터넷출금	60,000,000	0	030546	이명순	001749
20230610	입금	인터넷입금	14,500,000	14,500,000	3990	이민호	171205
20230610	출금	인터넷출금	14,500,000	0	9277	오미경	094040
20230726	입금	인터넷입금	34,000,000	34,000,000	205970	최태경	145222
20230726	출금	인터넷출금	12,000,000	22,000,000	1754	20590890159	160349
20230726	출금	인터넷출금	10,000,000	12,000,000	1754	20590890159	160702
20230726	출금	인터넷출금	8,000,000	4,000,000	1754	20590890159	161859
20230726	출금	인터넷출금	2,000,000	2,000,000	1754	20590890159	162238
20230726	출금	인터넷출금	2,000,000	0	9277	오미경	163324
20230812	입금	인터넷입금	56,000,000	56,000,000	263000	109511451	093000
20230812	출금	인터넷출금	56,000,000	0	1184	김종호	110908
20230827	입금	인터넷입금	12,000,000	12,000,000	013903	배형진	185027
20230827	입금	인터넷입금	8,000,000	20,000,000	006644	박상준	105348
20230827	입금	인터넷입금	27,000,000	47,000,000	004224	김정호	186240
20230827	출금	인터넷출금	47,000,000	0	011090	KIMJINUJO	201547

**거래내역 의뢰 조회표**  
(조회일시 : 2023.11.08 15:32:27)

계좌번호 : 1002-200-59\*\*\*8 (지급정지)  
조회기간 : 2022.02.14 ~ 2023.06.14

담당자 : 이은미 (인)

거래일자	상태	거래구분	거래금액	표면잔액	취급점	입금의뢰인성명	거래시간
20220322	출금	전화이체	85,000	34,500	1184	농협 김종호	112238
20220328	입금	대공통입금	700,000	734,500	2576	20590880254	173404
20220328	입금	대공통입금	900,000	1,634,500	2576	20590880254	173911
20220328	입금	대공통입금	400,000	2,034,500	2576	20590880254	174627
20220328	출금	인터넷출금	2,000,000	34,000	209600	농협 김종호	105910
20220405	입금	전자금융	1,200,000	1,233,300	263009	제일 전재정	001415
20220405	입금	전자금융	500,000	1,732,800	263009	제일 전재정	001850
20220406	출금	전화이체	1,700,000	32,100	030546	농협 이명순	001749
20220413	입금	현금입금	3,000,000	3,031,500	3990	우리 이민호	171205
20220413	출금	인터넷출금	3,000,000	30,900	9277	오미경	094040
20220419	입금	전자금융	5,900,000	5,930,100	205970	모두투어(주)	145222
20220419	출금	대공통출금	950,000	4,979,600	1754	205970890159	160349
20220419	출금	대공통출금	950,000	4,029,100	1754	205970890159	160702
20220419	출금	대공통출금	950,000	3,078,600	1754	205970890159	161859
20220419	출금	대공통출금	950,000	2,128,100	1754	205970890159	162238
20220419	출금	인터넷출금	2,000,000	127,600	9277	오미경	163324
20220505	입금	타행입금	16,000,000	16,127,100	263000	신한 01095154	093000
20220505	출금	전화이체	16,100,000	25,900	1184	농협 김종호	110908
20220517	입금	인터넷입금	1,500,000	1,525,200	013903	배형진	185027
20220518	입금	인터넷입금	1,850,000	3,074,700	006644	박상준	105348
20220518	입금	인터넷입금	270,000	3,344,200	004224	김정호	186240
20220525	출금	인터넷출금	3,340,000	3,600	011090	KIMJINUJO	201547

Account number (Suspended)  
& Inquiry Period

Inspector, Verifier, Recipient


검수자 : 정근식 (인)  
확인자 : 김홍중 (인)  
인수자 : 정준영 (인)

검수자 : 정근식 (인)  
확인자 : 김홍중 (인)  
인수자 : 정준영 (인)







## (Provider B)

Non-Disclosure Agreement

	<b>비밀유지서약서</b>	사건번호	2023고합3047호
		작성일자	2024년 03월 02일

아래와 같이 비밀유지 서약서를 제출합니다.

이원석	박종만	박석삼	김정규
			
검찰총장	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 것임을 서약합니다.
- 조사가 끝난 직후에도 3개월간 사건 내용을 이용하여 유출하거나 범인의 도주, 증거 인멸, 사건 유폐 제3자를 위하여 사용하지 않을 것임을 서약합니다.
- 만일 본인이 상기 3개 항목을 위반할 시에는 공무상 비밀 유지 조항에 관한 법규에 의거 엄중 처벌될 것을 인지했고 서약합니다.

단속접수자 귀하

대검찰청 총장 이원석  
Lee Wonseok

기안자: 황홍철 (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)

경찰청 폴-안티스파이 3.0  
경찰청 생산성  
★★★★★ 7,514

설치

위시리스트에 추가

스파이애플 검사

검사결과

검사결과

검사결과

검사결과

경찰청 폴-안티스파이 3.0의 주요 기능

- 스마트폰에 설치된 스파이애플 검색
- 공식 앱스토어가 아닌 앱을 직접 설치할 때 위험 권한 알림
- 스파이애플 탐지시 선택 삭제

## MalCalls (Provider C)

경찰청 폴-안티스파이 3.0  
경찰청 생산성  
★★★★★ 7,514

설치

위시리스트에 추가

스파이애플 검사

검사결과

검사결과

검사결과

검사결과

경찰청 폴-안티스파이 3.0의 주요 기능

- 스마트폰에 설치된 스파이애플 검색
- 공식 앱스토어가 아닌 앱을 직접 설치할 때 위험 권한 알림
- 스파이애플 탐지시 선택 삭제

## SyncCalls (Provider B)

경찰청 폴-안티스파이 3.0  
경찰청  
3.9 ★  
2만  
500만+  
다운로드

설치

위시리스트에 추가

스파이애플 검사

검사결과

검사결과

검사결과

검사결과

앱 정보

※ 폴-안티스파이 3.0를 이용해 주셔서 감사합니다.

경찰청에서 보이스피싱 등 악성앱을 더욱 효과적으로 차단할 수 있는 '시티즌 코난' 앱을 개발하였습니다.

이에 '폴-안티스파이' 서비스를 종료할 예정(2021. 12. 31.)이오니 '시티즌 코난'을 설치하여 사용하시기 바랍니다.

시티즌 코난 설치 : <https://play.google.com/store/apps/details?id=com.infinigru.police.phishingeyes>

※ 폴-안티스파이 3.0은 공식 구글 스토어 및 통신사 통합 원스토어에서만 배포되고 있습니다. 다른 인터넷 사이트에서 다운로드 받거나 개인적으로 파일을 전송해 설치하는 경우는 사칭 앱이므로 설치하지 마시길 당부드립니다.

최근 타인의 스마트폰의 음성, 문자 메시지, 사진 등을 훔쳐볼 수 있는 기능의 스파이애플이 유통되고 있습니다. 특정인의 개인 사생활을 감시하고 개인정보를 수집하는 불법적인 용도로 사용되고 있어 심각한 피해를 초래하고 있습니다. 이에 경찰청 사이버안전국에서는 '경찰청 폴-안티스파이'를 개발하여 스파이애플 설치 유무를 판단하고 삭제 기능을 제공합니다.

'경찰청 폴-안티스파이 3.0'의 주요 기능

# 3. Infrastructure – Provider A

114.44.203.60 (FAKE)

play.google.com (REAL)

114.44.203.60

경찰청 사이버캡

경찰청

3.6★ 리뷰 3.15천개 50만+ 다운로드 3세 이상

설치 Play 스토어 앱에서 보기 공유 위시리스트에 추가

**앱 지원**

경찰청의 앱 더보기 →

- 고등민원24(이파인) 경찰청 2.4★
- 스마트국민제보 경찰청 1.5★
- 안전Dream - 아동·여성·장애인경찰지원센터 경찰청 3.3★
- LOST112 경찰 로스트112 경찰청 2.9★
- 경찰 민원 모바일 경찰청 1.5★
- 폴케어(PolCare2) 경찰청 1.7★

앱 정보 →

□'경찰청 사이버캡'의 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

play.google.com/store/apps/details?id=kr.go.police.cybercop

경찰청 사이버캡

경찰청

3.6★ 리뷰 3.15천개 50만+ 다운로드 3세 이상

설치 공유 위시리스트에 추가

**앱 지원**

경찰청의 앱 더보기 →

- 고등민원24(이파인) 경찰청 3.1★
- 스마트국민제보(2024.4.20. 운영중단 예정) 경찰청 1.7★
- 안전Dream - 아동·여성·장애인경찰지원센터 경찰청 3.1★
- LOST112 경찰 로스트112 경찰청 2.9★
- 경찰 민원 모바일 경찰청 1.5★

앱 정보 →

□'경찰청 사이버캡'의 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)

play.google.com (REAL)

114.44.203.238

Google Play

## 피싱아이즈(라이트)

Infinigr Corporation

4.3★  
리뷰 3.15천개

50만+  
다운로드

3세 이상

설치

Play 스토어 앱에서 보기

공유

위시리스트에 추가

앱 지원

Infinigr Corporation의 앱 더보기

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

앱 정보

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

업데이트 날짜  
2022. 6. 2.

라이프스타일

play.google.com/store/apps/details?id=com.infinigr.lite.phishingeyes&hl=en\_US

Google Play

## 피싱아이즈 - 보이스피싱, 피싱차단, 스미싱, 시티즌코난

(주)인피니그루

3.5★  
408 reviews

100K+  
Downloads

Rated for 3+

Install

Share

Add to wishlist

App support

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

Similar apps

- 착한 의사-건강검진 예약부터 검진결과조회, VIVA INNOVATION 4.7★
- V3 Mobile Security Anti-Virus AhnLab Inc. 4.6★
- NH올원뱅크 NH농협은행 4.1★

About this app

피싱아이즈는 경찰청 및 제휴된 금융사와 다양한 유형의 피싱에 대해 실시간으로 공동 대응함으로써, 피싱범의 4대 현혹 행위(악성 앱, 원격제어 앱, 문자, 카카오톡)와 5대 갈취 채널(APP, WEB, ARS, ATM, 창구)로부터 보이스피싱을 예방하는 국내 유일의 '보이스피싱 민관 공동 대응망 서비스'입니다.

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

Updated on  
Jan 25, 2024

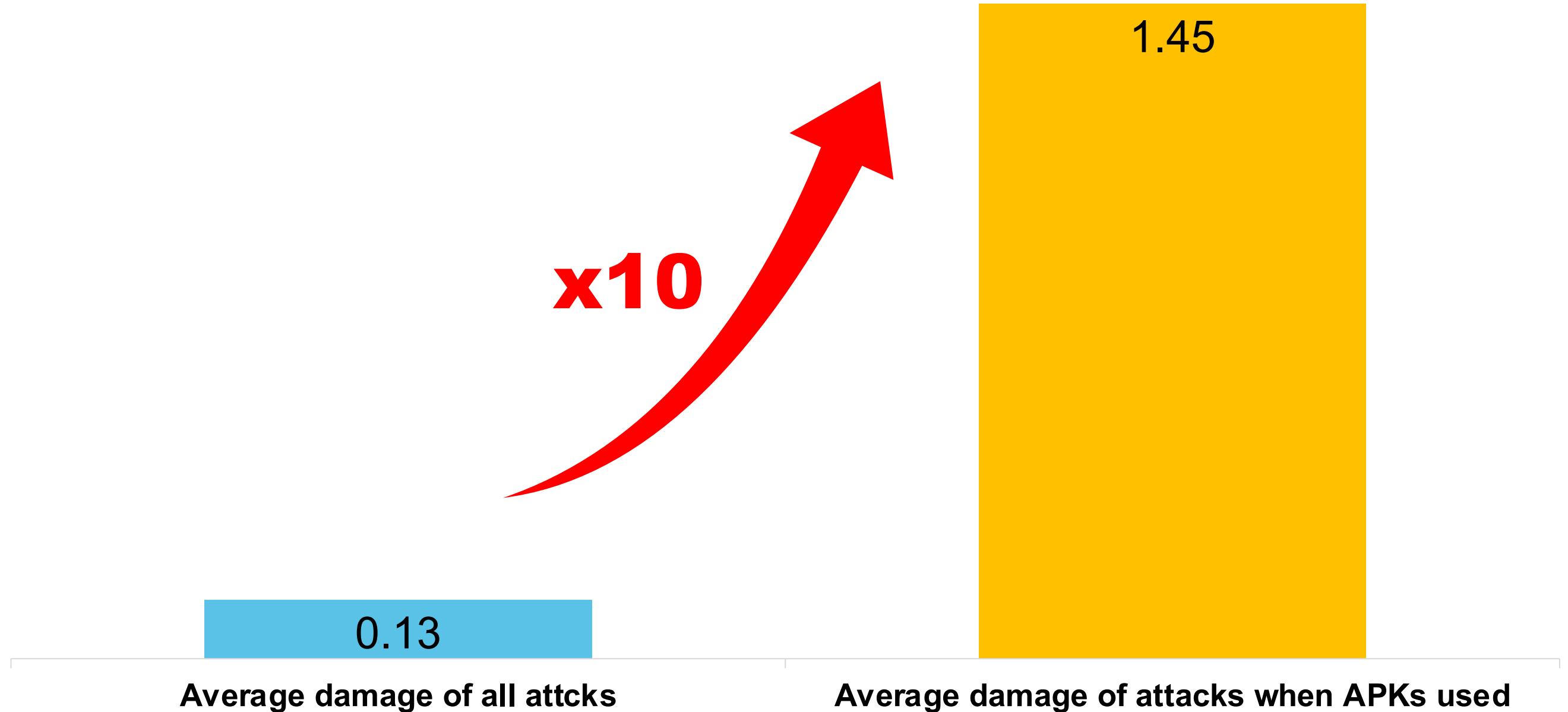
Tools

# 4. SecretCalls

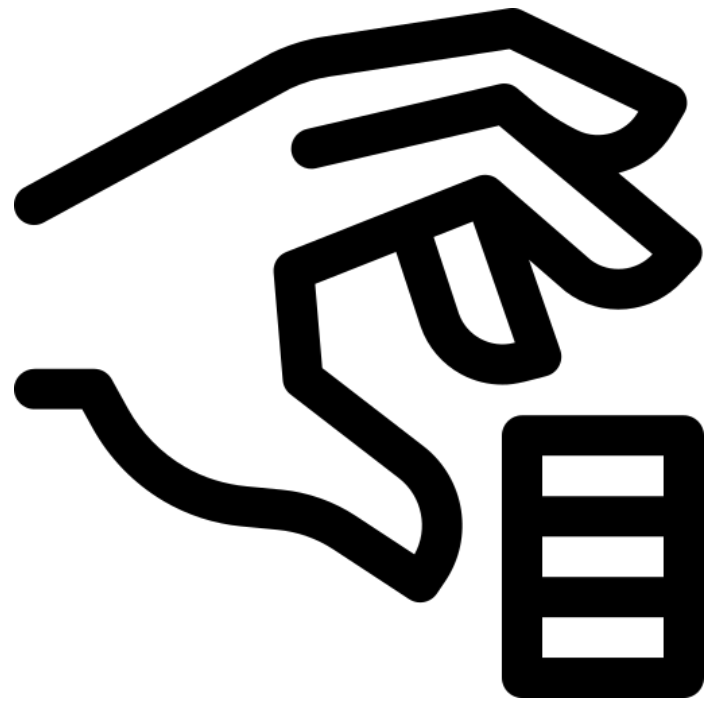
## 2019 Average damage per attack

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

Source: Board of Audit and Inspection of Korea



# 4. SecretCalls – Common VP Actions



**Data theft  
(photos, privacy)**

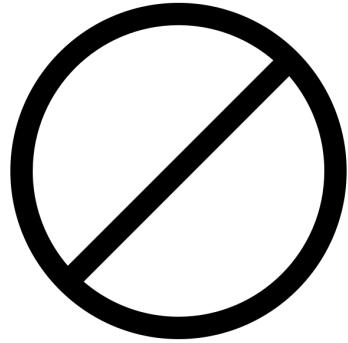


**Surveillance**



**Call redirect**

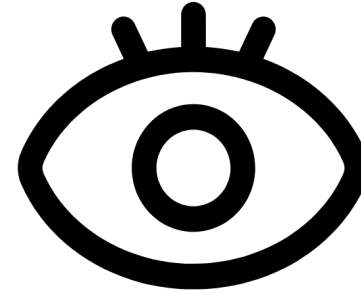
# 4. SecretCalls – Overview



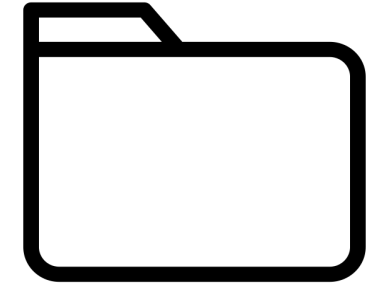
**Anti  
Decompile**



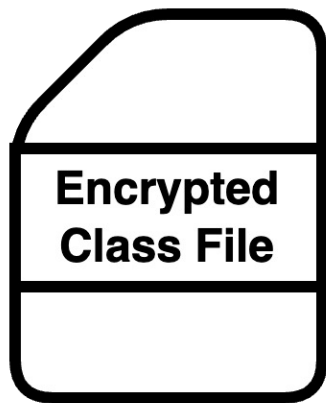
**Call  
Forwarding**



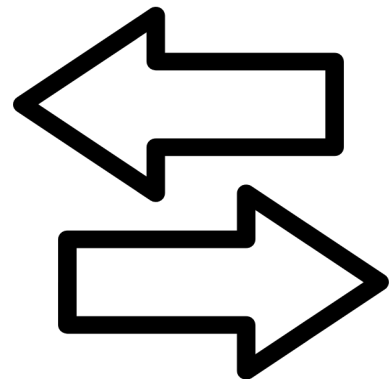
**Surveillance**



**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	<b>SecretCalls</b>	Police, Anti-virus, Banking	secret-classes[Num].dex kill-classes[Num].dex black-classes[Num].dex	libdn_ssl.so libbbed.so libset.so	AES-128-ECB	Hardcoded in DEX, Hardcoded in Lib, Get from Reddit	- postVal={data} - a{timestamp}={data}
2	<b>MalCalls</b>	Banking, Police, Anti-virus, Agency, E-commerce	obfdex[Num].dex obk[Num].dex	libbaiduprotect_sec_jni.so	AES-256-ECB	Google Drive	- /api/user/ping_server - /api/user/get_extra_message - /api/user/get_limit_phone_number
3	<b>SyncCalls</b>	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	<b>RcCalls</b>	Banking	classes1.dex	libopenssl.so	AES-128-ECB	Hardcoded in DEX	- {WebSocket}
5	<b>KKvoice</b>	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
frFlags	0	6h	2h	ushort
frCompression	17185	8h	2h	enum COMPTYPE...
frFileTime	10:03:54	Ah	2h	DOSTIME
frFileDate	07/04/2048	Ch	2h	DOSDATE
frCrc	B8BE7ADh	Eh	4h	uint
frCompressedSize	827850752	12h	4h	uint
frUncompressedSize	1245184	16h	4h	uint
frFileNameLength	0	1Ah	2h	ushort
frExtraFieldLength	28225	1Ch	2h	ushort

**1. Compression Method**

frCompression

17185

8(Deflate)

**2. Timestamp**

frFileDate

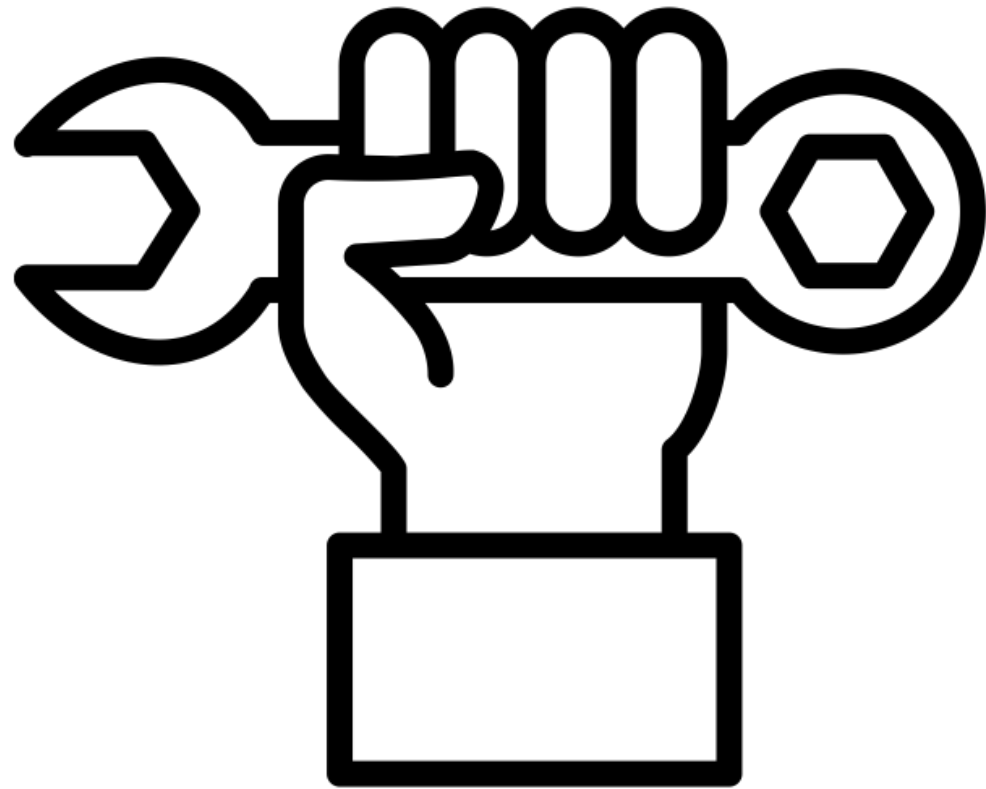
07/04/2048

07/04/2024

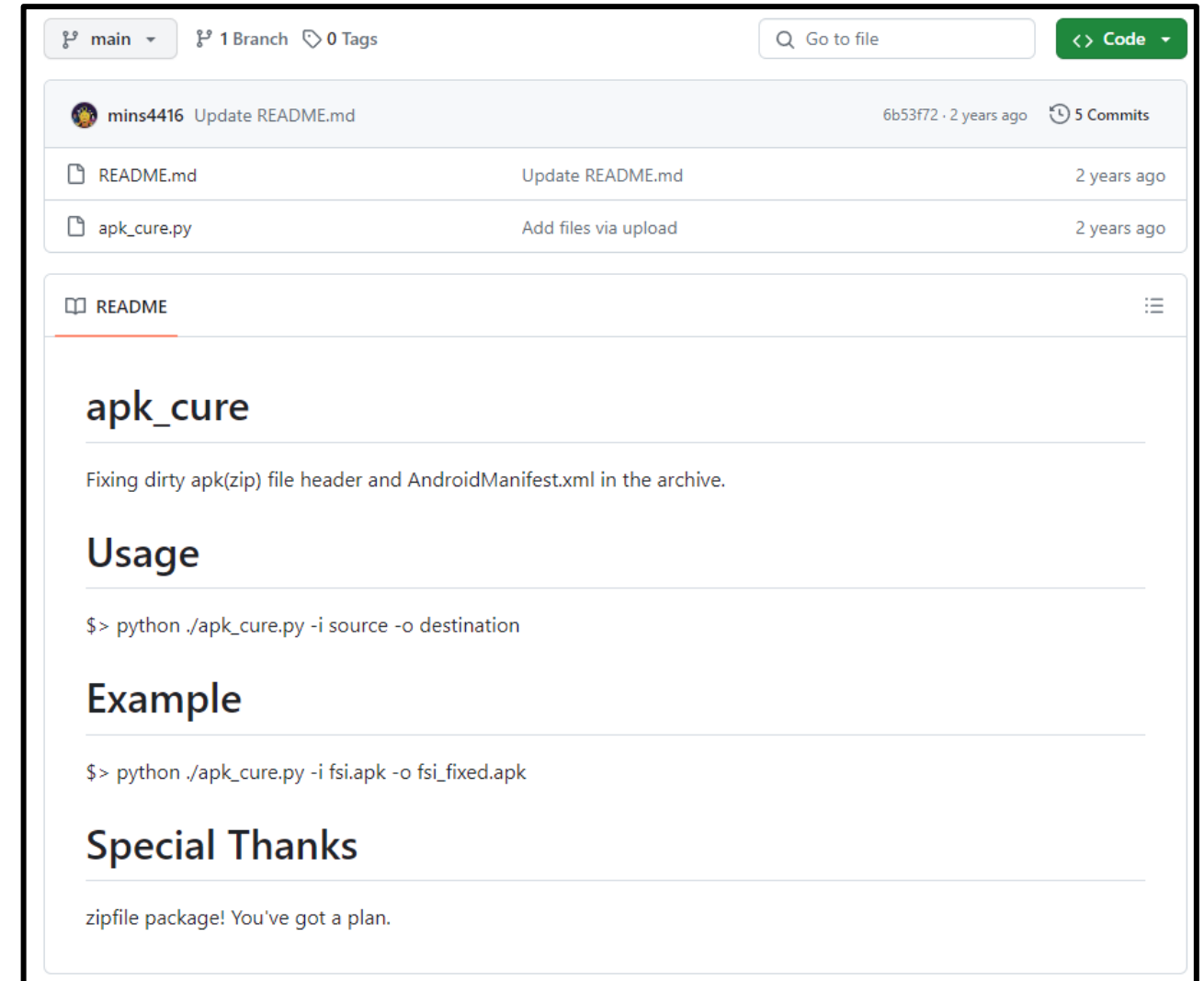
frCompression: 17185 is not valid, we can fix it to 8(Deflate)

frFileDate: Not so far from now

# 4. SecretCalls – Anti decompile

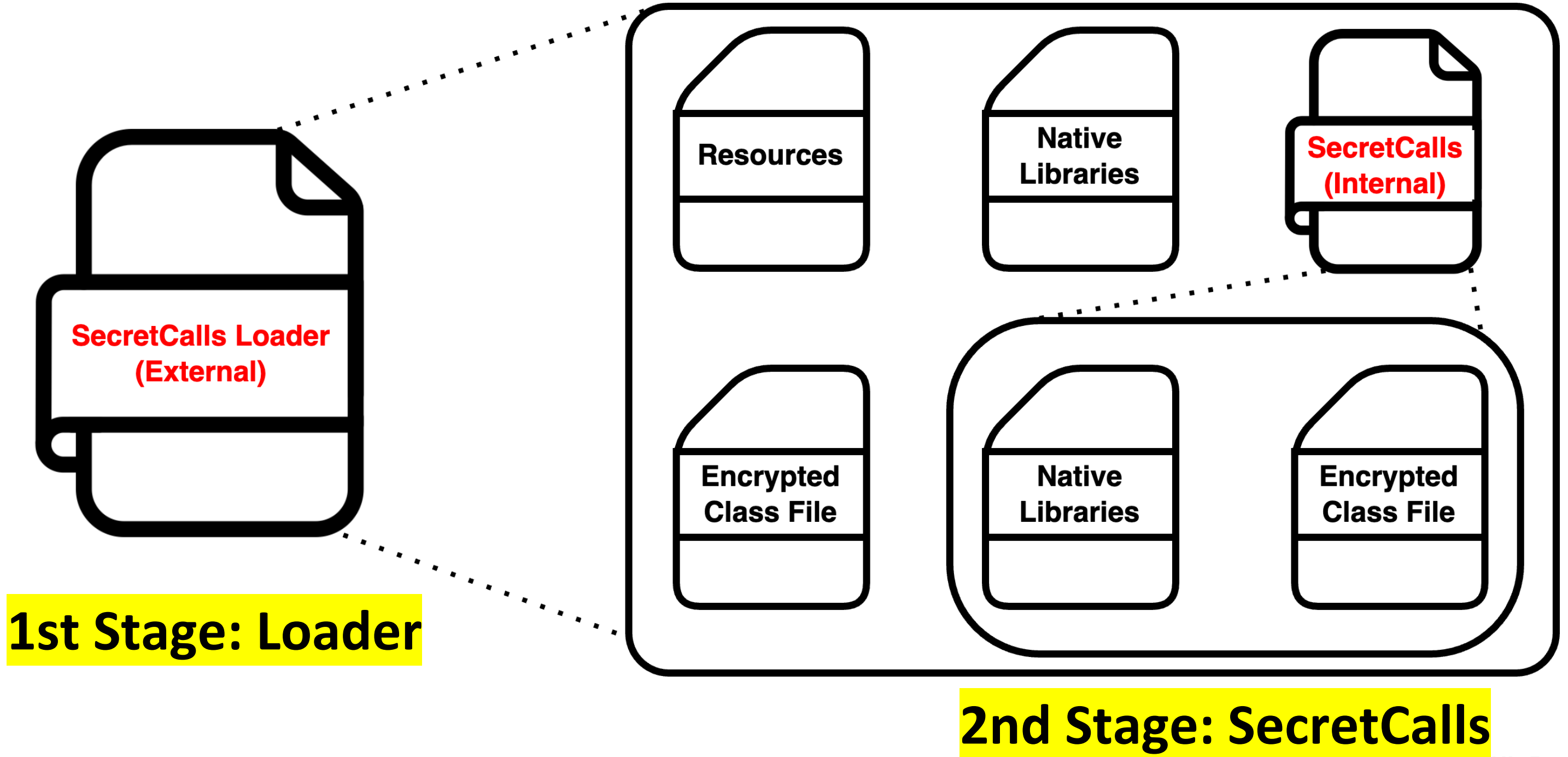


**Fix header manually**

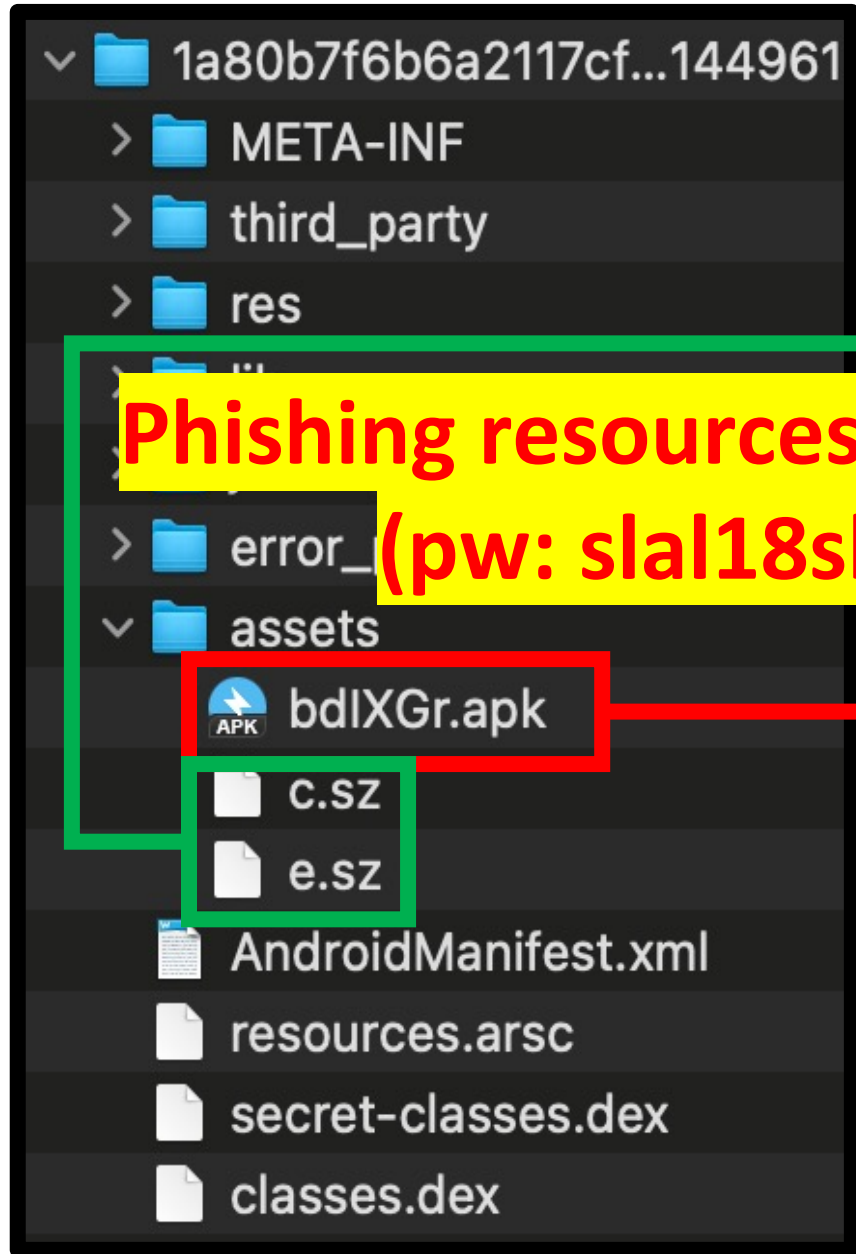


**Use open Source**  
 **mins4416**

# 4. SecretCalls – File Structure

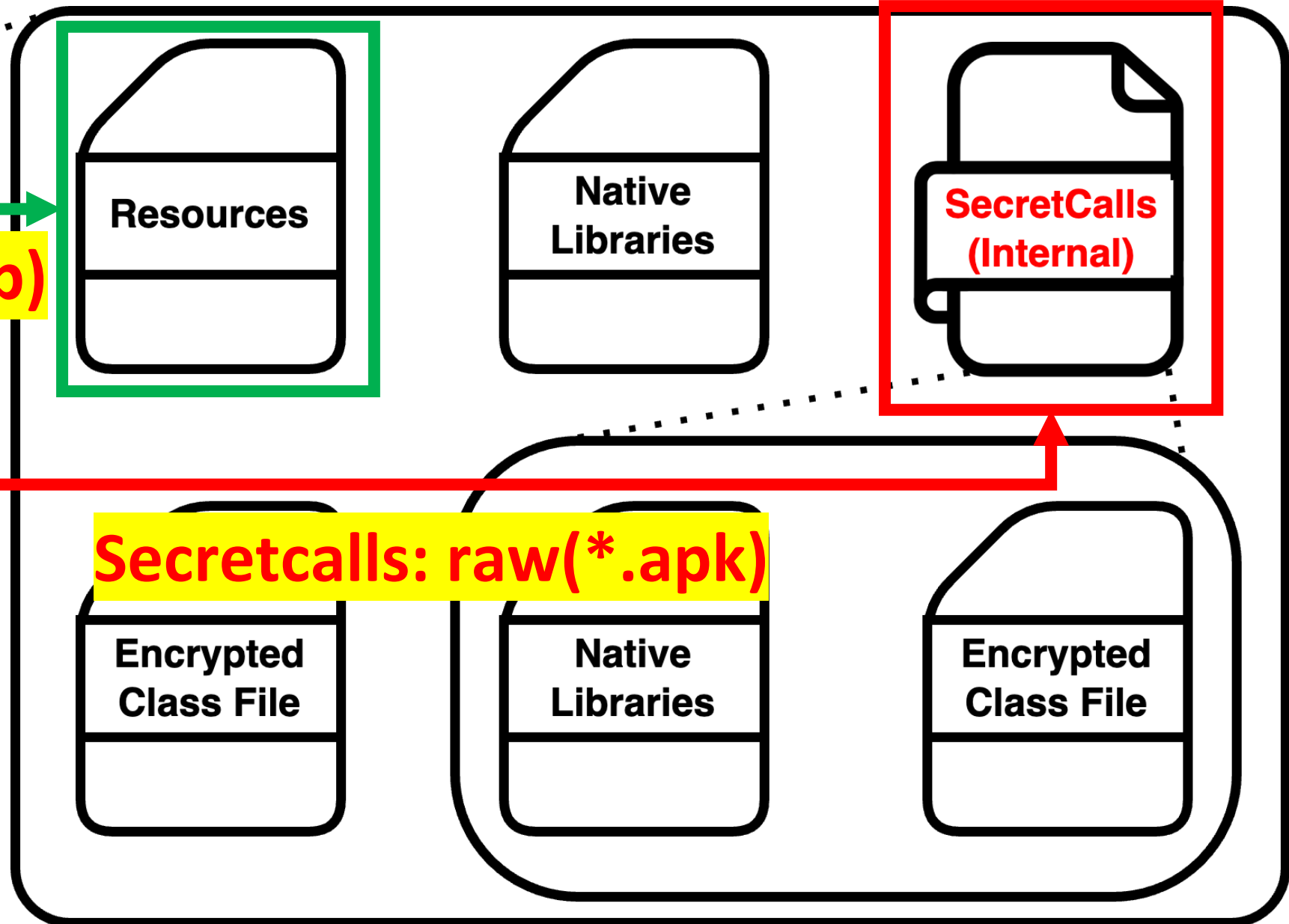


# 4. SecretCalls – File Structure (1)



Phishing resources: \*.sz(zip)  
(pw: slal18sha)

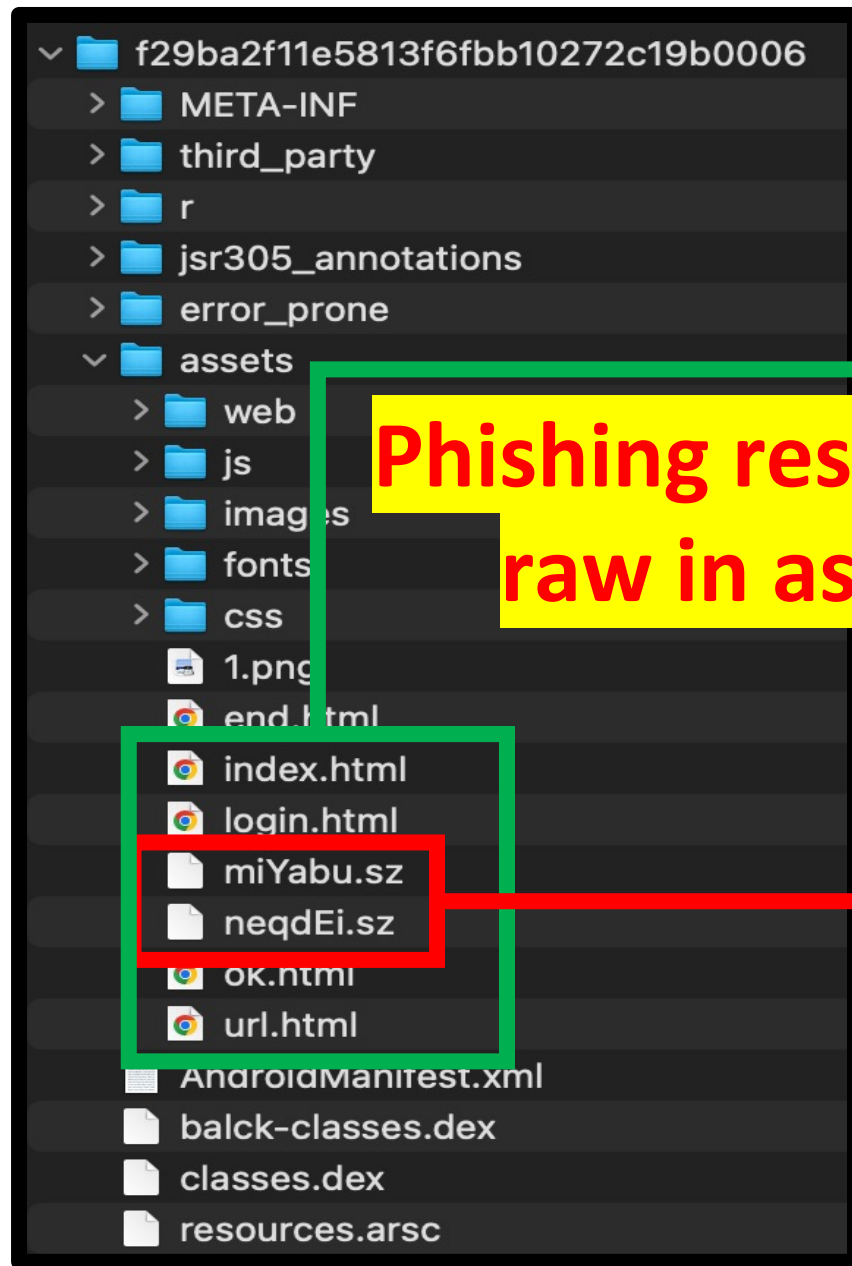
Secretcalls: raw(\*.apk)



SecretCalls Loader

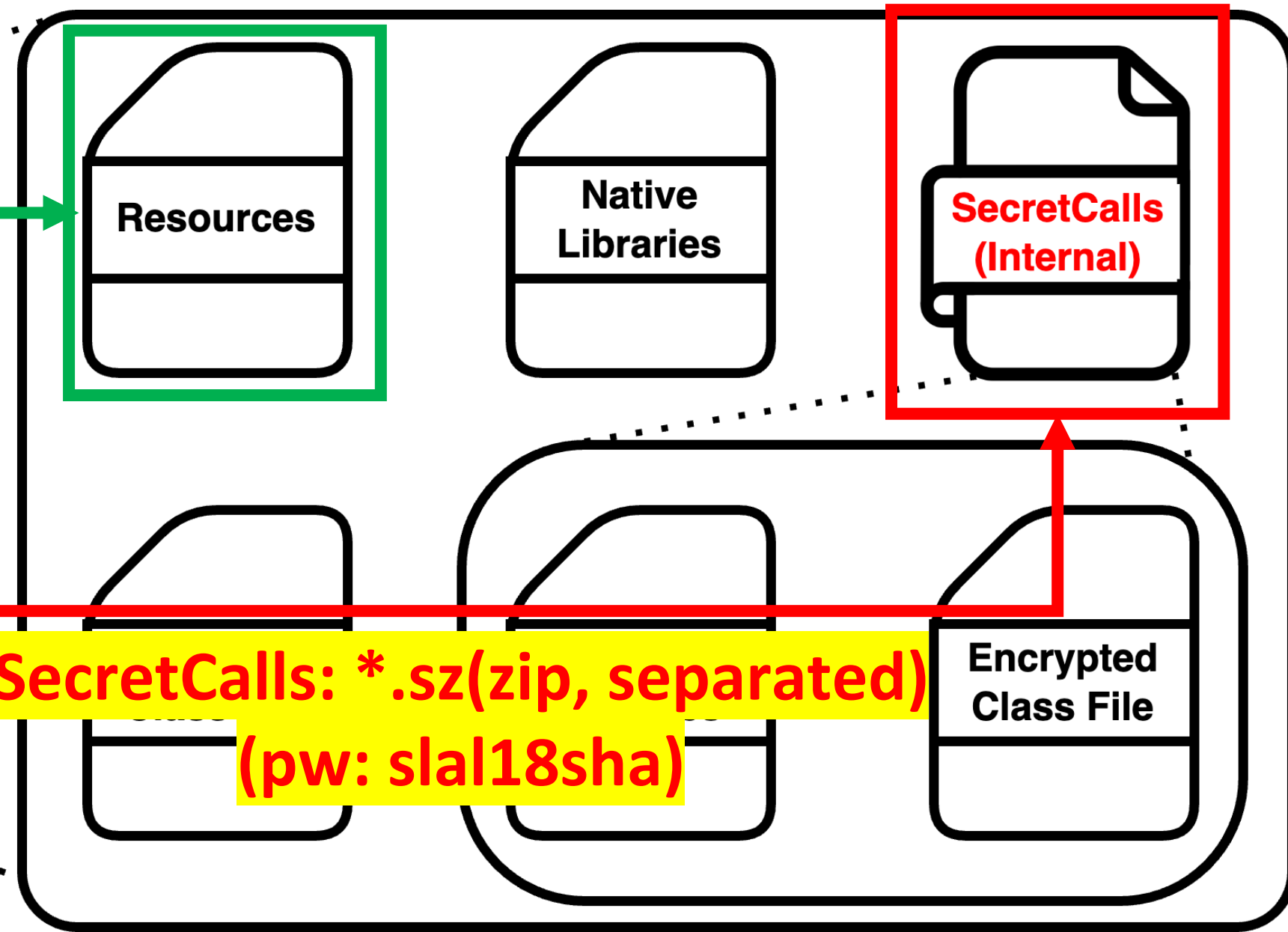
\*slal18sha: Korean profanity(moxxer fxxer)

# 4. SecretCalls – File Structure (2)



Phishing resources:  
raw in assets

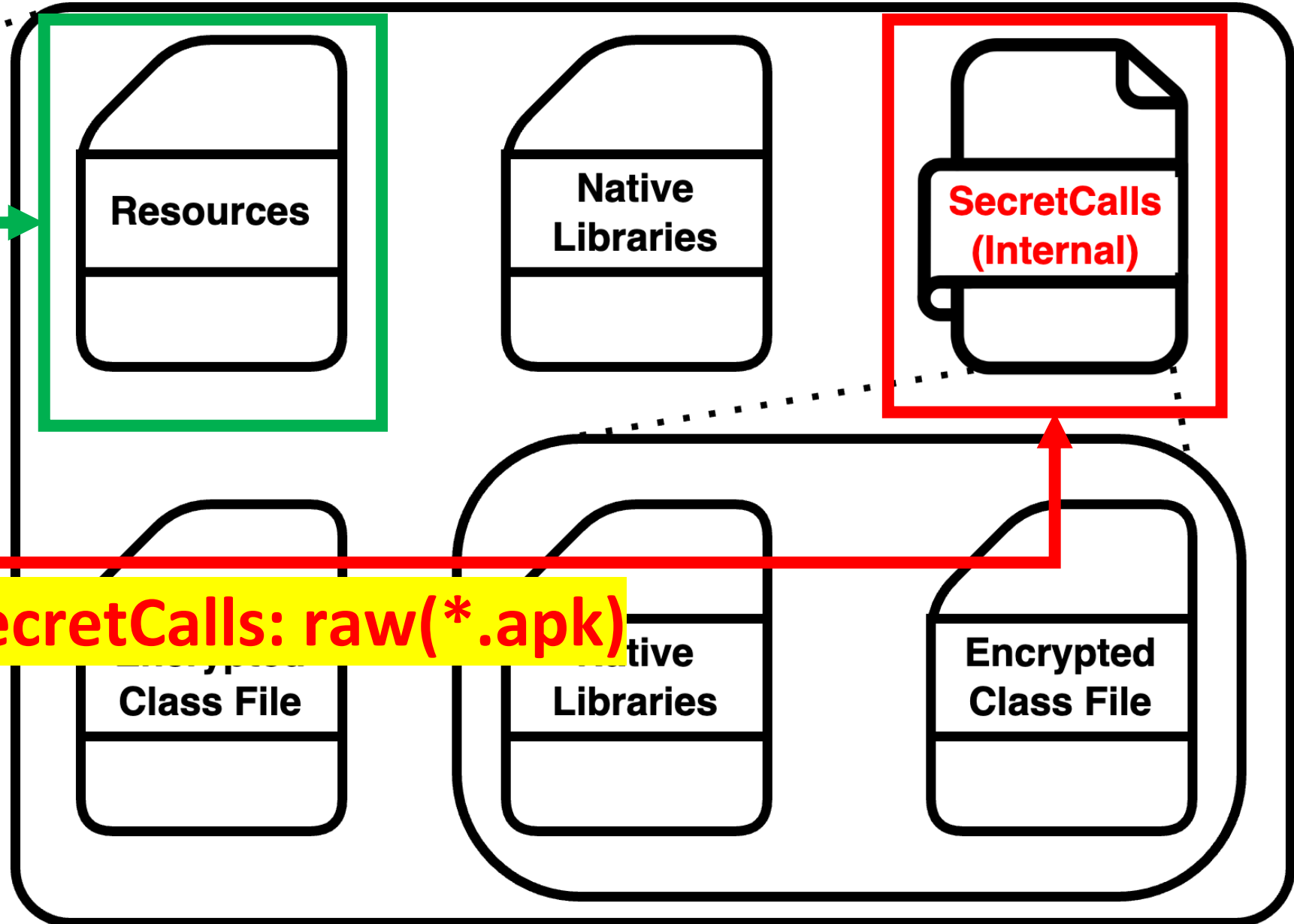
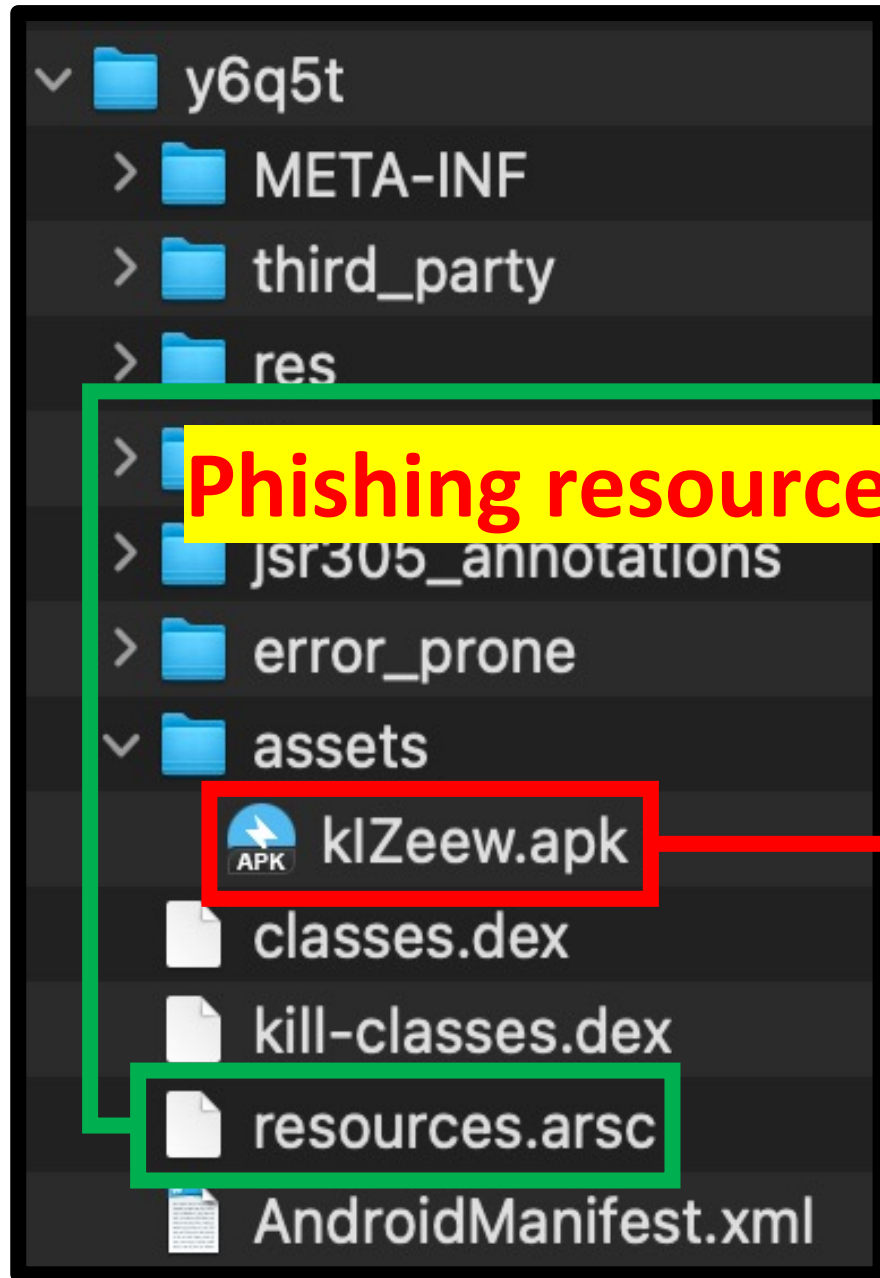
SecretCalls: \*.sz(zip, separated)  
(pw: slal18sha)



SecretCalls Loader

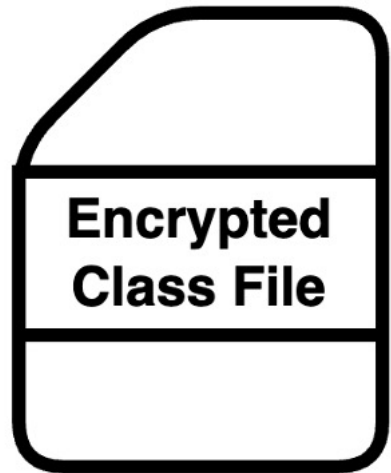
\*slal18sha: Korean profanity(moxxer fxxer)

# 4. SecretCalls – File Structure (3)



SecretCalls Loader

# 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**

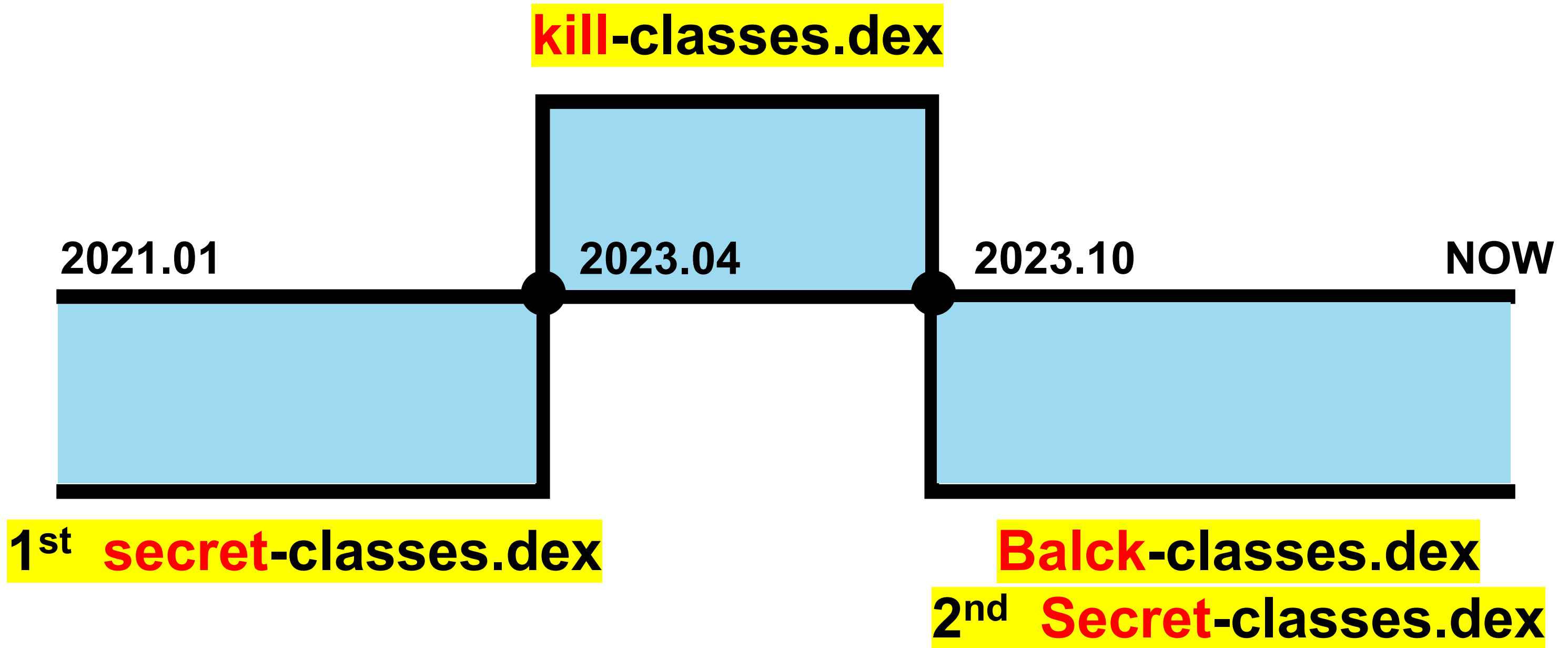
**secret-**  
**classes.dex**

**kill-**  
**classes.dex**

**balck-**  
**classes.dex**



# 4. SecretCalls – Encrypted Class file



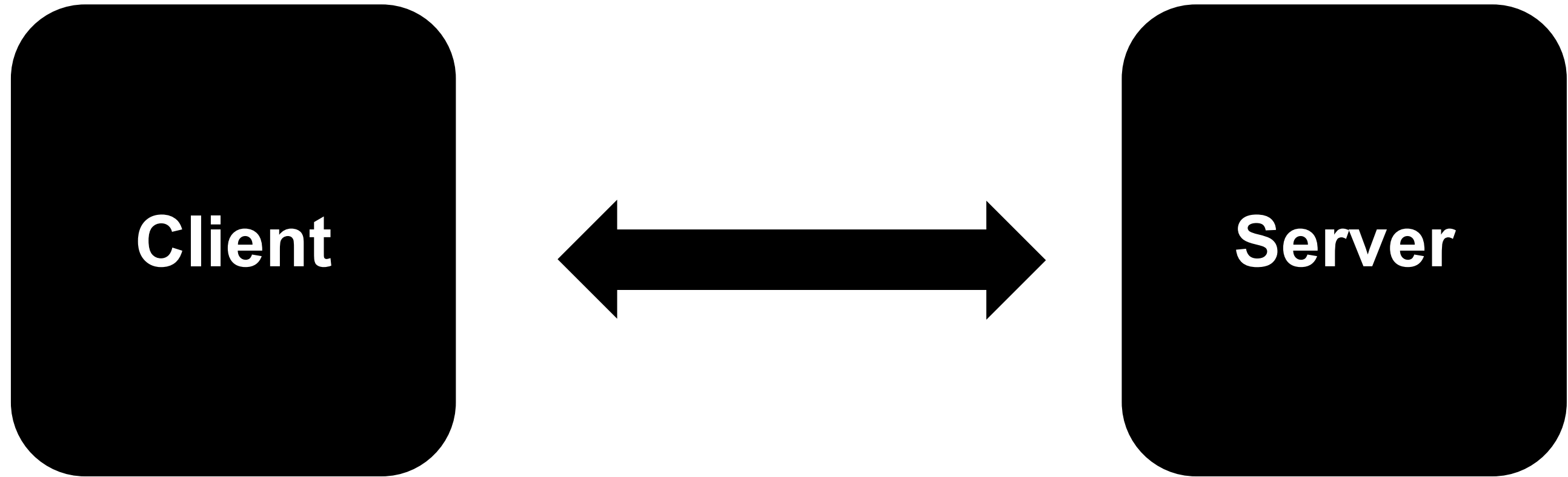
# 4. SecretCalls – Encrypted Class file

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

# 4. SecretCalls – Encrypted Class file

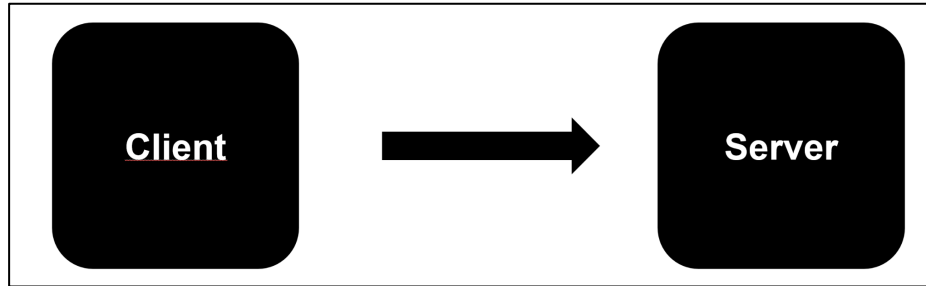
Encrypted class file	Key to decrypt class file (AES-128/ECB only)	key to decrypt <b>extra C&amp;C</b> (AES-128/CBC only)
1 <sup>st</sup> Secret	dbcdcfghijklmaop	rb!nBwXv4C%Gr^84(KEY) 1234567812345678(IV)
Kill		
Balck	xxxefgaxxdecccc dasdefvvvxxxxyyy	
2 <sup>nd</sup> Secret	dbcdcfghijklmaop	PY06RguZ68k2as6v(KEY) 1862971933292829(IV)

# 4. SecretCalls – Network Behavior(Protocol)



**WebSocket + HTTP**

# 4. SecretCalls – Network Behavior(Requests)



**App ID(key value)**

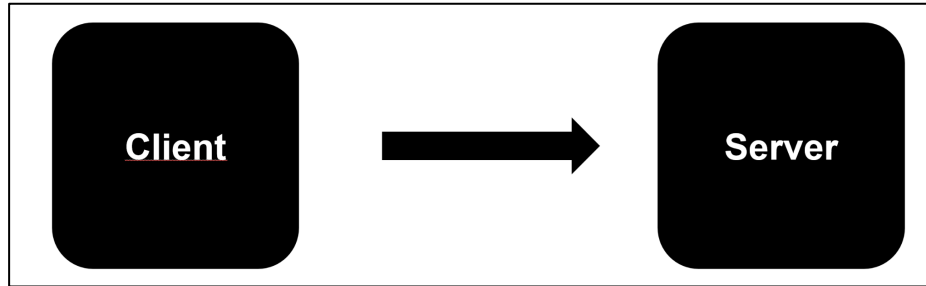


**Device's Information**

```
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\": \"8201054584424\", \"scr\": \"1\", \"adds\": \"\", \"bat\": \"100%\", \"map\": \"\", \"sys\": \"0\", \"chat\": \"0\", \"num\": \"+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%2FZVvhvIX9ZyfPx5fGC060L9oJp5mrvte6JU  
t6EmLNIDx0prJLhJ3DKCaTsDq3efD2V%2BCZjExsQKBI  
KYaemBT97K80AshBJjWaZEnHmvloa5b2RwcT2bUats1B  
b5Nc2hW5r5NQ87irUVxBEcX7kL69qNXcfkxv%2Bj0fwD
```

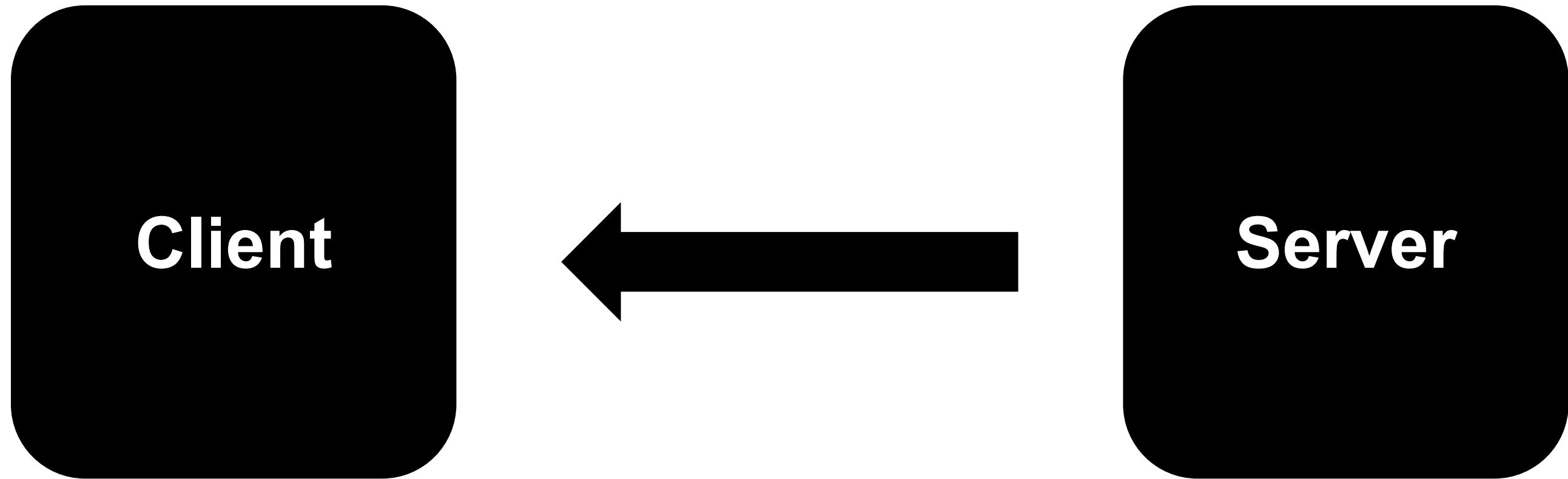
# 4. SecretCalls – Network Behavior(Requests)

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**

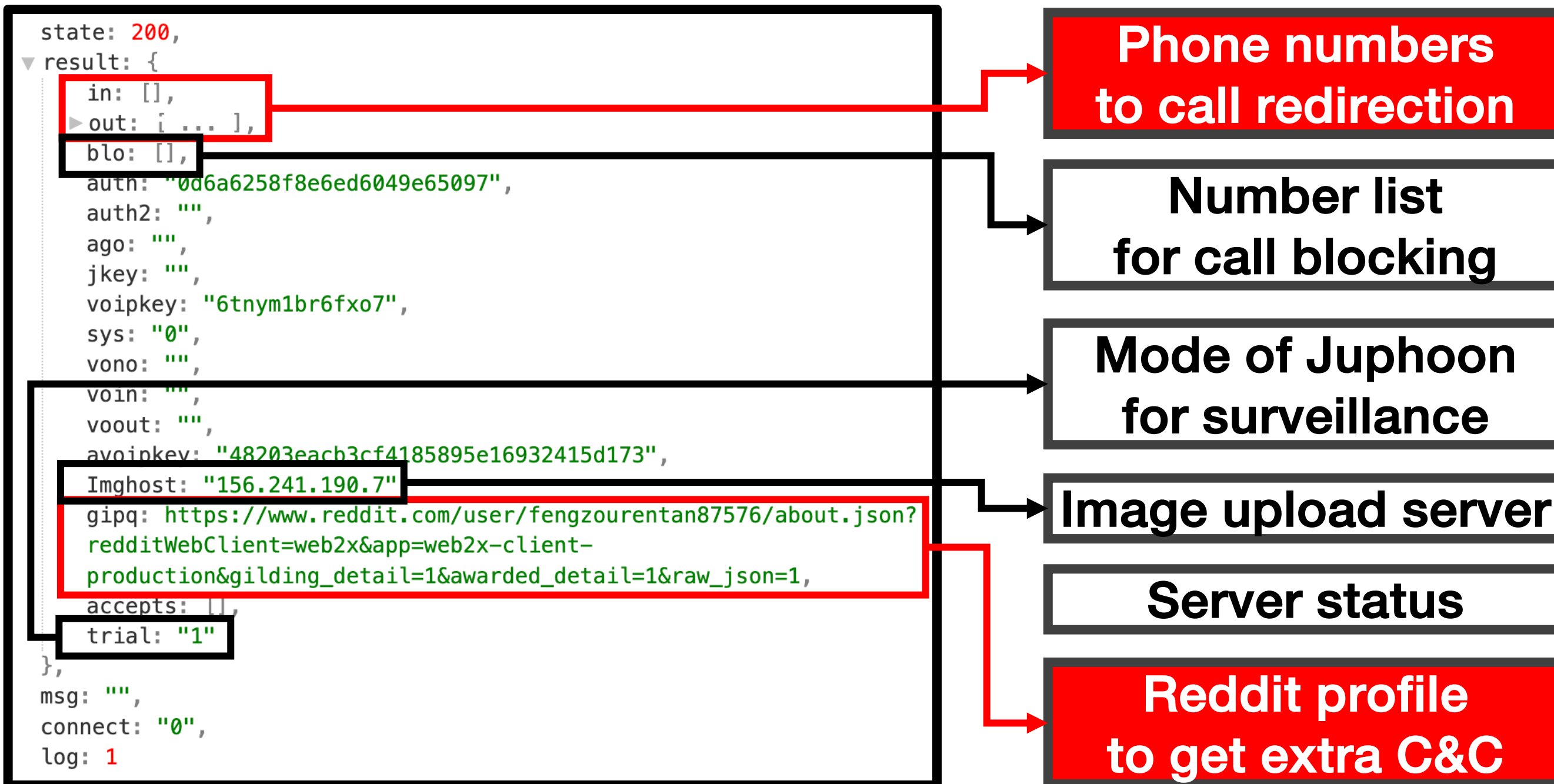
## 4. SecretCalls – Network Behavior(Response)



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



# 4. SecretCalls – Network Behavior(Response)



# 4. SecretCalls – Call Redirection

```
state: 200
result: {
  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"
    }
  ]
}
```

**Original Call**

**Attacker's number (pno)**

**New Call**

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

It may be difficult to notice

# 4. SecretCalls – Call Redirection

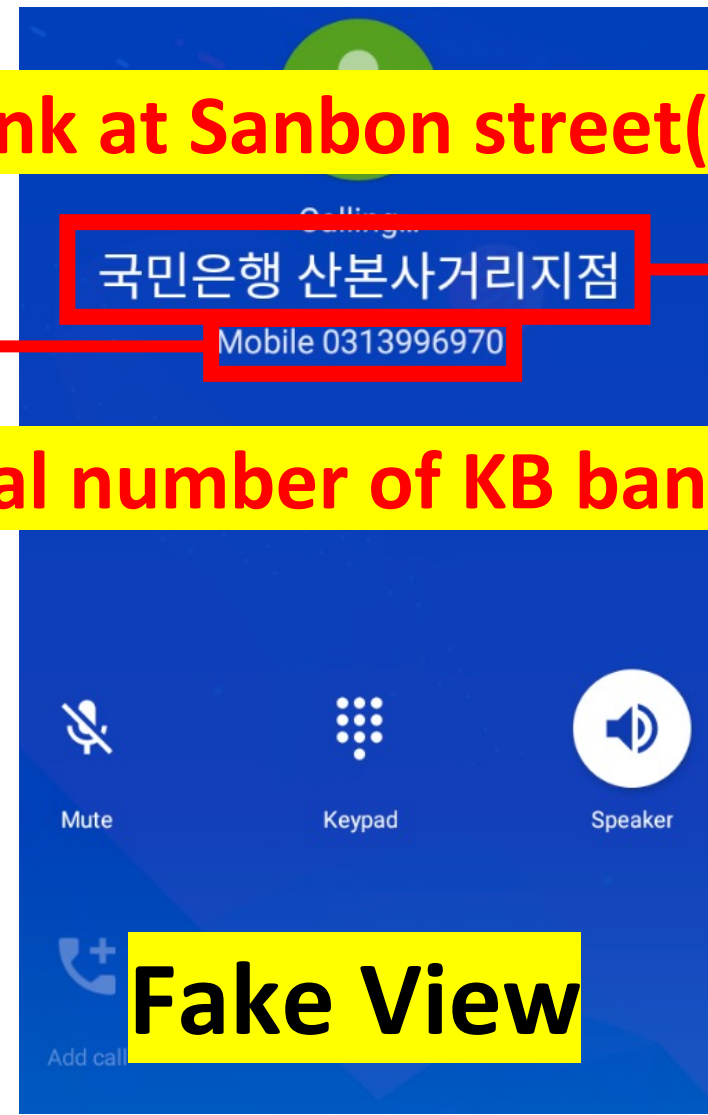
```
state: 200
result: {
  in: []
  out: [
    {
      name: "국민은행 산본사거리지점"
      fno: "0313996970",
      pno: "07078476690"
    },
    {
      name: "국민은행 호계동종합센터",
      fno: "0314577134",
      pno: "07078476690"
    },
    {
      name: "국민은행 당정동지점",
      fno: "0314777485",
      pno: "07078476690"
    },
    {
      name: "국민은행 호계남지점",
      fno: "0314278361",
      pno: "07078476690"
    }
  ]
},
msg: "",
connect: "0",
log: 1
```

KB bank at Sanbon street(name)

국민은행 산본사거리지점

Mobile 0313996970

Real number of KB bank(fno)



Fake View

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

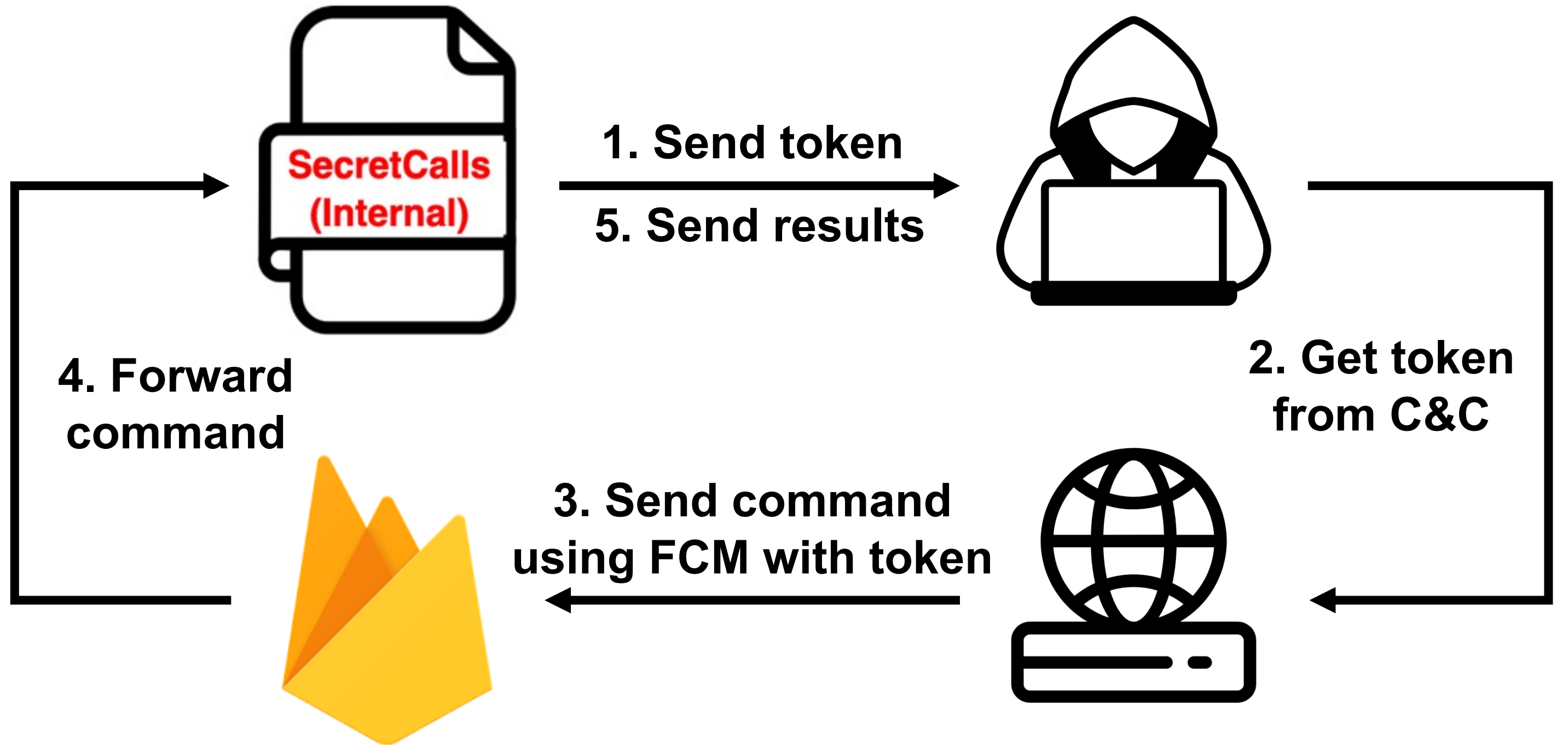
https://www.reddit.com/user/Defiant\_Pin7998/about.json?redditWebClient=web2x&app=web2x-client-production&gilding\_detail=1&

원시 데이터    헤더    **Username on Reddit**

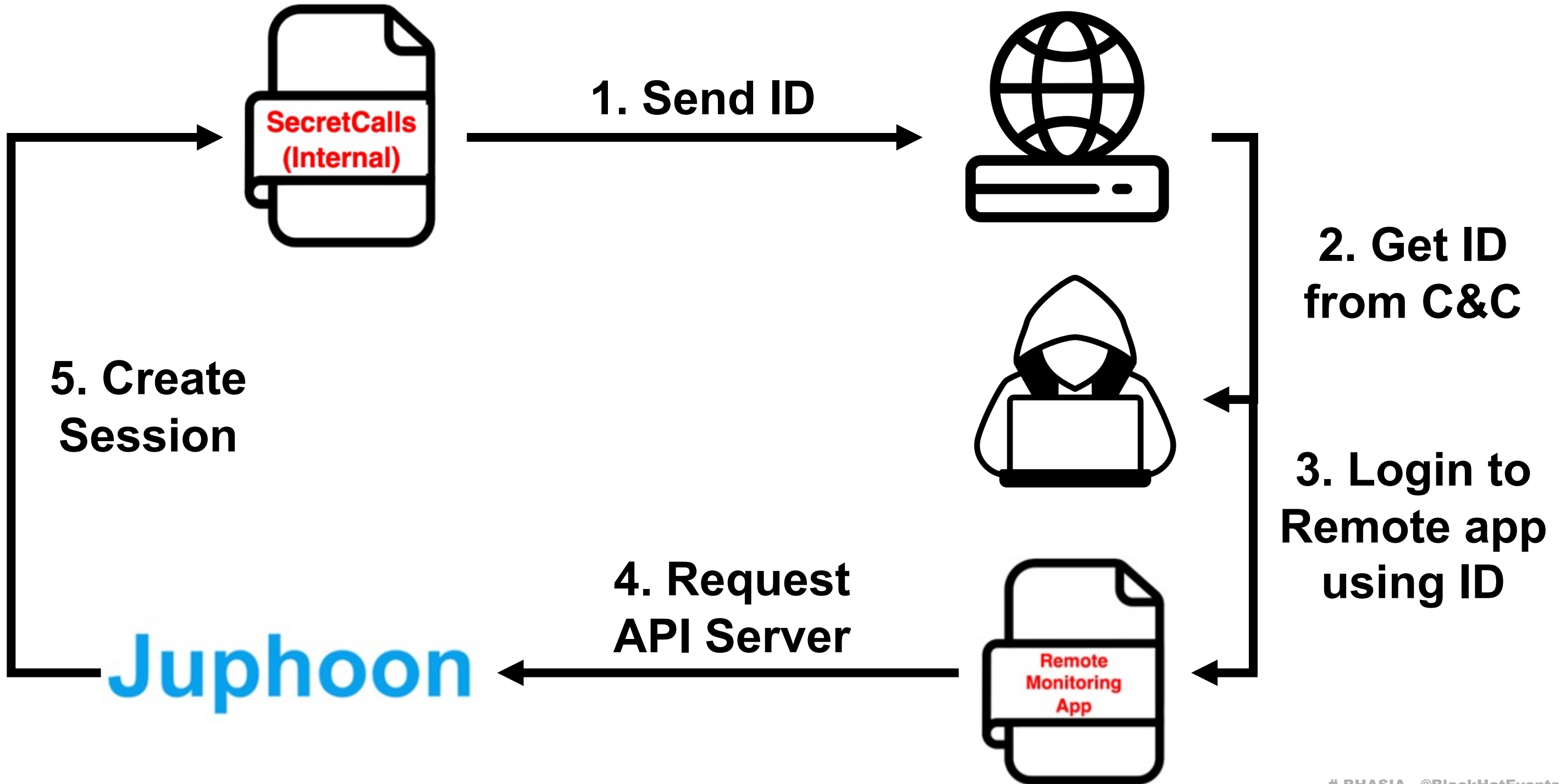
복사    모두 접기    모두 펼치기    JSON 필터

```
banner_size: null
user_is_moderator: null
accept_followers: true
public_description: "*1A2B3C*XEAYvH0+9IUprGajfmCbH97EIMo15dki5s0AV940UIM=*4D5E6F*"
link_flair_enabled: *1A2B3C*{Encrypted extra C&C address} *4D5E6F*
disable_contributor_requests: false
subreddit type: "user"
```

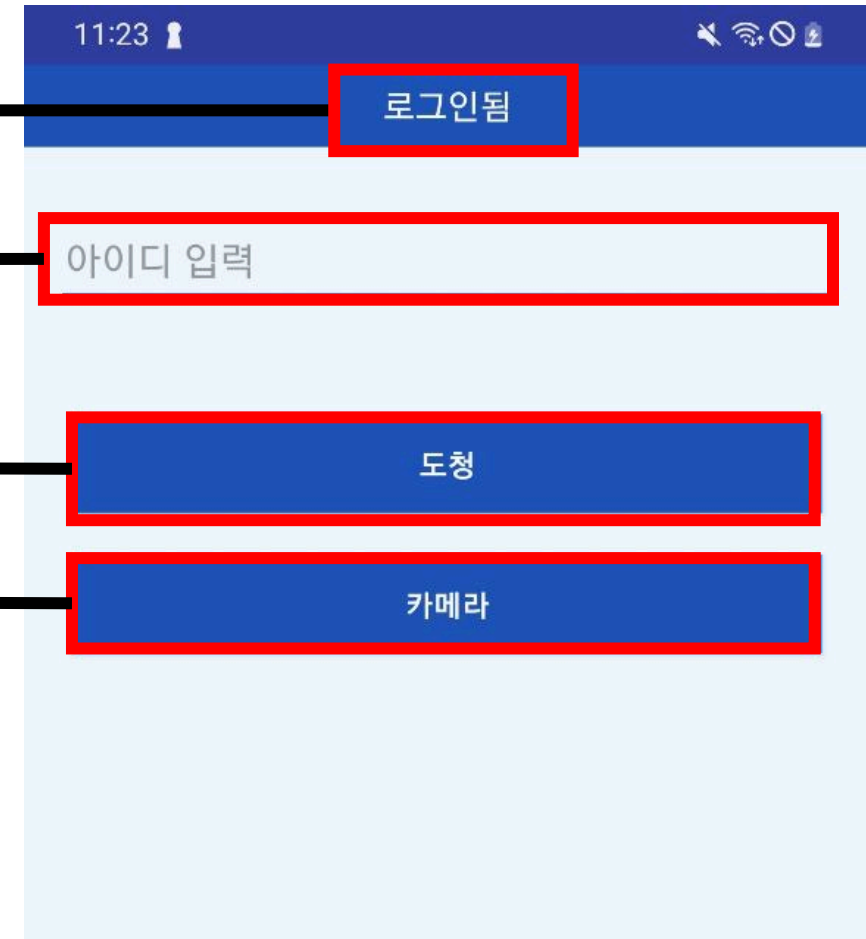
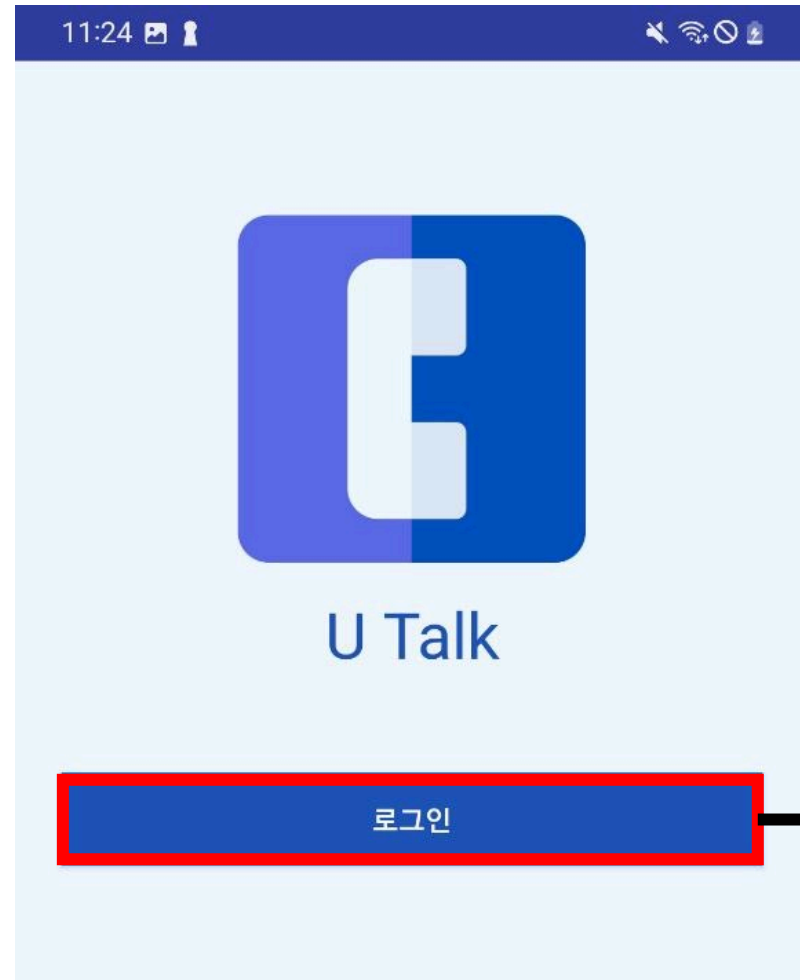
## C&C on Reddit profile changes irregularly



# 4. SecretCalls - Surveillance



# 4. SecretCalls – Custom App for Surveillance



Login

Input Juphoon ID

Eavesdropping

Camera

Login

로그인됨

아이디 입력

도청

카메라

로그인

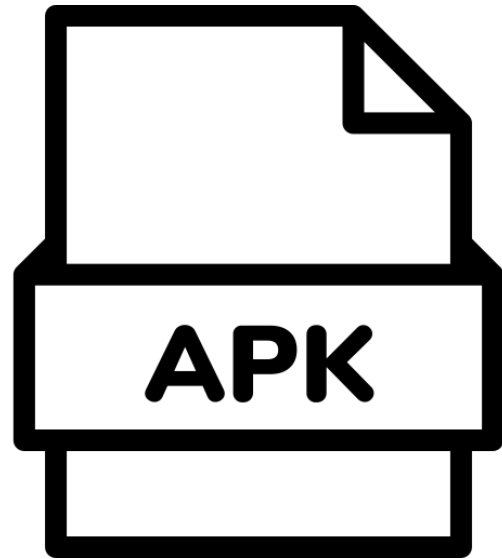
```
<string name="error_field_required">아이디 입력하세요</string>  
<string name="error_voice_cam_connection">도청실패! 아이디확인해주세요</string>
```

(error) input user ID

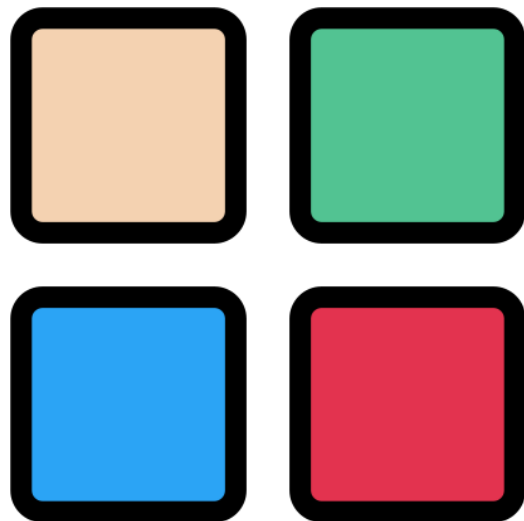
(error) Eavesdropping fail!  
Check your ID

# 5. Automation



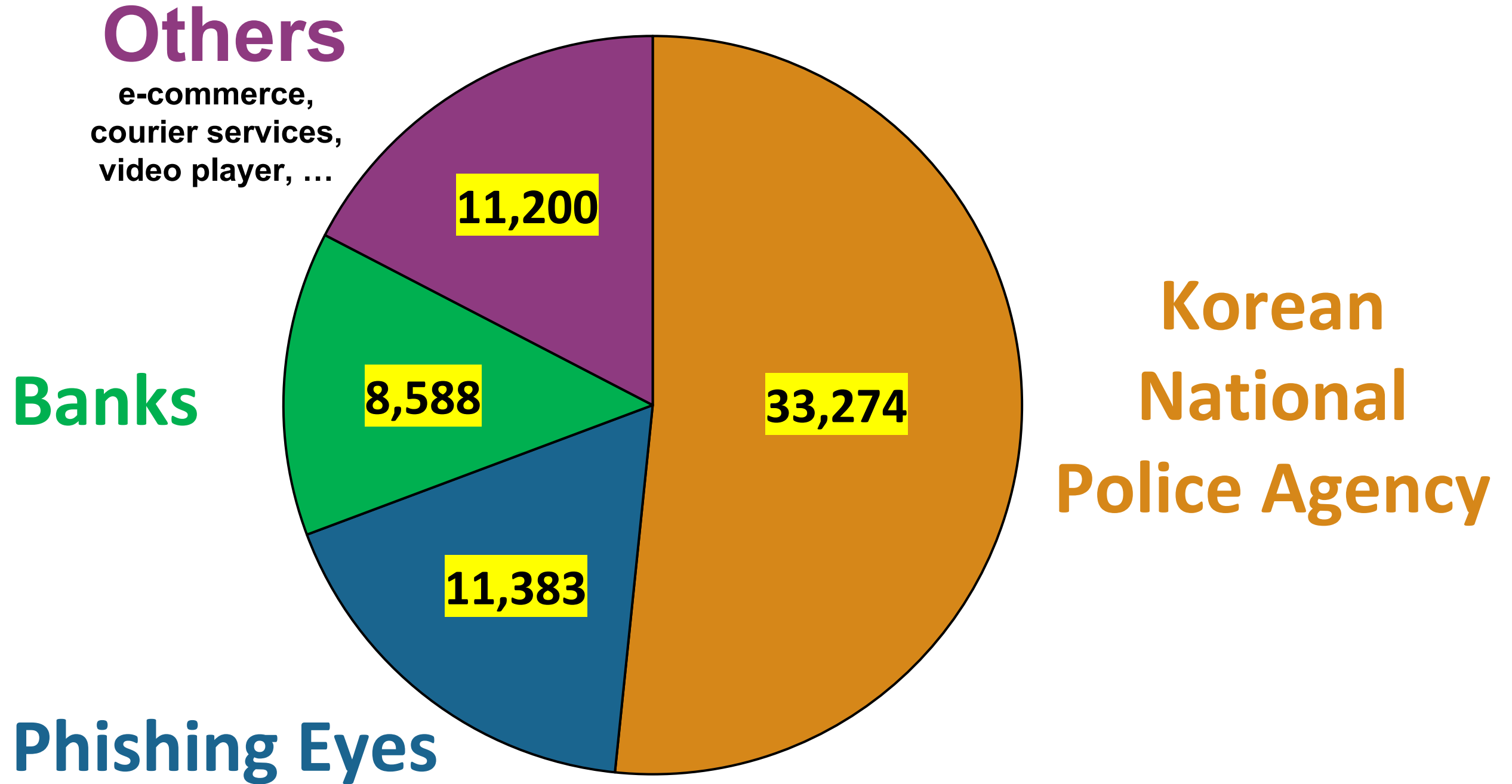


Collect Loader **64,000+**  
(including Secretcalls, it **doubles**)



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

# 5. Automation - Statistics



**Other**

e-commerce  
courier servi  
video player

**Banks**

**Phishing**



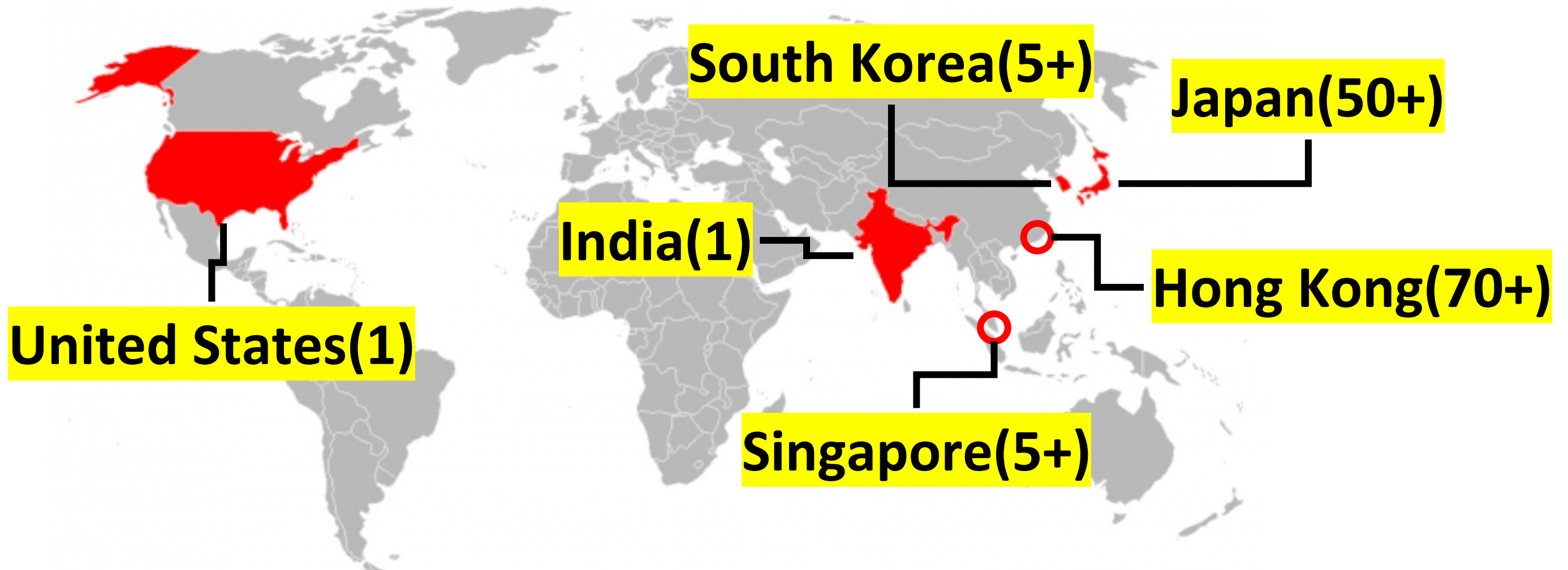
**Korean  
National  
Police Agency**

**So, we...**



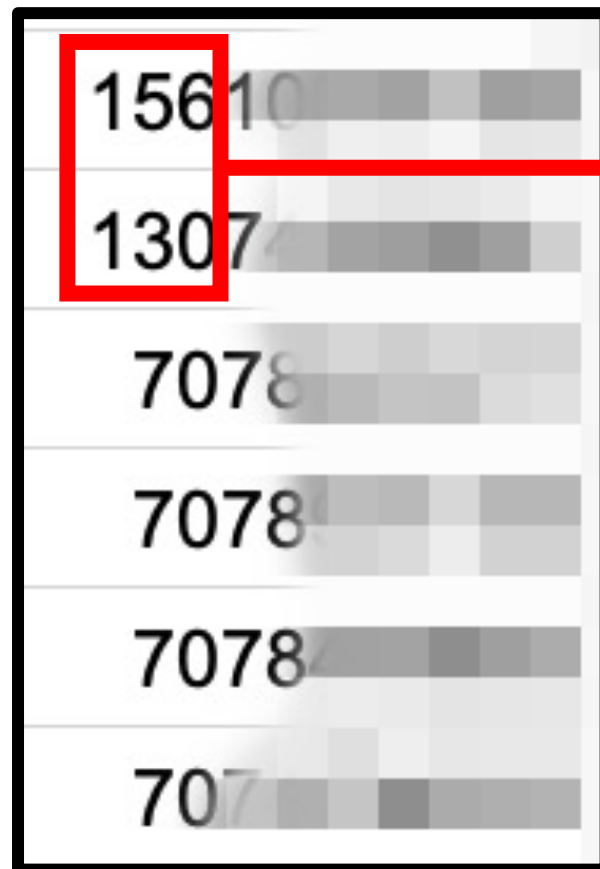
# 5. Automation - Conclusion

- **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



**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
305148cfd2598d04ec3afe84271e49f8	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](mailto:hypen@s2w.inc)*  
*Yeongjae: [teaf1001@naver.com](mailto:teaf1001@naver.com)*



**S2W**

**Safe and Secure World**



## Special Thanks to **Young-hyun, Jeong & Our Presentation Coach Anant**

### About S2W

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

**S2W** captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.

**S2W** Offers a threat intelligence solution **S2-XARVIS**, cryptocurrency anti-money laundering solution **S2-EYEZ**, digital fraud detection system **S2-TRUZ**.

### Contact

For any queries, please contact

[info@s2w.inc](mailto:info@s2w.inc)

[www.s2w.inc](http://www.s2w.inc)