Info-Stealing Tool Posing As Naver OTP

cyberandramen.net/2022/01/18/info-stealing-tool-posing-as-naver-otp/

January 18, 2022

Summary

- SHA256: 3275f42c85c9e2fcb80d1f8c1c6227c2bcde9c0e719905ddbd2ca7373c6a8ec6
- Filename: UpHelpers.exe
- Size: 3.41MB
- Extension: EXE
- Compilation Timestamp: 2022-01-05 23:41:20
- Sandbox analysis: https://tria.ge/220118-emrgjsgfb7

UpHelpers.exe is an information-stealing/reconnaissance tool disguised as a Naver One Time Password, (OTP) generator app. Naver is a South Korean web portal that first debuted in 1999 and offers a number of services.

The tool collects drive and directory information on the victim system through PowerShell, as well as gathering system information using systeminfo.exe. The stolen system information is uploaded to a C&C server.

High-Level Overview

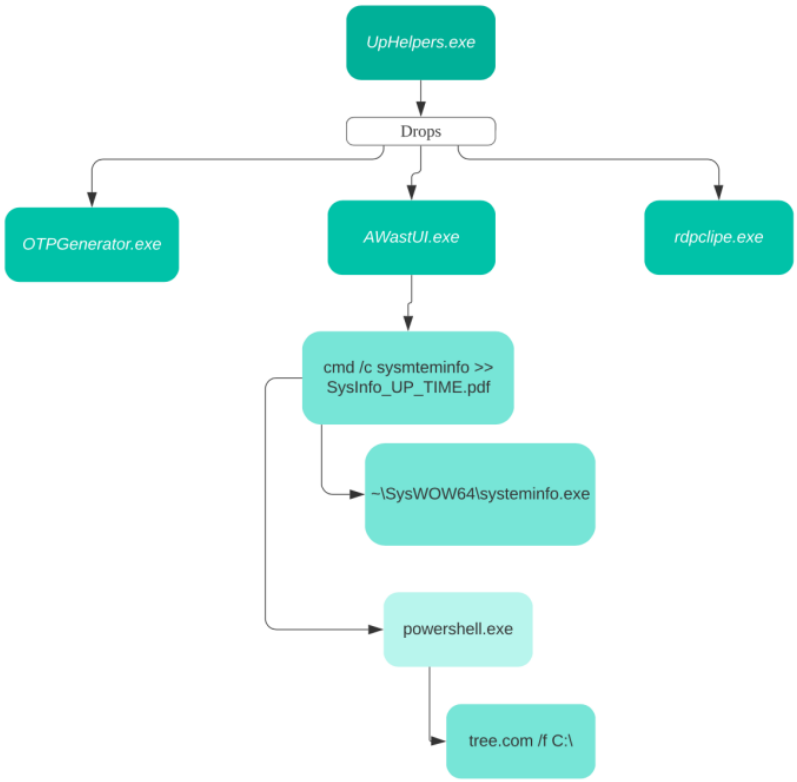

Figure 1: Malware Flow

Upon execution, UpHelpers.exe drops three executables as seen in Figure 1. The OTPGenerator.exe file is dropped into ~\AppData\Local\Temp. AWastUI.exe and rdpclipe.exe are dropped into the created folder ~\AppData\Local\MICROS~1\Outlooka. Shortcut files of the previous two files are dropped into the Startup folder to maintain persistence.

The computer name, username, and local IP are written to a file named nlashine.ini. Figure 2 provides an example of collected information after running the sample in a sandbox.

Upon execution, rdpclipe.exe ensures nlashine.ini is on the system, and if not, creates it. Additionally, the file contains the ability to log keystrokes and write what was captured to COMMA1UP_RKey.txt. The contents of the text file are written to a .dat file, and retrieved by the C2.

```
[amazon]
idnx=[RIBCQUHQ]Admin[10.127.0.100]d686
```

Figure 2: nlashine.ini

AWastUI.exe is responsible for collecting system data and communicating with the C2. After running the systeminfo command, the output is saved in a PDF file titled SysInfo_UP_day_hour_min.

Next, a hardcoded PowerShell command enumerates the drives of the victim system. This information is also written in the PDF file mentioned above.

```
powershell $dir = 'C:\Users\Admin\AppData\Local\MICROS~1\Outlooka\';$gps =
@('A','B','C','D','E','F','G','H','I','H','K','L','M','N','O','P','Q','R','S','T','U','V','W
 ($gp in $gps){$drv = $gp + ':\';if([System.IO.Directory]::Exists($drv)){$path = $dir +
'\UP' + $gp;tree /f "$drv" | Out-File -Encoding default -FilePath $path -Width 5000;}   }
```

As can be seen in the above code block, the tree command is used to collect the directory structure and folders within the C drive.

Network Indicators

The attacker infrastructure may have been taken down by the time I stumbled upon this sample as no useful network information was found.

Running a strings tool of your choice does however provide a window into the threat actors' infrastructure as well as URL paths to your blocklist.

The following network information was found throughout all the associated files:

- /ESOK/up2.php
- /ESOK/post2.php
- /ESOK/dwn.php?downfname=
- /ESOK/del2.php?delfname=
- Host: 66.94.98[.]48
- Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
- Content-Disposition: form-data; name="userfile"; filename="%s"

The above IP address belongs ASN AS40021 – CONTABO, Contabo Inc., and has ports 80, 443, and 3389 open. Figure 3 lists the most recent domain resolutions identified by RiskIQ:

Resolve	First Seen	Last Seen
mail2.daum.confirm-pw.link	2022-01-06	2022-01-18
navers.confirm-pw.link	2022-01-05	2022-01-18
downfile.navers.com-pass.online	2022-01-06	2022-01-18
nid.navrenewal.confirm-pw.link	2022-01-05	2022-01-18
nads.webemails.confirm-pw.link	2022-01-05	2022-01-18

Figure 3

Interesting Strings

- E:\Coding_Smart\Smart_Attack_Code\Oracle_Spy\src\Release\UpHelpers.pdb
- %sSysInfo_UP_%02d_%02d_%02d.pdf
- nlashine.ini
- /ESOK/up2.php
- /ESOK/post2.php
- dwn.dat
- pc.dat
- wanda_alpago613
- XJOIUUQ/EMM (possible obfuscated call to WINHTTPDLL)
- LFSOFM43/EMM (possible obfuscated call to KERNEL32DLL)
- OFUBQJ43/EMM (possible obfuscated call to NETAPI32DLL)

Indicators

SHA256 Hashes:

- AWastUI.exe::94306c7b1f1f1770e2ac2ba91bfd5f0d6e20b8878e6ad07253b50abccdd08c1d
- nlashine.ini::547e05c7cbf123aee2f7bd080719a1f8751faffc3e187b1ca72d1b9ce3301574
- rdpclipe.exe::7c82652f7f9f10c9541140a10d4fecc847907bb43374c7f29f37f9a3a956ac3b
- OTPGenerator.exe::2b082c52b754a984efa39036aaa711d23ae2bdf830f0005b19568e97a73bf918

Conclusion

Although Naver is widely used in South Korea, the group's brand has grown to a global audience. The threat actor(s) is targeting data from specific individuals who would use this app. Possible groups targeted could range from customer data to individuals affiliated with the government/military.

It is likely the threat actor would decide his/her next move based on the information collected and sent to the C2. I am unable to make a guess as to what follow-on infections there may be at this time.

References

Research by AhnLab ASEC:

> Infostealer Disguised as Well-Known Korean Web Portal File