UAC-0020 (Vermin) атакує Сили оборони України з використанням ШПЗ SPECTR в тандемі з легітимним SyncThing (кампанія "SickSync") (CERT-UA#9934)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у безпосередній взаємодії з Центром кібербезпеки ЗСУ (ЦКБ) виявлено та досліджено активність угрупування UAC-0020 (Vermin), спрямовану у відношенні Сил оборони України.

Нагадаємо, що діяльність угрупування Vermin скеровується співробітниками силових відомств тимчасово окупованого Луганська та в останнє була помічена у березні 2022 року.

Цього разу у якості засобів реалізації кіберзагрози використано відомий з 2019 року інструментарій - шкідливе програмне забезпечення SPECTR. При цьому, для вивантаження з комп'ютера викрадних документів, файлів, паролів та іншої інформації використано штатний функціонал синхронізації легітимного програмного забезпечення SyncThing, яке, серед іншого, підтримує встановлення peer-to-peer з'єднання між комп'ютерами.

Для проведення кібератаки жертві надіслано електронний лист із вкладенням у вигляді архіву "туррель.фоп.вовчок.rar", захищеного паролем. В зазначеному архіві знаходиться RARSFX-архів "туррель.фоп.вовчок.sfx.rar.scr", що містить файл-приманку "Wowchok.pdf", EXE-інсталятор "sync.exe", створений за допомогою InnoSetup та BAT-файл "run_user.bat", призначений для первинного запуску.

В свою чергу файл "sync.exe" містить як легітимні компоненти програми SyncThing, так і файли шкідливих програм SPECTR, в тому числі допоміжні бібліотеки та скрипти. При цьому, штатні файли програмного забезпечення SyncThing частково модифіковано з метою зміни назв каталогів, запланованих задач, відключення функціоналу відображення повідомлень користувачеві тощо.

Коротка інформація щодо модулів SPECTR наведена нижче.

- **SpecMon** - викликає PluginLoader.dll, який, у свою чергу, забезпечить виконання всіх DLL-файлів, які містять клас "IPlugin".
- **Screengrabber** - забезпечує виготовлення знімків екрану кожні 10 секунд за умови, якщо вікно програми містить такі назви: "word", "excel", "wps", "office", "notepad", "gram", "signal", "wickr", "wire", "threema", "viber", "whatsapp", "skype", "silence", "session", "adamant", "discord", "confide", "chrome", "mozilla", "edge", "vpn", "tor", "bat", "mail", "почта", "пошта", "диск", "disk", "drive", "box", "crypt", "wallet", "coin", "money", "подключение к", "remote", "1c:enterprise", "1c:предприятие", "1c предприятие", "1c-предприятие", "1cv", "faststone", "foxit", "pdf24 reader", "anydesk", "yandex with", "browser", "viewer".
- **FileGrabber** - за допомогою robocopy.exe з каталогів %USERPROFILE%\{Desktop, MyPictures, Personal, Downloads, OneDrive} та %APPDATA%\DropBox здійснює копіювання файлів з розширеннями: ".one", ".pdf", ".doc", ".docx", ".docm", ".xls", ".xlsx", ".xlsm", ".ppt", ".pptx", ".odt",

".odm", ".ods", ".odp", ".cdr", ".jpg", ".png", ".bmp", ".eml", ".tiff", ".txt", ".zip", ".rar", ".7z"; додаткові аргументи: "/S /COPY:DT /R:3 /W:5 /XO /MAXAGE:%MAXAGE% /MAX:5242880".

- **Usb** - за допомогою robocopy.exe зі знімних (USB) носіїв здійснює копіювання файлів з розширеннями: ".pdf", ".doc", ".docx", ".docm", ".xls", ".xlsx", ".xlsm", ".ppt", ".pptx", ".odt", ".odm", ".ods", ".odp", ".jpg", ".png", ".bmp", ".ogg", ".wav", ".mp3", ".mp4", ".txt", ".zip", ".rar", ".7z".
- **Social** - здійснює викрадення конфігураційних (автентифікаційних) даних месенджерів: Telegram (tdata), Signal (databases, Session Storage, Local Storage, sql, config.json), Skype (Local Storage), Element (leveldb).
- **Browsers** - здійснює викрадення даних (автентифікаційних даних, даних сесій, історії) Інтернет-браузерів браузерів: Firefox, Edge, Chrome (в т.ч., "Chromium", "Google", "Google(x86)", "Opera Software", "Amigo", "Orbitum", "Yandex", "Comodo", "Maxthon3", "Brave-Browser").

Слід зауважити, що викрадена інформація копіюється до підпапок в каталозі %APPDATA%\sync\Slave_Sync\, після чого, з використанням штатного функціоналу **синхронізації** легітимної програми **SyncThing**, вміст цих каталогів потрапляє на комп'ютер зловмисника, чим і забезпечується **ексфільтрація** даних.

З точки зору мережевих індикаторів (на випадок впевненості у не використанні згаданої технології санкціоновано), беручи до уваги встановлення peer-to-peer з'єднання, серед іншого, рекомендуємо звертати увагу на ознаки взаємодії з інфраструктурою SyncThing: *.syncthing.net.

Активність відстежується за ідентифікатором UAC-0020.

Ураховуючи не дуже вдале повернення угрупування Vermin після тривалої відсутності в публічному просторі та з метою спрощення сприйняття інформації, виявленій кампанії надано назву "SickSync".

Осіб, відповідальних за кіберзахист ІКС ЗСУ, з метою мінімізації вірогідності реалізації кіберзагроз закликаємо невідкладно звернутися до Центру кібербезпеки ЗСУ (email: csoc@post.mil.gov.ua, Signal: +380673321891) з метою отримання та подальшого встановлення на всі без виключення ЕОМ відповідних технологій захисту. Крім того, просимо впевнитись у наявності налаштувань на граничних мережевих пристроях для передачі по протоколу Syslog журналів мережевих з'єднань.

Індикатори кіберзагроз

Файли:

```
30a590611403c94c41289ab68b56ca48
 b452b0043533625da67e687c6050e9475d1a83337fa2b64735fc9a248179df10
 туррель.фоп.вовчок.rar
b51d8875e2502704416209c9eb46edf0
 db1e53f9b03363d595c9daf1eaafd1d851b5d984af9e4062204f18746b012d37
 туррель.фоп.вовчок.sfx.rar.scr
5aaa6594f0249df48190568edfcc01ef
 456732417161a749541bbc4016c9334a01ff3b209c29bc3995f3589dccb80f31
 run_user.bat
251d8e41f89e5807140b786c89723d4c
 b4d4e2602cd6c5286be56b71a8659dff380eafd4bf65b61268b5d29a2bd6c52b    sync.exe
```

63892a6d1eccbaf0edd7cd55654e0150
bf895dca1ea67bf39a6bd87168af8d4fdfd6321d2f2d071295dbd4d25508eb68
syncthing.exe (SyncThing)
49c40fb4f001a9b267b799f6d0b18500
48adf2450c4ae087c1c4982a2a789d8f1b1e88b8d959fb26db273a76ef8b1888
SyncthingFirewallRule.js
b283b1d1e746ccc6112ef85a6d2d73ef
8cccf28333d822da6b5d851ae4cb188fed6dd27a3046627c7a32850c9d959124
SetSyncthingConfig.js
f357833157928395b65e9d17b26dee0e
4d3c48917973daaf7e31aeab167e4611c60feed29bae25303c0543824bef027c
SyncthingLogonTask.js
f3a89edd5efe3a9269b4697ff3b386be
29d9cc9a79750c6c1a3052317fb172b9d76a7044b94cd1da3be00ace748a9878
ConfigSyncthingService.js
f6e436ad88fdf391b960ff28df25e80b
1cc0257d93b4d1c0b3bb5c923c2997f222d271591addbd2da0da019dbb5fe579
StartSyncthing.js
bd335dad7c46ec91d2816b5a0ca6d29a
67571ad65881dd4feb309c22f8e508da40bbf4f573fd97c45265394ac5b06659
config_final.xml
a1199e11d307e2c649c4b2487297896d
9b3994f395309b0fb4db23e66d8de822b47cd9d4c9544bc48ed0e0fa082251b0
startProc.ps1
2d1814ea39c8b33db1394dd2bf8e4a2a
711100e90de58762aa121a5f4a5fc50f1efc05499f1ee63b6bc1e3d479eb4c69 Install-SyncthingService.ps1
74874b31fcddef67d98cac666d86d375
0a43d77c67c0ff31660a19e69cdb26e55b5322cf63b51a97d4de0c4b48f78841
modConf.ps1
64b378abcd1bb4f2d064dbbe72570d3e
87f73bc1762913e46d4dad6464f92d0d3e3c785da4cc30a24460601a3ceed970
install.ps1
45a58147de34d9d3029b62ac48636f26
806db134f3b9db4a58dd8ff65498d2841f645ef7252857e57c46cd6680edcec7
startps.exe
8f3125d49dd0e38e2fd7a1351281005e
4c4db56997d9a44cfc5a03f3b401f96d6890a56cd32146c5605f159a97112df9 nssm.exe
d70e7aa26e5b90b971aaa5e16017249c
5ef47edc207e404c57ac83e2b55fb0b7c1687d721f26fc7a5a6e5294b28a2f6f
Wowchok.pdf (документ-приманка)
bb38d0bf2246ed55b46dd61dcf5693a6
bef8cf172fd4535738e3aa06a9c303f93c83a4da0053aba4cbea986729d4620b README.txt
8761d7bce160c25d9b2f1d0a72ad89a4
9221c2f936159b8446d329249fb4c0f25be510f447383a0f13336ac7985668a3
LICENSE.txt

```
471bdb3bb2807636f56fb238e6a2e047
 892a45e8adc92eb281a8f4cdba824cd69134bcb8378977747998b87c5a7fdec8
 AUTHORS.txt
(SPECTR DLLs)
076586ea295ad521e7dc793a5a2c38b7
 2b6622cc433aff6cb4bc582c7bc3bffc09e0fc6f0e1a97bab17485058bdcf3c9
 SpecMon_x86.dll
2666479686a91389afc44a02ee70038e
 0ad1cf00eed24ab07765d3670d1c8394b3d232f58bf939b69ada9e88c45b4b03
 SpecMon_x64.dll
52df00ffcb487f4967c480bc425376ba
 7198094549e30b8bff6865ce364e48dc324d92f2346dec9b0ce6664921c21888
 PluginLoader.dll
09570ab8f371adf8893c7e0da786cd2e
 c208408170c429af873849cecc4b7553598ba5a70fce7616e6adca66cfeb8d75    Common.dll
39534c1234b3dbfe37b774b967cfb4ee
 f8b696ae1011f6c5457eea1e215da81e85aef1b1a62c56dce3606e0512afdbb4
 MediaDevices.dll
cd4bc0795ce5d04efc0a7644d8ff6159
 00b3599f4bb48e2599f953191d526da432c280d5ae5bc43392eb37352fde5cb2
 Management.dll
debf2157d6192ac4d5be67104f7ba312
 117078cd63225cfed7cbe4bc4c2ffed6db4d4bd93bf353a87cc10fb05cc0151c
 Commander.dll
e508a05a71d29688b7916429894c09d5
 b05c65897fc449760fa5867e436205313448007e904e02aa77c0733a21d15bb2
 Browsers.dll
83811960db65d0d430062ad1ff92b7ca
 c3ac906b3228c4c9ce3dd0e46b6c5b0bed4dacd61911dc006730a31f90f424c7    Social.dll
ebe83a11b39bfd848fa557a79f2dff1b
 fbd8883e659d8082fe8e1ee15de12e2b710fd4c92d8d72b2cf34befcdc5be7fb    Usb.dll
aeda6f2d3669fb0d30b3e21437405d81
 6a13b98c7dc82ea2a492c0022fd93fa97247912dfa8ad5f015fb4b50e6c05fbb
 FileGrabber.dll
a816830220abe0cc2e3877eeadae0580
 bf62d5e034b4ce4fd122ab72fa388ea461fd6e5f317ad3274fe847a526c00282
 Screengrabber.dll
```

Мережеві:

```
(Інфраструктура SyncThing)
hXXps://crash.syncthing[.]net/newcrash
hXXps://data.syncthing[.]net/newdata
hXXps://upgrades.syncthing[.]net/meta.json
crash.syncthing[.]net
```

```
data.syncthing[.]net
upgrades.syncthing[.]net
syncthing[.]net

syncthing.net
```

Хостові:

```
%APPDATA%\Microsoft Configurator\
%APPDATA%\sync\Slave_Sync\
%APPDATA%\sync\Slave_Sync\.fs\
%APPDATA%\sync\Slave_Sync\.scrn\
%APPDATA%\sync\Slave_Sync\.usb\
%LOCALAPPDATA%\Programs\MSConfigurator\
%LOCALAPPDATA%\Programs\MSConfigurator\scrn\
%LOCALAPPDATA%\Programs\MSConfigurator\scrn\SpecMon_x64.dll
%LOCALAPPDATA%\Programs\MSConfigurator\scrn\SpecMon_x86.dll
%LOCALAPPDATA%\Programs\MSConfigurator\scrn\install.ps1
%LOCALAPPDATA%\Programs\MSConfigurator\syncthing.exe
%LOCALAPPDATA%\Syncthing\config.xml
C:\Projects\MediaDevices\Src\MediaDevicesFramework45\obj\Release\MediaDevices.pdb

W:\Projects\DEV\SpecMon\Browsers\obj\Release\Browsers.pdb
W:\Projects\DEV\SpecMon\Commander\obj\Release\Commander.pdb
W:\Projects\DEV\SpecMon\Common\obj\Release\Common.pdb
W:\Projects\DEV\SpecMon\FileGrabber\obj\Release\FileGrabber.pdb
W:\Projects\DEV\SpecMon\Messengers\obj\Release\Social.pdb
W:\Projects\DEV\SpecMon\PluginLoader\obj\Release\PluginLoader.pdb
W:\Projects\DEV\SpecMon\Screengrabber\obj\Debug\Screengrabber.pdb
W:\Projects\DEV\SpecMon\Usb\obj\Release\Usb.pdb
cscript.exe
"%userprofile%\Appdata\Local\Programs\MSConfigurator\StartSyncthing.js" /silent
distr\sync.exe /verysilent /currentuser /noicons /SP- /SUPPRESSMSGBOXES
/NOCANCEL
GoogleChromeUpdateDailyTask (Scheduled Task)
MicrosoftEdgeUpdateTaskMachineReg (Scheduled Task)
```

Графічні зображення

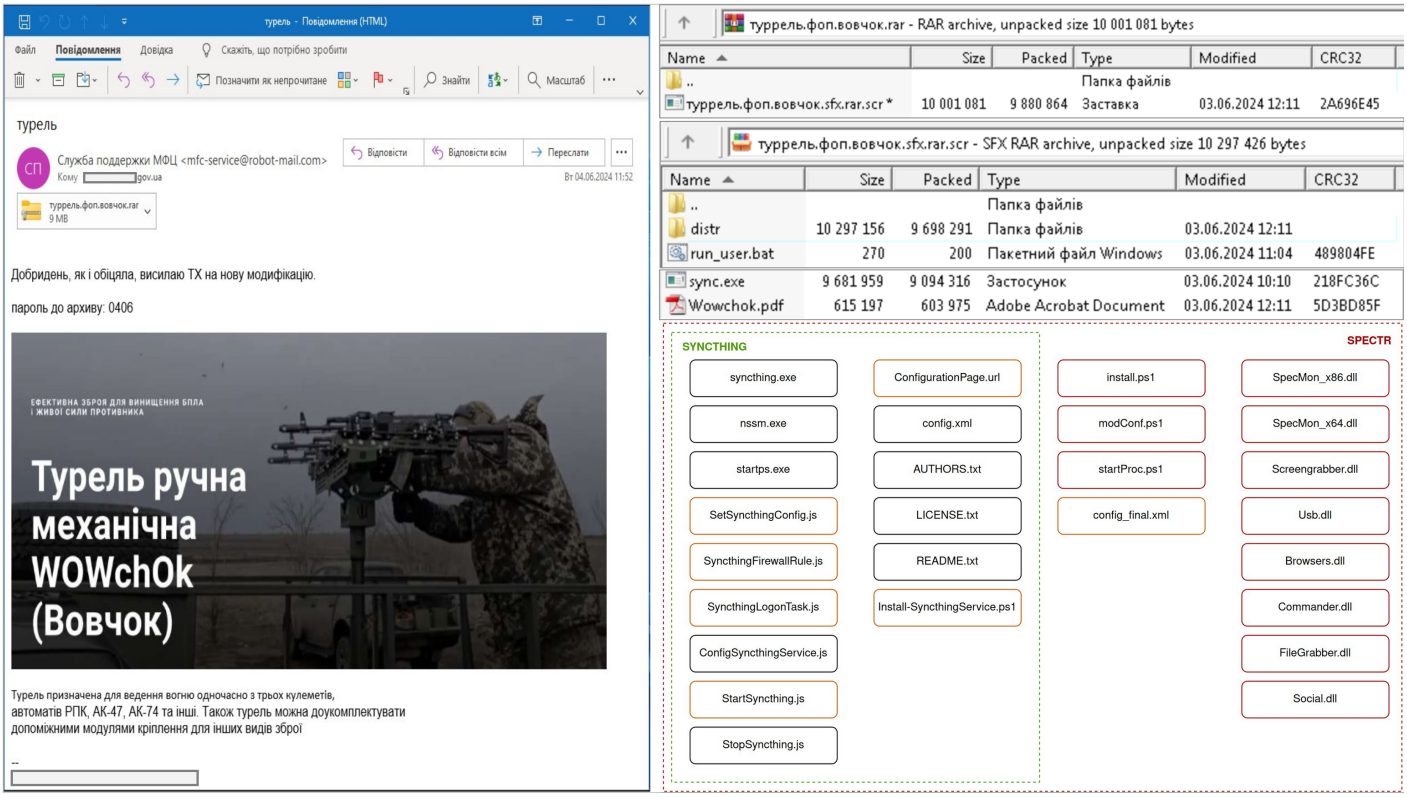

Рис.1 Приклад електронного листа та вмісту шкідливого інсталятора