cert.gov.ua /article/6279600

UAC-0020 (Vermin) attacks the Defense Forces of Ukraine using the SPECTR WPS in tandem with a legitimate SyncThing

General information

The government team of response to computer emergency events of Ukraine CERT-UA in direct interaction with the Cyber Security Center of the Armed Forces of Ukraine (CCB) has identified and investigated the activity of the UAC-0020 (Vermin) grouping, directed towards the Defense Forces of Ukraine.

Recall that the activities of the Vermin group are directed by employees of the law enforcement agencies of the temporarily occupied Luhansk and was last seen in March 2022.

This time, the tools for implementing cyber threats used the toolkit known since 2019 - malware SPECTR. In this case, to upload stolen documents, files, passwords and other information from the computer, a regular SyncThing software is used, which, among other things, supports the installation of peer-to-peer connection between computers.

To conduct a cyber attack, the victim sent an email with an attachment in the form of an archive "turrel.fop.wolf.rar", password-protected. The archive contains RARSFX-archive "turrel.fop.wolf.sfx.rar.scr", containing the bait file "Wowchok.pdf", EHE installer "sync.exe", created using InnoSetup and BAT file "run_user.bat", designed for initial launch.

In turn, the "sync.exe" file contains both legitimate components of the SyncThing program and SPECTR malware files, including auxiliary libraries and scripts. SyncTing software is partially modified to change directory names, scheduled tasks, disable message display functionality to the user, etc.

Brief information about SPECTR modules is given below.

- **SpecMon** - calls PluginLoader.dll, which in turn will provide the execution of all DLL files that contain the class "IPlugin".
- **Screengraver** - provides the manufacture of screenshots every 10 seconds provided that the program window contains the following names: "word", "excel", "wps", "office", "notepad", "gram", "signal", "wickr", "wire", "tree", "viber", "whatsapp", "skype", "silence", "session", "adamant", ""tor", "bat", "mail", "mail", "disk", "disk", "drive", "box", "crypt", "wallet", "coin", "money", "connect to", "remote", "1c:enterprise", "1c:pretrieved", "1s"" "1s"yandex with", "browser", "viewer".
- **FileGrabber** - using robocopy.exe from directories %USERPROFILE% ?Desktop, MyPictures, Personal, Downloads, OneDrive - and %APPDATA%?DropBox copies files with extensions: ".one", ".pdf", ".docx", ".doc", "xl", "xl", "xls", "xl", "xl", "xl", "xl", "xl", "xl", "x".t", ".odm", ".ods", ".odp", ".cdr", ".jpg", ".png", ".bmp", ".eml", ".tiff", ".txt", ".zip", ".rar", ".7z"; additional arguments:/S /COPY:DT /R:3 /W:5 /XO /MAXAGE:%MAX
- **Usb** - using robocopy.exe from removable (USB) media copy files with extensions: ".pdf", ".docx", ".docx", ".docm", ".xls", ".xlsx", ".xlsm", ".ppt", ".ppt", ".odm", ".ods", ".ods", ""."", ".mp4", ".txt", ".zip", ".rar", ".7z".
- **Social** - steals configuration (authentic) data of messengers: Telegram (tdata), Signal (databases, Session Storage, Local Storage, sql, config.json), Skype (Local Storage), Element (leveldb).
- **Browsers** - steals data (authenticing data, session data, history) browser browsers: Firefox, Edge, Chrome (including, "Chromium", "Google", "Google(x86)", "Opera Software", "Amigo", "Orbitum", "Yandex", "Codo", "Maxthon3", "Brow".

It should be noted that the stolen information is copied to the subfolders in the directory %APPDATA%?sync Slave_Sync?, then, using the standard **synchronization** functionality of **the** legitimate **SyncThing** program, the content of these directories enters the attacker's computer, which provides **exfiltration** of data.

In terms of network indicators (in case of confidence in not using the mentioned technology is authorized), taking into account the installation of peer-to-peer connection, among other things, we recommend paying attention to the signs of interaction with the SyncThing infrastructure: *.syncthing.net.

Activity is tracked by the UAC-0020 identifier.

Given the not very successful return of the Vermin group after a long absence in public space and in order to simplify the perception of information, the campaign was called "SickSync".

Persons responsible for cyber protection of the ICS of the Armed Forces, in order to minimize the likelihood of implementing cyber threats, we call on us to immediately contact the Cyber Security Center of the Armed Forces of Ukraine (email: csoc ?post.mil.gov.ua, Signal: +380673321891) in order to obtain and further install for all computer-related protection technologies without exception. In addition, please make sure that you have settings on boundary network devices for transmitting network connection logs viaslog protocol.

Cyberthreat Indicators

Files:

```
30a590611403c94c41289ab68b56ca48
b452b00433625da67e687c6050e9475d1a8337fa2b64735fc9a248179df10 turrel.fos.wolf.rar
b51d8875e25027044109c9eb46edf0
db1e53f9b03363d595c9d9d1daf1d851b5d984af9e4062204f1874b012d37
turrel.fop.wolf.sfx.rar.scr
5aaa6594f0249df48190568edfcc01ef
4567327161a749541bbc4016c9334a01ff3b209c29bc3995f3589dccb80f31 run_user.bat
251d8e41f89e5807140b786c89723d4cbb4cb602cd6c02cd5286be56b71a8659dff380efd4b65b61268b5d29a
 sinc.exe
63892a6d1eccbaf0edd7cd55654e0150
bf895dca1ea67bf39a6bd87168af8d4fd6321d2f2d071295dbd4d25508eb68 Syncthing.exe
(SyncThing)
49c40fb4f001a9b267b799f6d0b18500
48adf2450c4a087c1c4982a2a789d8f1b1e88b8b8d959fb273a76f8b1888 SyncthingFirewallRule.js
b283b1d1e746ccc6112ef85a6d2d73ef
8cccf2833d822da6b5d851ae4cb188fed6d27a30427c7a3280c99124 SetSyncingConfig.js
f357833157928395b65e9d17b26dee0e
4d3c48917973daaf7e31aeab167e4611c60feed29bae25303c053824bef027c SyncthingLogonTask.js
f3a89edd5efe3a9269b4697ff3b386be
29d9cc9a79750c6c1a3052317fb17b17b97d76a7044b94cd1da3be00ace748a9878
ConfigSyncingService.js
f6e436ad88fdf391b960ff28df25e80b
1cc0257d93b4d1c0b3c923c923c2997f222d271591addbdd2da0da019dbb5fe579 StartSyncthing.js
bd335dad7c46ec91d2816b5a0ca6d29a
67571ad65881dd4feb309c22f8e508da40bbf4f573fd97c4535393ac5b0659 config_final.xml
a1199e11d307e2c649c4b2487297896d
9b3994f395309b0fb4db2d23e66d8de82b47cd9d4c9544bc48ed0e0e20f2021b0 startProc.ps1
2d1814ea39c8b33db1394dd2bf8e4a2a
711100e90de58762aa121a5f4a5fc50f1efc05499f1ee63bc1e3e3d479eb4c69 Install-
SyncingService.ps1
74874b31fcdef67d98cac666d86d375
0a43d77c67c0ff31660a19e69cdb26e55b5322cf63b51a97d4de0c4b48f7841 modConf.ps1
```

```
64b378abcd1bb4f2d064dbbe72570d3e
87f73bc1762913e46d4d6464f92d3e3c785da4cc30a24460601a3ceed970 install.ps1
45a58147de34d9d3029b62ac48636f26
806db134f3b9db4a58dd8ff65498d2841f645ef7252857c46cd6680edcec7 startps.exe
8f3125d49d0e38e2fd7a1351285e
4c4db569997d9a44cfc5a03f3b401f96d6890a56cd3246c56c5605f59a97112df9 nssm.exe
d70e7aa26e5b90b971aaa5e16017249c
5ef47edc207e404c57ac83e2b55fb0b7c1687d721f26f2a5a5a5294b28af Wowchok.pdf (relide
document)
bb38d0bf2246ed55b46dd61dcf5693a6
bef8cf172fd4535738e3aa06a9c303f93c83a4da0053aba4cbea986729d4620b README.txt
8761d7bce160c25d9b2f1d1d0a72ad89a4
9221c2f9359b8446d329249fb4c0f25be510f447383a0f13336ac798568a3 LICENSE.txt
471bdb3bb2807636fb238e6a2e047
892a45e8adc92eb281a8f4cdba824cd69134bcbbbbbb87777798b87c5a7fdec8 AUTHORS.txt
(SPECTR DLLs)
076586ea295ad521e7dc793a5a2c38b7
2b66cc4333cf6cbb4bc582c7bc3bffc09e0fc6f0e1a97bab17485058bdcf3c9 SpecMon_x86.dll
2666479686a91389afc44a02ee700e0e
0ad1cf00ed24ab0765d3670d1c8394b3d232f58bf939b69ada9e88c45b4b03 SpecMon_x64.dll
52df00ffcb487f4967c480bc425376ba
719094549e30b8bff6865ce364e48dc324d92f2346dec9b0ce6664921c21888 PluginLoader.dll
09570ab8f371adf8893c7e0da786cd2e
c208408170c429af873849cecc4b753598ba5a70fce76e6adca66cfeb8d75 Common.dll
39534c1234b3dfe37b77b967cfb4ee
f8b696ae1011f6c5457ee1e215da81e85aef1b1b1a62c56dce3606e0512afdbb4 MediaDevices.dll
cd4bc0795ce5d04efc0a7644d8ff6159
00b3599f4bb48e2599f953191d526da432c280d5ae5bc4392eb37352fde5cb2 Management.dll
debf2157d6192ac4d5be67104f7ba312
117078cd63225cfed7cbe4bc4c2ffed6db4d4bd93bf353a87cc10fb05cc0151c Commander.dll
e508a05a71d29688b7916429894c09d5
b05c65897fc449760fa5867e4351344807e904e02aa77c0733a21d15bb2 Brossers.dll
83811960db65d0d430062ad1ff92b7ca
c3ac906b3228c4c9ce3dd0e46e46b6c5bed4dd4dd61911dc006730a31f90f424c7 Social.dll
ebe83a11b39bfd848fa557a79f2dff1b
fbd8883e659d8082fe8e1ee15e12e2b710fd4c92d8d72b2cfffcdcdc5be7fb Usb.dll
aida6f2d3669fb0d30b3e21437405d81
6a13b98c7dc82ea2a492c0022fd93fa977912dfa8ad5fb4fb4b50e6c05fbb FileGrabber.dll
a816830220abe0cc2e3877eeade0580
bf62d5e034b4ce4fd122ab72fa388ea461fd6e5f317ad3274fe847a526c002 Screengrabber.dll
```

Network:

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

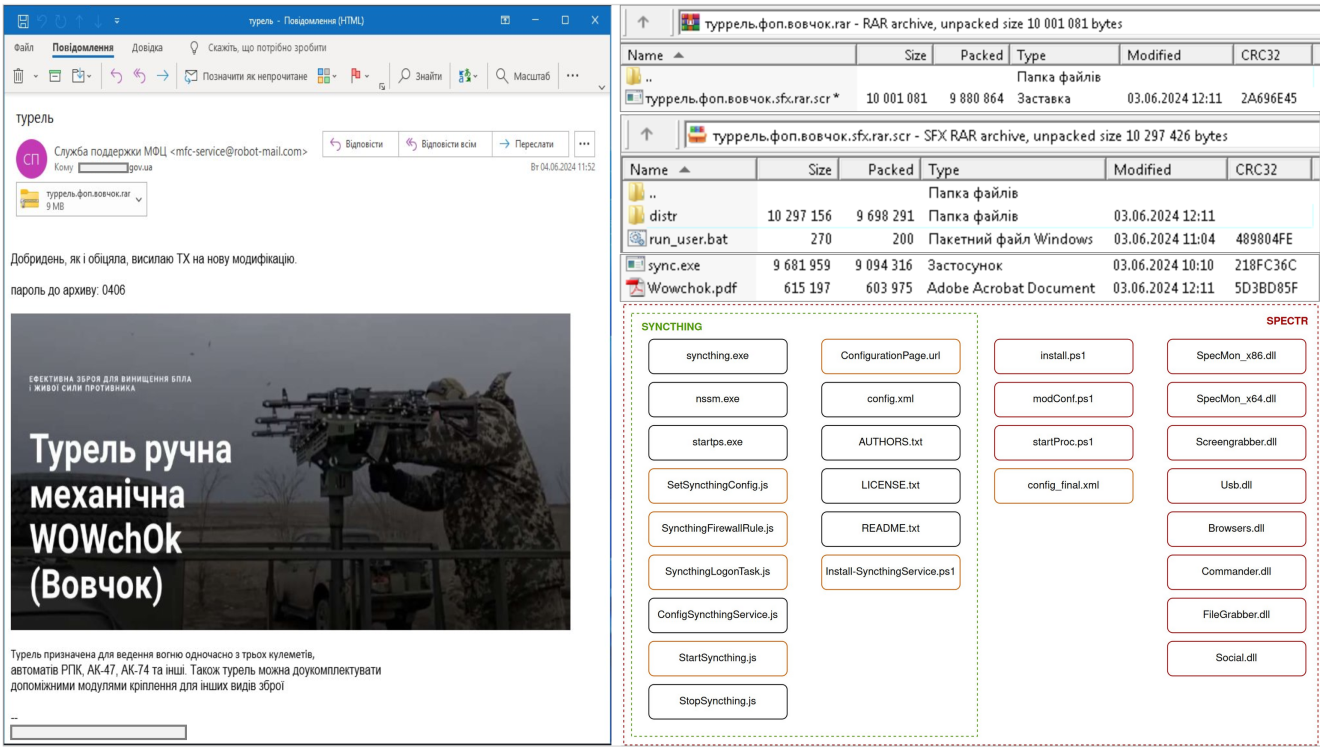
```
upgrades.syncthing[.]net
Syncthing[.]net
```

```
Syncthing.net
```

Host:

```
%APPDATA%Microsoft Configurator
%APPDATA%sync Slave_Sync
%APPDATA%sync Slave_Sync.fs
%APPDATA%?sync Slave_Sync.scrn
%APPDATA%sync Slave_Sync.usb
%LOCACAPDATA% > Programs MSConfigurator
%LOCACAPDATA% > Programs MSConfigurator?scrn
%LOCAPAPDATA% > Programs MSConfigurator > SpecPecMon_x64.dll
%LOCACAPDATA% > Programs MSConfigurator > SpecMon_x86.dll
%LOCACAPDATA% > Programs MSConfigurator >screen >ps1
%LOCAAPPDATA% > Programs MSConfigurator Syncthing.exe
%LOCACAPDATA% >Syncthing >config.xml
C: ?Projects MediaDevices Src MediaDevicesFramework45?objRelease MediaDevices.pdb
W: ?Projects?DEV?SpecMon?Browsers?objRelease?Browssers.pdb
W: ?Projects DEV SpecMon?Commander ?objRelease?Commander.pdb
W: ?Projects DEV ?SpecMon? Common?objRelease Common.pdb
W: ?Projects?DEV?SpecMon?FileGrabber?objRelease?FileGrabber.pdb
W: ?Projects?DEV?SpecMon?Mesengers?objRelease Social.pdb
W: ?Projects DEV SpecMon?PluginLoader?objRelease PluginLoader.pdb
W: ?Projects DEV?SpecMon?Screengrabber?objDebug Screengrabber.pdb
W: ?Projects ?DEV?SpecMon?Usb?ob?Release ?Usb.pdb
script.exe "%userprofile%-Appdata > Local > Programs >MSConfigurator
StartSyncthing.js» /silent
distr-syync.exe /verysilent /currentuser /noicons /SP- /SUPPRESSMSGBOXES /NOCANCEL
GoogleChromeUpdateDailyTask (Sccheduled Task)
MicrosoftEdgeUpdateTaskMachineReg (Sccheduled Task)
```

Graphic images



турель

Служба поддержки МФЦ <mfc-service@robot-mail.com>
Кому [redacted]gov.ua
Вт 04.06.2024 11:52

турреель.фоп.вовчок.rar
9 MB

Добридень, як і обіцяла, висилаю ТХ на нову модифікацію.

пароль до архиву: 0406

Турель призначена для ведення вогню одночасно з трьох кулеметів,
автоматів РПК, АК-47, АК-74 та інші. Також турель можна доукомплектувати
допоміжними модулями кріплення для інших видів зброї

--
[redacted]

туррель.фоп.вовчок.rar - RAR archive, unpacked size 10 001 081 bytes

Name	Size	Packed	Type	Modified	CRC32
..			Папка файлів		
туррель.фоп.вовчок.sfx.rar.scr *	10 001 081	9 880 864	Заставка	03.06.2024 12:11	2A696E45

туррель.фоп.вовчок.sfx.rar.scr - SFX RAR archive, unpacked size 10 297 426 bytes

Name	Size	Packed	Type	Modified	CRC32
..			Папка файлів		
distr	10 297 156	9 698 291	Папка файлів	03.06.2024 12:11	
run_user.bat	270	200	Пакетний файл Windows	03.06.2024 11:04	489804FE
sync.exe	9 681 959	9 094 316	Застосунок	03.06.2024 10:10	218FC36C
Wowchok.pdf	615 197	603 975	Adobe Acrobat Document	03.06.2024 12:11	5D3BD85F

SYNCTHING

syncthing.exe
nssm.exe
startps.exe
SetSyncthingConfig.js
SyncthingFirewallRule.js
SyncthingLogonTask.js
ConfigSyncthingService.js
StartSyncthing.js
StopSyncthing.js
ConfigurationPage.url
config.xml
AUTHORS.txt
LICENSE.txt
README.txt
Install-SyncthingService.ps1

SPECTR

install.ps1
modConf.ps1
startProc.ps1
config_final.xml
SpecMon_x86.dll
SpecMon_x64.dll
Screengrabber.dll
Usb.dll
Browsers.dll
Commander.dll
FileGrabber.dll
Social.dll

Fig.1 Example of email and content of a malicious installer