Кібератака групи UAC-0020 (Vermin) на державні організації України з використанням шкідливої програми SPECTR (CERT-UA#4207)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від Міністерства оборони України отримано повідомлення про розповсюдження електронних листів з темою "постачання" серед державних органів України. У додатку до листа знаходиться захищений паролем архів "ДВТПРОВТ.rar", який містить файл-ярлик "4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf.lnk" та EXE-файл з назвою "4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf", що буде виконаний у разі відкриття LNK-файлу.

В результаті атаки комп'ютер жертви буде уражено модульною шкідливою програмою SPECTR, що, серед іншого, включає: SPECTR.Usb, SPECTR.Shell, SPECTR.Fs, SPECTR.Info, SPECTR.Archiver та інші компоненти.

Атаку здійснено групою UAC-0020 (Vermin), діяльність якої асоційовано з т.з. органами безпеки т.з. ЛНР. Зауважимо, що для атаки 17.03.2022 року використано інфраструктуру, яка застосовувалася групою ще у липні 2019 року. Слід додати, що серверне обладнання групи UAC-0020 (Vermin) вже багато років розміщено на технічному майданчику луганського провайдера vServerCo (AS58271).

Індикатори компрометації:

Файли:

```
baf502b4b823b6806cc91e2c1dd07613    ДВТПРОВТ.rar
993415425b61183dd3f900d9b81ac57f    4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-
1324.rtf
1c2c41a5a5f89eccafea6e34183d5db9    4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-
1324.rtf.lnk
d34dbbd28775b2c3a0b55d86d418f293    data.out
67274bdd5c9537affbd51567f4ba8d5f    license.dat (2022-02-25) (SPECTR.Installer)
75e1ce42e0892ed04a43e3b68afdbc07    conhost.exe
e08d7c4daa45beca5079870251e50236    PluginExec.exe (SPECTR.PluginLoader)
adebdc32ef35209fb142d44050928083    Spectator2.exe (SPECTR.Spectator2)
3ed8263abe009c19c4af8706d52060f8    Archiver.dll (2021-04-09) (SPECTR.Archiver)
f0197bbb56465b5e2f1f17876c0da5ba    ClientInfo.dll (SPECTR.Info)
d0632ef34514bbb0f675c59e6ecca717    FileSystem.dll (2021-04-09) (SPECTR.Fs)
00a54a6496734d87dab6685aa90588f8    FileTransfer.dll (2021-04-09) (SPECTR.Ft)
5db4313b8dbb9204f8f98f2c129fd734    Manager.dll (SPECTR.Mgr)
32343f2a6b8ac9b6587e2e07989362ab    Shell.dll (2021-04-09) (SPECTR.Shell)
ecc7bb2e4672b958bd82fe9ec9cfab14    Usb.dll (SPECTR.Usb)
```

Мережеві:

```
hxxp://176[.]119.2.212/web/t/data.out
hxxp://getmod[.]host/DSGb3Y3X
```

hxxp://getmod[.]host/ThlAHy3S
hxxp://getmod[.]host/OcthdaLm
getmod[.]host (2019-07-12)
syncapp[.]host (2019-07-12)
netbin[.]host (2019-07-12)
stormpredictor[.]host
meteolink[.]host
176[.]119.2.212
176[.]119.2.214
176[.]119.5.194
176[.]119.5.195
AS58271

Хостові:

HKCU\Software\Google\Chrome\NativeMessagingHosts\com.microsoft.browsersec\EncodedProfile

HKCU\Software\Google\Chrome\NativeMessagingHosts\com.microsoft.browsercli\EncodedProfile

%APPDATA%\Microsoft\ExcelCnv\1033\license.dat
%APPDATA%\Microsoft\ExcelCnv\1033\conhost.exe
ESET_OPINIONS (змінна середовища)
MSO (змінна середовища)
MS Office Add-In Install Task (заплановане завдання)

Графічні зображення: