Інформація щодо кібератак групи UAC-0118 (FRwL) з використанням шкідливої програми Somnia (CERT-UA#5185)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вжито заходів з дослідження інциденту інформаційної безпеки, результатом якого стало порушення цілісності та доступності інформації внаслідок застосування шкідливого програмного забезпечення Somnia.

Відповідальність за несанкціоноване втручання в роботу автоматизованих систем та електронно-обчислювальних машин об'єкту атаки взяло на себе угруповання FRwL (aka Z-Team), активність якого відстежується CERT-UA за ідентифікатором UAC-0118.

В рамках дослідження з'ясовано, що початкова компрометація відбулася в результаті завантаження та запуску файлу, що імітував програмне забезпечення "Advanced IP Scanner", але, насправді, містив шкідливе програмне забезпечення Vidar.

Ми припускаємо, що тактика створення копій офіційних веб-ресурсів та розповсюдження шкідливих програм під виглядом популярних програмних продуктів є прерогативою так званих брокерів початкового доступу (initial access broker). У випадку конкретно розглянутого інциденту, з огляду на очевидну приналежність викрадених даних українській організації, відповідний брокер здійснив передачу скомпрометованих даних злочинному угрупованню FRwL з метою подальшого використання для здійснення кібератаки.

Слід звернути увагу, що стілер Vidar, серед іншого, здійснює викрадення даних сесії Telegram, що, за відсутності налаштованої двохфакторної автентифікації та пасс-коду, дозволяє отримати несанкціонований доступ до облікового запису відповідної жертви.

Як було з'ясовано, Telegram жертви використовувався для передачі користувачам конфігураційних файлів VPN-підключення (в тому числі, сертифікатів та автентифікаційних даних). Зважаючи на відсутність двохфакторної автентифікації під час встановлення VPN-з'єднання, зловмисники отримали можливість несанкціонованого підключення до корпоративної мережі.

Отримавши віддалений доступ до комп'ютерної мережі організації за допомогою VPN, зловмисники провели розвідку (зокрема, застосували Netscan), виконали запуск програми Cobalt Strike Beacon, а також, здійснили ексфільтрацію даних, про що свідчить використання програми Rclone. Окрім цього, наявні ознаки запуску Anydesk та Ngrok.

З урахуванням характерних тактик, технік та кваліфікації, починаючи з весни 2022 року групою UAC-0118, за сприяння інших злочинних угруповань, причетних, зокрема, до надання початкового доступу і передачі криптованих білдів програми Cobalt Strike Beacon, проведено декілька втручань в роботу комп'ютерних мереж українських організацій.

Зауважимо, що шкідлива програма Somnia також зазнала змін. В першій версії програми використовувався симетричний алгоритм 3DES. В другій версії реалізовано алгоритм AES; при цьому, зважаючи на динамічність ключа та вектору ініціалізації, ця версія Somnia, за теоретичним задумом зловмисників, не передбачає можливості розшифрування даних.

Індикатори компрометації

Файли:

```
c7948d1ffab0d0a165c56c35e1ae320c
100c5e4d5b7e468f1f16b22c05b2ff1cfaa02eafa07447c7d83e2983e42647f0
Somnia_07_08_22_with_FunnySomnia.rar
abaca1fac308ce6627c1d823c410b174
ac5e68c15f5094cc6efb8d25e1b2eb13d1b38b104f31e1c76ce472537d715e08
Somnia_07_08_22_with_FunnySomnia.exe (Somnia)
638725d249839aaf29fa122dc7aeb41e
99cf5c03dac82c1f4de25309a8a99dcabf964660301308a606cdb40c79d15317    1.exe (Cobalt
Strike Beacon)
93d7636729e908444ab21fb8213f809e
156965227cbeeb0e387cb83adb93ccb3225f598136a43f7f60974591c12fafcf    funnysomnia.exe
dc792b8e287f2f7ddea0469f26d88fb7
e449c28e658bafb7e32c89b07ddee36cadeddfc77f17dd1be801b134a6857aa9    text.exe (Somnia*)
47cd55b63e8e90d8f49352396f76bed6
fbed7e92caefbd74437d0970921bfd7cb724c98c90efd9b6d0c2ac377751c9e5    Ip_scanner.zip
7a4ab857659a40a69c0d29650d991a79
06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdba1f4323bb471591e1d2    Ip_scanner.exe
(Themida; Vidar)
c87261c139ecba1989a88e157a71e3af
1e0facd62d1958ccf79e049270061a9fce3223f7986c526f6f3a93ef85180a72
Ip_scanner_unpacked.exe (Vidar)
(пов'язані файли)
58c40d0ad81f25bcd68a5523d867eb34
1f4c5ab072f384b9adfafd35903c5b54b8a3ad167250728d0d400454300a4367    Ip_scanner.exe
(Vidar)
```

Мережеві:

```
franygreat@outlook.com (mega.nz)
hXXps://t[.]me/cheaptrains (Vidar)
hXXps://mastodon[.]social/@ffolegg94 (Vidar)
hXXp://193[.]43.146.42:80 (Vidar)
hXXps://advanced-ip-scaner.com.vuxuancuong[.]com/ (результат пошукової видачі в Google
за запитом "Advanced IP Scanner")
hXXps://advanced-ip-scanner[.]website/en/
https://onedrive.live.com/download?
cid=E8A357DC635F5F11&resid=E8A357DC635F5F11!552&authkey=AN-tOu0N0SGFnpg
hXXps://zambeziz[.]com/jquery-3.3.1.min.js
vuxuancuong[.]com
advanced-ip-scaner.com.vuxuancuong[.]com
zambeziz[.]com
hXXps://gofile[.]io/d/7KbRYr
hXXps://gofile[.]io/d/nycrb4
hXXps://store1.gofile[.]io/download/27a73fd4-a939-4a05-9c0e-54c0c5dfef3d/1.exe
hXXps://store3.gofile[.]io/download/939fad81-10ba-438e-b396-
```

c2f42f209ab0/netscan_portable.7z
hXXps://store8.gofile[.]io/download/43571707-464b-40c8-bf5e-2d9e07c554b8/Somnia_07_08_22_with_FunnySomnia.exe
hXXps://store8.gofile[.]io/download/8b9f91c9-b770-4ed5-b60f-ec1dd5ca8b43/1.jpeg
209[.]222.101.65 (несанкціоновані підключення до VPN)
139[.]60.161.52
193[.]43.146.42

(пов'язані індикатори)
hXXps://advanced-ip-scanner[.]click/en/
hXXps://advanced-ip-scanner[.]site/en/
hXXps://www.dropbox[.]com/s/26gri1ashi4rydb/Ip_scanner.zip?dl=1
advanced-ip-scanner[.]click
advanced-ip-scanner[.]site
hXXp://185[.]96.163.102:80
agrikoz[.]com
aluaadin[.]com
arminext[.]com
benokij[.]com
fudupdate[.]com
sinergil[.]com
softloadup[.]com
survefuz[.]com
vinergil[.]com
zbignef[.]com
139[.]60.161.165
139[.]60.161.167
139[.]60.161.213
139[.]60.161.47
139[.]60.161.63
185[.]170.144.217
185[.]96.163.102
193[.]43.146.39
5[.]252.22.96
94[.]232.41.105
95[.]217.244.218

Хостові:

C:\Users\Admin\source\repos\Somnia\FunnySomnia\obj\Release\FunnySomnia.pdb
%TMP%\text.exe
C:\ProgramData\VMware\VMware Tools\1.exe
C:\ProgramData\pe_https_x64_360_1.exe
C:\Users\%USERNAME%\Downloads\Ip_scanner.zip
C:\Users\%USERNAME%\Downloads\Ip_scanner\Ip_scanner.exe
C:\Users\frwl\Desktop\netscan_portable\64-bit\netscan.exe
C:\Users\frwl\Downloads\1.jpeg
C:\Users\frwl\Downloads\Somnia_07_08_22_with_FunnySomnia.exe

```
C:\Users\frwl\Downloads\netscan_portable.7z
C:\Users\%USERNAME%\Downloads\1.exe
D:\FunnySomnia.exe
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\FunnySomnia
```

Графічні зображення

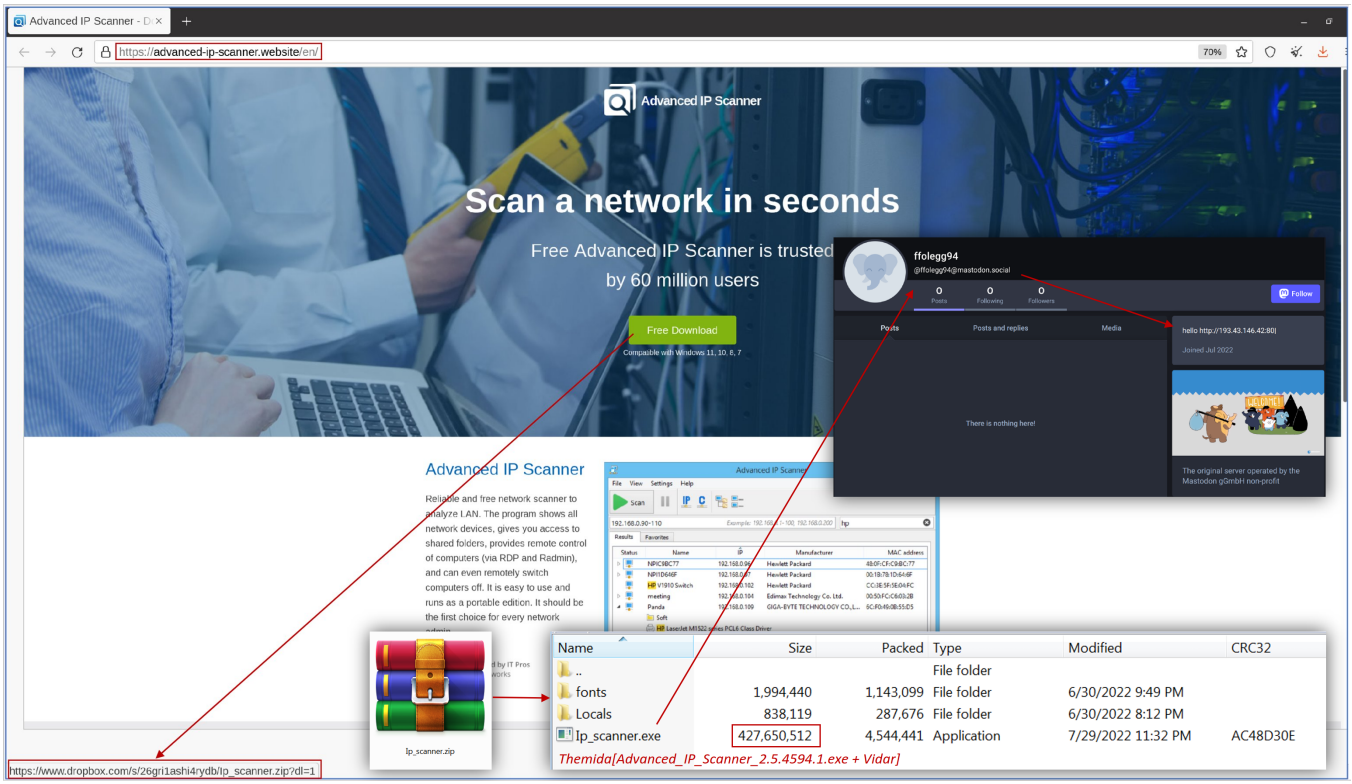

Рис.1 Приклад етапу початкового ураження

```
public static void CrashOne(string fname)
{
    string path = fname + ".somnia";
    using TripleDES tripleDES = TripleDES.Create();
    tripleDES.IV = CrashFile.IV;
    tripleDES.Key = CrashFile.Key;
    using FileStream fileStream = File.OpenRead(fname);
    using FileStream fileStream2 = new FileStream(path, FileMode.Create, FileAccess.Write);
    using CryptoStream cryptoStream = new CryptoStream(fileStream2, tripleDES.CreateEncryptor(), CryptoStreamMode.Write);
    fileStream2.SetLength(0L);
    fileStream.CopyTo(cryptoStream);
}
```

```
public static void CrashOne(string fname)
{
    string path = fname + ".somnia";
    byte[] IV = GenerateRandomByteArray(16);
    byte[] Key = GenerateRandomByteArray(32);
    using Aes AES = Aes.Create();
    AES.IV = IV;
    AES.Key = Key;
    AES.Mode = CipherMode.CBC;
    AES.Padding = PaddingMode.PKCS7;
    using FileStream fileStream = File.OpenRead(fname);
    using FileStream fileStream2 = new FileStream(path, FileMode.Create, FileAccess.Write);
    using CryptoStream cryptoStream = new CryptoStream(fileStream2, AES.CreateEncryptor(), CryptoStreamMode.Write);
    fileStream2.SetLength(0L);
    fileStream.CopyTo(cryptoStream);
}
```

Рис.2 Приклади криптографічних функцій двох різних версій шкідливої програми Somnia

```
'.txt', '.json', '.xml', '.xlsx', '.odt', '.ps1', '.csv', '.xls', '.db', '.sqlite3', '.sql', '.vdi', '.vhd', '.vmdk', '.pvm', '.vmem', '.vmsn',
'.vmsd', '.nvram', '.vmx', '.raw', '.qcow2', '.subvol', '.bin', '.vsv', '.avhd', '.vmrs', '.vhdx', '.avdx', '.vmcx', '.iso', '.4dd', '.4dl',
'.acc', '.adb', '.ade', '.adf', '.adp', '.arc', '.ora', '.alf', '.ask', '.btr', '.bdf', '.cat', '.cdb', '.ckp', '.cma', '.cpd', '.dac', '.dad',
'.das', '.db3', '.dbc', '.dbf', '.dbs', '.dbt', '.dbv', '.dbx', '.dcb', '.dct', '.dcx', '.ddl', '.dli', '.dp1', '.dqy', '.dsk', '.dsn', '.dts',
'.dxl', '.eco', '.ecx', '.edb', '.epi', '.exb', '.fcd', '.fdb', '.fic', '.fmp', '.fol', '.fp3', '.fp4', '.fp5', '.fp7', '.fpt', '.frm', '.gdb',
'.grd', '.gwi', '.hdb', '.his', '.ib', '.idb', '.ihx', '.itd', '.itw', '.jet', '.jtx', '.kdb', '.kex', '.lgc', '.lwx', '.maf', '.maq', '.mar',
'.mas', '.mav', '.mdb', '.mdf', '.mpd', '.mrg', '.mud', '.mwb', '.myd', '.ndf', '.nnt', '.nrm', '.ns2', '.ns3', '.ns4', '.nsf', '.nv', '.nv2',
'.nwd', '.nyf', '.odb', '.oqy', '.orx', '.owc', '.p96', '.p97', '.pan', '.pdb', '.pdm', '.pnz', '.qry', '.qvd', '.rbf', '.rct', '.rod', '.rpd',
'.rsd', '.sas', '.sbf', '.scx', '.sdb', '.sdc', '.sdf', '.sis', '.spq', '.te', '.tem', '.tmd', '.tps', '.trc', '.trm', '.udb', '.udl', '.usr',
'.v12', '.vis', '.vpd', '.vvv', '.wdb', '.wmd', '.wrk', '.xdb', '.xld', '.abc', '.abs', '.abx', '.adn', '.db2', '.fm5', '.hjt', '.icg', '.icr',
'.lut', '.maw', '.mdn', '.mdt', '.zip', '.rar', '.7z', '.tar', '.gz', '.mp4', '.avi', '.mkv', '.mpeg', '.mp3', '.wav', '.pdf', '.docx', '.doc',
'.gzip', '.wmv', '.flv', '.html', '.css', '.js', '.ppt', '.pptx', '.fb2', '.epub', '.mobi', '.torrent', '.ods', '.csproj', '.cs', '.cpp', '.jpg',
 '.png', '.bmp', '.gif', '.tif', '.jpeg', '.psd', '.ai', '.1cd', '.dat', '.dt', '.epf', '.ifd', '.ini'
```

```
'.txt', '.json', '.xml', '.xlsx', '.odt', '.ps1', '.csv', '.xls', '.db', '.sqlite3', '.sql', '.vdi', '.vhd', '.vmdk', '.pvm', '.vmem', '.vmsn',
'.vmsd', '.nvram', '.vmx', '.raw', '.qcow2', '.subvol', '.bin', '.vsv', '.avhd', '.vmrs', '.vhdx', '.avdx', '.vmcx', '.iso', '.4dd', '.4dl',
'.acc', '.acc', '.adb', '.ade', '.adf', '.adp', '.arc', '.ora', '.alf', '.ask', '.btr', '.bdf', '.cat', '.cdb', '.ckp', '.cma', '.cpd', '.dac',
'.dad', '.dad', '.das', '.db', '.db3', '.dbc', '.dbf', '.dbs', '.dbt', '.dbv', '.dbx', '.dcb', '.dct', '.dcx', '.ddl', '.dli', '.dp1', '.dqy',
'.dsk', '.dsn', '.dts', '.dxl', '.eco', '.ecx', '.edb', '.epi', '.exb', '.fcd', '.fdb', '.fic', '.fmp', '.fmp', '.fmp', '.fol', '.fp3', '.fp4',
'.fp5', '.fp7', '.fpt', '.frm', '.gdb', '.grd', '.gwi', '.hdb', '.his', '.ib', '.idb', '.ihx', '.itd', '.itw', '.jet', '.jtx', '.kdb', '.kex',
'.kex', '.kex', '.lgc', '.lwx', '.maf', '.maq', '.mar', '.mas', '.mav', '.mdb', '.mdf', '.mpd', '.mrg', '.mud', '.mwb', '.myd', '.ndf', '.nnt',
'.nrm', '.ns2', '.ns3', '.ns4', '.nsf', '.nv', '.nv2', '.nwd', '.nyf', '.odb', '.oqy', '.orx', '.owc', '.p96', '.p97', '.pan', '.pdb', '.pdm',
'.pnz', '.qry', '.qvd', '.rbf', '.rct', '.rod', '.rod', '.rpd', '.rsd', '.sas', '.sbf', '.scx', '.sdb', '.sdc', '.sdf', '.sis', '.spq', '.sql',
'.sql', '.sql', '.sql', '.te', '.tem', '.tmd', '.tps', '.trc', '.trm', '.udb', '.udl', '.usr', '.v12', '.vis', '.vpd', '.vvv', '.wdb', '.wmd',
'.wrk', '.xdb', '.xld', '.xml', '.abc', '.abs', '.abx', '.acc', '.adn', '.db2', '.fm5', '.hjt', '.icg', '.icr', '.kdb', '.lut', '.maw', '.mdn',
'.mdt', '.zip', '.rar', '.7z', '.tar', '.gz', '.mp4', '.avi', '.mkv', '.mpeg', '.mp3', '.wav', '.pdf', '.docx', '.xls', '.xlsx', '.sql', '.doc',
'.odt', '.csv', '.gzip', '.wmv', '.flv', '.html', '.css', '.js', '.ppt', '.pptx', '.fb2', '.epub', '.mobi', '.json', '.xml', '.torrent', '.ods',
'.csproj', '.cs', '.cpp', '.jpg', '.png', '.bmp', '.gif', '.tif', '.jpeg', '.psd', '.ai', '.1cd', '.dat', '.dt', '.epf', '.ifd', '.ini', '.rtf',
'.zip', '.rar', '.7z', '.JPG', '.PDF', '.1cd', '.epf', '.cf', '.dt', '.erf', '.mxl', '.efd', '.pfl'
```

Рис.3 Приклади розширень файлів, що підлягають шифруванню