Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA вжито невідкладних заходів з реагування на інцидент інформаційної безпеки, пов’язаний з цільовою атакою на об’єкт енергетики України.

Задум зловмисників передбачав виведення з ладу декількох інфраструктурних елементів об’єкту атаки, а саме:

- високовольтних електричних підстанцій – за допомогою шкідливої програми INDUSTROYER2; причому, кожен виконуваний файл містив статично вказаний набір унікальних параметрів для відповідних підстанцій (дата компіляції файлів: 23.03.2022);
- електронних обчислювальних машин (ЕОМ) під управлінням операційної системи Windows (комп’ютерів користувачів, серверів, а також автоматизованих робочих місць АСУ ТП) – за допомогою шкідливої програми-деструктора CADDYWIPER; при цьому для дешифрування і запуску останнього передбачено використання лоадеру ARGUEPATCH та шелкоду TAILJUMP;
- серверного обладнання під управлінням операційної систем Linux – за допомогою шкідливих скриптів-деструкторів ORCSHRED, SOLOSHRED, AWFULSHRED;
- активного мережевого обладнання.

Централізоване розповсюдження і запуск CADDYWIPER реалізовано за допомогою механізму групових політик (GPO). З метою додавання групової політики, що передбачає завантаження компонентів файлового деструктору з контролеру домену, а також створення запланованого завдання на ЕОМ, використано PowerShell-скрипт POWERGAP.

Можливість горизонтального переміщення між сегментами локальної обчислювальної мережі забезпечено шляхом створення ланцюгів SSH-тунелів. Для віддаленого виконання команд використано IMPACKET.

Відомо, що організація-жертва зазнала двох хвиль атак. Первинна компрометація відбулася не пізніше лютого 2022 року. Відключення електричних підстанцій та виведення з ладу інфраструктури підприємства було заплановане на вечір п’ятниці, 8 квітня 2022 року. Разом з тим, реалізації зловмисного задуму на поточний момент вдалося запобігти.

З метою виявлення ознак присутності подібної загрози в інших організаціях України, оперативну інформацію з рівнем обмеження доступу TLP:AMBER, включаючи зразки шкідливих програм,

індикатори компрометації та Yara-правила, передано обмеженому колу міжнародних партнерів та підприємствам енергетичного сектору України.

Окрему вдячність висловлюємо компаніям Microsoft та ESET.

Індикатори компрометації

Файли:

```
fbe32784c073e341fc57d175a913905c
43d07f28b7b699f43abd4f695596c15a90d772bfbd6029c8ee7bc5859c2b0861 sc.sh
(OrcShred)
73561d9a331c1d8a334ec48dfd94db99
bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99 wobf.sh
(AwfulShred)
97ad7f3ed815c0528b070941be903d07
87ca2b130a8ec91d0c9c0366b419a0fce3cb6a935523d900918e634564b88028 wsol.sh
(SoloShred)
9ec8468dd4a81b0b35c499b31e67375e
cda9310715b7a12f47b7c134260d5ff9200c147fc1d05f030e507e57e3582327 {zrada.exe,
peremoga.exe, vatt.exe} (ArguePatch)
1938380a81a23b8b1100de8403b583a7
1724a0a3c9c73f4d8891f988b5035effce8d897ed42336a92e2c9bc7d9ee7f5a pa.pay
(TailJump)
b63b9929b8f214c4e8dcff7956c87277
fc0e6f2effbfa287217b8930ab55b7a77bb86dbd923c0e8150551627138c9caa
caddywiper.bin (CaddyWiper)
3229e8c4150b5e43f836643ec9428865
7062403bccacc7c0b84d27987b204777f6078319c3f4caa361581825c1a94e87 108_100.exe
(2022-03-23) (Industroyer2)
```

Хостові:

```
C:\Users\peremoga.exe JRIBDFIMCQAKVBBP C:\Users\pa1.pay
reg save HKLM\SYSTEM C:\Users\Public\sys.reg /y
reg save HKLM\SECURITY C:\Users\Public\sec.reg /y
reg save HKLM\SAM C:\Users\Public\sam.reg /y
\\%DOMAIN%\sysvol\%DOMAIN%\Policies\%GPO ID%\Machine\zrada.exe
\\%DOMAIN%\sysvol\%DOMAIN%\Policies\%GPO ID%\Machine\pa.pay
C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll MiniDump
%PID% C:\Users\Public\mem.dmp full
C:\Windows\Temp\link.ps1
C:\Users\peremoga.exe
C:\Users\pa1.pay
```

```
C:\Dell\vatt.exe
C:\Dell\pa.pay
C:\Dell\108_100.exe
C:\tmp\cdel.exe
```

Мережеві:

```
91.245.255[.]243
195.230.23[.]19
```

Графічні зображення