cert-gov-ua.translate.goog /article/39518

Cyberattack by Sandworm Group (UAC-0082) on energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA # 4435)

Cyberattack by Sandworm Group (UAC-0082) on energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA # 4435)

General Information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA has taken urgent measures to respond to an information security incident related to a targeted attack on Ukraine's energy facility.

The idea of the attackers involved the decommissioning of several infrastructural elements of the object of attack, namely:

- high-voltage electrical substations - using the malicious program INDUSTROYER2; moreover, each executable file contained a statically specified set of unique parameters for the respective substations (file compilation date: 23.03.2022);
- electronic computers (computers) running the Windows operating system (user computers, servers, as well as automated workstations ACS TP) - using the malicious program-destructor CADDYWIPER; in this case, the decryption and launch of the latter involves the use of the ARGUEPATCH loader and the TAILJUMP silkcode;
- server equipment running Linux operating systems - using malicious destructive scripts ORCSHRED, SOLOSHRED, AWFULSHRED;
- active network equipment.

Centralized distribution and launch of CADDYWIPER is implemented through the Group Policy Mechanism (GPO). The POWERGAP PowerShell script was used to add a Group Policy that downloads file destructor components from a domain controller and creates a scheduled task on a computer.

The ability to move horizontally between segments of the local area network is provided by creating chains of SSH tunnels. IMPACKET is used for remote execution of commands.

It is known that the victim organization suffered two waves of attacks. The initial compromise took place no later than February 2022. The disconnection of electrical substations and the decommissioning of the company's infrastructure was scheduled for Friday evening, April 8, 2022. At the same time, the implementation of the malicious plan has so far been prevented.

In order to identify signs of similar threats in other Ukrainian organizations, operational information with TLP: AMBER access level, including malware samples, compromise indicators and Yara rules, was provided to a limited number of international partners and Ukrainian energy companies.

Special thanks to Microsoft and ESET.

Indicators of compromise

Files:

```
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)
```

Hosts:

```
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

Network:

91.245.255 [.] 243
195.230.23 [.] 19

Graphic images