Security for the greater good

Monthly Cyber Threat Intelligence report November 2023

2023-11-30 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

1. Executive summary

This month, aDvens' CERT highlights three noteworthy vulnerabilities in addition to those already published.

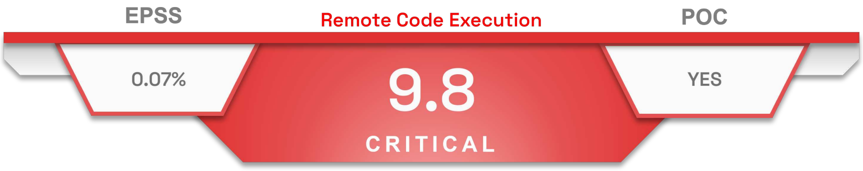
Through two articles, CERT analysts delineate the multifunctional malware named Mad Cat, which has been active since October. Additionally, they address an attack campaign orchestrated by the APT group Sandworm, specifically targeting industrial environments.

2. Vulnerabilities

This month, the CERT aDvens highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation…). Applying their patches or workarounds is highly recommended.

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

2.1. Fortinet - CVE-2023-36553



On 14 november 2023, Fortinet published security advisory about the CVE-2023-36553 affecting FortiSIEM servers.

A flaw in the neutralization of special characters in an *OS* command of the FortiSIEM report server, allows an unauthenticated remote attacker to execute unauthorized commands via API requests.

2.1.1. Risk

- Remote code execution

2.1.2. Type of vulnerability

- **CWE-78**: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.1.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Affected products

- FortiSIEM versions 4.7.x, 4.9.x, 4.10.x, 5.0.x, 5.1.x, 5.2.x, 5.3.x and 5.4.x

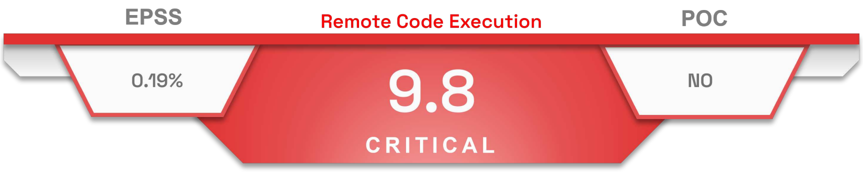
2.1.5. Recommendation

- Update FortiSIEM to versions 6.4.3, 6.5.2, 6.6.4, 6.7.6, 7.0.1, 7.1.0 or later.
- Additional information is available in Fortinet's advisory.

2.1.6. Proof of concept

A Proof of Concept is available in open sources.

2.2. Aruba - CVE-2023-45614



EPSS

0.19%

Remote Code Execution

9.8

CRITICAL

POC

NO

On 14 november 2023, Aruba published a security advisory about three critical vulnerabilities in ArubaOS and InstantOS. The vulnerability CVE-2023-45614, with a CVSS score of 9.8, have been discovered and reported by XiaoC from Moonlight Bug Hunter.

A buffer overflow error in the *CLI* service allows a remote, unauthenticated attacker, by sending specially forged requests to the port 8211 (UDP), to execute arbitrary code on the system with high privileges.

2.2.1. Risk

- Remote code execution

2.2.2. Type of vulnerability

- **CWE-120**: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

2.2.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Affected products

ArubaOS :

- Versions versions 10.5.x.x prior to 10.5.0.1
- Versions versions 10.4.x.x prior to 10.4.0.3
- Versions 1.6.x prior to 1.6.4

InstantOS :

- Versions 8.11.x.x prior to 8.11.2.0
- Versions 8.10.x.x prior to 8.10.0.9
- Versions 8.6.x prior to 8.6.0.23

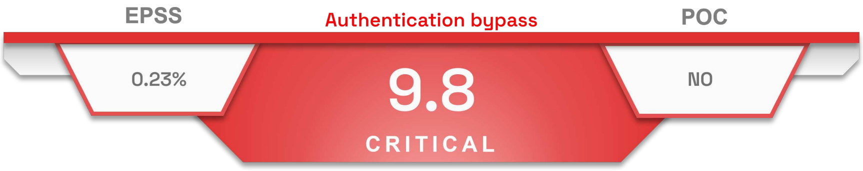
2.2.5. Recommendation

- Update ArubaOS to versions 10.4.0.3, 10.5.0.1 or later.
- Update InstantOS to versions 8.6.0.23, 8.10.0.9, 8.11.2.0 or later.
- If the patch cannot be deployed, it is recommended to enable the cluster-security feature on InstantOS versions 6.x and 8.x. This option is not available for ArubaOS 10 devices, but it is possible to block access to port 8211.
- Additional information is available in Aruba's advisory.

2.2.6. Proof of concept

To date, no Proof of Concept is available in open sources.

2.3. VMware - CVE-2023-34060



On 14 november 2023, VMware publised a security advisory about a critical vulnerability in VMware Cloud Director Appliance. This vulnerability, with a CVSS score of 9.8, allow a unauthenticated attacker to bypass the security policy.

This vulnerability is exploitable for components migrated to 10.5 from an earlier version. An attacker with remote access can bypass connection restrictions when authenticating on port 22 (ssh) or port 5480 (appliance management console).

> *VMWARE Cloud Director Appliance* instances deployed directly in version 10.5 are not affected by the vulnerability.

2.3.1. Risk

- Security policy bypass

2.3.2. Type of vulnerability

- **CWE-306** : Missing Authentication for Critical Function

2.3.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Affected products

- VMware Cloud Director Appliance version 10.5 if updated from version 10.4 or earlier.
- New installations of VMware Cloud Director Appliance version 10.5, and versions 10.4 and earlier, are not vulnerable.

2.3.5. Recommendation

- Applied the KB95534 to VMware Cloud Director Appliance version 10.5 ou later.
- Additional information is available in VMware's advisoriy.

2.3.6. Proof of concept

To date, no Proof of Concept is available in open sources.

3. Virology : study of a Mad Cat sample

Mad Cat is a multi-function malware whose emergence dates from the end of October 2023. After having infected a system, it can **erase data** (*wiper*), **encrypt data** (*ransomware*) and **steal cryptocurrencies** (*crypto hi-jacking*) from the victim.

Generated by the famous Chaos builder, Mad Cat is an iteration which seems to preserve an anatomy (structure) and physiology (functioning) similar to the viral strains of its siblings: a set of malware known as "*Chaos ransomware family*".

3.1. Main features

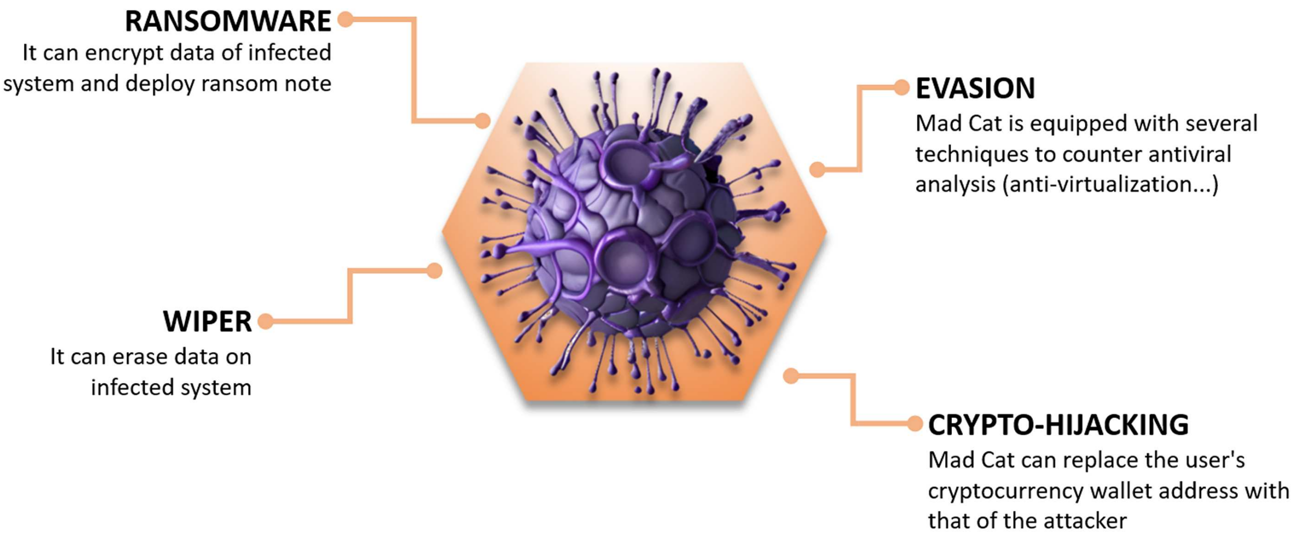

RANSOMWARE
It can encrypt data of infected system and deploy ransom note
EVASION
Mad Cat is equipped with several techniques to counter antiviral analysis (anti-virtualization...)
WIPER
It can erase data on infected system
CRYPTO-HIJACKING
Mad Cat can replace the user's cryptocurrency wallet address with that of the attacker

Figure 1. Main features of Mad Cat.

3.2. Virus lineage

Mad Cat ransomware appears to be an iteration generated by the Chaos builder, version 4.

Developed by a cybercriminal nicknamed RyukRans (unrelated to the Ryuk ransomware), the Chaos builder is a generator of viral strains whose emergence is announced on the XSS forum in June 2021. This builder is developed from the source code of the Hidden Tears ransomware, published in August 2015.

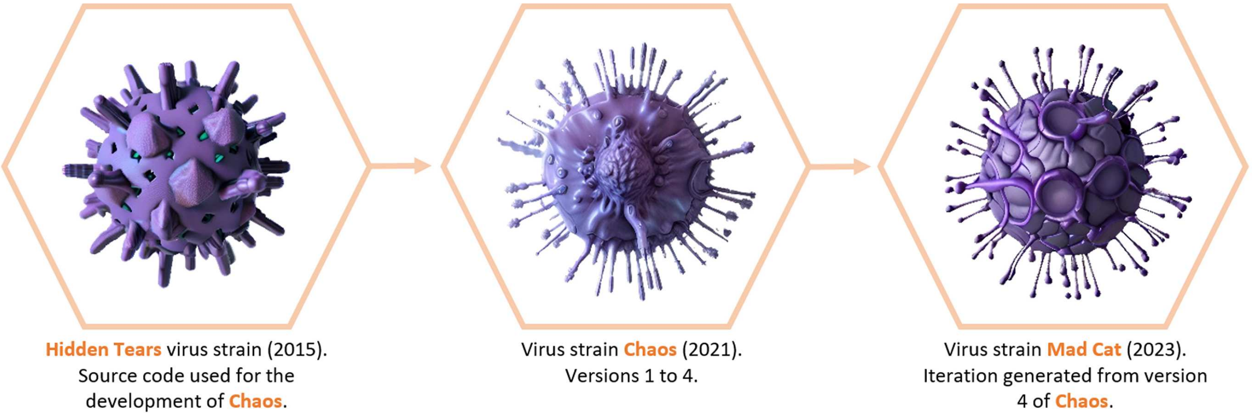

Hidden Tears virus strain (2015).
Source code used for the development of **Chaos**.
Virus strain **Chaos** (2021).
Versions 1 to 4.
Virus strain **Mad Cat** (2023).
Iteration generated from version 4 of **Chaos**.

Figure 2. Origin of Mad Cat : the Chaos builder developed by RyukRans.

3.3. Infectiology

Below are the infection vector used by the attackers to distribute the malware:

- Torrent websites
- Malicious advertisements
- Malicious attachments
- Hacked software ("*cracked*")

3.4. Victimology

Iterations generated by the Chaos builder are known to be used against organisations linked to the following sectors:

- Finance
- Agriculture
- Trade / Business
- Health

Victims are mainly located in America. Some analyses specify that samples of the Mad Cat ransomware were found in the Clouds of several companies.

3.5. Code analysis

This section contains a non-exhaustive analysis of the Mad Cat malicious code.

3.5.1. Execution

- Dropping a copy of the virus strain

```
Source: C:\Users\user\Desktop\1HeZK0tOCh.exe
File created: C:\Users\user\AppData\Roaming\Devenders.exe
```

3.5.2. Defense evasion

- Time-based evasion

```
Source: C:\Users\user\Desktop\1HeZK0tOCh.exe
Thread sleep time: -922337203685477s >= -30000s
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
Thread sleep count: 1052 > 30
```

- Evade the antivirus scan by stopping its execution

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
Last function: Thread delayed
```

- Detect virtualisation

```
Source: C:\Windows\System32\vds.exe
File opened / queried: scsi#disk&ven_vmware&prod_virtual_disk#4&1656f219&0&000000#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}
```

```
Binary or memory string: 2microsoft-hyper-v-client-migration-replacement.man8!
Binary or memory string: pEFI VMware Virtual SATA CDROM Drive (0.0)
Binary or memory string: KD:\sources\replacementmanifests\microsoft-hyper-v-migration-replacement.man
Binary or memory string: NECVMWar VMware SATA CD00
Binary or memory string: SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\4&1656F219&0&000000
Binary or memory string: +microsoft-hyper-v-migration-replacement.man
Binary or memory string: VMware Virtual disk SCSI Disk Device
```

- Disabling Task Manager

```
Registry Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Value: 1
```

- Delete Windows Catalogs

```
Source: C:\Windows\System32\cmd.exe
Process: C:\Windows\System32\wbadmin.exe wbadmin  delete catalog -quiet
```

- Anti-debugging

```
Source: C:\Users\user\Desktop\1HeZK0tOCh.exe
Process token adjusted: Debug (count 1)
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
Process token adjusted: Debug (count 1)
```

3.5.3. Persistence

- Three artifacts are dropped in the system *Startup* folder

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File created: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Devenders.url
```

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
```

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HACKED.TXT
```

3.5.4. Privilege escalation

- Process token adjusted to "Debug"

```
Source: C:\Users\user\Desktop\1HeZK0tOCh.exe
Process token adjusted: Debug
Privilege: Debug (Count = 1)
```

- Process token adjusted to "Security"

```
Source: C:\Windows\System32\wbengine.exe
Process token adjusted: Security
```

3.5.5. Collection and credential access

- Search for sensitive information (usernames and passwords)

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini.wt6i
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File opened: C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\v6zchhhv.default-
release\SiteSecurityServiceState.txt
```

3.5.6. Impact

- Deleting the shadow copy

```
Source: C:\Windows\System32\cmd.exe
Process created: C:\Windows\System32\vssadmin.exe vssadmin  delete shadows /all /quiet
```

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
Process created: C:\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe" /C vssadmin delete shadows
/all /quiet & wmic shadowcopy delete
```

```
Source: 1HeZK0tOCh.exe
Binary or memory string: /C yvssadmin delete shadows /all /quiet & wmic shadowcopy delete
```

- Inhibiting system recovery

```
C:\Windows\system32\bcdedit.exe
bcdedit  /set {default} recoveryenabled no
```

- Crypto hi-jacking. Some iterations of the Chaos builder are known to replace the user's cryptocurrency wallet address with that of the attacker.

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
```

```
Window created: window name: CLIPBRDWNDCLASS
Class name: CLIPBRDWNDCLASS (count = 1)
```

- Data encrypted for impact

```
Source: 1HeZK0tOCh.exe
String / Function: encryptDirectory
```

```
Source: Devenders.exe
String / Function: encryptDirectory
```

- According to Truesec, the iterations generated by version 4 of the builder have the following encryption characteristics

```
Strain: Chaos 4
```

```
Encrypts/Wipe : Encrypts files under 1 MB. Overwrites larger.
```

```
Key generation: 20-char password (System.Random). Key and IV generated from password with
Rfc2898DeriveBytes (1000 iteration and static salt)
```

```
Data crypto: AES-256-CBC
```

```
Secret crypto: RSA-1024
```

```
File format: AES key encrypted with RSA and prepended to the file within the ASCII "<EncryptedKey>".
Encrypted data is base64 encoded.
```

3.5.7. Ransom note

- Creation of the ransom note

```
Source: C:\Users\user\AppData\Roaming\Devenders.exe
File dropped: C:\Users\HACKED.TXT
```

- Content of the ransom note

```
all your files encrypted, and you can't recover it.
how to recover?
1- pay [ 0.02 btc ] to: [Address removed]
- send us transaction id here => telegram [Address removed]
payment informationamount: 0.05 btc
bitcoin address:  [Address removed]
```

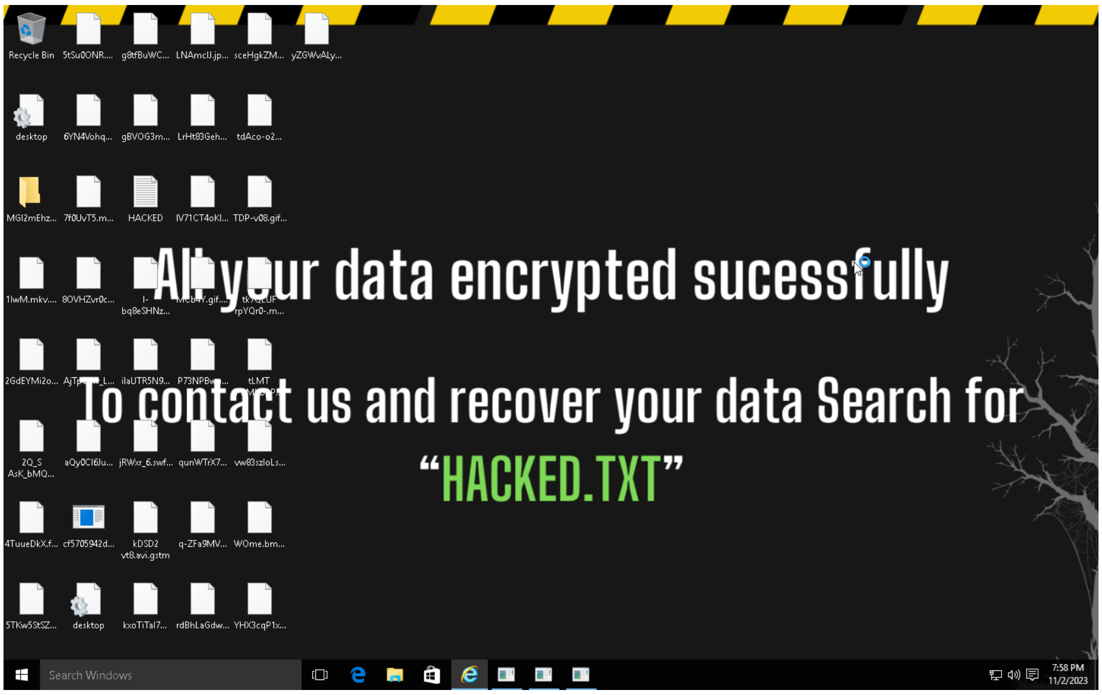
- Modification of the wallpaper

```
Process: Devenders.exe
\REGISTRY\USER\S-1-5-21-1861898231-3446828954-4278112889-1000\Control Panel\Desktop\Wallpaper =
"C:\\Users\\Admin\\AppData\\Local\\Temp\\dtwr8o4gz.jpg"
```

```
\REGISTRY\USER\S-1-5-21-1861898231-3446828954-4278112889-1000\Control Panel\Desktop\Wallpaper =
"C:\\Users\\Admin\\Pictures\\My Wallpaper.jpg"
```

3.5.8. Modified wallpaper

The screenshot below show the modified wallpaper by Mad Cat.



All your data encrypted sucessfully

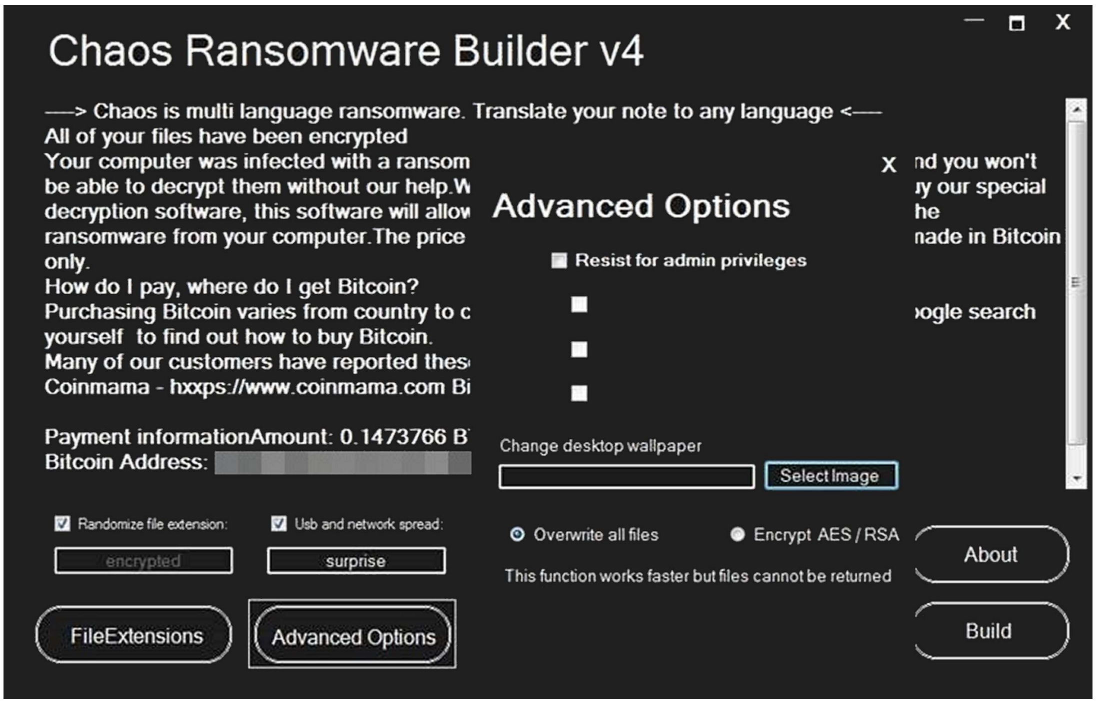
To contact us and recover your data Search for

"HACKED.TXT"

Figure 3. Wallpaper changed by Mad Cat.

3.6. Chaos Version 4

Below is the user interface of the builder Chaos, version 4. This fourth version is the only one that offers attackers the possibility of changing the wallpaper of the infected system.



Chaos Ransomware Builder v4

---> Chaos is multi language ransomware. Translate your note to any language <---
All of your files have been encrypted
Your computer was infected with a ransom ... nd you won't
be able to decrypt them without our help.W ... ty our special
decryption software, this software will allow ... he
ransomware from your computer.The price ... nade in Bitcoin
only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to c ... oogle search
yourself to find out how to buy Bitcoin.
Many of our customers have reported thes
Coinmama - hxxps://www.coinmama.com Bi

Payment informationAmount: 0.1473766 B
Bitcoin Address: [redacted]

Advanced Options

☐ Resist for admin privileges

☐

☐

☐

Change desktop wallpaper

Select Image

● Overwrite all files ○ Encrypt AES / RSA

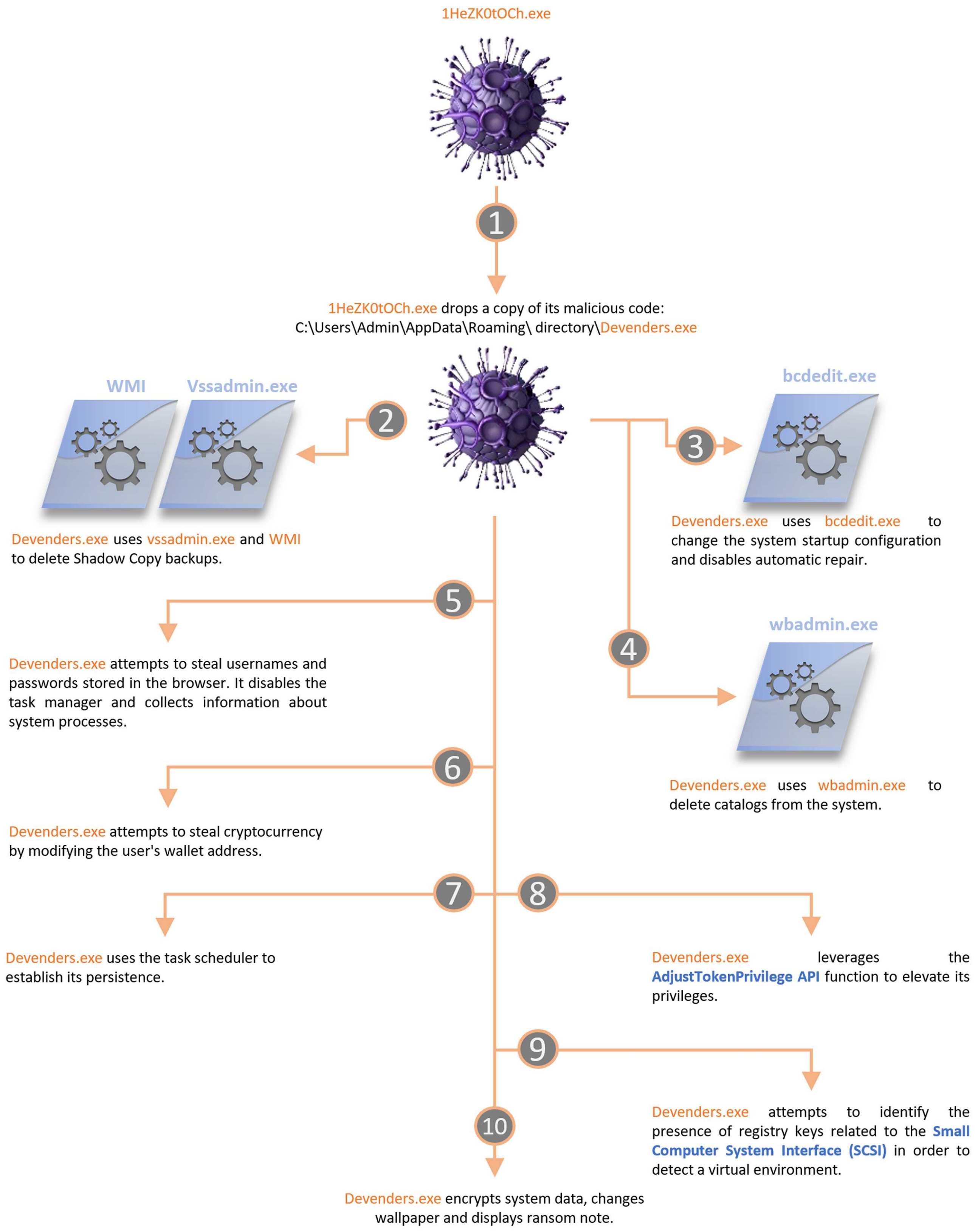
This function works faster but files cannot be returned

☑ Randomize file extension: encrypted

☑ Usb and network spread: surprise

Figure 4. Chaos V4 user interface.

3.7. Kill chain



1HeZK0tOCh.exe drops a copy of its malicious code:
C:\Users\Admin\AppData\Roaming\ directory\Devenders.exe

Devenders.exe uses vssadmin.exe and WMI to delete Shadow Copy backups.

Devenders.exe uses bcdedit.exe to change the system startup configuration and disables automatic repair.

Devenders.exe uses wbadmin.exe to delete catalogs from the system.

Devenders.exe attempts to steal usernames and passwords stored in the browser. It disables the task manager and collects information about system processes.

Devenders.exe attempts to steal cryptocurrency by modifying the user's wallet address.

Devenders.exe uses the task scheduler to establish its persistence.

Devenders.exe leverages the **AdjustTokenPrivilege API** function to elevate its privileges.

Devenders.exe attempts to identify the presence of registry keys related to the **Small Computer System Interface (SCSI)** in order to detect a virtual environment.

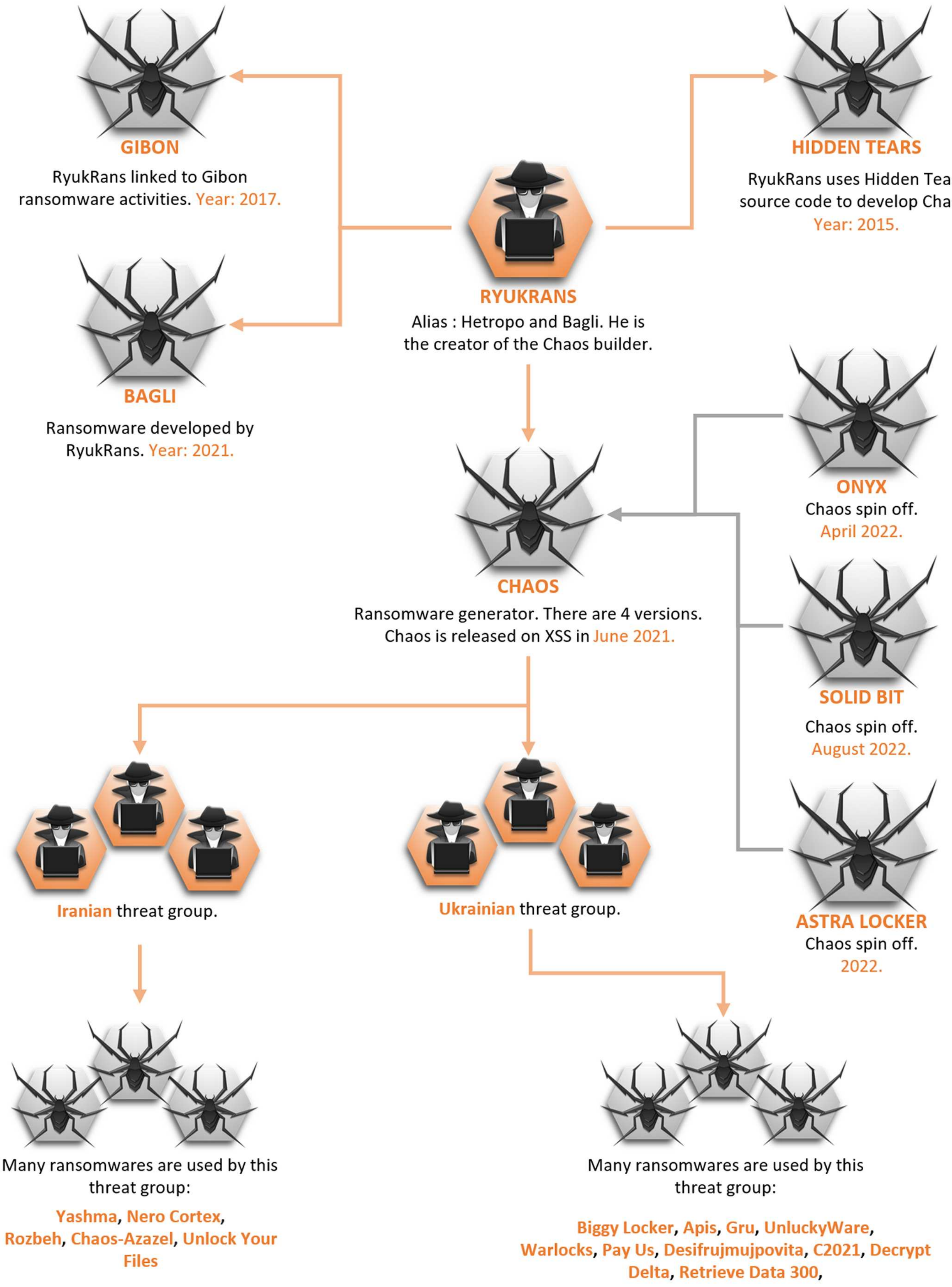
Devenders.exe encrypts system data, changes wallpaper and displays ransom note.

Figure 5. Mad Cat attack chain : main stages.

3.8. Chaos : threat mapping

Investigations revealed the existence of two threat group making significant use of the Chaos builder. The two most important threat groups are Ukrainian and the Iranian. The Ukrainian threat group is named KniveSpider.

3.8.1. State of the threat mapping before the sample study of Mad Cat (not exhaustive)



GIBON
RyukRans linked to Gibon ransomware activities. Year: 2017.

BAGLI
Ransomware developed by RyukRans. Year: 2021.

RYUKRANS
Alias : Hetropo and Bagli. He is the creator of the Chaos builder.

HIDDEN TEARS
RyukRans uses Hidden Tears source code to develop Chaos. Year: 2015.

ONYX
Chaos spin off. April 2022.

CHAOS
Ransomware generator. There are 4 versions. Chaos is released on XSS in June 2021.

SOLID BIT
Chaos spin off. August 2022.

ASTRA LOCKER
Chaos spin off. 2022.

Iranian threat group.

Ukrainian threat group.

Many ransomwares are used by this threat group:
Yashma, Nero Cortex, Rozbeh, Chaos-Azazel, Unlock Your Files

Many ransomwares are used by this threat group:
Biggy Locker, Apis, Gru, UnluckyWare, Warlocks, Pay Us, Desifrujmujpovita, C2021, Decrypt Delta, Retrieve Data 300,

Figure 6. Threat mapping: from Hidden Tears to Chaos.

3.8.2. State of the threat mapping after the sample study of Mad Cat (not exhaustive)

Studying the Mad Cat virus strain reveals similarities with other ransomware (Skull Locker, Shasha…). Furthermore, its similarities seem to stem directly from the Ukrainian threat group. In the infographic below, the virus strains indicated in red are attributed to the Ukrainian threat group with a high level of probability.

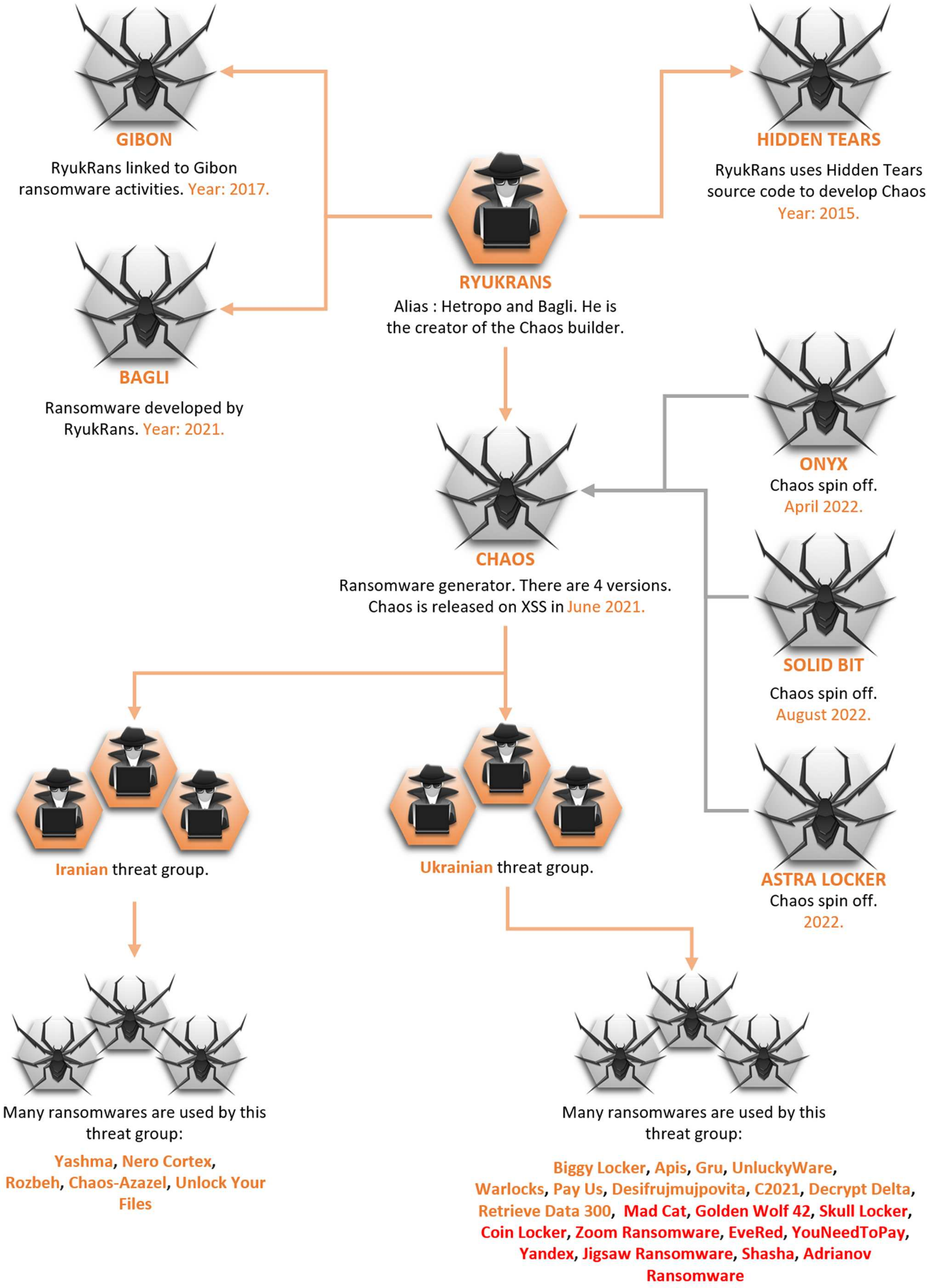
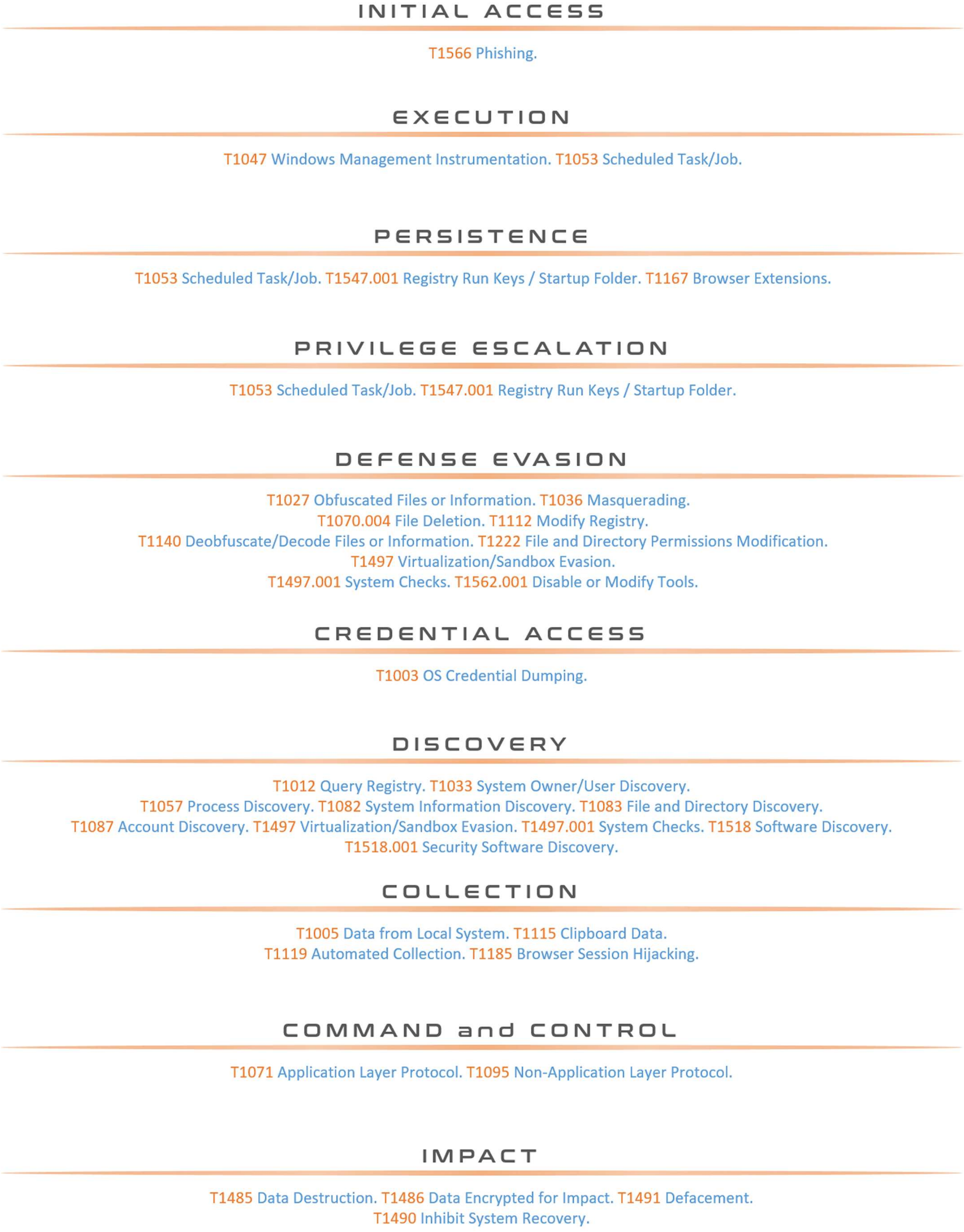

GIBON
RyukRans linked to Gibon ransomware activities. Year: 2017.
HIDDEN TEARS
RyukRans uses Hidden Tears source code to develop Chaos. Year: 2015.
RYUKRANS
Alias : Hetropo and Bagli. He is the creator of the Chaos builder.
BAGLI
Ransomware developed by RyukRans. Year: 2021.
ONYX
Chaos spin off. April 2022.
CHAOS
Ransomware generator. There are 4 versions. Chaos is released on XSS in June 2021.
SOLID BIT
Chaos spin off. August 2022.
Iranian threat group.
Ukrainian threat group.
ASTRA LOCKER
Chaos spin off. 2022.
Many ransomwares are used by this threat group:
Yashma, Nero Cortex, Rozbeh, Chaos-Azazel, Unlock Your Files
Many ransomwares are used by this threat group:
Biggy Locker, Apis, Gru, UnluckyWare, Warlocks, Pay Us, Desifrujmujpovita, C2021, Decrypt Delta, Retrieve Data 300, Mad Cat, Golden Wolf 42, Skull Locker, Coin Locker, Zoom Ransomware, EveRed, YouNeedToPay, Yandex, Jigsaw Ransomware, Shasha, Adrianov Ransomware

Figure 7. Threat mapping updated: from Hidden Tears, through Chaos to Mad Cat.

3.9. Mitre ATT&CK



INITIAL ACCESS

T1566 Phishing.

EXECUTION

T1047 Windows Management Instrumentation. T1053 Scheduled Task/Job.

PERSISTENCE

T1053 Scheduled Task/Job. T1547.001 Registry Run Keys / Startup Folder. T1167 Browser Extensions.

PRIVILEGE ESCALATION

T1053 Scheduled Task/Job. T1547.001 Registry Run Keys / Startup Folder.

DEFENSE EVASION

T1027 Obfuscated Files or Information. T1036 Masquerading.
T1070.004 File Deletion. T1112 Modify Registry.
T1140 Deobfuscate/Decode Files or Information. T1222 File and Directory Permissions Modification.
T1497 Virtualization/Sandbox Evasion.
T1497.001 System Checks. T1562.001 Disable or Modify Tools.

CREDENTIAL ACCESS

T1003 OS Credential Dumping.

DISCOVERY

T1012 Query Registry. T1033 System Owner/User Discovery.
T1057 Process Discovery. T1082 System Information Discovery. T1083 File and Directory Discovery.
T1087 Account Discovery. T1497 Virtualization/Sandbox Evasion. T1497.001 System Checks. T1518 Software Discovery.
T1518.001 Security Software Discovery.

COLLECTION

T1005 Data from Local System. T1115 Clipboard Data.
T1119 Automated Collection. T1185 Browser Session Hijacking.

COMMAND and CONTROL

T1071 Application Layer Protocol. T1095 Non-Application Layer Protocol.

IMPACT

T1485 Data Destruction. T1486 Data Encrypted for Impact. T1491 Defacement.
T1490 Inhibit System Recovery.

3.9.1. YARA 1

```
RULE: MAL_RANSOM_ExilenceTG_Mar23
RULE_SET: Livehunt - Default218 Indicators
RULE_TYPE: VALHALLA rule feed only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/MAL_RANSOM_ExilenceTG_Mar23
DESCRIPTION: Detects ExilenceTG ransomware
RULE_AUTHOR: MalGamy
Detection Timestamp: 2023-10-23 06:15
AV Detection Ratio: 47 / 72
```

3.9.2. YARA 2

```
RULE: SUSP_Ransomware_Indicators_Dec20_1
RULE_SET: Livehunt - Suspicious59 Indicators
RULE_TYPE: THOR APT Scanner's rule set only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_Ransomware_Indicators_Dec20_1
DESCRIPTION: Detects Ransomware and helpers
RULE_AUTHOR: Florian Roth
Detection Timestamp: 2023-10-23 06:15
AV Detection Ratio: 47 / 72
```

3.9.3. YARA 3

```
RULE: MAL_RANSOM_Chaos_Variants_May23
RULE_SET: Livehunt - Default233 Indicators
RULE_TYPE: VALHALLA rule feed only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/MAL_RANSOM_Chaos_Variants_May23
DESCRIPTION: Detects Chaos ransomware and its variants
REFERENCE: https://blog.cyble.com/2023/05/25/obsidian-orb-ransomware-demands-gift-cards-as-payment/
RULE_AUTHOR: MalGamy
Detection Timestamp: 2023-10-23 06:15
AV Detection Ratio: 47 / 72
```

3.10. IOC

TLP	TYPE	VALUE
TLP:CLEAR	Filename	HACKED.TXT
TLP:CLEAR	MD5	2a93808824f7eff995fe28d56f425c94
TLP:CLEAR	SHA1	98db35daee6ed87526d468af2d69f5c7de258b8c
TLP:CLEAR	SHA256	8e3345ccbc3cc6be204ea0eea181b447f977f0976b85e57cb00aa61db0983805
TLP:CLEAR	Filename	Devenders.exe
TLP:CLEAR	Filename	1HeZK0tOCh.exe
TLP:CLEAR	MD5	cc7490433d390dc919c20ed4a88155e2
TLP:CLEAR	SHA1	5cb9e9390015759fa10321f71c5d164f5152da04
TLP:CLEAR	SHA256	cf5705942d02b4585d0ee603e8773d888937e0f4221d38ea9404356a1d906392
TLP:CLEAR	SHA512	5d1a96f35213895c0a1c49f79ac929d6465c1da7c45d202ac9c12f68915ca954b5d990c8bad54c1efecc9ec0df3662b8b3534a2788e247237310abcc37653f72

4. SANDWORM or the specialization of targeting industrial systems

At the end of 2022, the group Sandworm (aka Voodoo Bear / Iridium), the cyber spearhead of Russian military intelligence, struck a power plant in Ukraine. To do this, the attackers targeted substation circuit breakers through an industrial supervision system, causing a power outage ahead of Russian tactical missile strikes.

With the offensive beginning in April 2022, the GRU appears to be pursuing a standard of attack that is streamlined and adapted to high-intensity warfare. Furthermore, the effectiveness of this attack illustrates the constant improvement of Russia's capabilities in terms of targeting industrial systems, or OT (*Operational Technology*).

As a reminder, Sandworm particularly stood out in 2015 by depriving many areas of Ukrainian territory of electricity in the middle of winter.

4.1. Description of the incident

The infiltration is said to have started as early as June 2022 before the attack struck in October of the same year. The attackers gained access to OT systems *via* a hypervisor hosting an industrial supervision system (SCADA system, developed by Hitachi) within the power plant's substations. In October, from the disk image file a.iso, attackers execute malicious commands with a native utility MicroSCADA, causing the power outage.

It is still unknown how initial access was obtained, but Sandworm has a habit of conducting reconnaissance of servers exposed on the Internet. In June 2022, attackers deploy the webshell Neo-REGEORG on one of these servers. A month later, they then deployed GOGETTER, developed in *go*, to tunnel to their C2 server. A service from the Systemd suite was used to enforce the persistence of GOGETTER.

The Systemd service allows the conditions under which a program should be executed. In the configuration file used by Sandworm, the *multi-user.target* value in the *WantedBy* parameter allows the connection of users to the execution of the program, when powering on the compromised terminal:

```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeOutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Sandworm then deploys a new technique by executing code in the MicroSCADA system of an end-of-life version, via its disk image file. This ISO file includes:

- un.vbs, which executes n.bat,
- n.bat, which probably runs the native MicroSCADA utility scilc.exe,
- s1.txt, which may contain MicroSCADA commands not allowed in SCIL language.

According to Hitachi, owner of MicroSCADA technology, SCIL is a high-level programming language for this control system. If the SCIL commands are not known in the study of this event, the purpose of the maneuver is that the MicroSCADA server relays the commands to the substation environment using the IEC-60870- protocols. 5-104 (TCP/IP connections) or IEC-60870-5-101 (serial connections).

4.2. Stage 2 : CADDYWIPER

Two days after the attack on the systems, Sandworm deployed its *wiper* CADDYWIPER. This is a data shredder developed in C, widely used by the group during its intrusions. It is the most used malware in Ukraine since the start of the 2022 offensive as part of a high-intensity confrontation, frequently observed against the administrative and financial sectors on Ukrainian territory.

The sample collected in this study is a new variant of wiper. It could be deployed *via* TANKTRAP, a utility written in PowerShell which uses the GPOs (*Group Policy*) of Windows. Two GPOs were used here:

```
    C:\Windows\SYSTEM32\GROUPPOLICY\DATASTORE\0\sysvol\<redacted>\{Policies31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

```
    C:\Windows\SYSTEM32\GROUPPOLICY\DATASTORE\0\sysvol\<redacted>\{Policies31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\Preferences\Files\Files.xml
```

4.3. SANDWORM Retrospective

The group, affiliated with the Russian army's GRU, has made a specialty of targeting industrial energy systems for years:

- In 2014, the group manipulated human-machine interfaces (HMI, Human Machine Interface) with the malware BlackEnergy2,
- In 2015, the group caused power outages with its BlackEnergy3 and KillDisk malware against power plants,
- In 2016, we observed the first use of the INDUSTROYER strain, which still causes power cuts in Ukraine,

Similarly, in November 2017, its cousin group ATK 91 (aka Xenotime, or TEMP.Veles), deployed the malware TRITON against industrial security systems. This group is affiliated with the Central Institute for Scientific Research in Chemistry and Mechanics of the Russian Federation, which has since been placed on the US sanctions list. After April 2022, version 2 of INDUSTROYER is actively deployed against industrial energy entities in Ukraine.

The October 2022 attack confirms a behavioral trend of the GRU:

If Russia, like other countries, is constantly investing in OT-oriented cyber capabilities, this *modus operandi* demonstrates simplified and streamlined deployment functionalities, such as V2 of INDUSTROYER, with the evocative name .

The attacks of 2015 and 2016 included numerous discreet but disruptive incidents on the systems: deactivation of UPS systems, blocking of serial-Ethernet converters, conduct of a DDoS attack against a SIPROTEC relay, erasure of OT systems, etc.

In the study of the 2022 incident, the activity of Sandworm is limited to ICS (*Industrial Control Systems*) commands, and the erasure is limited to the IT environment. It is possible that this rationalization is the acceleration of the pace linked to a context of high intensity war.

In addition, the attackers used a native binary of the SCADA product here, using a *Living-Off-the-Land* technique. This technique has the advantage of reducing the time and resources to carry out the attack, in addition to complicating the work of detecting defenders. The GRU here follows exactly its new attack standard, already observed in the aDvens monthly bulletin of July 2023:

- Living on the Edge: targeting infrastructures exposed on the Internet,
- Living off the Land: use integrated tools,
- Going for the GPO,
- Disrupt and Deny,

The final step is to communicate the results as a warning and threat ("telegraphing success"), often through activist groups on Telegram. In this specific case, the attackers rely on media coverage of a power plant to communicate for them and maintain pressure.

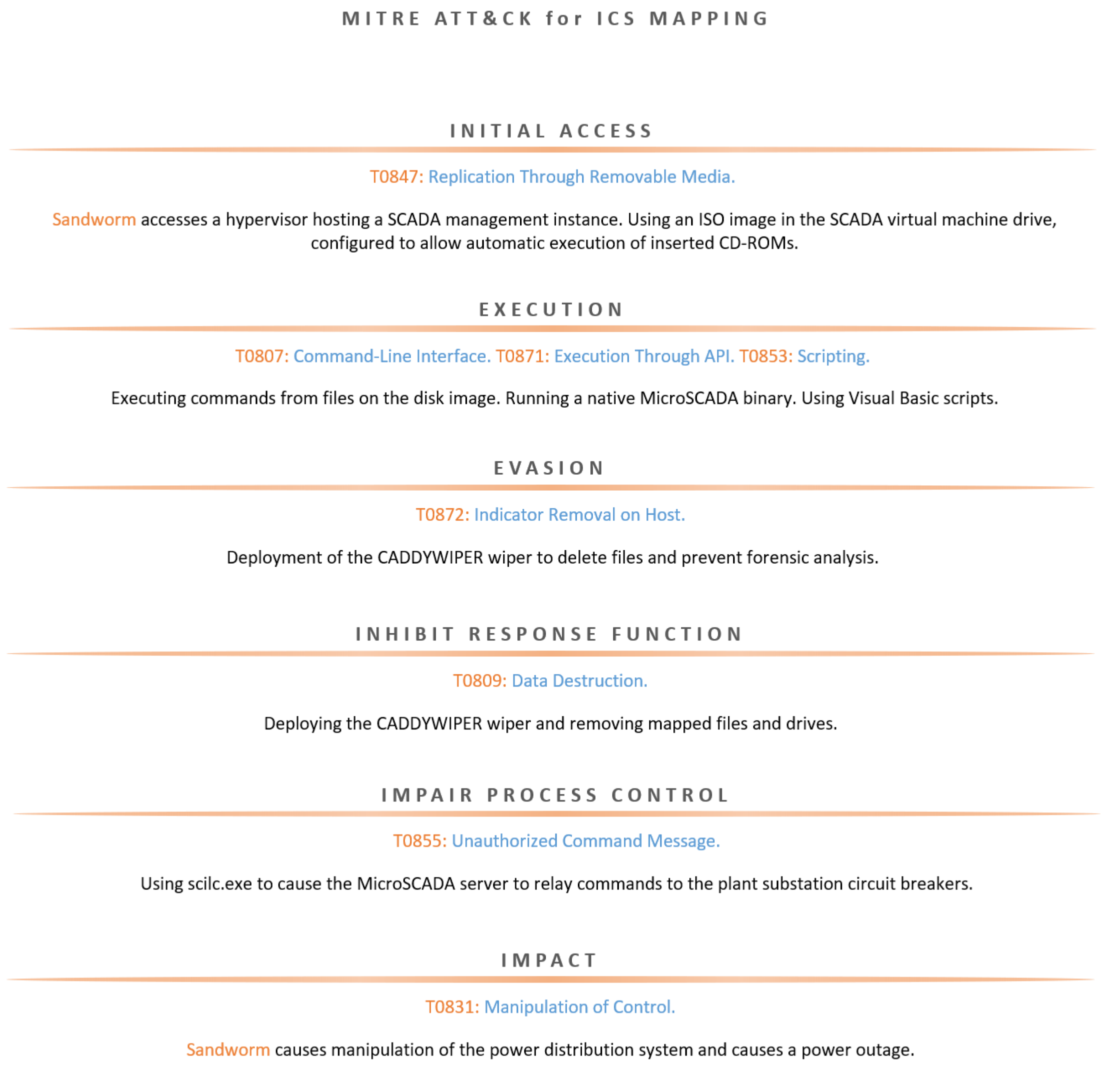
4.4. Exploiting Zyxell devices

These findings and analyzes are to be taken into account in the recent attack which hit several energy structures in Denmark in May 2023. A November 2023 report from the Danish organization SektorCERT traces and analyzes an attack in two stages carried out against around twenty Danish companies operating electricity production units.

A first wave on May 11, 2023 targeted 16 energy entities via CVE-2023-28771 affecting Zyxel firewalls. A second wave hit from May 22 to 25, with the exploitation of 2 other Zyxel flaws, CVE-2023-33009 and CVE-2023-33010, corrected by the compagny only 48 hours later. It is unknown at this stage whether the two waves were perpetrated by two different groups, coordinated with each other or not.

The organization that investigated the incident was able to trace the traffic to IP addresses believed to belong to the Sandworm group. As a conclusion, and a warning, the report notes the remarkable exploitation of CVEs affecting exposed Zyxel devices, the careful recognition of each target and the precision of the atatcks, not one of which missed his target.

4.5. MITRE ATT&CK of ICS mapping



MITRE ATT&CK for ICS MAPPING

INITIAL ACCESS

T0847: Replication Through Removable Media.

Sandworm accesses a hypervisor hosting a SCADA management instance. Using an ISO image in the SCADA virtual machine drive, configured to allow automatic execution of inserted CD-ROMs.

EXECUTION

T0807: Command-Line Interface. T0871: Execution Through API. T0853: Scripting.

Executing commands from files on the disk image. Running a native MicroSCADA binary. Using Visual Basic scripts.

EVASION

T0872: Indicator Removal on Host.

Deployment of the CADDYWIPER wiper to delete files and prevent forensic analysis.

INHIBIT RESPONSE FUNCTION

T0809: Data Destruction.

Deploying the CADDYWIPER wiper and removing mapped files and drives.

IMPAIR PROCESS CONTROL

T0855: Unauthorized Command Message.

Using scilc.exe to cause the MicroSCADA server to relay commands to the plant substation circuit breakers.

IMPACT

T0831: Manipulation of Control.

Sandworm causes manipulation of the power distribution system and causes a power outage.

Figure 8. Mitre Att&ck.

4.6. IOCs

TLP	TYPE	VALEUR
TLP:CLEAR	IP	82.180.150[.]197
TLP:CLEAR	IP	176.119.195[.]113
TLP:CLEAR	IP	176.119.195[.]115
TLP:CLEAR	IP	185.220.101[.]58
TLP:CLEAR	IP	190.2.145[.]24
TLP:CLEAR	MD5	3290cd8f948b8b15a3c53f8e7190f9b0
TLP:CLEAR	MD5	cea123ebf54b9d4f8811a47134528f12
TLP:CLEAR	MD5	26e2a41f26ab885bf409982cb823ffd1
TLP:CLEAR	MD5	b2557692a63e119af0a106add54950e6
TLP:CLEAR	MD5	61c245a073bdb08158a3c9ad0219dc23
TLP:CLEAR	MD5	82ab2c7e4d52bb2629aff200a4dc6630
TLP:CLEAR	MD5	26e2a41f26ab885bf409982cb823ffd1

4.7. YARA setection rules

```
rule M_Methodology_MicroSCADA_SCILC_Strings
{
     meta:
          author = "Mandiant"
          date = "2023-02-13"
          description = "Searching for files containing strings associated with the MicroSCADA Supervisory Control Implementation Language (SCIL) scilc.exe binary."
          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a production environment."

     strings:
          $s1 = "scilc.exe" ascii wide
          $s2 = "Scilc.exe" ascii wide
          $s3 = "SCILC.exe" ascii wide
          $s4 = "SCILC.EXE" ascii wide

     condition:
          filesize < 1MB and
          any of them
}
```

```
rule M_Hunting_MicroSCADA_SCILC_Program_Execution_Strings
{
     meta:
          author = "Mandiant"
          date = "2023-02-13"
          description = "Searching for files containing strings associated with execution of the MicroSCADA Supervisory Control Implementation Language (SCIL) scilc.exe binary."
          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a production environment."

     strings:
          $s = "scilc.exe -do" nocase ascii wide

     condition:
          filesize < 1MB and
          all of them
}
```

```
rule M_Methodology_MicroSCADA_Path_Strings
{
     meta:

          author = "Mandiant"

          date = "2023-02-27"

          description = "Searching for files containing references to MicroSCADA filesystem path containing
native MicroSCADA binaries and resources."

          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a
production environment."


     strings:

          $s1 = "sc\\prog\\exec" nocase ascii wide


     condition:

          filesize < 1MB and

          $s1

}
```

```
rule M_Hunting_VBS_Batch_Launcher_Strings

{

     meta:

          author = "Mandiant"

          date = "2023-02-13"

          description = "Searching for VBS files used to launch a batch script."

          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a
production environment."


     strings:

          $s1 = "CreateObject(\"WScript.Shell\")" ascii

          $s2 = "WshShell.Run chr(34) &" ascii

          $s3 = "& Chr(34), 0" ascii

          $s4 = "Set WshShell = Nothing" ascii

          $s5 = ".bat" ascii


     condition:

          filesize < 400 and

          all of them

}
```

```
rule M_Hunting_APT_Webshell_PHP_NEOREGEORG

{

     meta:

          author = "Mandiant"

          description = "Searching for REGEORG webshells."

          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a
production environment."
```

```
     strings:

          $php = "<?php" nocase

          $regeorg1 = {24 72 61 77 50 6f 73 74 44 61 74 61 20 3d 20 66 69 6c 65 5f 67 65 74 5f 63 6f 6e 74
65 6e 74 73 28 22 70 68 70 3a 2f 2f 69 6e 70 75 74 22 29 3b}

          $regeorg2 = {20 24 77 72 69 74 65 42 75 66 66 20 3d 20 24 5f 53 45 53 53 49 4f 4e 5b 24 77 72 69
74 65 62 75 66 5d 3b}

          $regeorg3 = {20 75 73 6c 65 65 70 28 35 30 30 30 30 29 3b}

          $regeorg4 = {20 24 61 72 68 5f 6b 65 79 20 3d 20 70 72 65 67 5f 72 65 70 6c 61 63 65 28 24 72 78
5f 68 74 74 70 2c 20 27 27 2c 20 24 6b 65 79 29 3b}

          $regeorg5 = {20 24 72 75 6e 6e 69 6e 67 20 3d 20 24 5f 53 45 53 53 49 4f 4e 5b 24 72 75 6e 5d 3b}

          $regeorg6 = {20 24 72 78 5f 68 74 74 70 20 3d 20 27 2f 5c 41 48 54 54 50 5f 2f 27 3b}


     condition:

          (5 of ($regeorg*)) and

          $php

}
```

```
rule M_Hunting_GOGETTER_SystemdConfiguration_1

{

     meta:

          author = "Mandiant"

          description = "Searching for Systemd Unit Configuration Files but with some known filenames
observed with GOGETTER"

          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a
production environment."


     strings:

          $a1 = "[Install]" ascii fullword

          $a2 = "[Service]" ascii fullword

          $a3 = "[Unit]" ascii fullword

          $v1 = "Description=" ascii

          $v2 = "ExecStart=" ascii

          $v3 = "Restart=" ascii

          $v4 = "RestartSec=" ascii

          $v5 = "WantedBy=" ascii

          $f1 = "fail2ban-settings" ascii fullword

          $f2 = "system-sockets" ascii fullword

          $f3 = "oratredb" ascii fullword

          $f4 = "cloud-online" ascii fullword


     condition:

          filesize < 1MB and (3 of ($a*)) and (3 of ($v*)) and (1 of ($f*))
}
```

4.8. SIGMA and YARA-L detection rules

```
title: MicroSCADA SCILC Command Execution
description: Identification of Events or Host Commands that are related to the MicroSCADA SCILC programming language and specifically command execution
author: Mandiant
date: 2023/02/27
logsource:
    product: windows
    service: security
detection:
    selection:
        NewProcessName|endswith:
            - \scilc.exe
        CommandLine|contains:
            - -do
    condition: selection
falsepositives:
    - Red Team
level: High
tags:
    - attack.execution
    - attack.T1059
```

```
rule M_YARAL_Methodology_ProcessExec_SCILC_Do_1

{

    meta:

        author = "Mandiant"

        description = "YARA-L rule hunting for instances of process execution of the scilc.exe process with -do parameters. This is intended to be a hunting rule. Analysts would need to verify the legitimacy of the file passed in the -do parameter."

        severity = "Low"

        reference = " https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-overview"



    events:

        $e.metadata.event_type = "PROCESS_LAUNCH"

        $e.target.process.command_line = /\s+\-do\s+[^\-\s]+/ nocase

        $e.target.process.file.full_path = /scilc\.exe$/ nocase



    condition:

        $e

}
```

5. Sources

FORTINET - CVE-2023-36553

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36553
- https://www.fortiguard.com/psirt/FG-IR-23-135

ARUBA - CVE-2023-45614

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-45614
- https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-017.txt

VMWARE - CVE-2023-34060

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34060
- https://www.vmware.com/security/advisories/VMSA-2023-0026.html

MAD CAT : Articles

- https://www.joesandbox.com/analysis/1336173/0/html*
- https://www.pcrisk.fr/guides-de-suppression/12303-mad-cat-ransomware
- https://www.virustotal.com/gui/file/cf5705942d02b4585d0ee603e8773d888937e0f4221d38ea9404356a1d906392/details
- https://bazaar.abuse.ch/sample/cf5705942d02b4585d0ee603e8773d888937e0f4221d38ea9404356a1d906392/
- https://www.cyclonis.com/remove-mad-cat-ransomware/
- https://www.stormshield.com/fr/actus/alerte-securite-ransomware-skulllocker-la-reponse-des-produits-stormshield/
- https://www.trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html
- https://www.vmray.com/analyses/_vt/cf5705942d02/report/ioc.html
- https://tria.ge/231102-wr2azsde9z/behavioral1
- https://medium.com/@shigeyuki.form/intelligence-feed-based-on-multiple-recent-recorded-future-reports-november-8-2023-3201ef0eae13

SANDWORM

- https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
- https://www.bleepingcomputer.com/news/security/russian-hackers-switch-to-lotl-technique-to-cause-power-outage/
- https://securityaffairs.com/153920/apt/russian-sandworm-ot-attacks.html
- https://fr.wikipedia.org/wiki/Piratage_du_syst%C3%A8me_%C3%A9nerg%C3%A9tique_ukrainien
- https://www.kaspersky.com/blog/blackenergy-2-a-good-set-or-bad-deeds/15024/
- https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf
- https://www.hsdl.org/c/view?docid=767255
- https://i.blackhat.com/USA-22/Wednesday/US-22-Cherepanov-Industroyer2-Sandworms-Cyberwarfare-Targets-Ukraines-Power-Grid-Again.pdf
- https://www.opensanctions.org/entities/NK-XnxxwRcviN5RLnv3Q3uWSx/
- https://blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure
- https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf