aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de novembre 2023

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

Sommaire

1. Synthèse

Ce mois ci, le CERT aDvens vous propose trois vulnérabilités présentant un intérêt, en complément de celles déjà publiées.

Au travers de deux articles, les analystes du CERT présentent le maliciel polymorphe Mad Cat actif depuis octobre. De plus, une campagne d'attaque perpétrée par le groupe APT Sandworm, ciblant des environnements industriels, est également examinée.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **trois** vulnérabilités affectant des technologies fréquemment utilisées au sein des entreprises.
Elles sont présentées par ordre de gravité (preuves de concept disponibles, exploitation …). L'application de leurs correctifs ou contournements est fortement recommandée.

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

2.1. Fortinet - CVE-2023-36553

Le 14 novembre 2023, Fortinet a publié un bulletin d'alerte concernant la CVE-2023-36553 affectant les serveurs FortiSIEM.

Un défaut de neutralisation de caractères spéciaux dans une *commande OS* du serveur de rapports FortiSIEM, permet à un attaquant distant non authentifié d'exécuter des commandes non autorisées via des requêtes API.

2.1.1. Risque

- Exécution de code arbitraire

2.1.2. Type de vulnérabilité

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

2.1.3. Criticité

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.1.4. Composants vulnérables

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

2.1.5. Recommandations

- Mettre à jour FortiSIEM vers les versions 6.4.3, 6.5.2, 6.6.4, 6.7.6, 7.0.1, 7.1.0 ou ultérieures.
- Des informations complémentaires sont disponibles dans le bulletin de Fortinet.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Aruba - CVE-2023-45614

Le 14 novembre 2023, Aruba a publié un bulletin concernant trois vulnérabilités critiques dans ArubaOS et InstantOS. La vulnérabilité CVE-2023-45614, avec un score CVSS de 9.8, a été découverte et reportée par XiaoC de Moonlight Bug Hunter.

Une erreur de dépassement de mémoire tampon dans le service *CLI* permet à un attaquant distant et non authentifié, en envoyant des requêtes spécifiquement forgées vers le port 8211 (UDP), d'exécuter du code arbitraire sur le système avec des privilèges élevés.

2.2.1. Risque

- Exécution de code arbitraire

2.2.2. Type de vulnérabilité

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

2.2.3. Criticité

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Composants vulnérables

ArubaOS :

- Versions versions 10.5.x.x antérieures à 10.5.0.1
- Versions versions 10.4.x.x antérieures à 10.4.0.3
- Versions 1.6.x antérieures à 1.6.4

InstantOS :

- Versions 8.11.x.x antérieures à 8.11.2.0
- Versions 8.10.x.x antérieures à 8.10.0.9
- Versions 8.6.x antérieures à 8.6.0.23

2.2.5. Recommandations

- Mettre à jour ArubaOS vers la version 10.4.0.3, 10.5.0.1 ou ultérieure.
- Mettre à jour InstantOS vers la version 8.6.0.23, 8.10.0.9, 8.11.2.0 ou ultérieure.
- Si le correctif ne peut pas être déployé, il est recommandé d'activer la fonctionnalité cluster-security sur InstantOS versions 6.x et 8.x. Cette option n'est pas disponible pour les appareils ArubaOS 10, toutefois il est possible de bloquer l'accès vers le port 8211.
- Des informations complémentaires sont disponibles dans le bulletin d'Aruba.

2.2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.3. VMware - CVE-2023-34060

Le 14 novembre 2023, VMware a publié un bulletin concernant une vulnérabilité critique dans VMware Cloud Director Appliance. Cette faille permet à un attaquant non authentifié de contourner la politique de sécurité.

Cette vulnérabilité est exploitable pour les composants migrés en 10.5 depuis une version antérieure. Un attaquant disposant d'un accès distant peut contourner les restrictions de connexion lors de l'authentification sur le port 22 (ssh) ou le port 5480 (appliance management console).

les instances *VMWARE Cloud Director Appliance* déployées directement en version 10.5 ne sont pas affectées par la vulnérabilité.

2.3.1. Risque

- Contournement de la politique de sécurité

2.3.2. Type de vulnérabilité

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

2.3.3. Criticité

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.3.4. Composants vulnérables

- VMware Cloud Director Appliance version 10.5 si mis à jour depuis une version 10.4 ou antérieure.
- Les nouvelles installations de VMware Cloud Director Appliance version 10.5, et les versions 10.4 et antérieures, ne sont pas vulnérables.

2.3.5. Recommandations

- Appliquer le KB95534 à VMware Cloud Director Appliance version 10.5 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de VMware.

2.3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

3. Virologie : étude d'un échantillon Mad Cat

Mad Cat est un logiciel malveillant multifonctions dont l'émergence date de la fin du mois d'octobre 2023. Aprés avoir infecté un système, il peut **effacer les données** (*wiper*), **chiffrer les données** (*ransomware*) et **voler la cryptomonaie** (*crypto hi-jacking*) de l'utilisateur.

Généré par le célèbre builder Chaos, le logiciel malveillant Mad Cat est une itération qui semble préserver une anatomie (structure) et une physiologie (fonctionnement) similaires aux souches virales de sa fratrie : un ensemble de malware connu en tant que "*Chaos ransomware family*".

3.1. Fonctionnalités

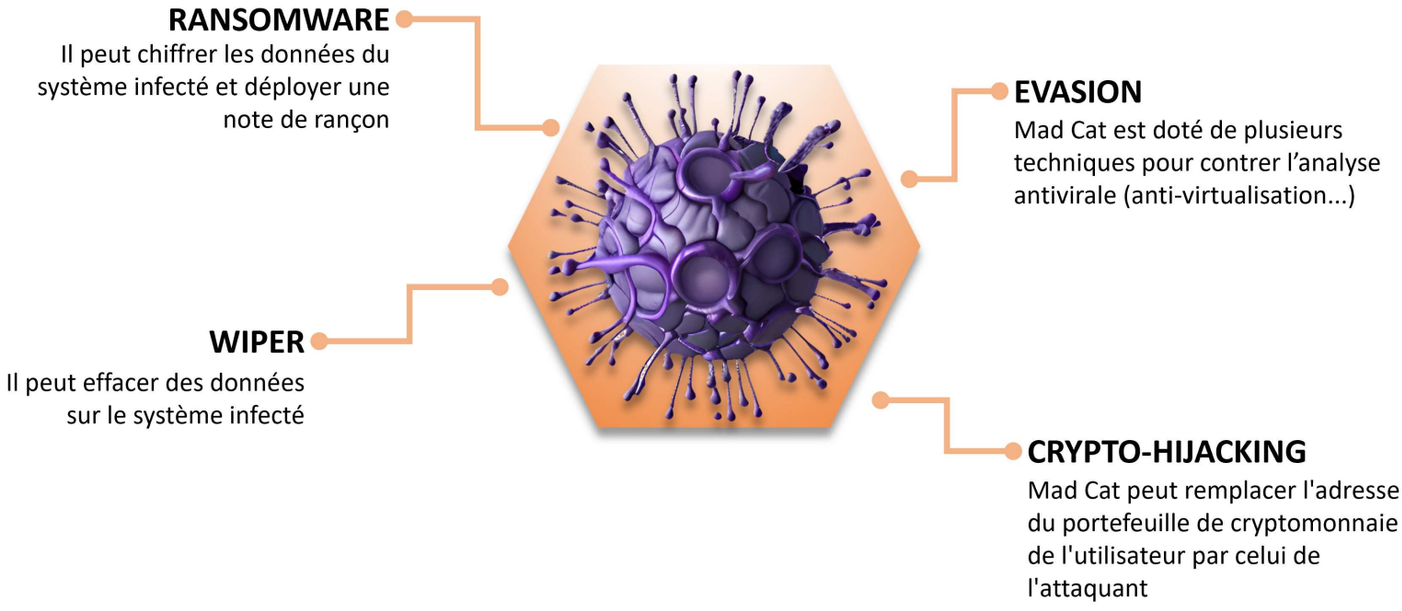

Figure 1. Les fonctionnalités de Mad Cat.

3.2. Arbre généalogique

Le rançongiciel Mad Cat serait une itération générée par le builder Chaos, version 4.

Développé par un cybercriminel surnommé RyukRans (sans lien avec le rançongiciel Ryuk), le builder Chaos est un générateur de souches virales dont l'émergence est annoncée sur le forum XSS en juin 2021. Ce builder est développé à partir du code source du rançongiciel Hidden Tears, publié en aout 2015.

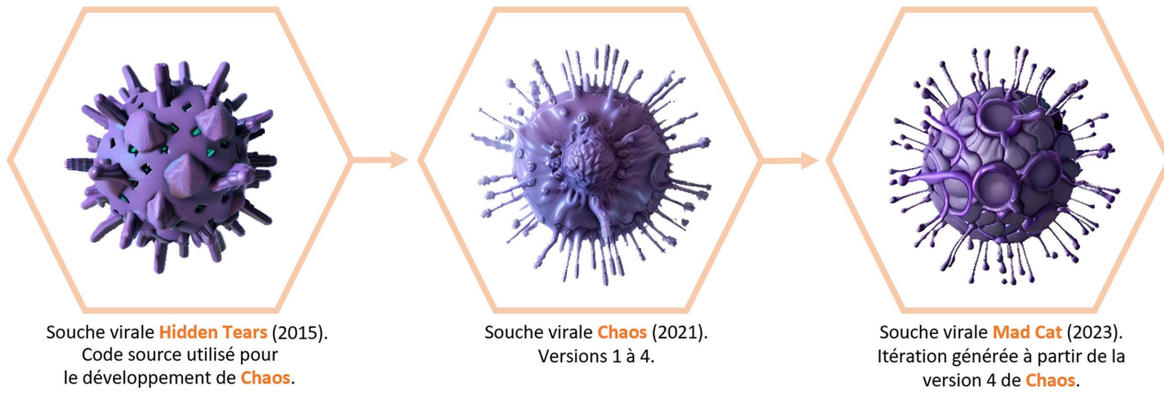

Figure 2. L'origine de Mad Cat : le builder Chaos développé par le cybercriminel RyukRans.

3.3. Infectiologie

les attaquants utilisent les vecteurs d'infection ci-dessous pour distribuer le logiciel malveillant :

- Sites web de torrents
- Publicités malveillantes
- Piéces jointes malveillantes
- Logiciels piratés ("*crackés*")

3.4. Victimologie

Les itérations générées par le builder Chaos sont connues pour être utilisées à l'encontre d'organisations liées aux secteurs suivant :

- Finance
- Agriculture
- Commerce
- Santé

Les organisations victimes sont essentiellement localisées en Amérique. Certaines analyses précisent que des échantillons du rançongiciel Mad Cat ont été trouvés au sein de *Cloud* de plusieurs entreprises.

3.5. Analyse de la souche virale

Cette section contient une analyse non exhaustive du code malveillant Mad Cat.

3.5.1. Exécution

- Déploiement d'une copie de la souche virale

```
Source : C:\Users\user\Desktop\1HeZK0tOCh.exe
Création de fichier : C:\Users\user\AppData\Roaming\Devenders.exe
```

3.5.2. Évasion de la défense

- Évasion de l'analyse antivirale via le temps

```
Source : C:\Users\user\Desktop\1HeZK0tOCh.exe
Temps de veille : -922337203685477s >= -30000s
```

```
Source : C:\Users\user\AppData\Roaming\Devenders.exe
Quantité de veille : 1052 > 30
```

- Évasion de l'analyse antivirale en stoppant son exécution

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

- Detection de la virtualisation

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

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

- Désactivation du gestionnaire de tâches

```
Clé registre : HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Valeur : 1
```

- Suppression des catalogues Windows

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

- Anti-debugging

```
Source : C:\Users\user\Desktop\1HeZK0tOCh.exe
Jeton de processus ajusté : Debug (count 1)
```

```
Source : C:\Users\user\AppData\Roaming\Devenders.exe
Jeton de processus ajusté : Debug (count 1)
```

3.5.3. Persistance

- Trois artéfacts sont placés dans le dossier *Startup* du système

```
Source : C:\Users\user\AppData\Roaming\Devenders.exe
Création de fichier : 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. Élévation de privilèges

- Obtient les privilèges "Debug"

```
Source : C:\Users\user\Desktop\1HeZK0tOCh.exe
Jeton de processus ajusté : Debug
Privilege : Debug (Count = 1)
```

- Obtient les privilèges "Security"

```
Source : C:\Windows\System32\wbengine.exe
Jeton de processus ajusté : Security
```

3.5.5. Collection et accès identifiants

- Recherche d'information sensible (identifiants et mots de passe)

```
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

- Suppression des sauvegardes shadow copy

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

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

```
Source : 1HeZK0tOCh.exe
Binaire : /C yvssadmin delete shadows /all /quiet & wmic shadowcopy delete
```

- Désactivation de la restauration

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

- Tentative de vol de cryptomonnaie ("*Crypto hi-jacking*"). Certaines itérations du builder Chaos sont connues pour remplacer l'adresse du portefeuille de cryptomonnaie de l'utilisateur par celle de l'attaquant.

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

```
Window : window name: CLIPBRDWNDCLASS
Classification : CLIPBRDWNDCLASS (count = 1)
```

- Chiffrement des données

```
Source : 1HeZK0tOCh.exe
Fonction : encryptDirectory
```

```
Source : Devenders.exe
Fonction : encryptDirectory
```

- Selon Truesec, les itérations générées par la version 4 du builder ont les caractéristiques de chiffrement suivantes

```
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. Note de rançon

- Création de la note de rançon

```
Source : C:\Users\user\AppData\Roaming\Devenders.exe
Création de fichier : C:\Users\HACKED.TXT
```

- Contenu de la note de rançon

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

- Modification du fond d'écran

```
Processus : 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. Fond d'écran modifié

Ci-dessous, le fond d'écran modifié par Mad Cat.

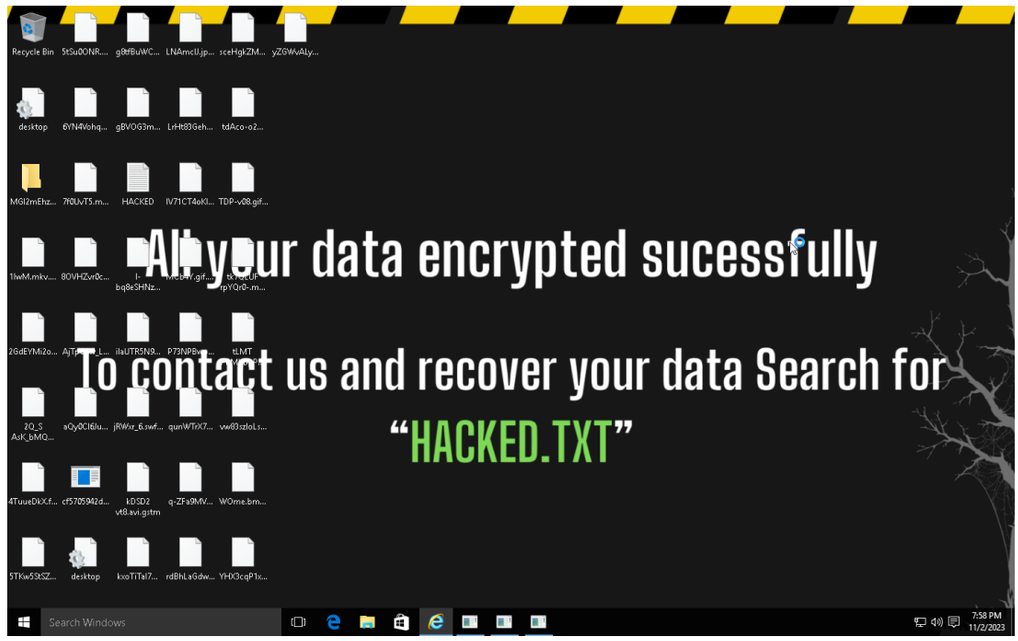

Figure 3. Fond d'écran imposé par Mad Cat.

3.6. Chaos Version 4

Ci-dessous, l'interface utilisateur du builder Chaos, version 4. Cette quatrième version est la seule qui offre la possibilité aux attaquants de changer le fond d'écran du système infecté.

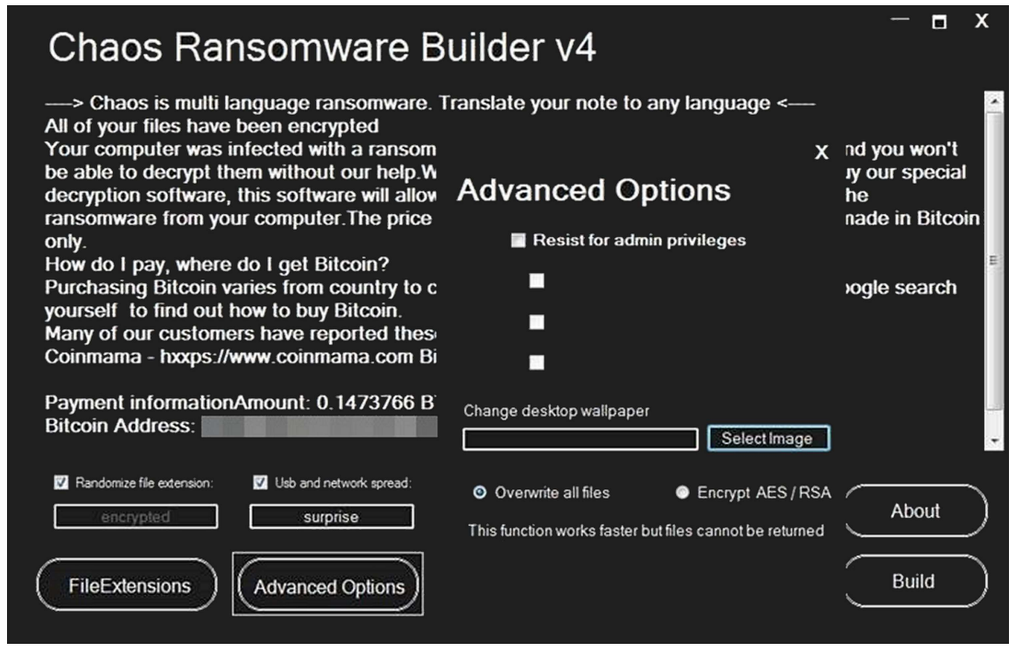

Figure 4. Interface utilisateur de Chaos V4.

3.7. Chaine d'attaque

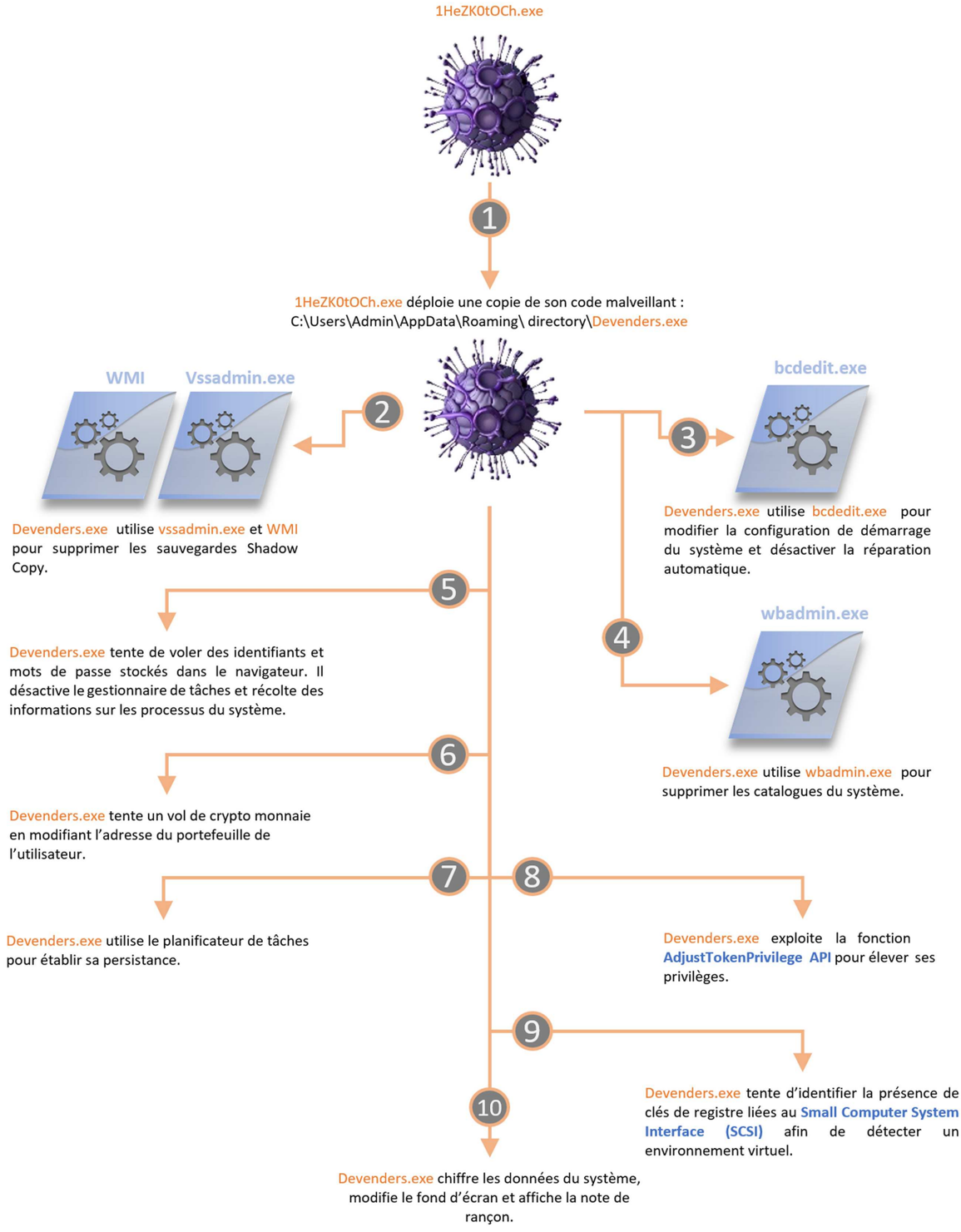

Figure 5. Les grandes étapes de la chaine d'attaque de Mad Cat.

3.8. Chaos : cartographie de la menace

Des analyses ont révélé l'existence de deux collectifs cybercriminels utilisant de manière significative le builder Chaos. L'un de ces collectifs serait ukrainien et l'autre iranien. Le collectif ukrainien est surnommé KniveSpider.

3.8.1. Cartographie avant l'étude de l'échantillon Mad Cat (non exhaustif)

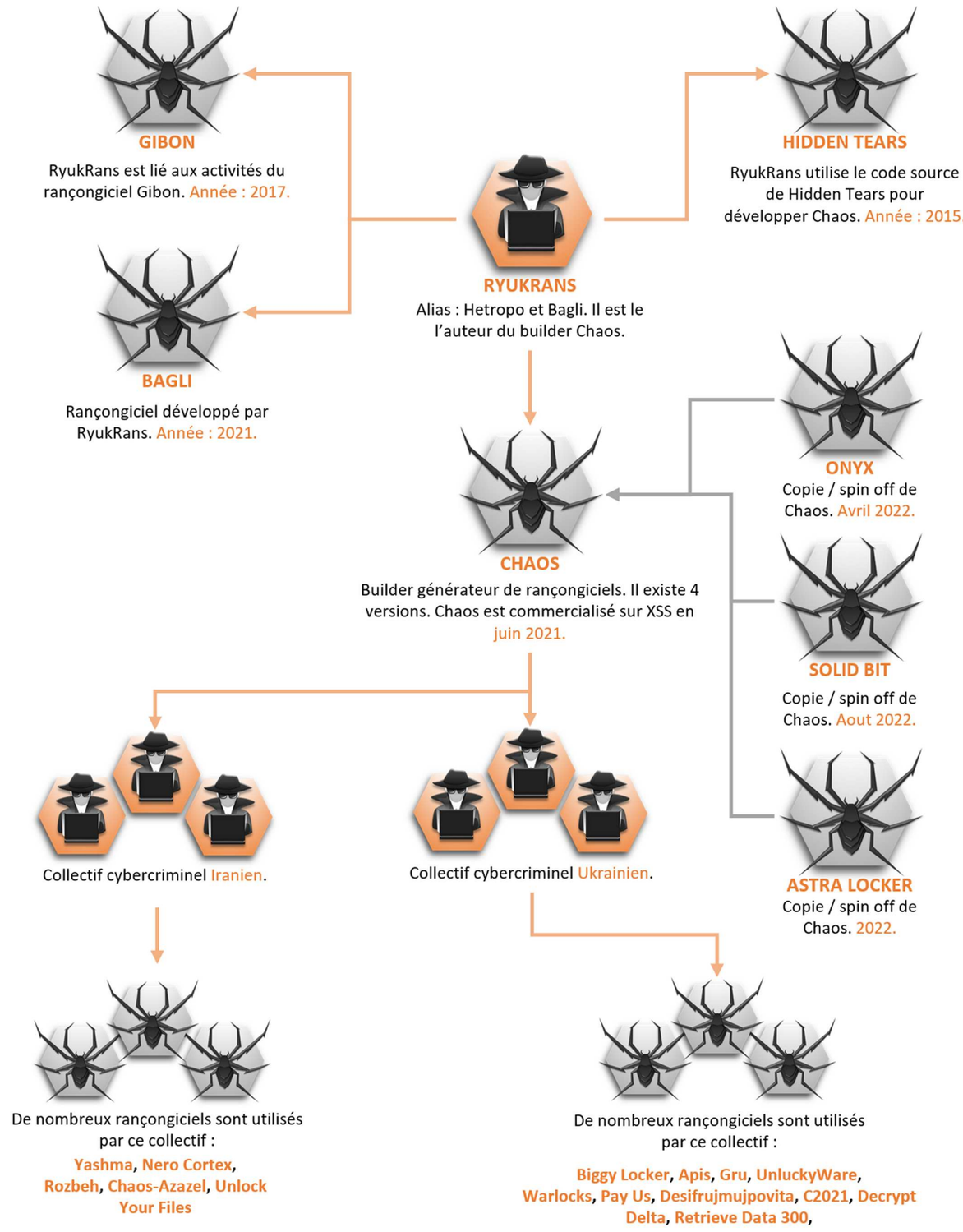

Figure 6. Cartographie : de Hidden Tears à Chaos.

3.8.2. Cartographie après l'étude de l'échantillon Mad Cat (non exhaustif)

L'étude de la souche virale Mad Cat permet de révéler des similitudes avec d'autres rançongiciels (Skull Locker, Shasha…). Par ailleurs, ses similitudes semblent découler directement du collectif cybercriminel ukrainien. Dans l'infographie ci-dessous, les souches virales indiquées en rouge sont attribuées (probabilité élevé) au collectif ukrainien.

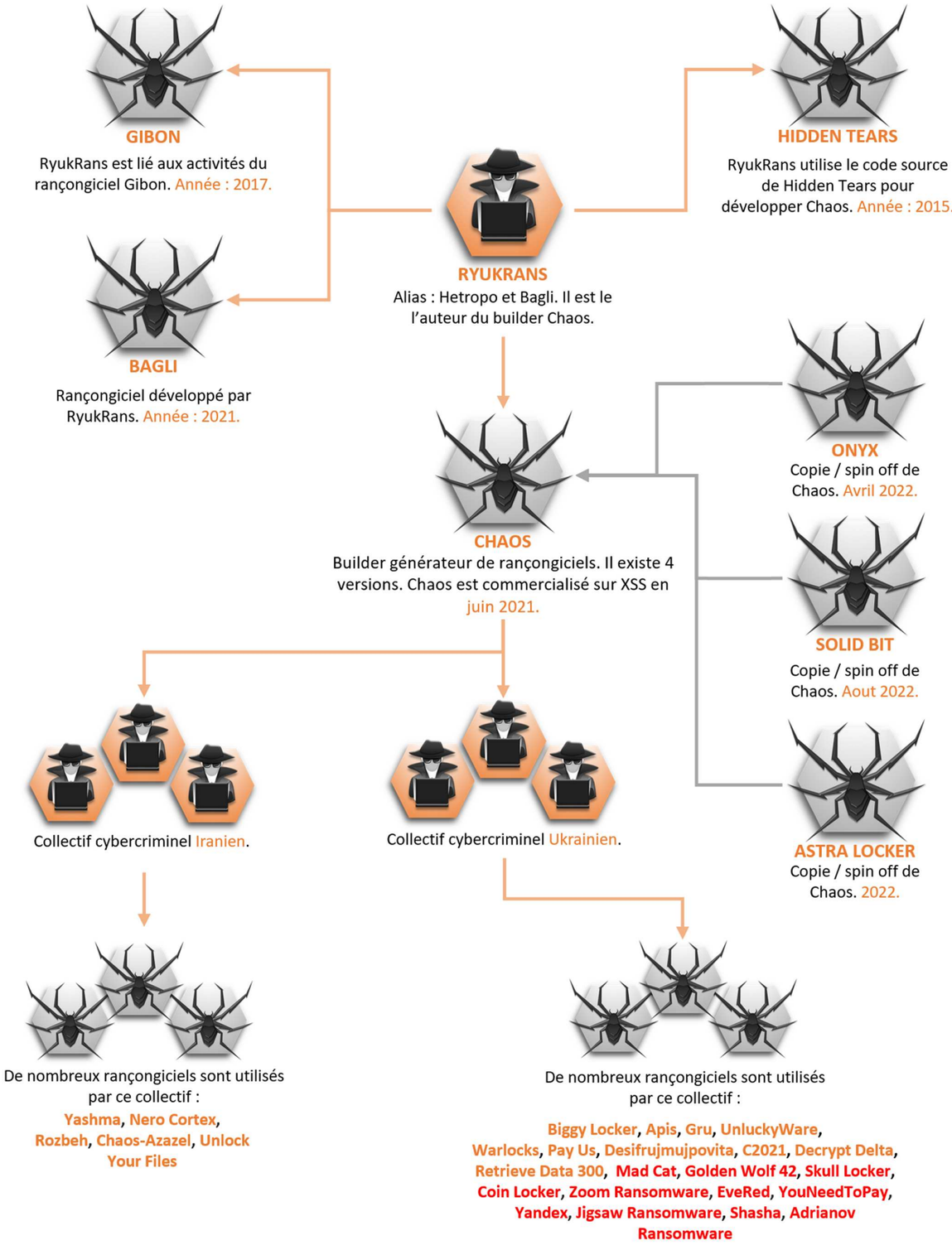

Figure 7. Cartographie mise à jour : de Hidden Tears, en passant par Chaos et enfin Mad Cat.

3.9. Matrice 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	VALEUR
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 : un spécialiste des systèmes industriels

Fin 2022, le groupe Sandworm (alias Voodoo Bear / Iridium), fer de lance cyber du renseignement militaire russe, frappait une centrale électrique en Ukraine. Pour cela, les attaquants ont ciblé les disjoncteurs des sous-stations par le biais d'un système de supervision industrielle, provoquant une coupure d'électricité en amont des frappes de missiles tactiques russes.

Avec l'offensive entamée en avril 2022, le GRU semble poursuivre un standard d'attaque rationnalisé et adapté à la guerre de haute intensité. De plus, l'efficacité de cette attaque illustre l'amélioration constante des capacités de la Russie en matière de ciblages de systèmes industriels, ou OT (*Operational Technology*).

Pour rappel, Sandworm s'était particulièrement illustré en 2015 en privant d'électricité de nombreuses zones du territoire ukrainien en plein hiver.

4.1. Description de l'incident

L'infiltration aurait commencé dès juin 2022 avant que l'attaque ne frappe en octobre de la même année. Les attaquants ont obtenu l'accès aux systèmes OT *via* un hyperviseur hébergeant un système de supervision industrielle (système SCADA, développé par Hitachi) au sein des sous-stations de la centrale. En octobre, à partir du fichier d'image disque a.iso, les attaquants exécutent des commandes malveillantes avec un utilitaire natif MicroSCADA, à l'origine de la panne de courant.

On ignore encore comment l'accès initial a pu être obtenu mais Sandworm a pour habitude de mener une reconnaissance des serveurs exposés sur Internet. En juin 2022, les attaquants déploient le *webshell* Neo-REGEORG sur un de ces serveurs. Un mois plus tard, ils déploient alors GOGETTER, développé en *go*, pour effectuer une tunnelisation vers leur serveur C2. Un service de la suite Systemd a été utilisé pour renforcer la persistence de GOGETTER.

Le service Systemd autorise les conditions selon lesquelles un programme doit être exécuté. Dans le fichier de configuration utilisé par Sandworm, la valeur *multi-user.target* dans le paramètre *WantedBy* permet la connexion des utilisateurs à l'exécution du programme, lors de la mise sous tension du terminal compromis :

```
[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 exécute des commandes dans le système MicroSCADA d'une version qui n'est plus mise à jour par l'éditeur, *via* son fichier d'image disque. Ce fichier ISO comprend :

- un.vbs, qui exécute n.bat,
- n.bat, qui exécute probablement l'utilitaire MicroSCADA natif scilc.exe,
- s1.txt, qui contient vraisemblablement les commandes MicroSCADA non autorisées en langage SCIL.

D'après Hitachi, propriétaire de la technologie MicroSCADA, SCIL est un langage de programmation de haut niveau pour ce système de contrôle. Si les commandes SCIL ne sont pas connues dans l'étude de cet incident, la finalité de la manoeuvre est que le serveur MicroSCADA relaye les commandes vers l'environnement des sous-stations par les protocoles IEC-60870-5-104 (connexions TCP/IP) ou IEC-60870-5-101 (connexions séries).

4.2. Phase 2 : CADDYWIPER

Deux jours après l'attaque des systèmes, Sandworm a déployé son *wiper* CADDYWIPER. Celui-ci est un destructeur de données développé en C très utilisé par le groupe lors de ses intrusions. C'est le maliciel le plus utilisé depuis le début de l'offensive de 2022 dans le cadre d'un affrontement de haute intensité, fréquemment observé contre les secteurs de l'administration et de la finance sur le territoire ukrainien.

L'échantillon récolté dans cette étude est un nouveau variant du *wiper*. Il a pu être déployé avec TANKTRAP, un utilitaire PowerShell qui utilise les GPO (*Group Policy*) de Windows. Deux GPO ont ici été utilisées :

```
    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. Rétrospective SANDWORM

Le groupe, affilié au GRU de l'armée russe, s'est fait une spécialité du ciblage de systèmes industriels énergétiques depuis des années :

- En 2014, le groupe manipule des interfaces homme-machine (HMI, *Human Machine Interface*) avec le malware BlackEnergy2,
- En 2015, le groupe provoque des coupures d'électricité avec ses malwares BlackEnergy3 et KillDisk contre des centrales électriques,
- En 2016, on observe la première utilisation de la souche INDUSTROYER, qui cause encore des coupures d'électricité en Ukraine,

De même, en novembre 2017, le groupe ATK 91 (alias Xenotime, ou TEMP.Veles), déploie le *malware* TRITON contre des systèmes de sécurité industriels. Ce groupe est affilié à l'Institut Central pour la Recherche Scientifique en Chimie et Mécanique de la Fédération de Russie, placé depuis sur la liste des sanctions des USA.

Après avril 2022, la version 2 d'INDUSTROYER est activement déployée contre les entités énergétiques industrielles en Ukraine.

L'attaque d'octobre 2022 permet de confirmer une tendance comportementale du GRU :

Si la Russie, comme d'autres pays, investit de façon constante dans des capacités de cyber orientée OT, ce mode opératoire témoigne de fonctionnalités de déploiement simplifiées et rationnalisées, comme la V2 d'INDUSTROYER, au nom évocateur.

Les attaques de 2015 et 2016 avaient comporté de nombreux incidents discrets mais perturbateurs sur les systèmes : désactivation des systèmes UPS, blocage des convertisseurs série-Ethernet, conduite d'une attaque DDoS contre un relais SIPROTEC, effacement des systèmes OT …

Dans l'étude de l'incident de 2022, l'activité de Sandworm se limite à des commandes ICS (*Industrial Control Systems*), et l'effacement est circonscrit à l'environnement informatique. Il est possible que cette rationalisation soit l'accélération du rythme liée à un contexte de guerre de haute intensité.

De plus, les attaquants ont utilisé ici un binaire natif du produit SCADA, selon une technique *Living-Off-the-Land*. Cette technique a l'avantage de réduire le temps et les ressources pour mener l'attaque, en plus de compliquer le travail de détection des défenseurs. Le GRU suit ici exactement son nouveau standard d'attaque, déjà observé dans le bulletin mensuel aDvens de juillet 2023 :

- *Living on the Edge* ("vivre en périphérie") : cibler des infrastructures exposées sur Internet,
- *Living off the Land* ("fourrager") : utiliser des outils intégrés,

- *Going for the GPO* ("passer par les GPO"),
- *Disrupt and Deny* ("Perturber et empêcher"),

La dernière étape est celle de la communication des résultats à titre d'avertissement et de menace ("*telegraphing success*"), souvent par le biais de groupes activistes sur Telegram. Dans ce cas précis, les attaquants présument du traitement médiatique concernant une centrale électrique pour communiquer à leur place et maintenir la pression.

4.4. Exploitation de périphériques Zyxell

Ces constatations et analyses sont à prendre en compte dans la récente attaque qui a frappé plusieurs structures énergétiques au Danemark en mai 2023. Un rapport de Novembre 2023 de l'organisation danoise SektorCERT retrace et analyse une attaque en deux temps menée contre une vingtaine de sociétés danoises exploitant des unités de production d'électricité.

Une première vague, le 11 mai 2023, a ciblé 16 entités énergétiques *via* la CVE-2023-28771 affectant des pare-feux Zyxel. Une seconde a frappé du 22 au 25 mai, avec l'exploitation de deux autres vulnérabilités Zyxel, les CVE-2023-33009 et CVE-2023-33010, corrigées par le constructeur seulement 48 heures plus tard.

On ignore à ce stade si les deux vagues ont été perpétrées par deux groupes différents, coordonnés entre eux ou non.

L'organisation qui a investigué l'incident a pu retracer le trafic jusqu'à des adresses IPs sensées appartenir au groupe Sandworm. En guise de conclusion, et d'avertissement, le rapport note l'exploitation remarquable des CVE affectant des périphériques Zyxel exposés, la reconnaissance minutieuse de chaque cible et la précision des attaques, dont pas une n'a manqué sa cible.

4.5. Matrice MITRE ATT&CK de l'attaque

MATRICE MITRE ATT&CK DE L'ATTAQUE

INITIAL ACCESS

T0847: Replication Through Removable Media.

Sandworm accède à un hyperviseur hébergeant une instance de gestion SCADA. Utilisation d'une image ISO dans le lecteur de la machine virtuelle SCADA, configuré pour permettre l'exécution automatique des CD-ROM insérés.

EXECUTION

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

Exécution de commandes à partir des fichiers présents sur l'image disque. Exécution d'un binaire MicroSCADA natif. Exploitation de scripts Visual Basic.

EVASION

T0872: Indicator Removal on Host.

Déploiement du *wiper* CADDYWIPER pour supprimer les fichiers et empêcher l'analyse *forensic*.

INHIBIT RESPONSE FUNCTION

T0809: Data Destruction.

Déploiement du *wiper* CADDYWIPER et suppression des fichiers et lecteurs cartographiés.

IMPAIR PROCESS CONTROL

T0855: Unauthorized Command Message.

Utilisation de scilc.exe pour amener le serveur MicroSCADA à relayer les commandes vers les disjoncteurs des sous-stations de la centrale.

IMPACT

T0831: Manipulation of Control.

Sandworm provoque une manipulation du système de distribution d'énergie et cause une coupure d'électricité.

Figure 8. Mitre Att&ck.

4.6. IOC

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. Règles de détection YARA

```
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. Règles de détection SIGMA et YARA-L

```
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. Références

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