aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de juillet 2024

2024-08-08 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

1. SYNTHÈSE 2
2. VULNÉRABILITÉS 3
2.1. ServiceNow - CVE-2024-4879 et CVE-2024-5217 3
2.1.1. Type de vulnérabilité 3
2.1.2. Risque 3
2.1.3. Criticité (score de base CVSS v3.1) 3
2.1.4. Produits impactés 3
2.1.5. Recommandations 4
2.1.6. Preuve de concept 4
2.2. Palo Alto - CVE-2024-5910 5
2.2.1. Type de vulnérabilité 5
2.2.2. Risque 5
2.2.3. Criticité (score de base CVSS v3.1) 5
2.2.4. Produits impactés 5
2.2.5. Recommandations 5
2.2.6. Preuve de concept 5
2.3. Progress Telerik - CVE-2024-6327 6
2.3.1. Type de vulnérabilité 6
2.3.2. Risque 6
2.3.3. Criticité (score de base CVSS v3.1) 6
2.3.4. Produits impactés 6
2.3.5. Recommandations 6
2.3.6. Preuve de concept 6
3. DISTRIBUTION D'HIJACKLOADER AVEC L'EXÉCUTABLE DRIVER BOOSTER D'IOBIT 7
3.1. HijackLoader 7
3.1.1. Chaîne d'attaque 7
3.1.2. Exploitation de la CVE-2024-21412 9
3.1.3. MITRE ATT&CK 10
3.1.4. Détection 11
3.1.5. Indicateurs de compromission 13
4. LA GESTION DES VULNÉRABILITÉS, UN PILIER DE LA SÉCURITÉ : UN EXEMPLE AVEC ESTATE RANSOMWARE 16
4.1. CVE-2023-27532 16
4.2. Estate Ransomware 16
4.2.1. Modèle Diamant 17
4.2.2. Chaîne d'attaque 17
4.2.3. Mitre Att&ck 20
4.2.4. IoC 21
5. RÉFÉRENCES 22

1. Synthèse

Ce mois-ci, le CERT aDvens vous propose quatre vulnérabilités d'intérêts, en complément de celles déjà publiées.

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

- Le modus operandi de déploiement d'un HijackLoader via l'exécutable Driver Booster d'IObit.
- La nécessité d'une politique de geston de vulnérabilité à travers une campagne d'attaque attribuée au groupe rançongiciel Estate.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **quatre** 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.

2.1. ServiceNow - CVE-2024-4879 et CVE-2024-5217

Le 10 juillet 2024, ServiceNow a publié deux vulnérabilités affectant leurs plateformes Utah, Vancouver et Washington DC.

Ces vulnérabilités proviennent de défauts de contrôle de données saisies par l'utilisateur et permettent à un attaquant d'exécuter du code arbitraire avec les privilèges de la plateforme.

Ces vulnérabilités sont exploitées.

2.1.1. Type de vulnérabilité

Pour la CVE-2024-4879

- CWE-1287 : Improper Validation of Specified Type of Input

Pour la CVE-2024-5217

- CWE-697 : Incorrect Comparison
- CWE-184 : Incomplete List of Disallowed Inputs

2.1.2. Risque

- Exécution de code arbitraire

2.1.3. Criticité (score de base CVSS v3.1)

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. Produits impactés

- Now Platform versions Utah, Vancouver et Washington DC

2.1.5. Recommandations

Mettre à jour ServiceNow selon les versions suivantes :

- **Utah**
  - Utah Patch 10 Hot Fix 3
  - Utah Patch 10a Hot Fix 2
- **Vancouver**
  - Vancouver Patch 6 Hot Fix 2
  - Vancouver Patch 7 Hot Fix 3b
  - Vancouver Patch 8 Hot Fix 4
  - Vancouver Patch 9
  - Vancouver Patch 10
- **Washington DC**
  - Washington DC Patch 1 Hot Fix 2b
  - Washington DC Patch 2 Hot Fix 2
  - Washington DC Patch 3 Hot Fix 1
  - Washington DC Patch 4
- Des informations complémentaires sont disponibles dans les bulletins CVE-2024-4879 et CVE-2024-5217 de ServiceNow.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Palo Alto - CVE-2024-5910

Un défaut de contrôle d'authentification dans une fonction critique de Palo Alto Networks Expedition permet à un attaquant de prendre le contrôle du compte administrateur d'Expedition.

2.2.1. Type de vulnérabilité

- CWE-306 : Missing Authentication for Critical Function

2.2.2. Risque

- Compromission de compte

2.2.3. Criticité (score de base CVSS v3.1)

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. Produits impactés

- Expedition versions antérieures à 1.2.92

2.2.5. Recommandations

- Mettre à jour Expedition vers la version 1.2.92 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Palo Alto.

2.2.6. Preuve de concept

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

2.3. Progress Telerik - CVE-2024-6327

Une désérialisation non sécurisé dans Progress Telerik permet à un attaquant d'exécuter du code arbitraire.

2.3.1. Type de vulnérabilité

- CWE-502 : Deserialization of Untrusted Data

2.3.2. Risque

- Exécution de code arbitraire

2.3.3. Criticité (score de base CVSS v3.1)

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

2.3.4. Produits impactés

- Telerik Report Server versions antérieures à 10.1.24.709

2.3.5. Recommandations

- Mettre à jour Telerik Report Server vers la version 10.1.24.709 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Progress.

2.3.6. Preuve de concept

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

3. Distribution d'HijackLoader avec l'exécutable Driver Booster d'IObit

En mai et juin 2024, des chercheurs en sécurité de *Lab52* et *Kroll* ont observé l'utilisation de la charge malveillante HijackLoader dans le cadre d'attaques visant à installer des implants pour voler des données. *Lab52* a détaillé une campagne de phishing menée par APT-C-36 ciblant la Colombie, où le maliciel AsyncRAT a été déployé. De son côté, *Kroll* a documenté une campagne d'attaque par téléchargement furtif via un site de films piratés bollywoodiens.

Lors de ces deux campagnes, les attaquants ont utilisé une archive ZIP contenant plusieurs fichiers, dont un exécutable légitime signé par IObit (RttHlp.exe), des fichiers Borland Package Library (BPL), ainsi que divers autres fichiers malveillants. Cette distribution d'HijackLoader a également introduit de nouvelles techniques d'obfuscation pour dissimuler le code malveillant et échapper à la détection par les solutions de sécurité basées sur des signatures.

3.1. HijackLoader

HijackLoader (aka IDAT Loader, DOILoader) est un **chargeur malveillant (loader)** observé pour la première fois en **juillet 2023** par *Zscaler ThreatLabz*. Ce maliciel utilise les appels système pour échapper à la détection des solutions de sécurité, détecte plusieurs processus spécifiques en se basant sur une liste de blocage et retarde l'exécution du code à différents stades du déploiement. Il intègre également plusieurs modules pour faciliter l'injection et l'exécution de code malveillant.

HijackLoader sert de vecteur pour des charges utiles de **voleurs de mot de passe (infostealer)** comme Lumma, Redline, Amadey, Vidar, Raccoon, StealC, ainsi que des **outils de prise de contrôle à distance** comme AsyncRAT ou Remcos.

3.1.1. Chaîne d'attaque

Le mode opératoire détaillé ci-dessous repose sur la campagne de téléchargement furtif observée par *Kroll*. L'attaquant piège les victimes en utilisant un site de téléchargement de films piratés. Lorsqu'un utilisateur tente de télécharger une vidéo, il est redirigé vers une page web hébergée sur le réseau de diffusion de contenu (Content Delivery Network) Bunny, qui fourni un lien raccourci bit[.]ly pour télécharger un fichier ZIP.

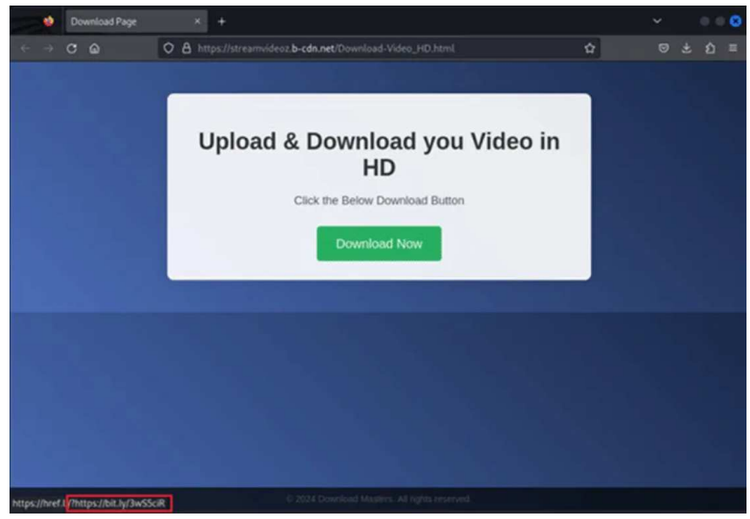

Figure 1. Page de téléchargement fournissant le lien vers le fichier zip - Source: Kroll

Cette archive ZIP contient un fichier ZIP supplémentaire protégé par mot de passe ainsi qu'un fichier TXT fournissant ce mot de passe. Une fois décompressée, l'archive protégée renferme un fichier LNK de 192 Mo et un fichier leurre contenant la "bande-annonce" de la vidéo.

Le fichier LNK malveillant utilise l'exécutable Microsoft mshta.exe pour télécharger une clé secrète OpenPGP hébergée sur le CDN Bunny. Cette clé est en réalité un contenu spécialement forgé incluant un script **HTML Application (HTA)**, l'exécutable légitime calc.exe de Microsoft, et des octets supplémentaires, dont les deux premiers correspondent aux Magic bytes d'une clé OpenPGP. Cette configuration permet de contourner les mesures de protection basées sur l'IA, se traduisant par un taux de détection extrêmement bas sur VirusTotal, avec seulement une détection sur 64 solutions de sécurité lors de l'analyse par *Kroll*.

Mshta.exe exécute ensuite le code malveillant HTA, même s'il n'est pas conforme à la norme HTML. Les navigateurs web tentent généralement d'afficher une page HTML, même en présence d'erreurs, en raison des incohérences entre navigateurs, des mauvaises pratiques de développement ou du manque de tests pour les millions de sites web. Le processus mshta.exe n'échappe pas à cette règle. Cependant, contrairement aux navigateurs souvent protégés par des environnements bac-à-sable empêchant les scripts d'interagir avec le système d'exploitation, les scripts HTA exécutés via mshta.exe peuvent interagir avec le système hôte sans restrictions.

Cette technique permet à un script malveillant d'imiter presque tout type de fichier, ces fichiers étant analysés différemment en fonction des solutions de sécurité utilisées, facilitant ainsi leur contournement. L'attaquant exploite ce comportement pour distribuer HijackLoader.

Le code HTA dans le fichier forgé comporte également **quatre couches d'obfuscation**, rendant le code invalide pour HTML. Une fois désobfusqué, le code permet de télécharger deux archives ZIP distinctes. Le script contient une fonction de désarchivage qui extrait le contenu de l'archive dans *%AppData%* et tente d'exécuter ce contenu comme commande. Si le fichier ZIP contient plusieurs fichiers ou un fichier non exécutable, le code échoue. En revanche, si l'archive ne contient qu'un seul fichier exécutable, celui-ci est exécuté.

L'analyse des deux archives K1.zip et K2.zip par *Kroll* révèle que la première contient plusieurs fichiers, tandis que la seconde renferme le binaire légitime RttHlp.exe d'IOBit, renommé jdekl.exe.

```
Shell No. 1
djt|kali-re> ls -l K1 K2
K1:
total 5876
-rw-rw-r-- 1 djt djt 1081320 Jun 19 15:11 Register.dll
-rw-rw-r-- 1 djt djt   23826 Jun 19 15:11 babyface.eps
-rw-rw-r-- 1 djt djt 1774330 Jun 19 15:11 hydrogeology.wmv
-rw-rw-r-- 1 djt djt 1112040 Jun 19 15:11 rtl120.bpl
-rw-rw-r-- 1 djt djt 2015208 Jun 19 15:11 vcl120.bpl
drwxrwxr-x 2 djt djt    4096 Jun 19 15:11 x64

K2:
total 136
-rw-rw-r-- 1 djt djt 138728 Jun 19 15:11 jdekl.exe
djt|kali-re>
```

Figure 2. Contenu des fichiers zip téléchargés - Source: Kroll

Le fichier hydrogeology.wmv contient des parties de code chiffrée d'HijackLoader. Il est déchiffré et exécuté par le loader.

L'exécutable jdekl.exe est développé et compilé en **Delphi**. Il importe les fichiers **Borland Package Library (BPL)** rtl120.bpl et vcl120.bpl qui sont des fichiers de type **DLL** créés par **Borland** pour être utilisés avec leurs outils de compilation, notamment **Delphi**. Ainsi, au lieu de charger en parallèle une DLL classique, c'est ici une BPL qui est chargée avec l'exécutable. Cette sous-technique est aujourd'hui inexistante dans le référentiel **MITRE**. Sa création a été demandée par *Kroll*.

La librairie vcl120.bpl contient du code accédant au fichier de données chiffrées hydrogeology.wav, ce qui confirme que ce fichier contient le code malveillant d'HijackLoader.

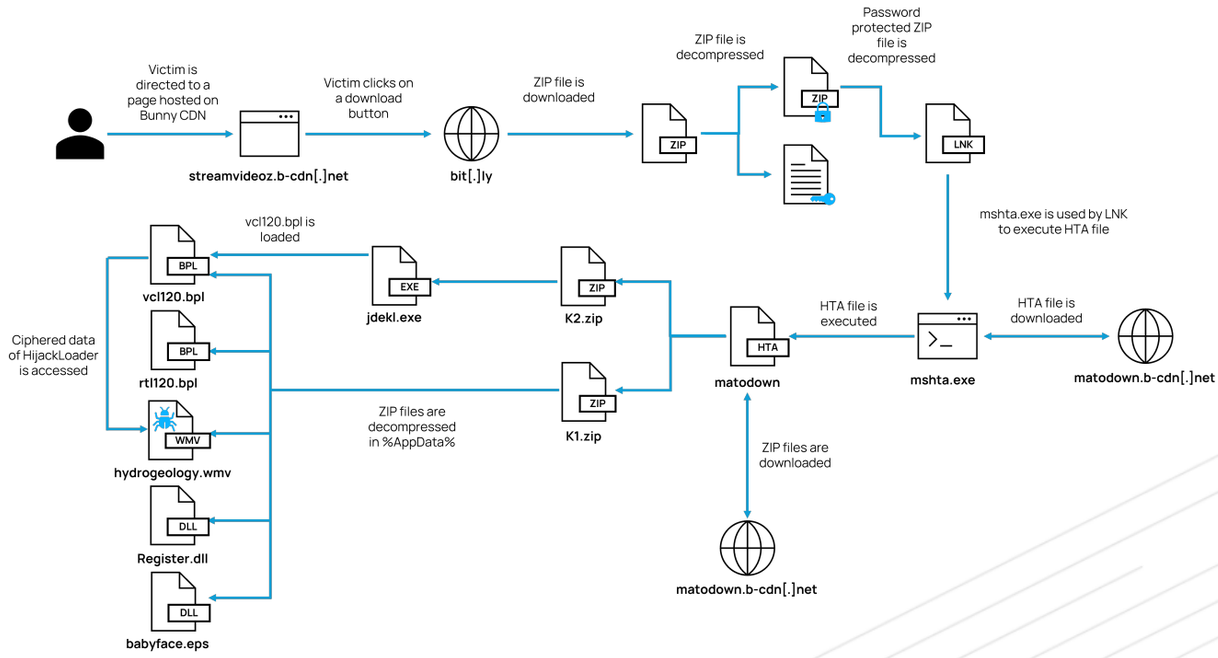

Figure 3. Chaîne d'attaque HijackLoader

3.1.2. Exploitation de la CVE-2024-21412

Des campagnes plus récentes observées en juillet pour le déploiment d'infostealers via HijackLoader exploitent la CVE-2024-21412. Cette vulnérabilité de type **contournement de la sécurité** dans Microsoft Windows SmartScreen permet à un attaquant d'empêcher l'apparition d'une fenêtre d'avertissement SmartScreen pour délivrer des fichiers malveillants.

En persuadant un utilisateur de cliquer sur un fichier URL spécifiquement forgé, l'attaquant déploie sur la machine de la victime un fichier LNK malveillant hébergé sur un partage **WebDAV**.

Figure 4. Contenu d'un fichier URL - Source: Cyble

Le fichier LNK récupéré utilise l'exécutable légitime Windows forfiles.exe pour invoquer PowerShell, exécuter mshta.exe et télécharger le script HTA. Dans la campagne détaillée par *Cyble*, le fichier HTA est assemblé avec l'exécutable légitime dialer.exe pour contourner la sécurité. L'obfuscation de ce fichier est similaire à celle déjà observée par *Kroll*.

3.1.3. MITRE ATT&CK

INITIAL ACCESS

T1189 Drive-by Compromise T1566.001 Phishing: Spearphishing Attachment T1566.002 Phishing: Spearphishing Link

EXECUTION

T1204.002 User Execution: Malicious File T1059.001 Command and Scripting Interpreter: PowerShell

PRIVILEGE ESCALATION

T1055 Process Injection

DEFENSE EVASION

T1202 Indirect Command Execution T1218.005 System Binary Proxy Execution: Mshta T1574 Hijack Execution Flow: BPL Sideloading T1564.003 Hide Artifacts: Hidden Windows T1036.003 Masquerading: Rename System Utilities T1036.005 Masquerading: Match Legitimate Name or Location T1036.007 Masquerading: Double File Extension T1562.002 Impair Defenses: Disable Windows Event Logging T1027 Obfuscated Files or Information T1553.004 Subvert Trust Controls: Install Root Certificate

DISCOVERY

T1082 System Information Discovery T1012 Query Registry

LATERAL MOVEMENT

T1021.002 Remote Services: SMB/Windows Admin Shares

COMMAND AND CONTROL

T1071 Application Layer Protocol

Figure 5. MITRE ATT&CK HijackLoader

3.1.4. Détection

Sigma:

```
title: Remotely Hosted HTA File Executed Via Mshta.EXE
id: b98d0db6-511d-45de-ad02-e82a98729620
status: test
description: Detects execution of the "mshta" utility with an argument containing the "http" keyword, which
could indicate that an attacker is executing a remotely hosted malicious hta file
references:
    - https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-
disable-anti-Virus-scans-log4shell.html
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022/08/08
modified: 2023/02/06
tags:
    - attack.defense_evasion
    - attack.execution
    - attack.t1218.005
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: '\mshta.exe'
        - OriginalFileName: 'MSHTA.EXE'
    selection_cli:
        CommandLine|contains:
            - 'http://'
            - 'https://'
            - 'ftp://'
    condition: all of selection_*
falsepositives:
    - Unknown
level: high
```

Yara:

```
rule MAL_Loader_IDAT_August_2023
{
    meta:
        description = "IDAT Loader August 2023"
        author = "Natalie Zargarov"
    strings:
        $trait_0 = {C6 A5 79 EA F4 B4 07 9A}
        $trait_1 = {3D ED C0 D3}
        $trait_2 = {C6 45 FC 4D C6 45 FD 5A}
        $trait_3 = {68 77 94 91 2C 8B 45 ?? 50 E8}
    condition:
        2 of ($trait_*)
}
```

```
rule MAL_Loader_IDAT_Shellcode_Dec_2023
{
     meta:
        author = "Thomas Elkins - Rapid7"
        description = "Yara detects in memory IDAT Loader shellcode"
        date = "20-12-2023"
    strings:
        $stage1_32_1 = { 8B D1 8D 04 09 D1 EA 33 D0 8D 04 09 56 81 E2 55 55 55 55 33 D0 8B F2 8B C2 C1 E0 02
C1 EE 02 33 } // function from IDAT API Hashing Routine
        $stage1_32_2 = { 8A 44 0D 08 30 04 32 8D 41 01 83 E9 03 42 F7 D9 1B C9 23 C8 3B D7 72 E8 } // XOR
encrpytion routine for creation of encrypted temp file
        $stage1_64_1 = { 8B 44 24 08 25 55 55 55 55 D1 E0 8B 4C 24 08 D1 E9 81 E1 55 55 55 55 0B C1 89 44 24
08 } // function from IDAT API Hashing Routine
        $stage1_64_2 = { 8B 04 24 8B 4C 24 04 0F B6 4C 0C 08 48 8B 54 24 20 0F B6 04 02 33 C1 8B 0C 24 48 8B
54 24 20 88 } // XOR encryption for creation of encrypted temp file
        $stage2_1 = { FF 57 0C 33 D2 6A 1A 59 F7 F1 66 0F BE 44 15 DC 66 89 04 73 46 3B 75 FC 72 E6 } //
Function turns computer name into UpperCase only characters using srand function
        $stage2_2 = { 8B 00 33 04 8A 8B 4D E8 89 01 8B 55 E4 83 EA 01 39 55 F4 75 } // decryption loop for
final payload
    condition:
        2 of ($stage1_32_*) or 2 of ($stage1_64_*) or 2 of ($stage2_*)
}
```

```
rule Malicious_LNK
{
    meta:
        author = "CRIL"
        description = "Yara Rule to Identify Malicious LNK Files"
    strings:
        $str1 = "C:\\Windows /m win.ini /c" wide ascii
        $str2 = "C:\\Windows\\System32\\forfiles.exe" wide ascii
        $str3 = "powershell . mshta http" wide ascii
    condition:
        (uint32(0) == 0x0000004C) and all of ($str*)
}
```

3.1.5. Indicateurs de compromission

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA256	6cede3165d85ab681491f4ff7f2362e6f4d332b2c385037a2390bcea423ab70f	Video HD (1080p).lnk
TLP:CLEAR	SHA256	7c78c287bbd93eaa79a792d5be6a2ef1522ff377a1fcd8daaebf152df5f174b7	matodown
TLP:CLEAR	SHA256	97db294fe0daf6c8dd581ca8f7eacd573ff00416d00839fad252cfb0b127e462	K1.zip
TLP:CLEAR	SHA256	372b14fce2eb35b264f6d4aeef7987da56d951d3a09ef866cf55ed72763caa12	Register.dll
TLP:CLEAR	SHA256	24d7ac3a5e97c764b1607b45e04545a311b3155887bf0a79dd6b79adad042e90	babyface.eps
TLP:CLEAR	SHA256	1da4ed3380f7477e728f6881129a20e33efcaa21191043eda902cf923332f924	hydrogeology.wmv
TLP:CLEAR	SHA256	d6dd7a4f46f2cfde9c4eb9463b79d5ff90fc690da14672ba1da39708ee1b9b50	rtl120.bpl
TLP:CLEAR	SHA256	7d0f90081a1b3500d724731a5c2f1bf120267a4803a59e59c734bcaff291220b	vcl120.bpl
TLP:CLEAR	SHA256	2f4f9fae763b5c99421a845449240b305ecdc288804268e2a411db2cce8035c3	K2.zip
TLP:CLEAR	SHA256	8aed681ad8d660257c10d2f0e85ae673184055a341901643f27afc38e5ef8473	jdekl.exe (RttHlp.exe)
TLP:CLEAR	URL	hxxps://streamvideoz[.]b-cdn[.]com/Download-Video_HD.html	Téléchargement initial
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn.net/matodown	Téléchargement du fichier hta masqué en clé secrète OpenPGP
TLP:CLEAR	URL	hxxps://vidstreemz[.]b-cdn.net/matodown	Téléchargement du fichier hta masqué en clé secrète OpenPGP (autre échantillon)
TLP:CLEAR	URL	hxxps://mato2[.]b-cdn.net/matodown	Téléchargement du fichier hta masqué en clé secrète OpenPGP (autre échantillon)
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn[.]com/K1.zip	Téléchargement de la deuxième étape
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn[.]com/K2.zip	Téléchargement de la deuxième étape
TLP:CLEAR	SHA256	4a3bbdb727e0e8fc2b41d5ebb8f7887defd468af19ac76e94b7f452e668555cd	08 CITACION DEMANDA.zip
TLP:CLEAR	SHA256	8aed681ad8d660257c10d2f0e85ae673184055a341901643f27afc38e5ef8473	08 CITACION DEMANDA.exe (RttHlp.exe)
TLP:CLEAR	SHA256	1dd7ae853911217095d2254337bedecee7267eea1ac9d0840eaf13506f40c9ab	vcl120.bpl
TLP:CLEAR	SHA256	0f6b87db9f0ae16d439b92514b3a63ae294ab5232901bbd8d87f14be47f7a67c	dreamland.m4a
TLP:CLEAR	SHA256	bb83ecbdd3c3dd6ec0a63b4c0cb480edb748165ed3a4a8720cb6605ac7173a6c	cutcherry.vcf
TLP:CLEAR	SHA256	c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2	Crowdstrike-hotfix.zip
TLP:CLEAR	SHA256	2bdf023c439010ce0a786ec75d943a80a8f01363712bbf69afc29d3e2b5306ed	vclx120.bpl

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA256	4f450abaa4daf72d974a830b16f91deed77ba62412804dca41a6d42a7d8b6fd0	instrucciones.txt
TLP:CLEAR	SHA256	52019f47f96ca868fa4e747c3b99cba1b7aa57317bf8ebf9fcbf09aa576fe006	maddisAsm_.bpl
TLP:CLEAR	SHA256	835f1141ece59c36b18e76927572d229136aeb12eff44cb4ba98d7808257c299	madexcept_.bpl
TLP:CLEAR	SHA256	931308cfe733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6	maidenhair.cfg
TLP:CLEAR	SHA256	b1fcb0339b9ef4860bb1ed1e5ba0e148321be64696af64f3b1643d1311028cb3	rtl120.bpl
TLP:CLEAR	SHA256	b6f321a48812dc922b26953020c9a60949ec429a921033cfaf1e9f7d088ee628	vcl120.bpl
TLP:CLEAR	SHA256	be074196291ccf74b3c4c8bd292f92da99ec37a25dc8af651bd0ba3f0d020349	battuta.flv
TLP:CLEAR	SHA256	d6d5ff8e9dc6d2b195a6715280c2f1ba471048a7ce68d256040672b801fda0ea	madBasic_.bpl
TLP:CLEAR	SHA256	58e2b766dec37cc5fcfb63bc16d69627cd87e7e46f0b9f48899889479f12611e	LNK malveillant
TLP:CLEAR	SHA256	268a0de2468726a106fd92563a846e764f2ba313e37b5fc0cf76171b0a363f6f	LNK malveillant
TLP:CLEAR	SHA256	aceee450c55d61671c2d3d154b5f77e7f99688b6da8a8f3256a4bae2cdb76a4c	LNK malveillant
TLP:CLEAR	SHA256	2460e7590e09af09ced6f75c001a9066c18629d956edbe8041f08cd21b7528b2	LNK malveillant
TLP:CLEAR	SHA256	4eccb7813cee8c8039424aebf69f4269d4a6c2c72d81a001254bcdce80034555	LNK malveillant
TLP:CLEAR	SHA256	6481462f15ad4213f83a3d28304f14496bae1feb8580056959a657d0ee8981db	LNK malveillant
TLP:CLEAR	SHA256	7ee31fa89e9e68f20004bdc31f8f05a95861b6c678bfa3b57f09fdfad9ef5290	LNK malveillant
TLP:CLEAR	SHA256	81e89754ae2324c684fce71acafc30f8085870be947e7a76971b4fec1b24b5d1	LNK malveillant
TLP:CLEAR	SHA256	473abb2c272295473e5556ec7dec06f2018c0a67f208d8ab33de1fb6d40895f5	LNK malveillant
TLP:CLEAR	URL	hxxps://lajollaautorepairs[.]com/cart/ionama	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxps://lajollaautorepairs[.]com/ext/paola	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxps://offshorenergytoday[.]com/shop/gklakdgasd	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxp://172.233.43.[]49/testone	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxps://21centuryart[.]com/arc/msncjsudh	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxps://offshorenergytoday[.]com/mod/mvnashd	Téléchargement du fichier HTA malveillant
TLP:CLEAR	URL	hxxps://21centuryart[.]com/au/okasjhdd	Téléchargement du fichier HTA malveillant
TLP:CLEAR	IP	62.133.61[.]26	Partage WebDAV
TLP:CLEAR	IP	62.133.61[.]43	Partage WebDAV
TLP:CLEAR	IP	5.42.107[.]78	Partage WebDAV

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	Domaine	scratchedcards[.]com	Téléchargement du fichier HTA malveillant
TLP:CLEAR	Domaine	proffyrobharborye[.]xyz	Téléchargement du fichier HTA malveillant
TLP:CLEAR	Domaine	answerrsdo[.]shop	Téléchargement du fichier HTA malveillant
TLP:CLEAR	SHA256	e15b200048fdddaedb24a84e99d6d7b950be020692c02b46902bf5af8fb50949	DR_Mod_180_2023.pdf
TLP:CLEAR	SHA256	547b6e08b0142b4f8d024bac78eb1ff399198a8d8505ce365b352e181fc4a544	DR_Mod_200_2023.PDF.lnk
TLP:CLEAR	SHA256	bd823f525c128149d70f633e524a06a0c5dc1ca14dd56ca7d2a8404e5a573078	ES_Mod_180_2023.PDF.url
TLP:CLEAR	SHA256	bc6933a8fc324b907e6cf3ded3f76adc27a6ad2445b4f5db1723ac3ec86ed10d	package_full.pdf.lnk
TLP:CLEAR	SHA256	59d2c2ca389ab1ba1fefa4a06b14ae18a8f5b70644158d5ec4fb7a7eac4c0a08	DIALER.EXE
TLP:CLEAR	SHA256	8568226767ac2748eccc7b9832fac33e8aa6bfdc03eafa6a34fb5d81e5992497	DIALER.EXE
TLP:CLEAR	SHA256	4043aa37b5ba577dd99f6ca35c644246094f4f579415652895e6750fb9823bd9	DIALER.EXE
TLP:CLEAR	SHA256	0604e7f0b4f7790053991c33359ad427c9bf74c62bec3e2d16984956d0fb9c19	DIALER.EXE
TLP:CLEAR	SHA256	8c6d355a987bb09307e0af6ac8c3373c1c4cbfbceeeb1159a96a75f19230ede6	flutter_windows.dll
TLP:CLEAR	SHA256	de6960d51247844587a21cc0685276f966747e324eb444e6e975b0791556f34f	IDMan.exe
TLP:CLEAR	SHA256	6c779e427b8d861896eacdeb812f9f388ebd43f587c84a243c7dab9ef65d151c	docpad.exe
TLP:CLEAR	SHA256	08c75c6a9582d49ea3fe780509b6f0c9371cfcd0be130bc561fae658b055a671	Invoice.pdf.lnk
TLP:CLEAR	SHA256	abc54ff9f6823359071d755b151233c08bc2ed1996148ac61cfb99c7e8392bfe	DIALER.EXE
TLP:CLEAR	SHA256	643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2	mr_0x0003B03B43F6EE12.exe

4. La gestion des vulnérabilités, un pilier de la sécurité : un exemple avec Estate ransomware

La surveillance et la gestion des vulnérabilités affectant le système d'information d'une organisation représentent un défi quotidien pour les équipes de sécurité, avec plus de cinquante nouvelles failles publiées chaque jour.

Certaines de ces vulnérabilités récemment divulguées peuvent déjà être exploitées, nécessitant une réponse rapide et appropriée pour atténuer les risques pour l'infrastructure de l'entreprise. Ce risque est exacerbé par la disponibilité de preuves de concept (PoC) en sources ouvertes. Bien que ces PoC facilitent la compréhension d'une vulnérabilité et l'ajustement des stratégies de détection et des mesures de contournement, elles peuvent également être exploitées par des acteurs malveillants.

Il est crucial de prioriser ces vulnérabilités dans le cadre d'une politique de gestion des correctifs (patch management). Cependant, il est également important de ne pas négliger les vulnérabilités ayant un score CVSS faible ou celles pour lesquelles il n'existe pas encore de PoC ou d'exploitation connue. Les retards dans le déploiement des correctifs peuvent offrir des opportunités aux attaquants, soulignant ainsi la nécessité d'une approche proactive et rigoureuse en matière de gestion des risques de sécurité.

4.1. CVE-2023-27532

Le 7 mars 2023, *Veeam* a publié un bulletin de sécurité concernant la vulnérabilité CVE-2023-27532 affectant les produits **Veeam Backup & Replication** et **Veeam Cloud Connect**. Cette vulnérabilité permet à un attaquant non authentifié d'**obtenir des identifiants en clair**, en envoyant des requêtes spécifiquement forgées vers le port 9401 du processus vulnérable.

En avril 2023, des chercheurs de *WithSecure*, ont révélé que le groupe cybercriminels FIN7 ciblait les serveurs de sauvegarde utilisant les solutions *Veeam* affectées par cette vulnérabilité. Ces attaques avaient pour objectif de compromettre les serveurs de sauvegarde afin de **dérober des données sensibles** ou **perturber les opérations de sauvegarde** et de restauration.

Suite à la publication de la vulnérabilité, des preuves de concept ont été rapidement diffusées, ce qui a facilité et accéléré son exploitation, augmentant ainsi considérablement sa dangerosité

Plus d'un an après, la CVE-2023-27532 est encore exploitée par des groupes d'attaquants, notamment le groupe Estate Ransomware. Selon les chercheurs de *Groupe-IB*, les opérateurs de ce nouveau rançongiciel ont exploitée cette vulnérabilité en avril 2024 pour voler des identifiants valides et se **déplacer latéralement** dans le système compromis.

4.2. Estate Ransomware

Estate Ransomware a été observé pour la **première fois** en avril 2024. Plusieurs victimes ont été identifiées en **France**, aux **Émirats Arabes Unis**, à **Hong Kong**, en **Malaisie** et aux **États-Unis**, bien que les secteurs touchés restent inconnus.

4.2.1. Modèle Diamant

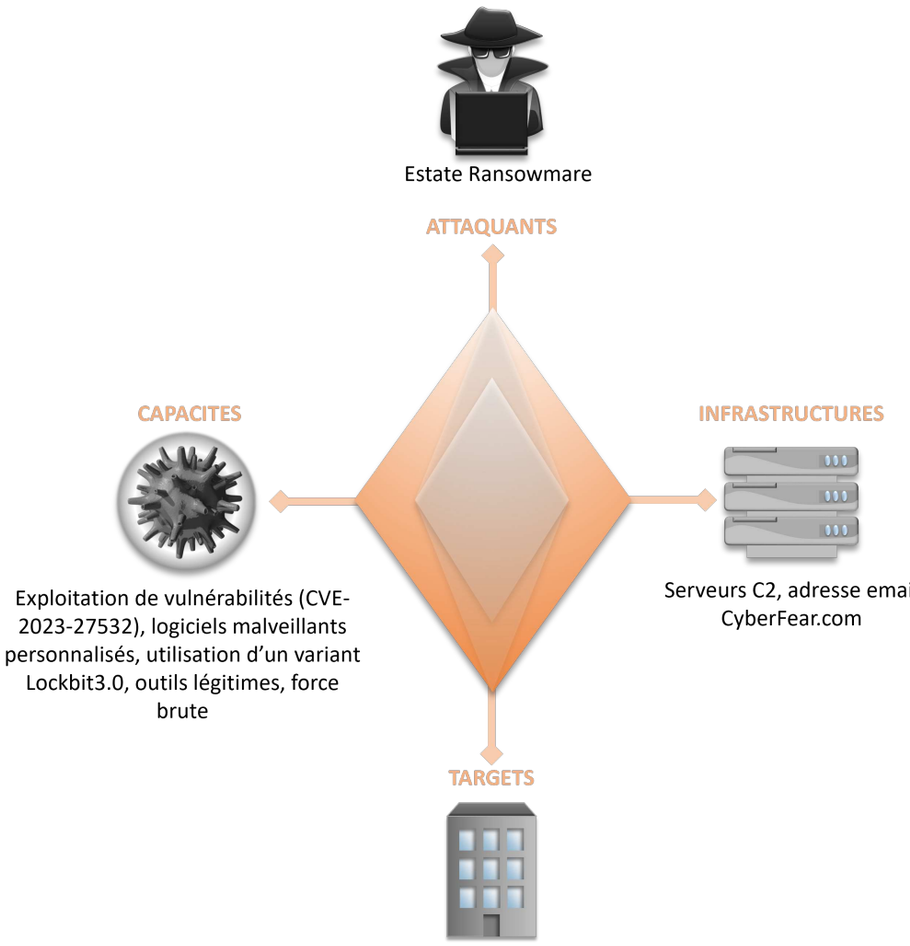

Figure 6. Modèle Diamant

4.2.2. Chaîne d'attaque

La **première manifestation d'intrusion** est survenue en avril 2024 lorsque l'acteur de la menace a utilisé le **service VPN SSL du pare-feu *FortiGate*** pour accéder au système compromis. Avant l'attaque par rançongiciel, des **tentatives de force brute** via VPN ont été observées en utilisant un compte dormant, **'Acc1'**. Quelques jours plus tard, une connexion VPN réussie utilisant ce compte a été reliéee à l'adresse IP 149.28.106[.]252.

En avril 2024, plusieurs connexions VPN utilisant 'Acc1' ont été observées à partir d'adresses IP situées aux États-Unis (149.28.106[.]252, 149.28.99[.]61 et 45.76.232[.]205). Peu après, des connexions RDP ont été établies du pare-feu au serveur compromis. Les adresses IP partagent le même système autonome : AS-CHOOPA. Les attaquants ont probablement sélectionné ces adresses pour contourner les dispositifs de sécurité, en raison de leur géolocalisation et de la mutualisation des services hébergés, ce qui peut entraîner le blocage de services légitimes.

Figure 7. Virus Total.

Figure 8. Virus Total.

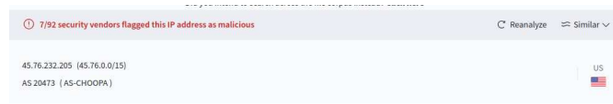

Figure 9. Virus Total.

Lors d'une session à distance, les opérateurs du ransomware Estate ont déployé une porte dérobée persistante nommée "svchost.exe" et ont configuré une tâche planifiée pour son exécution quotidienne. En utilisant le nom d'un processus *Windows* légitime, ils cherchaient à rester discrets et à échapper aux outils de protection. Après avoir installé cette porte dérobée, les attaquants se sont déconnectés du VPN et aucune autre connexion n'a été observée.

Ce logiciel malveillant permet à l'attaquant d'établir une **communication vers l'extérieur** avec l'IP 77.238.245[.]11:30001. L'utilisation du port 30001 n'est pas commune. C'est un port Transmission Control Protocol (TCP) déjà identifié par des chercheurs en sécurité lors de déploiement de chevaux de Troie. Dans le cadre d'Estate Ransomware, le fichier svchost.exe établit un tunnel utilisant le protocole HTTP pour se connecter au serveur C2 afin d'**exécuter à distance des commandes** sur le serveur compromis.

A date, le port 30001 n'est plus en écoute, les opérateurs d'Estate semblent avoir démanteler cette infrastructure.

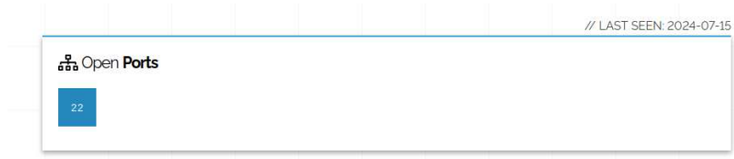

Figure 10. Source: Shodan.

L'IP Néerlandaise 77.238.245[.]11 appartient à un hébergeur Russe et utiliséee par **plusieurs groupes malveillants**. Elle a été identifiée dans des campagnes de déploiement de **Chevaux de Troie bancaire**. Les attaquants priviligient des adresses **IP mutualisées** pour des raisons stratégiques et techniques, car il est difficile de les bloquer sans affecter des sites **légitimes** partageant la même adresse. Cela leur permet de polonger leurs activités malveillantes sans être rapidement **détectés** ou **bloqués**.

Figure 11. Source: VirusTotal.

Le lendemain, l'attaquant a accédé à un serveur de fichiers via RDP et a effectué diverses activités malveillantes, principalement axées sur l'exfiltration d'identifiants et l'exploitation des vulnérabilités de Veeam Backup & Replication. Selon Groupe-IB, le groupe aurait exploité une preuve de concept publiée par Horizon3 et sfewer-R7 sur GitHub pour la vulnérabilité CVE-2023-27532, disponible depuis plus d'un an.

L'acteur malveillant a utilisé SoftPerfect Netscan et des outils de récupération de mots de passe de Nirsoft pour scanner le réseau et récolter des informations et identifiants. Des informations supplémentaires ont été extraites du serveur de sauvegarde via le compte 'VeeamBkp', permettant se latéraliser vers le serveur Active Directory (AD) via RDP.

Depuis le serveur AD, AdFind a été téléchargé et exécuté pour énumérer les utilisateurs du domaine. Une fois suffisamment d'informations recueillies, l'attaquant s'est déplacé vers d'autres serveurs et postes de travail en utilisant des comptes de domaine compromis.

Le rançongiciel a été déployé en utilisant trois binaires : DC.exe, LB3.exe et PsExec.exe. Sur chaque hôte, Windows Defender a été désactivé avec Defender Control (DC.exe), un outil largement utilisé lors des attaques. Ensuite, PsExec a permis de se connecter à l'hôte et d'exécuter le fichier rançongiciel LB3.exe, suivi de la création de la première note de rançon. Pour éviter la détection et entraver les investigations, le rançongiciel a effacé les journaux d'événements Windows sur tous les systèmes compromis.

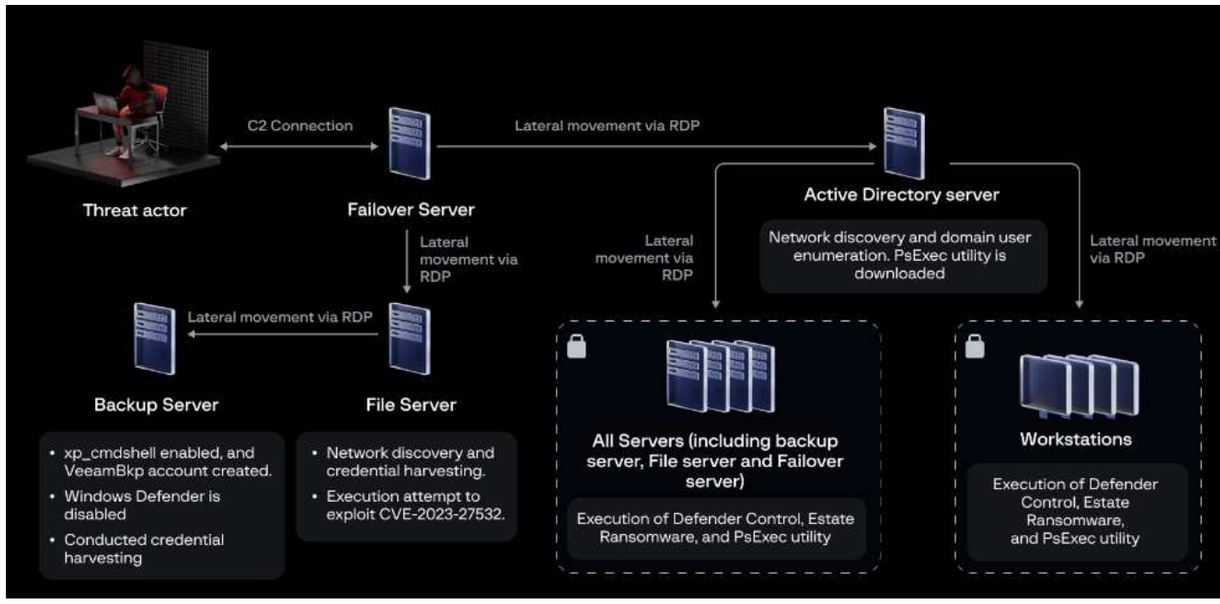

Figure 12. Chaine d'attaque. Source : Groupe-IB.

Ce rançongiciel utilise le service de messagerie *CyberFear* pour communiquer avec ses victimes, en les incitant à utiliser une adresse ProtonMail. Ce service, réputé sécurisé, chiffré de bout en bout et sans logs, avec des serveurs offshore, est également utilisé par d'autres rançongiciels comme Worry.

Dans l'attaque de Estate ransomware, le seul outil personnalisé était la porte dérobée "Svchost.exe", le reste de l'attaque reposant sur des outils connus et disponibles publiquement. L'exécutable de chiffrement était une variante du rançongiciel LockBit3.0 dont le code source avait fuité en 2023. Cela montre que le groupe n'est actuellement pas très sophistiqué et utilise des moyens courants. Cependant, étant donné la nouveauté de ce rançongiciel, il est probable que les attaques se personnalisent et s'améliorent avec le temps.

4.2.3. Mitre Att&ck

INITIAL ACCESS

T1078 Valid Accounts. T1133 External Remote Services.

EXECUTION

T1204.002 User Execution: Malicious File. T1569.002 System Services: Service Execution.

PERSISTENCE

T1053.005 Scheduled Task/Job: Scheduled Task. T1136.001 Create Account: Local Account. T1505.001 Server Software Component: SQL Stored Procedures.

DEFENSE EVASION

T1070.001 Indicator Removal: Clear Windows Event Logs. T1070.004 Indicator Removal: File Deletion. T1562.001 Impair Defenses: Disable or Modify Tools.

CREDENTIAL ACCESS

T1555 Credentials from Password Stores.

DISCOVERY

T1018 Remote System Discovery. T1087.002 Account Discovery: Domain Account.

LATERAL MOVEMENT

T1021.001 Remote Services: Remote Desktop Protocol.

COMMAND & CONTROL

T1571 Non-Standard Port. T1071.001 Application Layer Protocol: Web Protocols.

IMPACT

T1486 Data Encrypted for Impact.

Figure 13. Chaine d'infection. Source : Groupe-IB.

4.2.4. IoC

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	IP	149.28.106[.]252	Utilisée pour du force brut
TLP:CLEAR	IP	149.28.99[.]61	Utilisée pour du force brut
TLP:CLEAR	IP	45.76.232[.]205	Utilisée pour du force brut
TLP:CLEAR	IP	77.238.245[.]11:30001	Connexion C2 depuis le Svchost.exe
TLP:CLEAR	SHA1	CB704D2E8DF80FD3500A5B817966DC262D80DDB8	CD.exe
TLP:CLEAR	SHA1	2C56E9BEEA9F0801E0110A7DC5549B4FA0661362	DC.ini
TLP:CLEAR	SHA1	5E460A517F0579B831B09EC99EF158AC0DD3D4FA	Svchost.exe
TLP:CLEAR	SHA1	107EC3A7ED7AD908774AD18E3E03D4B999D4690C	LB3.exe
TLP:CLEAR	Fichier	netscan.exe	
TLP:CLEAR	Fichier	veeam-creds-main	
TLP:CLEAR	Fichier	CVE-2023-27532.exe	
TLP:CLEAR	Fichier	VeeamHax	
TLP:CLEAR	Fichier	BulletsPassView64.exe	
TLP:CLEAR	Fichier	netpass64.exe	
TLP:CLEAR	Fichier	PasswordFox64.exe	
TLP:CLEAR	Fichier	ChromePass.exe	
TLP:CLEAR	Fichier	WirelessKeyView64.exe	
TLP:CLEAR	Fichier	mspass.exe	
TLP:CLEAR	Fichier	VNCPassView.exe	
TLP:CLEAR	Fichier	WebBrowserPassView.exe	
TLP:CLEAR	Fichier	mailpv.exe	
TLP:CLEAR	Fichier	RouterPassView.exe	
TLP:CLEAR	Fichier	PstPassword.exe	
TLP:CLEAR	Fichier	OperaPassView.exe	
TLP:CLEAR	Fichier	Dialupass.exe	
TLP:CLEAR	Fichier	BulletsPassView64.exe	
TLP:CLEAR	Fichier	ExtPassword.exe	
TLP:CLEAR	Fichier	pspv.exe	
TLP:CLEAR	Fichier	iepv.exe	
TLP:CLEAR	Fichier	SniffPass64.exe	
TLP:CLEAR	Fichier	rdpv.exe	

5. Références

Distribution d'HijackLoader avec l'exécutable Driver Booster d'IObit

- https://lab52.io/blog/dll-side-loading-through-iobit-against-colombia/
- https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution
- https://www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/
- https://cyble.com/blog/increase-in-the-exploitation-of-microsoft-smartscreen-vulnerability-cve-2024-21412/
- https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed

La gestion des vulnérabilités, un pilier de la sécurité : un exemple avec Estate ransomware

- https://www.group-ib.com/blog/estate-ransomware/
- https://www.mycert.org.my/portal/advisory?id=MA-1076.052024
- https://www.pcrisk.com/removal-guides/25608-worry-ransomware