



En cybersécurité aussi, le savoir n'a de valeur
que si il est partagé.

In Cybersecurity too, knowledge only
increases in value once shared.

WOCSA

- WOCSA (Worldwide Open Cyber Security Association) is a federation of **non profit association** with a head quarter based in France.
- Cybersecurity is a public affair in which **everyone has to take a part**.
- WOCSA joins experts with other people **to take care of our digital life**.

Meetup Ethical Hacking Workshop

- 1 animateur propose un sujet sur la thématique de la cybersécurité
- L'atelier a un format d'environ 2 heures
 - Une partie pour introduire le sujet et les notions
 - Une partie pratique pour mettre en application
- Exemple : rubber ducky, OSINT, forensic, attaques sur le wifi...

Les bases du forensic Windows

- Domaine de la cyber qui consiste à collecter, préserver et analyser des preuves numériques pour comprendre les incidents de sécurité
- Objectif :
 - Comprendre les étapes d'un incident
 - Identifier le point d'entrée
 - Proposer des améliorations
- Environnement : A peu près partout où il y a des traces
- Etapes :
 - Collecter les logs
 - Sécuriser les logs (copie)
 - Analyser
 - Restituer

Indicateurs de Compromissions (IOCs)

- Un IoC est une donnée permettant d'identifier la présence d'une infection. Un IOC peut prendre plusieurs formes:
 - Adresse IP, un nom de domaine, une URL
 - Hash de fichier
 - Un chemin / nom de fichier
 - Une clé de registre
 - ...
- Les IOCs peuvent être utilisés lors de l'investigation numérique d'un système pour rechercher la présence d'une menace spécifique.

Artefact

- Dans le domaine de l'investigation numérique, le terme **Artefact** désigne un type de données pouvant fournir des éléments permettant de retracer l'activité d'un système.
- Exemples d'artefacts connus:
 - Historique de navigation
 - Documents récents
 - Logs firewall
 - ...

Horodatage

- Lors d'une investigation numérique, il est fréquent de plusieurs sources de données soient analysées et que le résultat de ces analyses soient combinées pour avoir une vue globale.
- Pour que cette vue globale soit cohérente, il faut que tous les événements soient exprimés en utilisant le même fuseau horaire. On utilise généralement l'UTC.
 - Déterminer le fuseau horaire pour chaque système
 - Vérifier si les systèmes sont à l'heure
 - Pour chaque source de données, déterminer si les dates et heures sont stockées en UTC ou en Local Time
 - Vérifier comment les outils interprètent les dates!

Système de fichiers

- Un système de fichiers représente les différentes structures, noms et agencements nécessaires à l'organisation des données sur un support de stockage. Il permet ainsi de retrouver la donnée et d'y accéder.
- 3 couches peuvent être discernées:
 - Logique: présente les API accessibles par les applications depuis le système d'exploitation
 - Virtuelle: niveau d'abstraction supplémentaire permettant de gérer plusieurs disques physiques avec un seul disque virtuel
 - Physique: gère la communication et les opérations sur le support physique

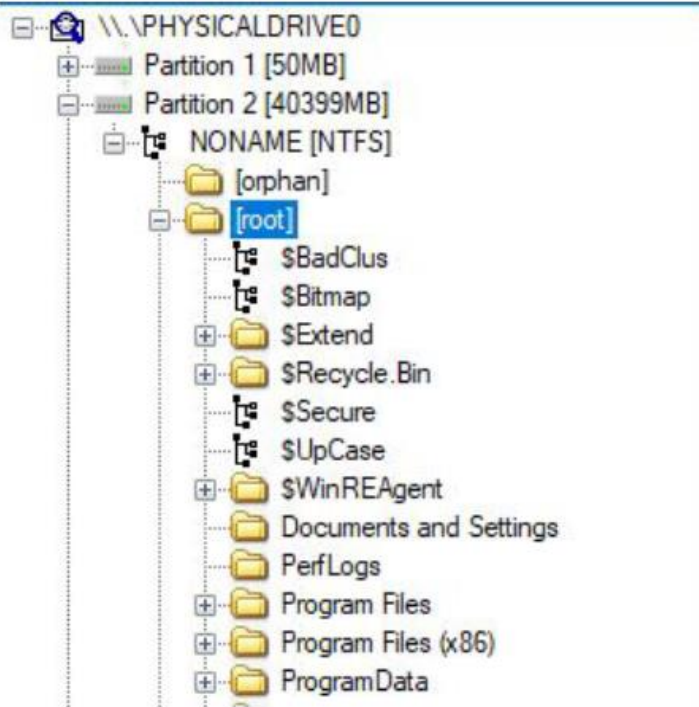
Système de fichiers : NTFS

- Système de fichiers propriétaire à Microsoft dont la première version a été publiée en 1993. Depuis 5 versions majeures se sont succédées. La dernière en date est NTFS 3.1 sortie en 2001 (Windows XP). Il n'y a pas eu de mise à jour majeure depuis, les nouvelles fonctionnalités ajoutées se reposant sur des composants existants.
- Particularité : NTFS est un système de fichiers avec journal (*\$LogFile*) permettant de tracer les métadonnées des changements afin d'être reproductible en cas de dysfonctionnement.

Artefact #1 : MFT

- La MFT est le composant principal du système de fichiers NTFS. Elle contient les métadonnées associées à chaque fichier du système, ainsi que l'emplacement des blocs qui les composent. Pour les très petits fichiers, elle peut même embarquer la donnée elle-même.
- Pour chaque fichier du système, la MFT contient notamment son nom, son emplacement, sa taille, les permissions associées, ainsi que 8 timestamps (Creation, Modification, Metadata and Access pour "Standard Information" et "Filename").
- Les informations sur les fichiers supprimés sont conservées tant que le bloc n'est pas réutilisé.
- Fichier \$MFT à la racine de la partition

Artefact #1 : MFT

	<table><tr><th>Name</th><th>Size</th><th>Type</th><th>Date Modified</th></tr><tr><td>Program Files (x86)</td><td>1</td><td>Directory</td><td>12/05/2021 12:50:04</td></tr><tr><td>ProgramData</td><td>1</td><td>Directory</td><td>12/05/2021 12:50:04</td></tr><tr><td>Recovery</td><td>1</td><td>Directory</td><td>12/05/2021 11:32:33</td></tr><tr><td>System Volume Information</td><td>1</td><td>Directory</td><td>12/05/2021 11:36:12</td></tr><tr><td>Users</td><td>1</td><td>Directory</td><td>12/05/2021 11:47:54</td></tr><tr><td>Windows</td><td>1</td><td>Directory</td><td>12/05/2021 14:46:20</td></tr><tr><td>\$AttrDef</td><td>3</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$BadClus</td><td>0</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$Bitmap</td><td>1,263</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$Boot</td><td>8</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$I30</td><td>8</td><td>NTFS Index All...</td><td>12/05/2021 14:46:20</td></tr><tr><td>\$LogFile</td><td>55,952</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$MFT</td><td>229,632</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr><tr><td>\$MFTMirr</td><td>4</td><td>Regular File</td><td>12/05/2021 13:27:58</td></tr></table>	Name	Size	Type	Date Modified	Program Files (x86)	1	Directory	12/05/2021 12:50:04	ProgramData	1	Directory	12/05/2021 12:50:04	Recovery	1	Directory	12/05/2021 11:32:33	System Volume Information	1	Directory	12/05/2021 11:36:12	Users	1	Directory	12/05/2021 11:47:54	Windows	1	Directory	12/05/2021 14:46:20	\$AttrDef	3	Regular File	12/05/2021 13:27:58	\$BadClus	0	Regular File	12/05/2021 13:27:58	\$Bitmap	1,263	Regular File	12/05/2021 13:27:58	\$Boot	8	Regular File	12/05/2021 13:27:58	\$I30	8	NTFS Index All...	12/05/2021 14:46:20	\$LogFile	55,952	Regular File	12/05/2021 13:27:58	\$MFT	229,632	Regular File	12/05/2021 13:27:58	\$MFTMirr	4	Regular File	12/05/2021 13:27:58
Name	Size	Type	Date Modified																																																										
Program Files (x86)	1	Directory	12/05/2021 12:50:04																																																										
ProgramData	1	Directory	12/05/2021 12:50:04																																																										
Recovery	1	Directory	12/05/2021 11:32:33																																																										
System Volume Information	1	Directory	12/05/2021 11:36:12																																																										
Users	1	Directory	12/05/2021 11:47:54																																																										
Windows	1	Directory	12/05/2021 14:46:20																																																										
\$AttrDef	3	Regular File	12/05/2021 13:27:58																																																										
\$BadClus	0	Regular File	12/05/2021 13:27:58																																																										
\$Bitmap	1,263	Regular File	12/05/2021 13:27:58																																																										
\$Boot	8	Regular File	12/05/2021 13:27:58																																																										
\$I30	8	NTFS Index All...	12/05/2021 14:46:20																																																										
\$LogFile	55,952	Regular File	12/05/2021 13:27:58																																																										
\$MFT	229,632	Regular File	12/05/2021 13:27:58																																																										
\$MFTMirr	4	Regular File	12/05/2021 13:27:58																																																										

Artefact #1 : MFT

- **Outils (Eric Zimmerman)**
- Parser la MFT du poste sur lequel on est (nécessite les droits admin)
 - PS C:\Users\Arnaud>MFTECmd.exe --csv C:\Users\Arnaud\Documents --csvf mft_parse.csv
- Parser un fichier extrait d'une image disque :
 - PS C:\Users\Arnaud >MFTECmd.exe -f .\MFT --csv C:\Users\Arnaud\Documents --csvf mft_parse.csv
- Il est aussi possible d'utiliser l'utilitaire MFTExplorer qui fournit une version graphique.

Artefact #2 : ADS

- Au sein du système de fichiers NTFS, tous les fichiers disposent de différents attributs, ils peuvent notamment posséder plusieurs attributs \$DATA.
- Lors de l'accès à un fichier, c'est le datastream "" (vide) qui est accédé (par exemple pour un fichier texte, ce sera le contenu du fichier).
- Mais il est possible de créer d'autres stream en ajoutant ":" puis le nom du stream à utiliser sur un nom de fichier.

```
echo "Ceci est un test VISIBLE" > Test.txt  
echo "!!!HIDDEN!!!" > Test.txt:hidden
```

Artefact #2 : ADS

- Depuis Windows XP2, lorsqu'un fichier est téléchargé depuis Internet depuis un navigateur sur un volume NTFS, un Alternate Data Stream (ADS) nommé **Zone.Identifieur** est créé.
- Les fichiers contenant un ADS et une ZoneID = 3 proviennent d'Internet:
 - ZoneID = 2 ⇒ URLZONE_TRUSTED
 - ZoneID = 3 ⇒ URLZONE_INTERNET
 - ZoneID = 4 ⇒ URLZONE_UNTRUSTED

```
PS C:\Users\ArnaudL'Hutereau\Downloads> Get-Content -path '.\dormir.png' -stream Zone.Identifieur
```

```
[ZoneTransfer]
```

```
ZoneId=3
```

```
ReferrerUrl=https://www.flaticon.com/fr/chercher?type=icon&search-
```

```
group=all&word=dormir&license=&color=&shape=&current_section=&author_id=&pack_id=&family_id=&style_id=&choice=&type=
```

```
HostUrl=https://www.flaticon.com/fr/download/icon/6117351?icon_id=6117351&author=203&team=203&keyword=dormir&pack=packs%2Fpilates-56&style=2&format=png&color=%23000000&colored=1&size=512&selection=1&premium=0&type=standard&search=dormir
```

Artefact #3 : Prefetch

- Les fichiers Prefetch ont pour but d'accélérer le lancement d'applications.
- Un fichier est créé avec le nom du programme à chaque lancement d'un programme, quel que soit l'emplacement d'origine de l'application.
- Localisation : C:\Windows\Prefetch
- Un fichier contient des métadonnées comme :
 - Le nom de l'exécutable (dans la limite de 29 caractères)
 - Le nombre de lancement (run count) ou les dates de lancement de l'application
 - Le Volume Path et le numéro de série du volume de stockage de l'application
 - Les fichiers et répertoires appelés par l'application durant son exécution
 - Horodatage :
 - Horodatage du dernier lancement
 - Horodatage de la création du volume sur lequel le fichier Prefetch a été créé
- Volume
 - 1 entrée par volume utilisé par l'application

CTFMON.EXE-795F8130.pf	PfPre_4d5fb56e.mkd
DASHOST.EXE-4B84F273.pf	PfPre_4d607b4b.mkd
DEFRAG.EXE-3D9E8D72.pf	PfPre_8444caa4.mkd
DLLHOST.EXE-15CDDA9C.pf	PfPre_8446565e.mkd
DLLHOST.EXE-4427C062.pf	PICKERHOST.EXE-DE4B8E61.pf
DLLHOST.EXE-4B6CB38A.pf	POWERSHELL.EXE-CA1AE517.pf
DLLHOST.EXE-4F1B3E7E.pf	ResPriStaticDb.ebd
DLLHOST.EXE-5DC108BA.pf	RUNDLL32.EXE-15665F3A.pf
DLLHOST.EXE-6389524F.pf	RUNDLL32.EXE-52A71BD0.pf
DLLHOST.EXE-8A53FEB5.pf	RUNDLL32.EXE-90265CDD.pf
DLLHOST.EXE-960426D8.pf	RUNDLL32.EXE-BF72C764.pf
DLLHOST.EXE-A010D183.pf	RUNDLL32.EXE-C0B1E5EB.pf
DLLHOST.EXE-ACFEFA21.pf	RUNDLL32.EXE-FDCB85A1.pf
DLLHOST.EXE-BF54A4C5.pf	RUNTIMEBROKER.EXE-09C87F04.pf
DLLHOST.EXE-C60C3853.pf	RUNTIMEBROKER.EXE-1163E293.pf
DLLHOST.EXE-E9BDD97B.pf	RUNTIMEBROKER.EXE-175F5C00.pf
DRVINST.EXE-39D9EAC7.pf	RUNTIMEBROKER.EXE-20710195.pf
DWM.EXE-314E93C5.pf	RUNTIMEBROKER.EXE-22F13460.pf
dynresprl.7db	RUNTIMEBROKER.EXE-29D58CE3.pf
EXPLORER.EXE-D5E97654.pf	RUNTIMEBROKER.EXE-3DE22D03.pf
FILESYNCCONFIG.EXE-17AB0230.pf	RUNTIMEBROKER.EXE-4551A062.pf
FILESYNCCONFIG.EXE-2A1D7AE2.pf	RUNTIMEBROKER.EXE-736BE57C.pf
FILESYNCCONFIG.EXE-3C280014.pf	RUNTIMEBROKER.EXE-79DB8DE5.pf
FILESYNCCONFIG.EXE-56B37223.pf	RUNTIMEBROKER.EXE-7B4A2CEC.pf
FILESYNCCONFIG.EXE-781A5767.pf	RUNTIMEBROKER.EXE-8430E41C.pf

Artefact #3 : Prefetch

NOTEPAD.EXE-C5670914.pf

Windows Prefetch File (PF) information:

```
Format version          : 30
Prefetch hash           : 0xc5670914
Executable filename     : NOTEPAD.EXE
Run count                : 3
Last run time: 1        : Sep 19, 2020 03:47:39.738845500 UTC
Last run time: 2        : Sep 19, 2020 03:45:39.879332600 UTC
Last run time: 3        : Sep 19, 2020 03:45:34.507248900 UTC
Last run time: 4        : Sep 18, 2020 22:50:37.518407300 UTC
Last run time: 5        : Sep 18, 2020 22:48:08.283848600 UTC
Last run time: 6        : Sep 18, 2020 22:47:38.408830000 UTC
Last run time: 7        : 0
Last run time: 8        : 0
```

```
Filename: 71 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\WINDOWS\SYSTEM32\PROFAP1.DLL
Filename: 72 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\DOCUMENTS\DESKTOP.INI
Filename: 73 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\MUSIC\DESKTOP.INI
Filename: 74 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\PICTURES\DESKTOP.INI
Filename: 75 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\VIDEOS\DESKTOP.INI
Filename: 76 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\DOWNLOADS\DESKTOP.INI
Filename: 77 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMINISTRATOR\ONEDRIVE\DESKTOP.INI
Filename: 78 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\MORTYSMITH\DOCUMENTS\PLANS.TXT
Filename: 79 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\MORTYSMITH\DOCUMENTS\DESKTOP.INI
Filename: 80 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\WINDOWS\SYSTEM32\DRIVERS\DXGKRNL.SYS
Filename: 81 : \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\MORTYSMITH\DOCUMENTS\MY SOCIAL SECURITY NUMBER.TXT
```


Artefact #3 : Prefetch

- **Outils**
 - EZ PECmd.exe (Windows)
 - Commande : PECmd.exe -f NOM_FICHER

Artefact #4 : SRUM

- Le System Ressource Usage Monitor surveille la consommation des ressources par les applications en cours d'exécution.
- Dans un contexte Forensic, l'analyse de la base de données ainsi constituée fournit des informations sur les applications lancées, les accès réseau, etc.
- **Localisation :**
 - C:\Windows\System32\sru
- **Outil**
 - SrumECmd (<https://ericzimmerman.github.io/#!index.md>)

Artefact #4 : SRUM

SRUM ENTRY CREATION TIME	Application	User SID	Interface	Bytes Sent	Bytes Received
2020-09-18 5:44:00	System\IPv6 Control Message	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_CSMACD	1576	0
2020-09-18 5:44:00	System	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_CSMACD	162	0
2020-09-18 5:44:00	Dhcp	S-1-5-19 (LocalService)	IF_TYPE_ETHERNET_CSMACD	1256	0
2020-09-18 5:44:00			IF_TYPE_ETHERNET_CSMACD	8955	2536
2020-09-18 5:57:00			IF_TYPE_ETHERNET_CSMACD	16445	303
2020-09-18 5:57:00	Dhcp	S-1-5-19 (LocalService)	IF_TYPE_ETHERNET_CSMACD	157	0
2020-09-18 5:57:00	System\IPv6 Control Message	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_CSMACD	180	0

Pratique

- Un employé d'une entreprise a téléchargé un document et l'a exécuté sur son poste de travail.
- Après l'exécution, il s'est rendu compte que le fichier n'a pas effectué l'action attendue : afficher la nouvelle campagne marketing.
- Il a contacté le service de sécurité de l'entreprise pour signaler le problème.
- Vous êtes chargé d'analyser le poste de travail pour comprendre ce qui s'est passé sur l'ordinateur depuis le téléchargement du fichier.

A disposition (sur github)

- **Outils**
 - EZ PECmd.exe (Windows)
 - Commande : PECmd.exe -f NOM_FICHER
 - MFTECmd.exe (Windows)
 - SRU-Dump
- **Artefacts / Fichiers**
 - Fichier « ads.txt » (Flux ADS Zone. Identifier du fichier téléchargé sur Internet)
 - Base SRUM
 - Fichiers des Prefetch
 - MFT (déjà en CSV)
 - Fichier « Window ServicextFG.bat.txt »
 - Fichier « libb1.py.txt »

Objectif

- **Confirmer la compromission du poste**
- **Identifier les actions malveillantes réalisées (création de fichiers, exécution...)**
- **Déterminer si une exfiltration de données a eu lieu**

Infostealers

- Un infostealer, ou « voleur d'informations », est un type de logiciel malveillant conçu pour infiltrer un système informatique afin de voler des informations sensibles telles que des identifiants de connexion, des données personnelles, des informations financières, etc.
- Les principaux objectifs d'un infostealer sont les suivants :
 - **Vol d'identifiants et de mots de passe** : identifiants de connexion, des mots de passe et d'autres informations d'authentification à partir des navigateurs web, des clients de messagerie, des applications de messagerie instantanée, etc.
 - **Collecte de données personnelles** : noms, les adresses, les numéros de téléphone, les numéros de sécurité sociale, etc.
 - **Exfiltration d'informations financières** : numéros de carte de crédit, les informations de compte bancaire, les numéros de sécurité sociale, etc.
 - **Surveillance des activités de l'utilisateur** : frappes au clavier, en prenant des captures d'écran, en enregistrant les sessions de navigation web, etc.

Infostealers

- Les méthodes de compromission utilisées par les infostealers peuvent varier
- Quelques techniques couramment observées :
 - **Phishing/Spam** : Les attaquants peuvent distribuer des infostealers via des e-mails de phishing contenant des pièces jointes malveillantes ou des liens vers des sites web compromis.
 - **Téléchargement malveillant** : Les infostealers peuvent être téléchargés et installés sur un système par l'utilisateur lui-même, souvent en se faisant passer pour des logiciels légitimes ou des mises à jour de logiciels.
 - **Infection par des logiciels malveillants déjà présents** : Les infostealers peuvent être installés sur un système déjà compromis par d'autres types de logiciels malveillants, tels que des chevaux de Troie ou des ransomwares.



<https://cyberint.com/blog/financial-services/raccoon-stealer/>