

Introduction aux systèmes Windows, et à leur analyse forensique

Simon Garrelou - Sylvain Peyrefitte

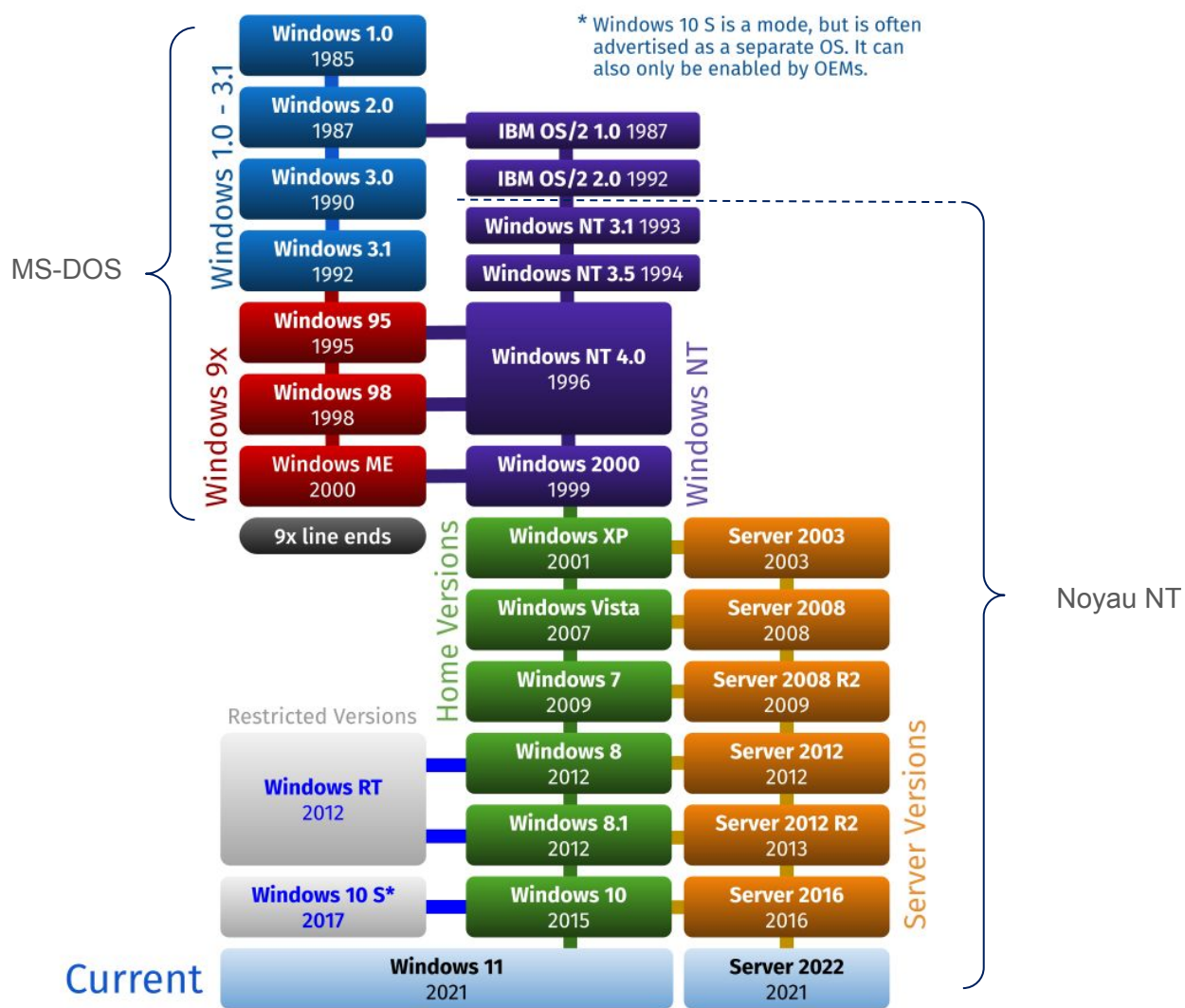
2025/2026

Objectifs

- Présenter le fonctionnement de mécanismes présents dans l'OS Windows (version 7 et +)
 - Organisation bas niveau de l'OS Windows
 - Mécanismes de sécurité
 - Mécanismes de journalisation
- Etudier les traces laissées par ceux-ci
- Corréler ces informations pour en extraire des informations sur les actions effectuées sur une machine



Historique des OS Windows



Windows basés sur MS-DOS

- MS-DOS: Microsoft Disk Operating System (1981)
- Système d'exploitation en ligne de commande seulement
- Pas d'utilisateurs, pas de multi-processus, pas de segmentation mémoire (*mode réel*)
- 16 bits (processeurs Intel 8086, puis x86)

```
Starting MS-DOS...

HIMEM is testing extended memory...done.

C:\>C:\DOS\SMARTDRV.EXE /X
C:\>dir

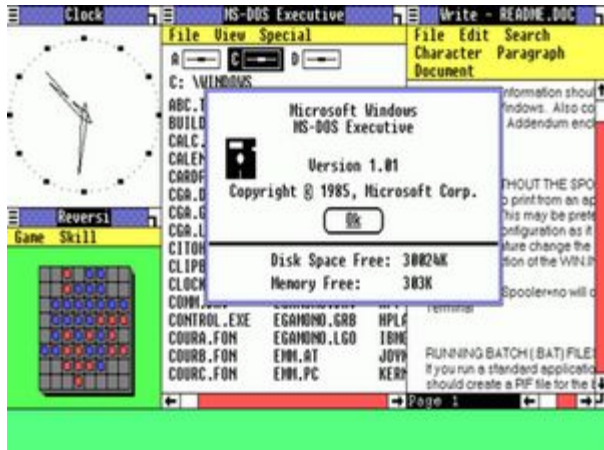
Volume in drive C is MS-DOS_6
Volume Serial Number is 4B77-00E8
Directory of C:\

DOS             <DIR>             11-23-17  12:07a
COMMAND  COM           54,645  05-31-94   6:22a
WINA20    386           9,349  05-31-94   6:22a
CONFIG   SYS              71  11-23-17  12:07a
AUTOEXEC BAT            78  11-23-17  12:07a
          5 file(s)           64,143 bytes
                               517,021,696 bytes free

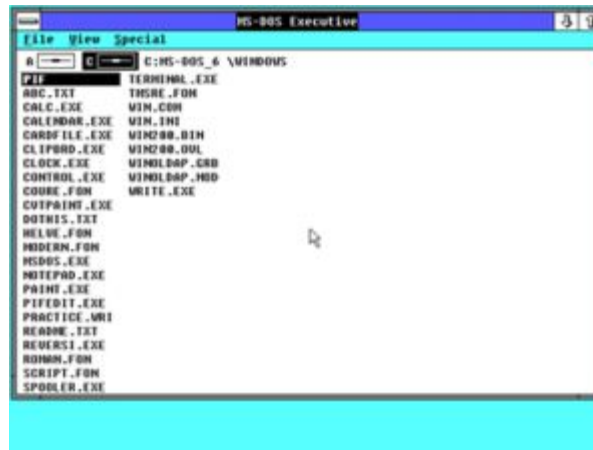
C:\>_
```

Windows basés sur MS-DOS

- Windows (1985) ajoute un support du mode protégé (multitâche coopératif)
- Introduction de la base de registre, début d'hybridation 16/32 bits



Windows 1.0 (1985)



Windows 2.0 (1987)



Windows 3.1 (1992)

Windows basés sur MS-DOS

- Windows 95 (1995): MS-DOS ne sert plus qu'à démarrer le système d'exploitation
 - Le système principal tourne en mode protégé, 32 bits, multitâche préemptif
 - MS-DOS n'est utilisé qu'en tant que couche de compatibilité



Windows basés sur NT

- Windows NT 3.1 (1993): refonte totale de l'architecture
 - Suppression totale de la dépendance à MS-DOS
 - Nouveau micro-noyau: NT kernel
 - “Orienté objet”: chaque ressource est vue comme un objet (processus, fichier, thread, etc.)
 - Portabilité: écrit en C et C++, peu d'assembleur (tourne sur x86, MIPS, Alpha, PowerPC)
- Windows NT 4 (1996): release grand public



Windows basés sur NT

- Windows NT (1996)
- Windows 2000 (1999)
- Windows XP (2001) / Server 2003
- Windows Vista (2006) / Server 2008
- Windows 7 (2009)
- Windows 8 (2012) / Server 2012
- Windows 10 (2015) / Server 2016 / Server 2019
- Windows 11 (2021) / Server 2022



Introduction à la réponse sur incident

Réponse sur incident & forensique numérique

- **Contexte:** une intrusion dans un système d'information a été détectée
- **But:** retrouver la source de l'intrusion, ainsi que les action effectuées par l'intrus, afin de pouvoir remédier au problème
- Livrables:
 - Rapport d'incident détaillant les étapes de l'analyse
 - Timeline reprenant les actions importantes effectuées par l'attaquant et les défenseurs
 - Liste d'actions permettant d'exclure l'intrus du SI, et d'empêcher son retour
 - Conseils de remédiation afin d'empêcher une ré-intrusion

Réponse sur incident & **forensique numérique**

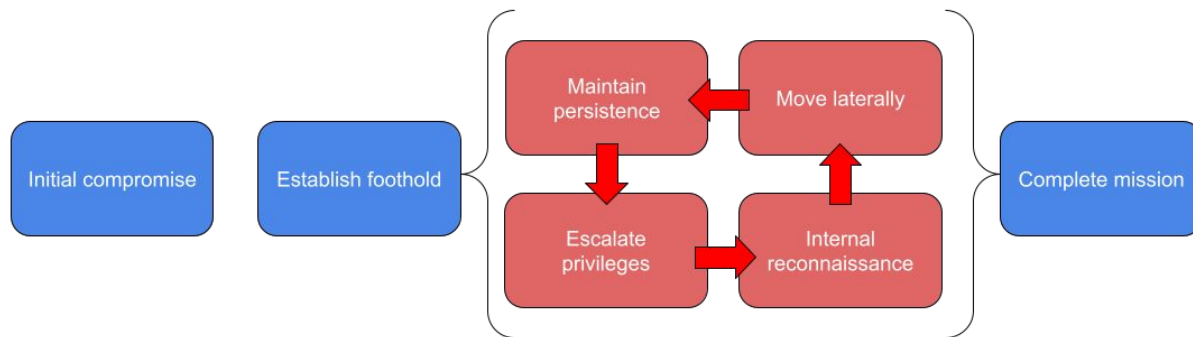
- Analyse scientifique dédiée à un travail d'investigation
- Concrètement:
 - Analyse de la mémoire RAM capturée sur des postes infectés
 - Analyse de fichiers journaux de pare-feux, VPN, utilisés par l'attaquant
 - Analyse de traces réseaux capturées par des outils de surveillance
 - Analyse de disque dur de machines utilisées par l'intrus comme rebond

Outils d'investigation

- Mémoire RAM
 - Capture: Surge
 - Analyse: Volatility
- Analyse de fichiers journaux
 - Capture: Surge (fichiers), dd (disque complet)
 - Analyse: evtx_dump, grep, less, Splunk
- Analyse de traces réseaux capturées par des outils de surveillance
 - Capture: Wireshark, sondes réseau
 - Analyse: Wireshark, tshark
- Analyse de disque dur de machines utilisées par l'intrus comme rebond
 - Capture: dd, FTK Imager
 - Analyse: The Sleuthkit, Autopsy, TestDisk, regrippy, ...

Tactiques, Techniques et Procédures

- L'intrus n'est pas là par hasard: il vient de quelque part, et il a un but
- **Idéalement:** définir les Tactiques, Techniques et Procédures (TTP) utilisées par l'attaquant
- Les définir permet ensuite de chercher ces indicateurs sur votre parc pour débusquer d'autres machines utilisées par l'attaquant



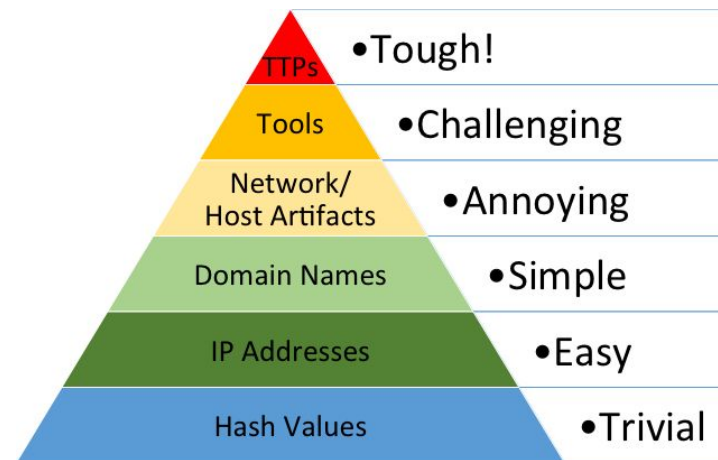
Advanced Persistent Threats (APT)

- Acteurs malveillants ayant accès à des ressources importantes
- **But:** espionnage industriel, vol de données, sabotage industriel
- Par opposition aux cybercriminels (but: argent rapide)

- Généralement des groupes opérés par des Etats
 - Les opérateurs sont salariés, c'est souvent leur travail
 - Organisés en plusieurs niveaux
 - Exemple: APT10 (Tianjin State Security Bureau ) , Equation Group (National Security Agency ) , Animal Farm (Direction Générale de la Sécurité Extérieure )

Indicateurs de compromission

- Marqueurs techniques indiquant la présence de l'attaquant sur un système
- Divers et variés
 - Domaine (DNS) contacté, par exemple un serveur de Commande & Contrôle (C2, C&C)
 - Adresse IP utilisée pour se connecter au SI
 - Condensat (hash) d'outils ou programmes malveillants utilisés
 - Nom d'une tâche planifiée ou d'un service utilisé pour la persistance
 - Etc.
- Identifier un IoC permet de trouver d'autres machines utilisées par l'attaquant (pivot)
 - *Exemple:* vous comprenez que l'attaquant lance ses commandes depuis `cmd.exe` copié sur un partage réseau
 - Vous pouvez effectuer une recherche listant tous les processus `cmd.exe` dont l'exécutable n'est pas dans C : ou D :
 - Super ! Vous identifiez une nouvelle machine contrôlée par l'attaquant



Analyse de malware

- Au cours d'un incident, il est courant de rencontrer des logiciels malveillants utilisés par les attaquants
- But de l'analyse: identifier rapidement le type de logiciel, son utilité, ses capacités
 - Recherche en sources ouvertes (VirusTotal, rapports publics)
 - Utilisation de sandboxes (Cuckoo, Any.Run, VMRay, etc.)
 - Analyse statique automatisée (YARA, Capa, strings)
 - Rétro-ingénierie statique (IDA, Ghidra, dnSpy, jadx, ...)

Une brève histoire du temps

- Le concept de *temps* est complexe
 - Fuseau horaire, heure d'été, calendriers différents
 - Il existe un point de référence: UTC, ou Coordinated Universal Time
 - Un horaire sans fuseau horaire n'a pas de sens
-
- Timestamp: nombre de secondes depuis une date donnée
 - Unix: 1er janvier 1970 (UTC, 00:00)
 - Windows: 1er janvier 1601 (UTC, 00:00)
 - ISO 8601: représentation d'un horaire au format textuel
 - 2023-01-26T11:49:25+00:00
 - "+00:00" peut aussi s'écrire Z

Les temps “MACB”

Lettre	Signification
M	Modification du contenu
A	Accès au fichier
C	Changement des méta-données
B	Création

MACB - le format “Body file”

MD5 | name | inode | mode_as_string | UID | GID | size | atime | mtime | ctime | btime



mactime

2020-01-01T00:05:08Z	84793	macb	0	0	128876	\\Program Files (x86)\\VERITAS\\VxPBX\\log\\50936-103-520130604-200101-0000000000.log
2020-01-01T06:43:49Z	0	macb	0	0	121542	\\Users\\XXX\\AppData\\Local\\Microsoft\\Windows\\[...]\\favicon10USZ6X1.png
	0	macb	0	0	140014	\\Users\\XXX\\AppData\\Local\\Microsoft\\Windows\\[...]\\faviconCUNVP46P.png
2020-01-01T06:44:08Z	574	mac.	0	0	116443	\\Users\\[...]\\Roaming\\Microsoft\\Windows\\Recent\\New Text Document.txt.lnk
(resident)						
2020-01-01T06:54:43Z	0	macb	0	0	128977	\\Users\\XXX\\AppData\\Local\\Microsoft\\Windows\\[...]\\favicon5DSZX0Y2.png
2020-01-01T17:11:19Z	0	macb	0	0	134198	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\devicefi.log.010120
	496	macb	0	0	138619	\\Program Files\\Common Files\\Symantec Shared\\[...]\\emccлариionfi.log.010120
(resident)						
	0	macb	0	0	141923	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\emcsymfi.log.010120
	1228	macb	0	0	141926	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\hitachifi.log.010120
	448	macb	0	0	141927	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\hpevafi.log.010120
(resident)						
	536	macb	0	0	141929	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\hpmsafi.log.010120
(resident)						
	476	macb	0	0	141931	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\ibmtsfi.log.010120
(resident)						
	0	macb	0	0	141932	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\ostfi.log.010120
	1354	macb	0	0	142066	\\Program Files\\Common Files\\Symantec Shared\\VxFI\\4\\logs\\vss.log.010120

Création de *timelines*

- Une partie importante de votre investigation est votre rapport d'investigation
- Bonne pratique: intégrer une *timeline* des actions importantes, côté *blue team* comme côté attaquant.
- Permet d'avoir une vue haut-niveau du déroulement de l'attaque et de l'investigation
- Précision des dates: dépend du niveau de précision de vos sources, ainsi que du niveau de granularité de l'action

Date	Action
2020-01-12	Exploitation of Netscaler in Limoges office
2020-01-14	Exploitation of CVE-2019-19781 and set up a basic webshell (<code>tiny.php</code>)
2020-01-18	First detection
2020-02-24	Netscaler patched and initial IM analysis
2020-04-22	TTPs shared during conference call
2020-05-26	Attacker harvests passwords by changing Netscaler login web page (<code>login.js</code>). Credentials were stored in a file named <code>netcaler.1</code> by a script called <code>netcaler.php</code> .
2020-06-10	Threat actor posts a topic on a well known underground forum - Raid forums
2020-06-13	Attacker improves their backdoor with chunkyTuna -- live interaction backdoor (filename: <code>debug.php</code>) and starts reconnaissance (nmap)
2020-06-13	Attacker performs first live demo
2020-06-13	We get notified of the forum post
2020-06-13	Investigation starts
2020-06-15	Attacker performs second live demo
2020-06-15	Network reconnaissance using publicly-available tools

Petit TP - utilisation de mactime

<https://tls-sec.skyblue.team/tp-forensics.html>

“Les temps MACB, et le Body file”

A problem has been detected and win
to your computer.

A process or thread crucial to sys
terminated.

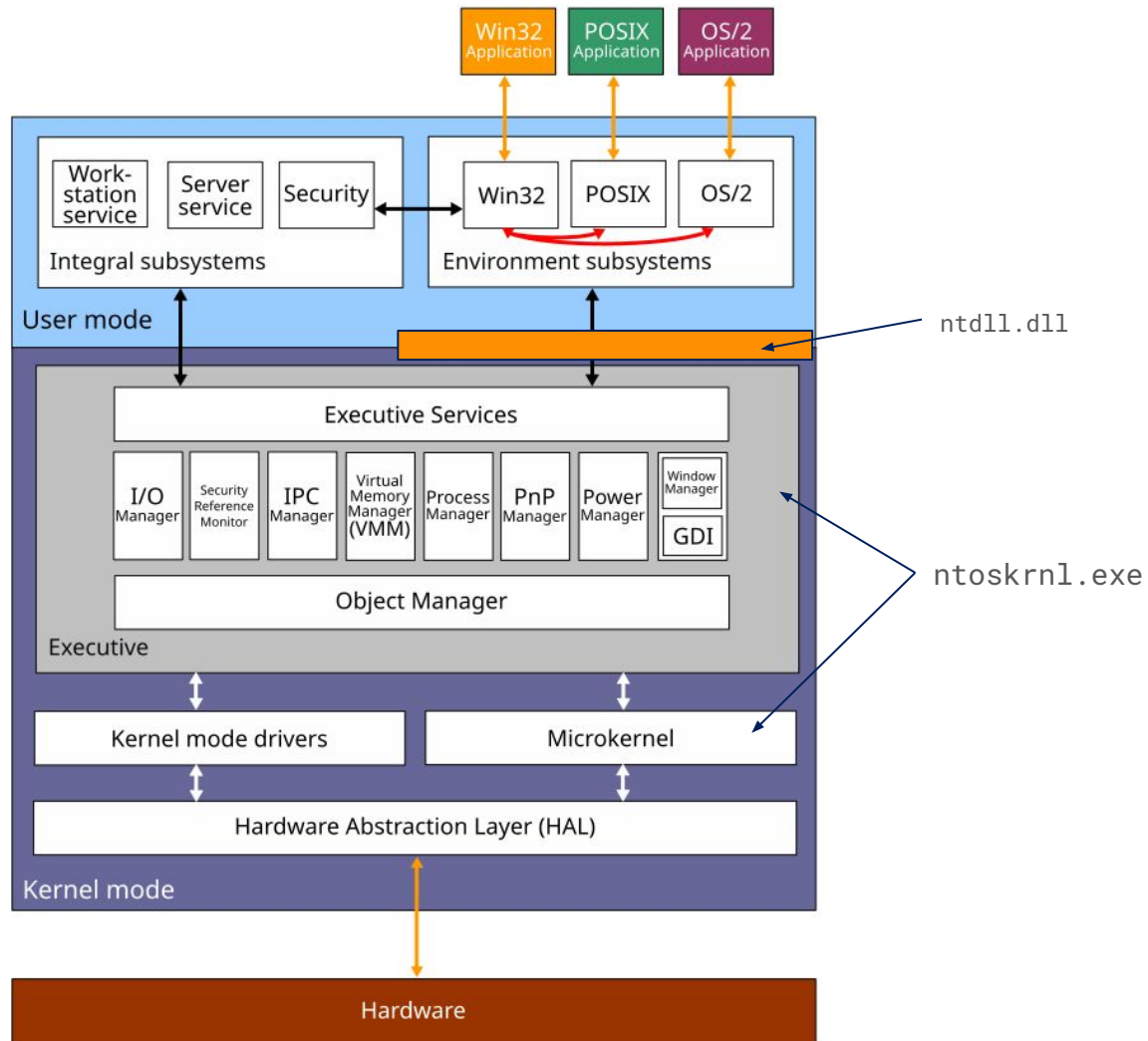
If this is the first time you've s
restart your computer. If this scr
these steps:

check to make sure any new hardwa
If this is a new installation, ask
for any windows updates you might

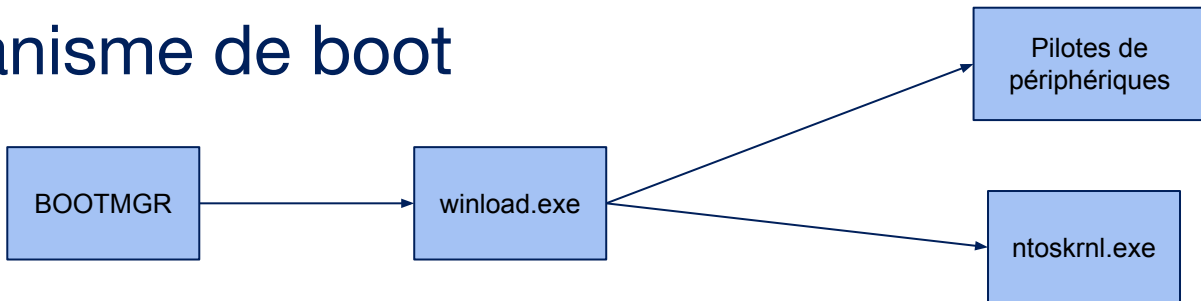
If problems continue, disable or
or software. Disable BIOS memory
If you need to use Safe Mode to r
your computer, press F8 to select
select Safe Mode.

ical information:
000000F4 (0x00000000
780)
dump

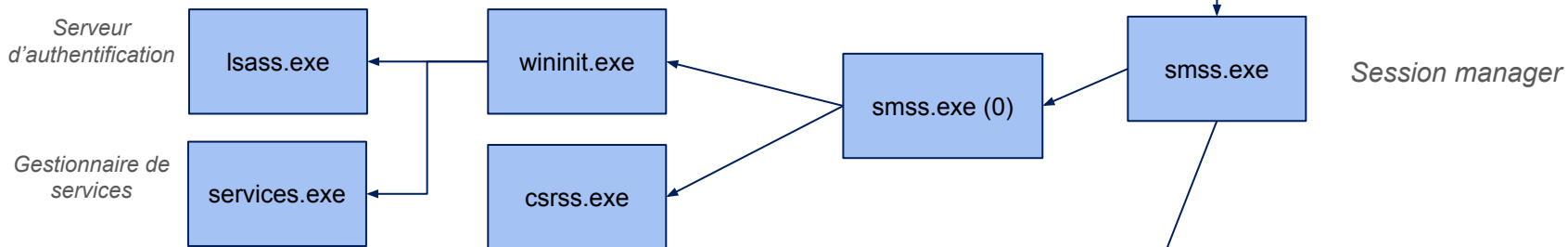
Fonctionnement du noyau NT



Mécanisme de boot

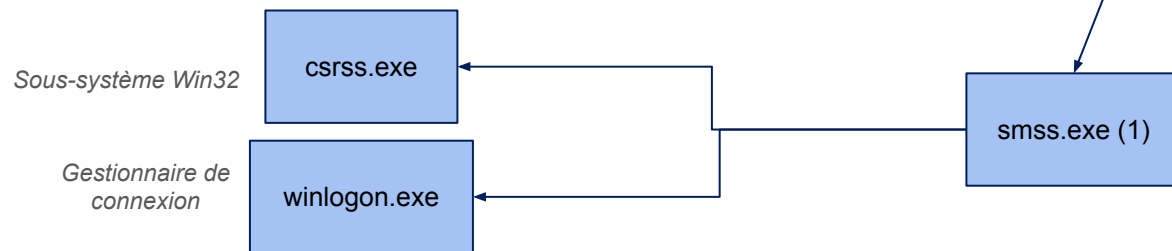


Kernel mode



Session 0

Session 1



Processus & threads

- Processus: 1 processus pour n threads ($n \geq 1$)
- Fonction kernel32!CreateProcess() -> ntdll!NtCreateUserProcess()
- Loader Windows:
 - Charge l'exécutable (.exe)
 - Le parse
 - Alloue les structures (PROCESS, THREAD, ...)
 - Alloue la mémoire, et copie le code (.text) en mémoire
 - Résout les imports (DLL), charge les bibliothèques si nécessaire
 - Positionne le EIP/RIP du processus au début du code

```
typedef struct _PROCESS_INFORMATION {  
    HANDLE hProcess;  
    HANDLE hThread;  
    DWORD  dwProcessId;  
    DWORD  dwThreadId;  
} PROCESS_INFORMATION, *PPROCESS_INFORMATION, *LPPROCESS_INFORMATION;
```

Processus: le cas des Prefetch



- C:\Windows\Prefetch
- Fichiers contenant des informations sur les programmes lancés récemment
 - Utilisé par Windows pour accélérer le lancement d'exécutables utilisés régulièrement
- Peut vous donner des informations sur les exécutables démarrés
- Prefetch
- Windows-Prefetch-Parser
- PECmd

Objets Windows

- Kernel Objects (non accessibles par les programmes en userspace)
 - Process
 - File
 - Mutex
 - Device
 - ...
- Executive Objects (encapsulent les objets kernel)
 - Accessibles en userspace à travers l'API: `CreateFile()`, `OpenProcess()`, ...
- User / GDI Objects (fenêtres, curseurs, bitmaps, etc.)

- Accès à un objet à travers un **HANDLE** (~fd sous Linux)



WinObj

Descripteurs de sécurité (associé à un objet)

- Identifiant du propriétaire (SID)
- Identifiant du groupe principal (SID)
- DACL: liste de droits
 - SID, Droits
 - SID, Droits
 - ...
- SACL: liste de droits qui doivent générer une alerte (audit)
 - SID, Droits
 - SID, Droits
 - ...

SID = Security Identifier

S-1-5-21-3623811015-3361044348-30300820-1013

Autorité ayant édité le SID

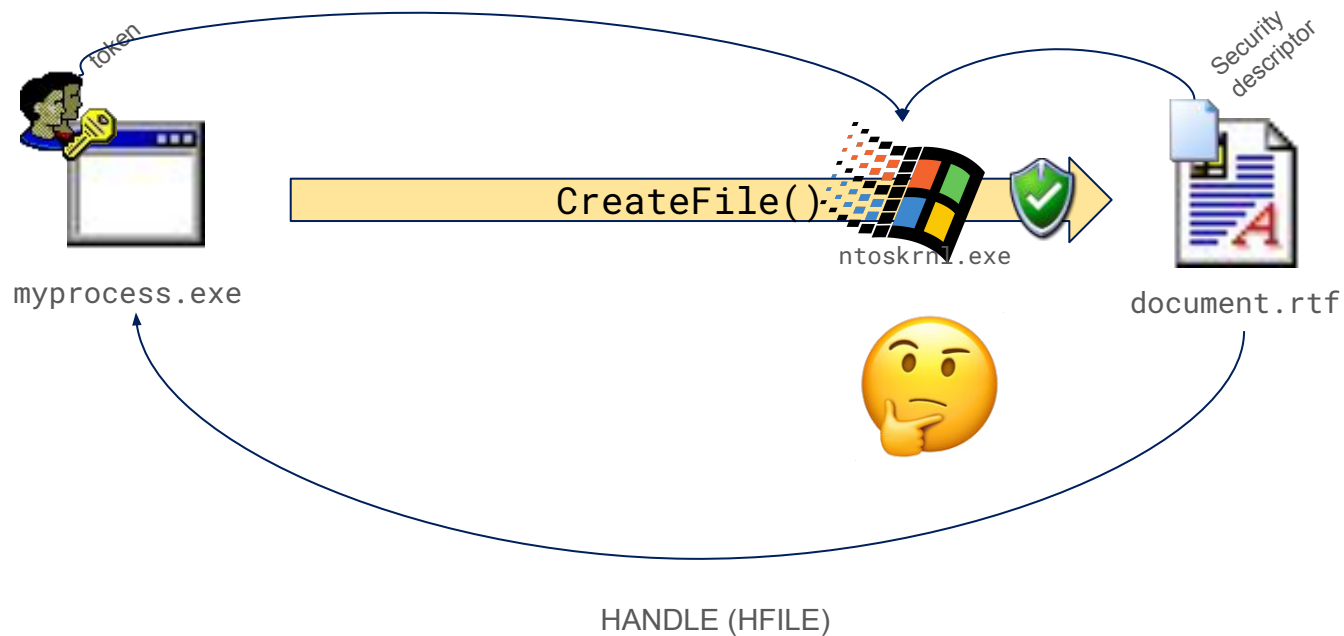
Sous-autorité, ou identifiant du domaine

Identifiant du compte

Jetons d'accès (token) (associé à un processus)

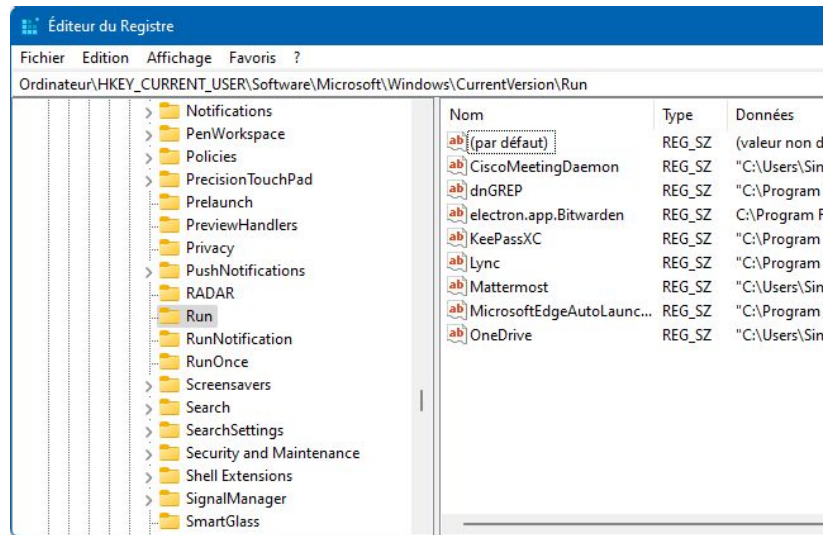
- Identifiant du jeton et de la session de connexion
- SID de l'utilisateur
- Privilèges du token
 - Permettent d'ignorer les DACL pour certains types d'objets
 - SeBackupPrivilege: lire tous les fichiers
 - SeDebugPrivilege: déboguer n'importe quel processus
 - SeTakeOwnership: prendre possession d'objets (fichiers par exemple)
- Les valeurs par défaut appliquées aux objets créés par le processus
 - SID de l'utilisateur propriétaire de l'objet
 - SID du groupe principal
 - DACL

Association du jeton et du descripteur de sécurité



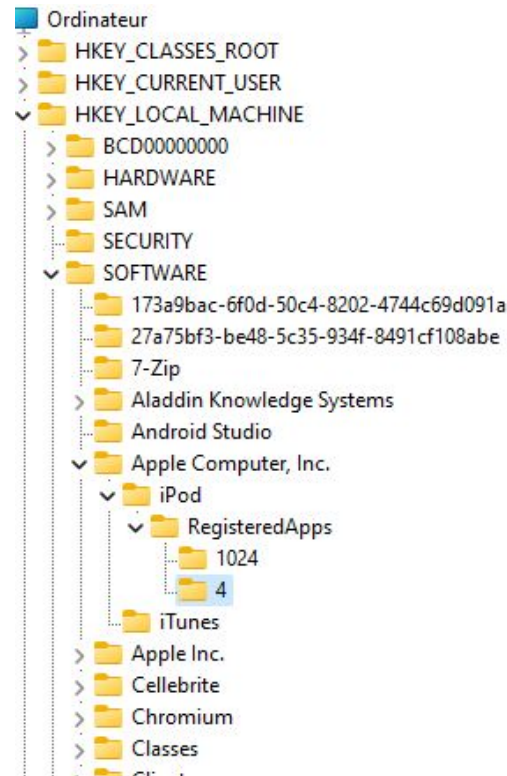
Le registre

- Arborescence similaire à un système de fichiers
 - Dossiers: “clés” (*key*)
 - ACL
 - Timestamp de modification
 - Fichiers: “valeurs” (*values*)
- Une valeur possède un *type* et des *données*
 - Type: REG_SZ, REG_BIN, REG_DWORD, ...
 - Données: dépend du type
- Utilisé pour stocker la configuration du système et des applications
- Depuis Windows 3.1, mais utilisé massivement depuis Windows 95



Le registre - clés de niveau 1

- HKEY_LOCAL_MACHINE (HKLM)
 - configuration de l'ordinateur et du système
 - ACL: Administrateur seulement
- HKEY_USERS (HKU)
 - configuration de chaque utilisateur
 - ACL: chaque utilisateur peut modifier son arborescence
- HKEY_CURRENT_USER (HKCU)
 - lien symbolique vers HKU\[SID utilisateur]
- HKEY_CLASSES_ROOT (HKCR)
 - liste d'associations de fichiers et de GUID pour les objets COM
 - Fusion de HKLM\Software\Classes et HKCU\Software\Classes



Le registre - ruches

- Les données du registre sont enregistrées sur le disque dans des fichiers
- Fichiers “bloqués” en lecture/écriture par ntoskrnl.exe: kernel32!LockFile()
- 1 fichier = 1 *ruche* (hive)
 - C:\Windows\System32\config\
 - **SYSTEM**: HKLM\SYSTEM
 - **SOFTWARE**: HKLM\SOFTWARE
 - **SECURITY**: HKLM\SECURITY
 - **SAM**: Comptes utilisateur locaux (HKLM\SECURITY\SAM)
 - C:\Users\[Utilisateur]\
 - **NTUSER.DAT**: HKCU
 - AppData\Local\Microsoft\Windows**UsrClass.dat**: HKCR

Le registre - persistance



- Liste de programmes se lançant à la connexion de l'utilisateur
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- Liste de programmes se lançant à la connexion de chaque utilisateur
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
 - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- Liste des services
 - HKLM\SYSTEM\CurrentControlSet\Services

Le registre - analyse



- Format des ruches: rétro-conçu
- Masse d'information: nécessité de filtrer ce qu'on cherche
 - Programmes au démarrage ?
 - Services ?
 - Historique de la boîte de dialogue "Exécuter" ?
- regripper
- regrippy
- regipy

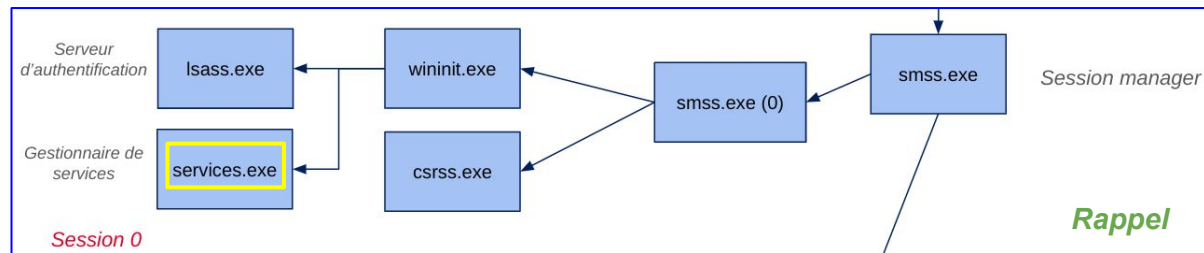
Petit TP - analyse de registre

<https://tls-sec.skyblue.team/tp-forensics.html>

“Extraction d'informations depuis des ruches de registre”

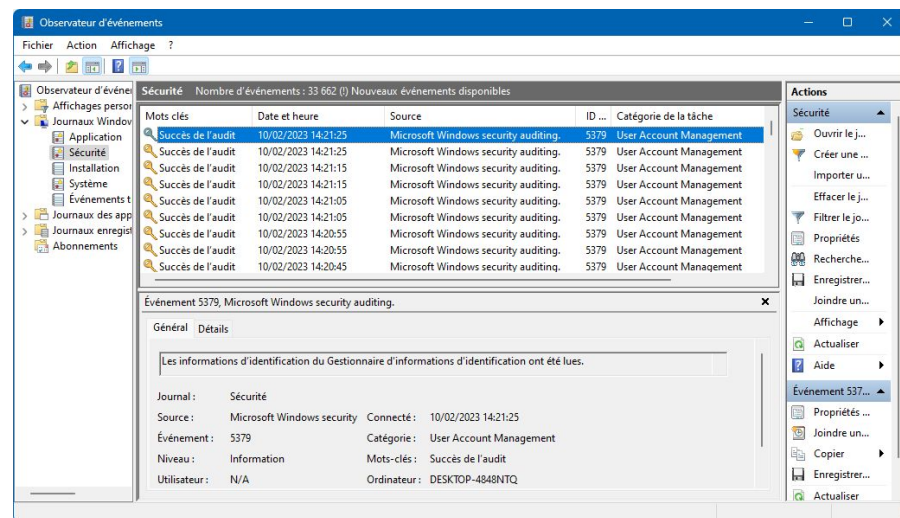
Services

- Processus “longue durée”, en arrière plan (~démons sous Linux)
- Service hosté = fichier DLL, chargé dans svchost . exe (*service host*)
 - 1 svchost par groupe de services (jusqu’à Windows 10)
 - 1 svchost par service (Windows 10+)
- Session 0: pas d’interaction avec la session utilisateur
- Tourne généralement avec un SID disposant de peu de privilèges (Network Service, Local Service)
- Géré à travers sc . exe



Journaux d'événements

- Contiennent des logs sur le fonctionnement du système (~journalctl sous Linux)
- C:\Windows\System32\winevt\log*.evtx
- Fichiers “bloqués” par le service EventLog
- Accès aux logs à travers l'API Win32
 - advapi32!ReportEvent()
 - advapi32!ReadEventLog()
 - advapi32!ClearEventLog()
- Possible de supprimer des lignes de log individuellement ?
 - Laissé en exercice au lecteur 😊



Journaux d'événement - analyse



- Format des EVT: documenté par Microsoft
 - La plupart sortent du XML: nécessité de post-traitement
-
- evtx_dump
 - evtxexport
 - evtx_dump.py

Journaux d'événements - Sysmon



- Sysinternals Sysmon - service non-officiel écrit par Mark Russinovich et Thomas Garnier
- Surveille et écrit dans le journal:
 - Création / fin de processus
 - Création de fichier
 - Connexions réseau
 - Résolutions DNS
 - Accès aux named pipes
 - Processus accédant à d'autres processus
 - Liste complète ici

Petit TP - analyse de journaux

<https://tls-sec.skyblue.team/tp-forensics.html>

“Les journaux d'événements Windows”

Le NT File System (NTFS)

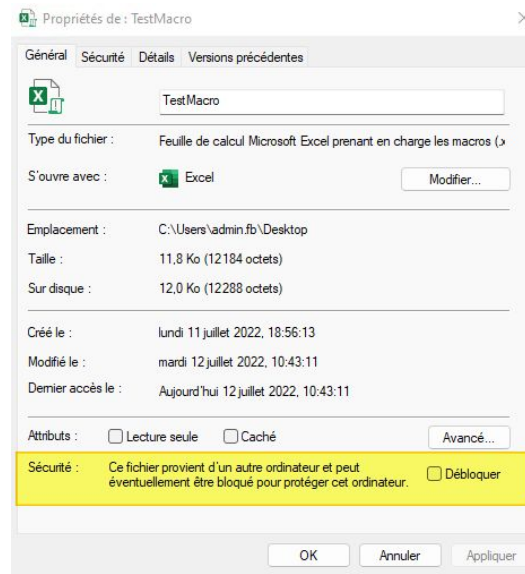
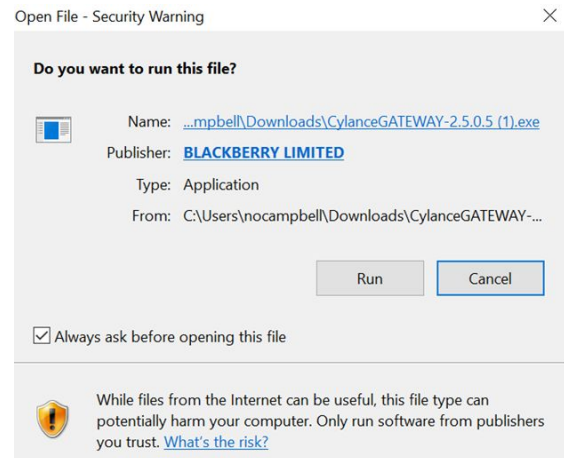
- Successeur de FAT16/FAT32
- Supporte les ACL (en cascade)
- Liens symboliques, liens durs (comme sous Linux)
- Volume Shadow Copies (VSS): snapshots
- Alternate Data Streams (ADS): plusieurs flux de données pour un même fichier
- Journalisation: réduit les risques de perte de données

NTFS - Master File Table (MFT)

- Base de données contenant une liste de tous les fichiers sur le disque
 - Nom
 - Parent
 - ACL
 - Dates en tout genre (dernier accès, dernière modification, création)
 - Pointeurs vers les blocs de données
- Chaque entrée = 1024 octets (1KiB)
 - Chaîne magique: "FILE0" (46 49 4c 45 30)

NTFS - Alternate Data Stream (ADS)

- Chaque fichier possède un flux de données (contenu) par défaut
- ADS: flux de données alternatif, nommé
 - Exemple: *?SummaryInformation, Zone.Identifier*
- Invisible dans l'Explorateur de fichiers, ou avec *dir*
- Représenté par le caractère deux-points (:)
 - Firefox-Installer-129.0.exe:**Zone.Identifier**
- “Suit” les fichiers quand ils sont déplacés, renommés, supprimés



NTFS - analyse



- Format de la MFT: documenté par Microsoft
 - Possibilité de sortir la liste des fichiers présents sur le disque, certains fichiers supprimés
 - Recherche dans les zones “non-utilisées”, récupération de structures écrasées par d'autres entrées
-
- MFTECmd
 - analyzeMFT
 - TestDisk

Conclusion

- Sous Linux, tout est fichier
- Sous Windows, tout est **objet**
- Toutes les interactions avec le système passent par l'API Win32
- Le format des fichiers stockant les informations est propriétaire
 - Format différent pour chaque fichier
 - Parfois documentés, parfois pas
 - Nécessité d'utiliser des logiciels tiers pour parser les fichiers

Mise en pratique

<https://tls-sec.skyblue.team/tp-forensics.html>

“Réponse à incident, analyse de machine compromise par un groupe APT”