



# AmCache Investigation

CoRI&IN 2019



# Intervenante

Blanche LAGNY

ANSSI, Investigation Numérique

[blanche.lagny@ssi.gouv.fr](mailto:blanche.lagny@ssi.gouv.fr)

## D'où vient l'AmCache ?

- > AmCache = Artefact d'exécution de binaires “shimés” et d'installation de programmes à partir de Windows 7 et Server 2008 R2
- > Application Experience and Compatibility
  - Solutions techniques permettant d'assurer la compatibilité des applications sur différents systèmes
- > Infrastructure de Shim (Infrastructure de Compatibilité d'Application) :
  - “The Shim Infrastructure implements a form of application programming interface (API) hooking. Specifically, it leverages the nature of linking to redirect API calls from Windows itself to alternative code—the shim itself.” - docs.microsoft.com

# Sait-on bien exploiter l'AmCache aujourd'hui ?

- > Outils existants pour parser...
  - AmCacheParser, plugin RegRipper
- > Mais artefact peu documenté et difficilement interprétable :
  - Vérification des affirmations
  - Analyse approfondie des mécanismes et résultats
- > Rapport technique pour disposer d'une référence
  - ➔ <https://www.ssi.gouv.fr/agence/publication/>



# Plan

- > Fonctionnement
- > Scénario 1 : « À la rencontre de l'AmCache »
- > Scénario 2 : « Blanche-Neige et le Chasseur »
- > Scénario 3 : « Y a-t-il un pilote dans l'avion ? »

## Fonctionnement : Disclaimer

- > Plusieurs modes de fonctionnement de l'AmCache
- > Dépend des versions de bibliothèques (ae\*.dll)
  - 1 version par mise à jour majeure d'OS
  - Backport jusqu'à Windows 7
- > Détails selon les versions de Windows avec les bibliothèques originelles

# Fonctionnement AmCache

- > Mise à jour de l'artefact en deux temps :
  - Exécution du PE
  - Exécution d'une tâche planifiée : Microsoft\Application Experience\ProgramDataUpdater

# Windows 7\* : Exécution PE

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:11:05,1179606	malware.exe	2752	Load Image	C:\Users\Lambda\bin\malware.exe	SUCCESS	
10:11:05,1180366	malware.exe	2752	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x400000, Image Size: 16384
10:11:05,1180934	malware.exe	2752	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x777b0000, Image Size: 16384
10:11:05,1182091	malware.exe	2752	CreateFile	C:\Windows\Prefetch\MALWARE.EXE-B39D57D4.pf	NAME NOT FOUND	Desired Access: Generic Read & Write
...						
10:11:05,1241263	svchost.exe	896	CreateFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	Desired Access: Read Attributes
10:11:05,1241500	svchost.exe	896	QueryBasicInformationFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	CreationTime: 14/07/2009 0
10:11:05,1241618	svchost.exe	896	CloseFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	
10:11:05,1242782	svchost.exe	896	CreateFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	Desired Access: Generic Read & Write
10:11:05,1243025	svchost.exe	896	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	AllocationSize: 16384, EndOfFile: 0
10:11:05,1243192	svchost.exe	896	CreateFileMapping	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	FILE LOCKED OR WAITING	SyncType: SyncTypeCreate
10:11:05,1243303	svchost.exe	896	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	AllocationSize: 16384, EndOfFile: 0
10:11:05,1243532	svchost.exe	896	CreateFileMapping	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	SyncType: SyncTypeOther
10:11:05,1245332	svchost.exe	896	CreateFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	Desired Access: Read Attributes
10:11:05,1245524	svchost.exe	896	QueryBasicInformationFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	CreationTime: 27/12/2018 1
10:11:05,1245632	svchost.exe	896	CloseFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	
10:11:05,1247445	svchost.exe	896	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	AllocationSize: 16384, EndOfFile: 0
10:11:05,1247564	svchost.exe	896	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	AllocationSize: 16384, EndOfFile: 0
10:11:05,1247697	svchost.exe	896	WriteFile	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	SUCCESS	Offset: 14248, Length: 4, Bytes Written: 4

\*version des DLLs : 6.1.7600



# Windows 7\*

- > Exécution du PE :
  - C:\Windows\AppCompat\Programs\RecentFileCache.bcf

\*version des DLLs : 6.1.7600

# Windows 7\* : Tâche planifiée

Planificateur de tâches

Fichier Action Affichage ?

Planificateur de tâches (Local)

- Bibliothèque du Planificateur de tâches
  - Microsoft
    - Windows
      - Active Directory Rights Manag...
      - AppID
      - Application Experience
      - Autochk
      - Bluetooth
      - CertificateServicesClient
      - Customer Experience Improver
      - Defrag
      - Diagnosis
      - DiskDiagnostic
      - Location
      - Maintenance
      - Media Center
      - MemoryDiagnostic
      - MobilePC
      - MUI
      - Multimedia

Nom	Statut	Déclencheurs	Prochaine exécution
AitAgent	En attente	À 02:30 tous les jours	08/01/2019 02:30:00
ProgramDataUpdater	En attente	À 00:30 tous les jours	08/01/2019 00:30:00

Général Déclencheurs Actions Conditions Paramètres Historique (désactivé)

Lorsque vous créez une tâche, vous devez spécifier l'action qui se produira au démarrage de la tâche. Pour modifier ces i Propriétés.

Action	Détails
Démarrer un programme	%windir%\system32\rundll32.exe aepdu.dll,AePduRunUpdate

\*version des DLLs : 6.1.7600

# Windows 7\* : Tâche planifiée

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:44:09,7622346	svchost.exe	896	CreateFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	SUCCESS	Desired Access: Read Contr
11:44:09,7622685	svchost.exe	896	QuerySecurityFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	BUFFER OVERF...	Information: Owner, Group, C
11:44:09,7622858	svchost.exe	896	CloseFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	SUCCESS	
11:44:09,7626478	svchost.exe	896	CreateFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	SUCCESS	Desired Access: Read Contr
11:44:09,7626708	svchost.exe	896	QuerySecurityFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	SUCCESS	Information: Owner, Group, C
11:44:09,7626838	svchost.exe	896	CloseFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramData Updater	SUCCESS	
11:44:09,7627571	svchost.exe	896	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum A
11:44:09,7627771	svchost.exe	896	RegQueryValue	HKLM	SUCCESS	Query: HandleTags, Handle
11:44:09,7627909	svchost.exe	896	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Application Experience...	SUCCESS	Desired Access: Read
11:44:09,7628151	svchost.exe	896	RegCloseKey	HKLM	SUCCESS	
11:44:09,7628313	svchost.exe	896	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Application Experience...	SUCCESS	Type: REG_SZ, Length: 78,
11:44:09,7628458	svchost.exe	896	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Application Experience...	SUCCESS	
...						
11:44:11,7067971	rundll32.exe	644	Load Image	C:\Windows\System32\rundll32.exe	SUCCESS	Image Base: 0xff690000, Im
11:44:11,7068358	rundll32.exe	644	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x777b0000, In
11:44:11,7069151	rundll32.exe	644	CreateFile	C:\Windows\Prefetch\RUNDLL32.EXE-411A328D.pf	SUCCESS	Desired Access: Generic Re
...						
11:44:11,7532699	rundll32.exe	644	CreateFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	Desired Access: Read Data,
11:44:11,7532836	rundll32.exe	644	SetBasicInformationFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	CreationTime: 01/01/1601 0
11:44:11,7532901	rundll32.exe	644	QueryAttributeTagFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	Attributes: A, ReparseTag: 0
11:44:11,7532957	rundll32.exe	644	QueryFileInternalInformation...	C:\Users\Lambda\bin\malware.exe	SUCCESS	IndexNumber: 0x100000000
11:44:11,7533016	rundll32.exe	644	CreateFileMapping	C:\Users\Lambda\bin\malware.exe	FILE LOCKED WI...	SyncType: SyncTypeCreate
11:44:11,7533067	rundll32.exe	644	QueryStandardInformationFile	C:\Users\Lambda\bin\malware.exe	SUCCESS	AllocationSize: 540 672, End
11:44:11,7533175	rundll32.exe	644	CreateFileMapping	C:\Users\Lambda\bin\malware.exe	SUCCESS	SyncType: SyncTypeOther
11:44:11,7533562	rundll32.exe	644	CreateFile	C:\Users\Lambda\bin\api-ms-win-core-console-l1-1-0.dll	SUCCESS	Desired Access: Read Data,
11:44:11,7533693	rundll32.exe	644	SetBasicInformationFile	C:\Users\Lambda\bin\api-ms-win-core-console-l1-1-0.dll	SUCCESS	CreationTime: 01/01/1601 0
11:44:11,7533757	rundll32.exe	644	QueryAttributeTagFile	C:\Users\Lambda\bin\api-ms-win-core-console-l1-1-0.dll	SUCCESS	Attributes: A, ReparseTag: 0
...						
11:44:15,4039736	rundll32.exe	644	CreateFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Desired Access: Generic Wr
11:44:15,4040536	rundll32.exe	644	WriteFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Offset: 0, Length: 5 460, Pric
11:44:15,4040987	rundll32.exe	644	WriteFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Offset: 5 460, Length: 4 549
11:44:15,4041284	rundll32.exe	644	WriteFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Offset: 10 009, Length: 4 26
11:44:15,4041537	rundll32.exe	644	WriteFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Offset: 14 270, Length: 4 15
11:44:15,4041783	rundll32.exe	644	WriteFile	C:\Windows\AppCompat\Programs\AEINV_WER_{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}_20181227_095424.xml	SUCCESS	Offset: 18 422, Length: 4 13

\*version des DLLs : 6.1.7600

# Windows 7\*

- > Exécution du PE :
  - C:\Windows\AppCompat\Programs\RecentFileCache.bcf
- > Tâche planifiée : ProgramDataUpdater (00h30 tous les jours)
  - Vide RecentFileCache.bcf
  - C:\Windows\AppCompat\Programs\AEINV\_WER\_{GUID}\_YYYYMMDD\_hhmm.xml

# Windows 8\* : Exécution PE

Time of Day	Process Name	PID	Operation	Path	Result	Detail
17:51:28,2721324	malware.exe	3164	Load Image	C:\Users\Lambda\malware.exe	SUCCESS	Image Base: 0x400000, Ima
17:51:28,2721435	malware.exe	3164	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7f3e590000
17:51:28,2721543	malware.exe	3164	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77540000, I
17:51:28,2722337	malware.exe	3164	CreateFile	C:\Windows\Prefetch\MALWARE.EXE-6C404B93.pf	NAME NOT FOUND	Desired Access: Generic Re
17:51:28,2724491	malware.exe	3164	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Ti
17:51:28,2726778	malware.exe	3164	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attrh
...						
17:51:28,2850436	svchost.exe	864	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	AllocationSize: 524 288, Enc
17:51:28,2850820	svchost.exe	864	CloseFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	
17:51:28,2850973	svchost.exe	864	RegLoadKey	\REGISTRY\A\{e46eaa25-cd2c-535a-3340-7e81eec04d3}	SUCCESS	Hive Path: C:\Windows\Apy
17:51:28,2851088	svchost.exe	864	CreateFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	Desired Access: None 0x0,
17:51:28,2851812	svchost.exe	864	FileSystemControl	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	Control: FSCTL_SET_COMF
17:51:28,2851956	svchost.exe	864	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	AllocationSize: 524 288, Enc
17:51:28,2852359	svchost.exe	864	CloseFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	
17:51:28,2854456	svchost.exe	864	CreateFile	C:\Windows\AppCompat\Programs\Amcache.hve	SHARING VIOLAT...	Desired Access: Read Data
17:51:28,2854714	svchost.exe	864	RegOpenKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}	SUCCESS	
17:51:28,2854813	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}	SUCCESS	
17:51:28,2855925	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}	SUCCESS	
17:51:28,2856845	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}	SUCCESS	Query: HandleTags, Handle
...						
17:51:28,2869032	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File	SUCCESS	Query: HandleTags, Handle
17:51:28,2869134	svchost.exe	864	RegOpenKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Desired Access: Read
17:51:28,2869299	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Query: HandleTags, Handle
17:51:28,2869368	svchost.exe	864	RegOpenKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37	NAME NOT FOUND	Desired Access: Read
17:51:28,2869509	svchost.exe	864	RegCloseKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	
17:51:28,2870020	svchost.exe	864	CreateFile	C:\Users\Lambda\malware.exe	SUCCESS	Desired Access: Generic Re
...						
17:51:28,2927272	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File	SUCCESS	Query: HandleTags, Handle
17:51:28,2927365	svchost.exe	864	RegCreateKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Desired Access: All Access,
17:51:28,2927461	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Query: HandleTags, Handle
17:51:28,2927530	svchost.exe	864	RegCreateKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37	SUCCESS	Desired Access: All Access,
17:51:28,2928308	svchost.exe	864	CreateFile	C:\Users\Lambda\malware.exe	SUCCESS	Desired Access: Read Attrb
17:51:28,2928428	svchost.exe	864	QueryNetworkOpenInformati...	C:\Users\Lambda\malware.exe	SUCCESS	Creation Time: 21/12/2018
17:51:28,2928497	svchost.exe	864	CloseFile	C:\Users\Lambda\malware.exe	SUCCESS	
17:51:28,2928684	svchost.exe	864	RegQueryValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\17	SUCCESS	Type: REG_QWORD, Leng
17:51:28,2928777	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\17	SUCCESS	Type: REG_QWORD, Leng
17:51:28,2928855	svchost.exe	864	RegCloseKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	
17:51:28,2928927	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\15	SUCCESS	Type: REG_SZ, Length: 56,
17:51:28,2928999	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\16	SUCCESS	Type: REG_DWORD, Leng
17:51:28,2929059	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\3	SUCCESS	Type: REG_DWORD, Leng
17:51:28,2929143	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\8	SUCCESS	Type: REG_SZ, Length: 90,
17:51:28,2929204	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DBB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\9	SUCCESS	Type: REG_QWORD, Leng

\*version des DLLs : 6.2.9200

# Windows 8\*

- > Exécution du PE :
  - C:\Windows\AppCompat\Programs\AmCache.hve



# Windows 8\* : Tâche planifiée

Process Monitor - Sysinternals: www.sysinternals.com						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
13:49:32.7749630	svchost.exe	812	CreateFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	SUCCESS	Desired Access: Read Contr
13:49:32.7749849	svchost.exe	812	QuerySecurityFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	BUFFER OVERF...	Information: Owner, Group, I
13:49:32.7749903	svchost.exe	812	CloseFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	SUCCESS	
13:49:32.7750717	svchost.exe	812	CreateFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	SUCCESS	Desired Access: Read Contr
13:49:32.7750828	svchost.exe	812	QuerySecurityFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	SUCCESS	Information: Owner, Group, I
13:49:32.7750871	svchost.exe	812	CloseFile	C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater	SUCCESS	
13:49:32.7751240	svchost.exe	812	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum A
...						
13:49:32.8006864	rundll32.exe	1884	Load Image	C:\Windows\System32\rundll32.exe	SUCCESS	Image Base: 0xe50000, Ima
13:49:32.8007009	rundll32.exe	1884	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77d20000, In
13:49:32.8007456	rundll32.exe	1884	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Query Valu
13:49:32.8007583	rundll32.exe	1884	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rundll32.exe	SUCCESS	Desired Access: Query Valu
...						
13:49:34.6089374	rundll32.exe	1884	QueryStandardInformationFile	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	AllocationSize: 57 344, EndC
13:49:34.6089404	rundll32.exe	1884	CreateFileMapping	C:\Windows\System32\Drivers\VBBoxDrv.sys	FILE LOCKED WI...	SyncType: SyncTypeCreate
13:49:34.6089419	rundll32.exe	1884	QueryStandardInformationFile	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	AllocationSize: 57 344, EndC
13:49:34.6089458	rundll32.exe	1884	CreateFileMapping	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	SyncType: SyncTypeOther
13:49:34.6089608	rundll32.exe	1884	QueryStandardInformationFile	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	AllocationSize: 57 344, EndC
13:49:34.6089710	rundll32.exe	1884	QueryStandardInformationFile	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	AllocationSize: 57 344, EndC
13:49:34.6089756	rundll32.exe	1884	CreateFileMapping	C:\Windows\System32\Drivers\VBBoxDrv.sys	FILE LOCKED WI...	SyncType: SyncTypeCreate
13:49:34.6089783	rundll32.exe	1884	QueryStandardInformationFile	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	AllocationSize: 57 344, EndC
13:49:34.6089849	rundll32.exe	1884	CreateFileMapping	C:\Windows\System32\Drivers\VBBoxDrv.sys	SUCCESS	SyncType: SyncTypeOther
...						
13:49:34.9118319	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{32781662-3DBD-4055-A94B-4CE805656B08}_20190102_131746.xml	SUCCESS	Offset: 5 460, Length: 4 549
13:49:34.9118568	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{32781662-3DBD-4055-A94B-4CE805656B08}_20190102_131746.xml	SUCCESS	Offset: 10 009, Length: 4 24
13:49:34.9118763	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{32781662-3DBD-4055-A94B-4CE805656B08}_20190102_131746.xml	SUCCESS	Offset: 14 255, Length: 4 14
13:49:34.9118968	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{32781662-3DBD-4055-A94B-4CE805656B08}_20190102_131746.xml	SUCCESS	Offset: 18 399, Length: 4 11
13:49:34.9119199	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{32781662-3DBD-4055-A94B-4CE805656B08}_20190102_131746.xml	SUCCESS	Offset: 22 510, Length: 4 10
...						
13:49:35.2375055	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	Offset: 265 028, Length: 660
13:49:35.2375100	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	Offset: 265 688, Length: 1 1
13:49:35.2375170	rundll32.exe	1884	WriteFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	Offset: 266 812, Length: 316
13:49:35.2375227	rundll32.exe	1884	CloseFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	
13:49:35.2377850	Explorer.EXE	544	NotifyChangeDirectory	C:\Windows\AppCompat\Programs\DevInvcache	SUCCESS	Filter: FILE_NOTIFY_CHAN
13:49:35.2379490	rundll32.exe	1884	CreateFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	Desired Access: Read Attri
13:49:35.2379761	rundll32.exe	1884	QueryAttributeTagFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	Attributes: AT, ReparseTag:
13:49:35.2379902	rundll32.exe	1884	QueryBasicInformationFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	CreationTime: 04/01/2019 1
13:49:35.2380617	rundll32.exe	1884	CreateFile	C:\Windows\AppCompat\Programs\DevInvcache	SUCCESS	Desired Access: Write Data
13:49:35.2381059	rundll32.exe	1884	SetRenameInformationFile	C:\Windows\AppCompat\Programs\DevInvcache\Pr9822.tmp	SUCCESS	ReplaceIfExists: True, FileN
13:49:35.2382702	Explorer.EXE	544	NotifyChangeDirectory	C:\Windows\AppCompat\Programs\DevInvcache	SUCCESS	Filter: FILE_NOTIFY_CHAN
13:49:35.2383279	Explorer.EXE	544	NotifyChangeDirectory	C:\Windows\AppCompat\Programs\DevInvcache	SUCCESS	Filter: FILE_NOTIFY_CHAN
13:49:35.2383787	rundll32.exe	1884	CloseFile	C:\Windows\AppCompat\Programs\DevInvcache	SUCCESS	
13:49:35.2384172	Explorer.EXE	544	NotifyChangeDirectory	C:\Windows\AppCompat\Programs	SUCCESS	Filter: FILE_NOTIFY_CHAN
13:49:35.2384463	rundll32.exe	1884	CloseFile	C:\Windows\AppCompat\Programs\DevInvcache\PropCache.bin	SUCCESS	

\*version des DLLs : 6.2.9200

## Windows 8\* : Tâche planifiée

- > Exécution du PE :
  - C:\Windows\AppCompat\Programs\AmCache.hve
- > Tâche planifiée : ProgramDataUpdater (~3:00 tous les 3 jours)
  - Met à jour AmCache.hve
  - C:\Windows\AppCompat\Programs\AEINV\_AMI\_WER\_{GUID}\_YYYYMMDD\_hhmm.xml
  - C:\Windows\AppCompat\Programs\DevInvCache\PropCache.bin  
(si PE = pilote)



# Windows 10\*

- > Exécution du PE :
  - C:\Windows\AppCompat\Programs\AmCache.hve
- > Tâche planifiée : ProgramDataUpdater (~3:00 tous les 3 jours)
  - Ne semble pas écrire ou mettre à jour de nouveaux fichiers

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier						
Chemin du fichier						
SHA-1						
Programme						
Suivi Répertoire installation						
Pilote						
Chemin du pilote						



# Plan

- > Fonctionnement
- > Scénario 1 : « À la rencontre de l'AmCache »
- > Scénario 2 : « Blanche-Neige et le Chasseur »
- > Scénario 3 : « Y a-t-il un pilote dans l'avion ? »

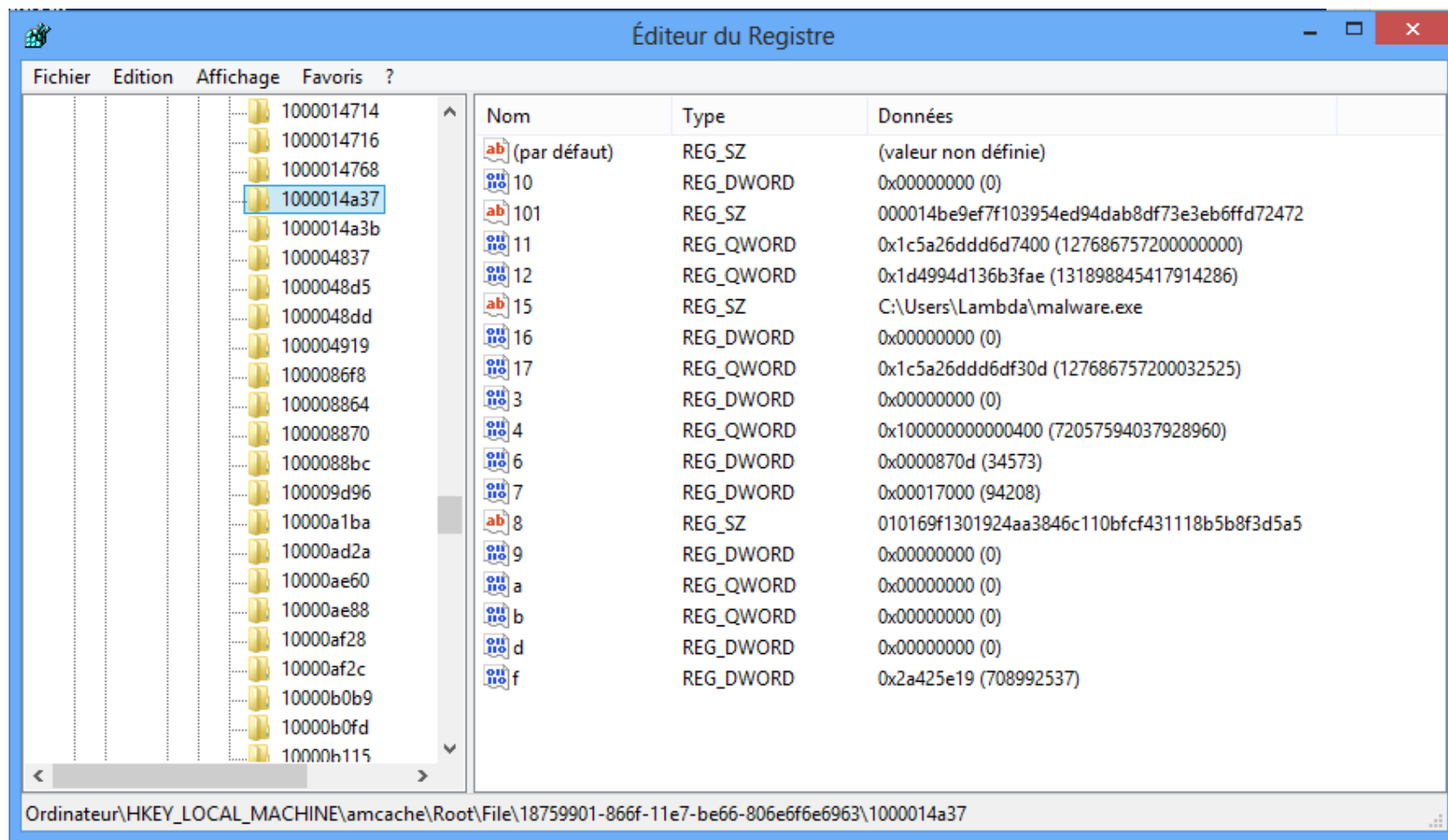
## À la rencontre de l'AmCache : Attaquant

- > L'attaquant compromet un compte utilisateur « Lambda » sur une machine Windows 8
- > L'attaquant se connecte sur le compte Lambda
- > L'attaquant exécute `C:\Users\Lambda\malware.exe`
- > L'attaquant supprime le fichier

## À la rencontre de l'AmCache : Analyste

- > Comportement suspect identifié sur une machine Windows 8
- > Plusieurs artefacts indiquent l'exécution de  
« C:\Users\Lambda\malware.exe »
- > Problème : malware.exe n'est plus sur le disque

# À la rencontre de l'AmCache : Analyste





## À la rencontre de l'AmCache : Ouverture

- > Analyse d'AmCache.hve : SHA-1 de malware.exe
- > Recherche en source ouverte
- > Ajout du hash dans les marqueurs

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier			X			X
Chemin du fichier			X			X
SHA-1			X			X
Programme						
Suivi Répertoire installation						
Pilote						
Chemin du pilote						



## À la rencontre de l'AmCache 2 : Windows 7

0000:3730	64 00 6F 00	77 00 73 00	5C 00 73 00	79 00 73 00	d.o.w.s.\.s.y.s.
0000:3740	74 00 65 00	6D 00 33 00	32 00 5C 00	77 00 65 00	t.e.m.3.2.\.w.e.
0000:3750	72 00 6D 00	67 00 72 00	2E 00 65 00	78 00 65 00	r.m.g.r...e.x.e.
0000:3760	00 00 20 00	00 00 63 00	3A 00 5C 00	77 00 69 00	.. .c.:.\.w.i.
0000:3770	6E 00 64 00	6F 00 77 00	73 00 5C 00	73 00 79 00	n.d.o.w.s.\.s.y.
0000:3780	73 00 74 00	65 00 6D 00	33 00 32 00	5C 00 76 00	s.t.e.m.3.2.\.v.
0000:3790	65 00 72 00	63 00 6C 00	73 00 69 00	64 00 2E 00	e.r.c.l.s.i.d...
0000:37A0	65 00 78 00	65 00 00 00	1F 00 00 00	63 00 3A 00	e.x.e.....c.:.
0000:37B0	5C 00 75 00	73 00 65 00	72 00 73 00	5C 00 6C 00	\.u.s.e.r.s.\.l.
0000:37C0	61 00 6D 00	62 00 64 00	61 00 5C 00	62 00 69 00	a.m.b.d.a.\.b.i.
0000:37D0	6E 00 5C 00	6D 00 61 00	6C 00 77 00	61 00 72 00	n.\.m.a.l.w.a.r.
0000:37E0	65 00 2E 00	65 00 78 00	65 00 00 00		e...e.x.e. .

RecentFileCache.bcf

# À la rencontre de l'AmCache 2 : Analyste

- > Limitations de RecentFileCache.bcf :
  - Uniquement le chemin du fichier
  - Contenu de RecentFileCache.bcf vidé tous les jours à 00h30 par Microsoft\Windows\Application Experience\ProgramDataUpdater
  - Tous les exécutables ne sont pas enregistrés dans RecentFileCache.bcf :
    - Exécutions depuis un média externe ou un partage réseau non enregistrées
    - Exceptions dans C:\Users (liste empiriques et non exhaustive) :
      - C:\Users\<username>\Downloads
      - C:\Users\<username>\Documents
      - Date de modification du binaire > 12h

# À la rencontre de l'AmCache 2 : Tâche planifiée

```
- <Report Version="1.3" TimeStamp="12/27/2018 09:54:27" SequenceNumber="1" ThrottlingRuleSetGuid="{F7D0E8C8-2DA8-4889-A910-3DE830B4148F}">
  <System MachineId="{D8E8BE6B-E0B2-4D29-802A-484BA7270D94}" MajorVersion="6" MinorVersion="1"
  ServicePackMajor="1" ServicePackMinor="0" BuildNumber="7601" Sku="4" ProcessorArchitecture="2"
  OSPlatform="2" LocaleId="1036" GeoId="84"/>
  <ProgramList>
    + <Installed></Installed>
    + <Orphan></Orphan>
  </ProgramList>
  <IEAddOnList InstanceVersion="8.0.7601.17514">
    + <Installed></Installed>
  </IEAddOnList>
  <Installations/>
</Report>
```

AEINV\_WER\_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}\_20181227\_142615.xml

# À la rencontre de l'AmCache 2 : Tâche planifiée

<**File Name**="malware.exe" **Id**="0000c686bc8fcbeec14be0993ce74db89fa864975970"  
**SwitchBackContext**="0x01000000000000501" **Size**="0x83200" **SizeOfImage**="0x87000"  
**PeHeaderHash**="01013246bfaf67ffa917fc960cbd8581ddb93a3f78b" **PeChecksum**="0x0"  
**LinkerVersion**="14.0" **LinkDate**="11/09/2018 15:57:03" **BinaryType**="32BIT" **Created**="12/27/2018  
09:09:15" **Modified**="11/09/2018 09:57:18"

AEINV\_WER\_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}\_20181227\_142615.xml

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier	X	X	X	X		X
Chemin du fichier	X		X			X
SHA-1		X	X	X		X
Programme						
Suivi Répertoire installation						
Pilote						
Chemin du pilote						



# Plan

- > Fonctionnement
- > Scénario 1 : « À la rencontre de l'AmCache »
- > **Scénario 2 : « Blanche-Neige et le Chasseur »**
- > Scénario 3 : « Y a-t-il un pilote dans l'avion ? »

## Blanche-Neige et le Chasseur : Attaquant

- > L'attaquant compromet un compte utilisateur « Lambda » sur une machine Windows 7
- > L'attaquant se connecte sur le compte Lambda
- > Il cache un logiciel malveillant « hidden-malware.exe » dans C:\Program Files\7-Zip\

## Blanche-Neige et le Chasseur : Analyste

- > Recherche de compromission sur un poste Windows 7
- > Pas de piste spécifique



# Blanche-Neige et le Chasseur : Analyste

```
- <Report Version="1.3" TimeStamp="12/27/2018 14:26:17" SequenceNumber="1" ThrottlingRuleSetGuid="{F7D0E8C8-2DA8-4889-A910-3DE830B4148F}">
  <System MachineId="{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}" MajorVersion="6" MinorVersion="1"
  ServicePackMajor="1" ServicePackMinor="0" BuildNumber="7601" Sku="4" ProcessorArchitecture="2"
  OSPlatform="2" LocaleId="1036" GeoId="84"/>
- <ProgramList>
  + <Installed></Installed>
  + <Orphan></Orphan>
  + <Updated></Updated>
</ProgramList>
+ <IEAddOnList InstanceVersion="8.0.7601.17514"></IEAddOnList>
  <Installations/>
</Report>
```

AEINV\_WER\_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}\_20181227\_142615.xml

## Aparté Fonctionnement

- > Dans l'AEINV, programme défini par des indicateurs :
  - RegistryIndicators ;
  - AddRemoveProgramIndicators ;
  - ShellIndicators ;
  - MsiIndicators ;
  - FileExtIndicators ;
  - DirectoryIndicators.
- > Modification d'un indicateur ➔ Entrée dans Updated

# Blanche-Neige et le Chasseur : Analyste

```
- <Updated>
- <Program Name="7-Zip 16.04 (x64)" Type="Application" Source="AddRemoveProgram" Publisher="Igor
  Pavlov" Version="16.04" OnSystemDrive="true" EvidenceId="0xa"
  Id="00000931f4d8fa1b9e536d7f9acd977cfba40000ffff">
- <Indicators>
- <AddRemoveProgramIndicators>
  <AddRemoveProgram DisplayName="7-Zip 16.04 (x64)" CompanyName="Igor Pavlov"
    ProductVersion="16.04" RegistrySubKey="7-Zip" UniqueId="0xa"
    Id="00004a5829309b3720eae59cf2ff4ca1a3722122f3bd"/>
  </AddRemoveProgramIndicators>
- <ShellIndicators>
  <Shell ShellName="7-Zip File Manager" TargetFileName="7zFM.exe" UniqueId="0xaa"
    Id="0000e65b909be1fb18415c27543f039977d2fbd8b95b"/>
  </ShellIndicators>
- <DirectoryIndicators>
  <Directory UniqueId="0xb" Id="00002a6048a1135a6b01c84bbf27f9e4f2bbc1779ea9"/>
  </DirectoryIndicators>
  </Indicators>
+ <StaticProperties></StaticProperties>
</Program>
</Updated>
```

AEINV\_WER\_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}\_20181227\_142615.xml

# Blanche-Neige et le Chasseur : Analyste

```
<File Name="hidden-malware.exe"  
Id="000014be9ef7f103954ed94dab8df73e3eb6ffd72472"  
ShortName="HIDDEN~1.EXE"  
SwitchBackContext="0x01000000000000400" Size="0x870d"  
SizeOfImage="0x17000"  
PeHeaderHash="010169f1301924aa3846c110bfcf431118b5b8f3d5a5"  
PeChecksum="0x0" LinkerVersion="2.25"  
LinkDate="06/19/1992 22:22:17" BinaryType="32BIT"  
Created="12/28/2018 12:41:20" Modified="08/16/2005 14:22:00"  
LongPathHash="0000add69fa4eb4d9c413eda8bab40408f1dc561a278"  
UniqueId="0x12"/>
```

AEINV\_WER\_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}\_20181227\_142615.xml

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier	X	X	X	X		X
Chemin du fichier	X		X	X		X
SHA-1		X	X	X		X
Programme		X	X	X		X
Suivi Répertoire installation		X				
Pilote						
Chemin du pilote						



# Plan

- > Fonctionnement
- > Scénario 1 : « À la rencontre de l'AmCache »
- > Scénario 2 : « Blanche-Neige et le Chasseur »
- > Scénario 3 : « Y a-t-il un pilote dans l'avion ? »

## Y a-t-il un pilote dans l'avion ? : Attaquant

- > L'attaquant compromet une machine Windows 10
- > Il charge un pilote légitime mais vulnérable « vboxdrv.sys » afin d'avoir une backdoor pour élever ses privilèges

## Y a-t-il un pilote dans l'avion ? : Analyste

- > Comportement suspect identifié sur une machine Windows 10
- > Remédiation immédiate effectuée par l'analyste
- > Est-ce que l'attaquant a laissé des backdoors ?



# Y a-t-il un pilote dans l'avion ? : Analyse

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\amcache\Root\InventoryDriverBinary\c:/windows/system32/drivers/vboxdrv.sys

Name	Type	Data
(Default)	REG_SZ	(value not set)
DriverChecksum	REG_DWORD	0x000189e5 (100837)
DriverCompany	REG_SZ	Missing
DriverId	REG_SZ	0000b7fa8278ab7bc485727d075e761a72042c4595f7
DriverInBox	REG_SZ	0
DriverIsKernelMode	REG_SZ	1
DriverLastWriteTime	REG_SZ	05/31/2008 09:42:46
DriverName	REG_SZ	vboxdrv.sys
DriverPackageStrongName	REG_SZ	
DriverSigned	REG_SZ	1
DriverTimeStamp	REG_DWORD	0x48408f1c (1212190492)
DriverType	REG_DWORD	0x0081008a (8454282)
DriverVersion	REG_SZ	Missing
ImageSize	REG_DWORD	0x0000bd20 (48416)
Inf	REG_SZ	
Product	REG_SZ	Missing
ProductVersion	REG_SZ	Missing
Service	REG_SZ	vboxdrv
WdfVersion	REG_SZ	

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier	X	X	X	X		X
Chemin du fichier	X		X	X		X
SHA-1		X	X	X		X
Programme		X	X	X		X
Suivi Répertoire installation		X				
Pilote						X
Chemin du pilote						X

## Y a-t-il un pilote dans l'avion ? 2 : Windows 8

- > AmCache.hve ne contient pas les pilotes
- > Tâche planifiée ProgramDataUpdater existe toujours...

# Y a-t-il un pilote dans l'avion ? 2 : Analyste

```
- <Report Version="1.12" ClientVersion="1.12.0" TimeStamp="01/02/2019 13:17:50" SequenceNumber="1" ThrottlingRuleSetGuid="{F7D0E8C8-2DA8-4889-A910-3DE830B4148F}">
  <System MachineId="{32781662-3DBD-4055-A94B-4CE805656B08}" MajorVersion="6" MinorVersion="2" ServicePackMajor="0"
    ServicePackMinor="0" BuildNumber="9200" Sku="48" ProcessorArchitecture="1" OSPlatform="1" LocaleId="1036" GeoId="84"
    VirtualMachine="false" PortableWorkSpace="false"> </System>
+ <ProgramList></ProgramList>
+ <IEAddOnList InstanceVersion="9.10.9200.16384"></IEAddOnList>
+ <InstallerList></InstallerList>
+ <DeviceList></DeviceList>
+ <DriverList></DriverList>
  <DriverPackageList> </DriverPackageList>
  <AitAnalysis> </AitAnalysis>
</Report>
```

AEIN\_AMI\_WER[...].xml

## Y a-t-il un pilote dans l'avion ? 2 : Analyste

```
<Driver DriverId="0000b7fa8278ab7bc485727d075e761a72042c4595f7"  
Name="vboxdrv.sys" Type="0x0001008a" Version="Missing"  
TimeStamp="0x48408f1c" CheckSum="0x000189e5"  
ImageSize="0x0000bd20" PagedSize="0x00001060"  
Company="Missing" Product="Missing" ProductVersion="Missing">  
</Driver>
```

AEIN\_AMI\_WER[...].xml

## Y a-t-il un pilote dans l'avion ? 2 : Analyste

0003:4950	00 00 00 00	00 00 18 00	00 00 76 00	62 00 6F 00	.....v.b.o.
0003:4960	78 00 64 00	72 00 76 00	2E 00 73 00	79 00 73 00	x.d.r.v...s.y.s.
0003:4970	00 00 01 00	00 00 01 00	00 00 5A 00	00 00 30 00	.....Z...0.
0003:4980	30 00 30 00	30 00 62 00	37 00 66 00	61 00 38 00	0.0.0.b.7.f.a.8.
0003:4990	32 00 37 00	38 00 61 00	62 00 37 00	62 00 63 00	2.7.8.a.b.7.b.c.
0003:49A0	34 00 38 00	35 00 37 00	32 00 37 00	64 00 30 00	4.8.5.7.2.7.d.0.
0003:49B0	37 00 35 00	65 00 37 00	36 00 31 00	61 00 37 00	7.5.e.7.6.1.a.7.
0003:49C0	32 00 30 00	34 00 32 00	63 00 34 00	35 00 39 00	2.0.4.2.c.4.5.9.
0003:49D0	35 00 66 00	37 00 00 00	01 00 00 00	03 00 00 00	5.f.7. ....
0003:49E0	10 00 00 00	4D 00 69 00	73 00 73 00	69 00 6E 00	...M.i.s.s.i.n.
0003:49F0	67 00 00 00	01 00 00 00	04 00 00 00	10 00 00 00	g.....
0003:4A00	4D 00 69 00	73 00 73 00	69 00 6E 00	67 00 00 00	M.i.s.s.i.n.g...
0003:4A10	01 00 00 00	05 00 00 00	10 00 00 00	4D 00 69 00	.....M.i.
0003:4A20	73 00 73 00	69 00 6E 00	67 00 00 00	01 00 00 00	s.s.i.n.g.....
0003:4A30	06 00 00 00	10 00 00 00	4D 00 69 00	73 00 73 00	.....M.i.s.s.
0003:4A40	69 00 6E 00	67 00 00 00	00 00 00 00	09 00 00 00	i.n.g.....

PropCache.bin

## Résumé traces trouvées par OS (version DLL)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Windows 10 (10.0.14913)
	RecentFile Cache.bcf	AEINV_WER .xml	AmCache .hve	AEINV_AMI .xml	PropCache .bin	AmCache .hve
Nom du fichier	X	X	X	X		X
Chemin du fichier	X		X	X		X
SHA-1		X	X	X		X
Programme		X	X	X		X
Suivi Répertoire installation		X				
Pilote				X	X	X
Chemin du pilote					X	X

# Conclusion

- > Artefact complexe :
  - Attention à la version des DLLs et pas de l'OS !
  - Penser à récupérer tous les fichiers !
- > Attention aux conclusions tirées :
  - Sur l'exécution du PE,
  - Sur la date d'exécution,
  - Sur l'absence d'un PE dans l'artefact.
- > Mais artefact précieux dans une investigation
- > Rapport technique de référence pour aider l'analyste :
  - ➔ <https://www.ssi.gouv.fr/agence/publication/>





# Questions ?

# Date d'exécution ? – Exemple sous Windows 8

- > Si le PE fait partie d'un programme :
  - Si le PE a besoin d'être shimé et a été exécuté avant ProgramDataUpdater
    - ➔ Date de dernière écriture semble être la date d'exécution du PE
  - Sinon si ProgramDataUpdater a été lancée depuis l'installation du programme
    - ➔ Date de dernière écriture semble être la date de lancement de ProgramDataUpdater
  - Sinon
    - ➔ Date de dernière écriture semble être la date d'installation du programme
- > Sinon, si le PE est "l'installateur" d'un programme :
  - Si ProgramDataUpdater a été lancée depuis l'installation du programme
    - ➔ Date de dernière écriture semble être la date de lancement de ProgramDataUpdater
  - Sinon
    - ➔ Date de dernière écriture semble être la date d'exécution du PE
- > Sinon :
  - Si le PE est "interne"
    - ➔ Date de dernière écriture semble être la date d'exécution du PE
  - Sinon, si ProgramDataUpdater a été lancée depuis l'exécution du PE
    - ➔ Date de dernière écriture semble être la date de lancement de ProgramDataUpdater
  - Sinon
    - ➔ Date de dernière écriture semble être la date d'exécution du PE