AmCache Investigation

#DFIRSummit US - 2019

Speaker

Blanche LAGNY
Digital Forensic Investigator
ANSSI, CERT-FR
blanche.lagny@ssi.gouv.fr

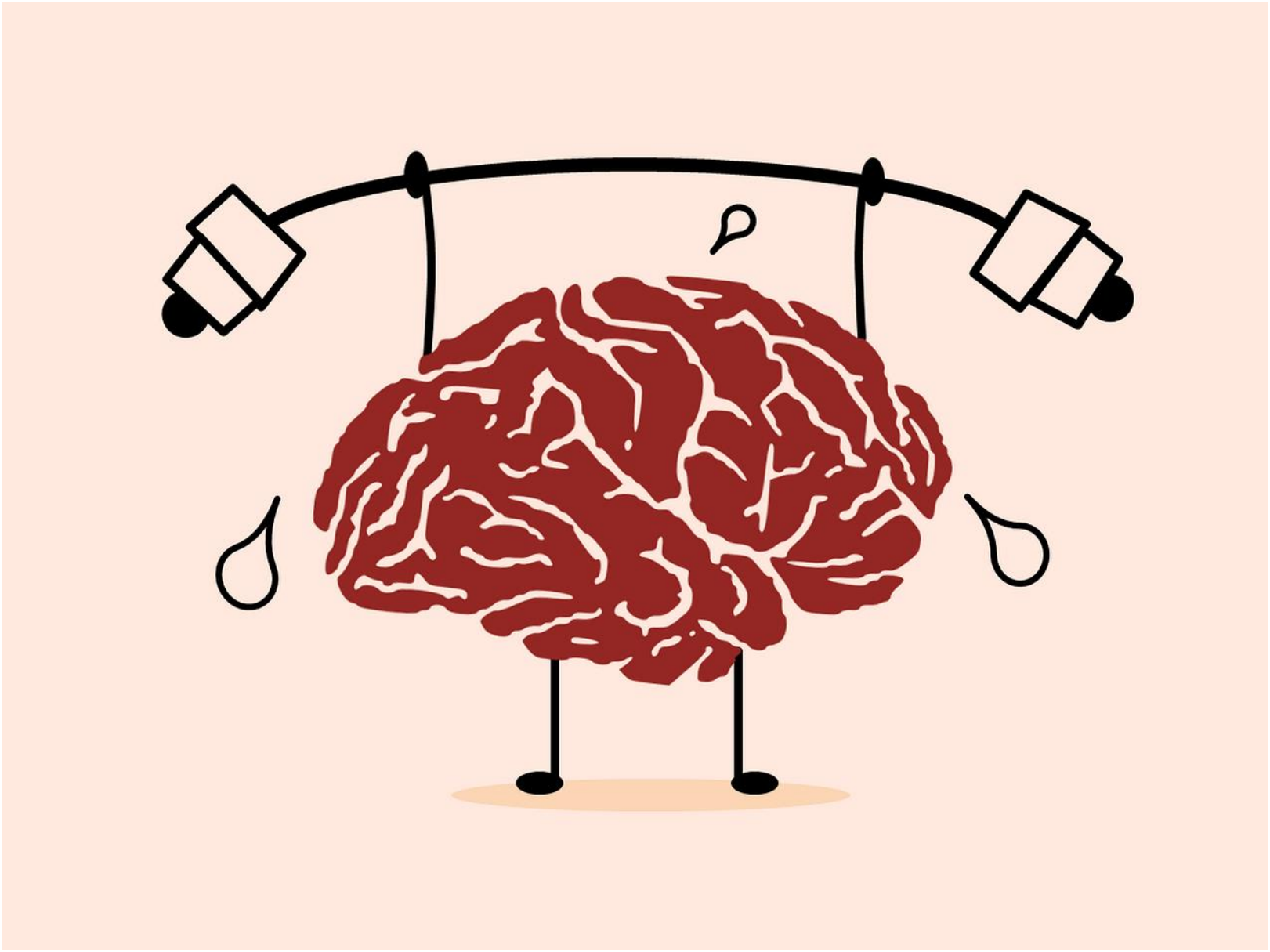
AmWhaaat?

- Stores metadata related to executed shimmed PE since Windows 7 and Server 2008 R2
- Existing tools to parse it: AmCacheParser, RegRipper plugin
- Lack of documentation and interpretation is not as easy as it seems
- Technical report to have a reference of the inner workings of this artifact

➔ https://www.ssi.gouv.fr/en/publication/amcache-analysis/

Plan

- Inner workings
- Scenario 1: « Welcome to the Hellmouth »
- Scenario 2: « Same Time, Same Place »
- Scenario 3: « The Killer in Me »



Inner workings: Disclaimer

- The AmCache behaves differently depending on the libraries version (ae*.dll)
  - 1 version by major release of Windows
  - Backport until Windows 7
- Details according to the libraries version of the original OS version

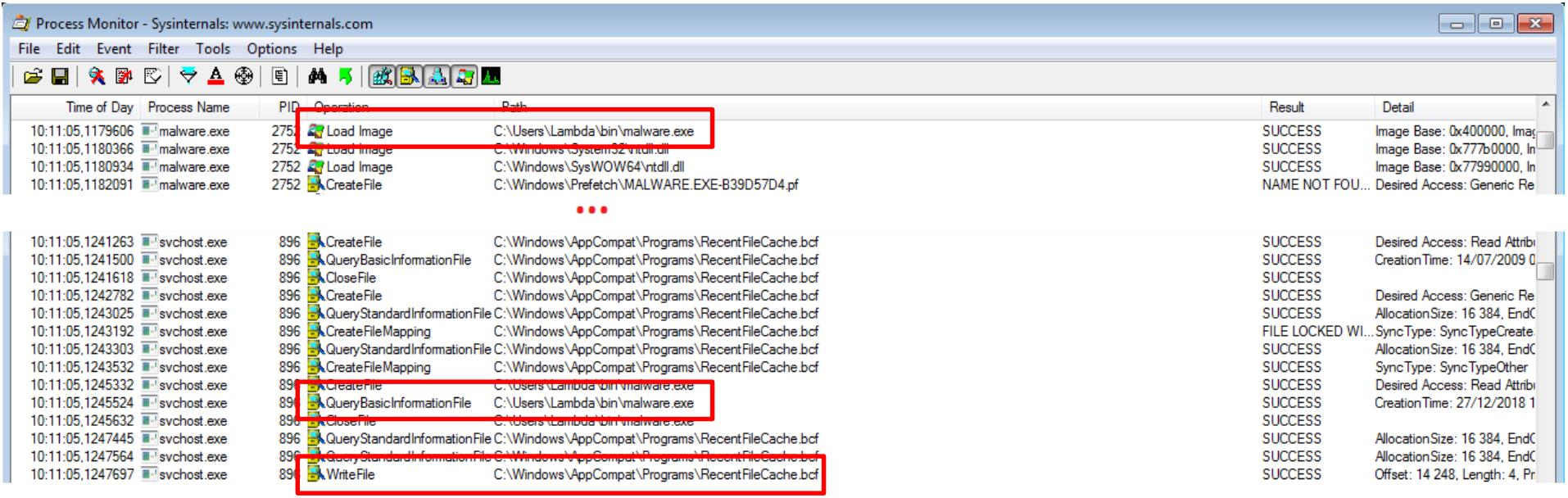
Inner workings of the AmCache

- Artifact is updated in 2 phases :
  - PE execution
  - Scheduled tasks :
    - Microsoft\Application Experience\ProgramDataUpdater
    - Microsoft\Application Experience\Microsoft Compatibility Appraiser (since Windows 8.1 (6.3.9600.17415))

Windows 7

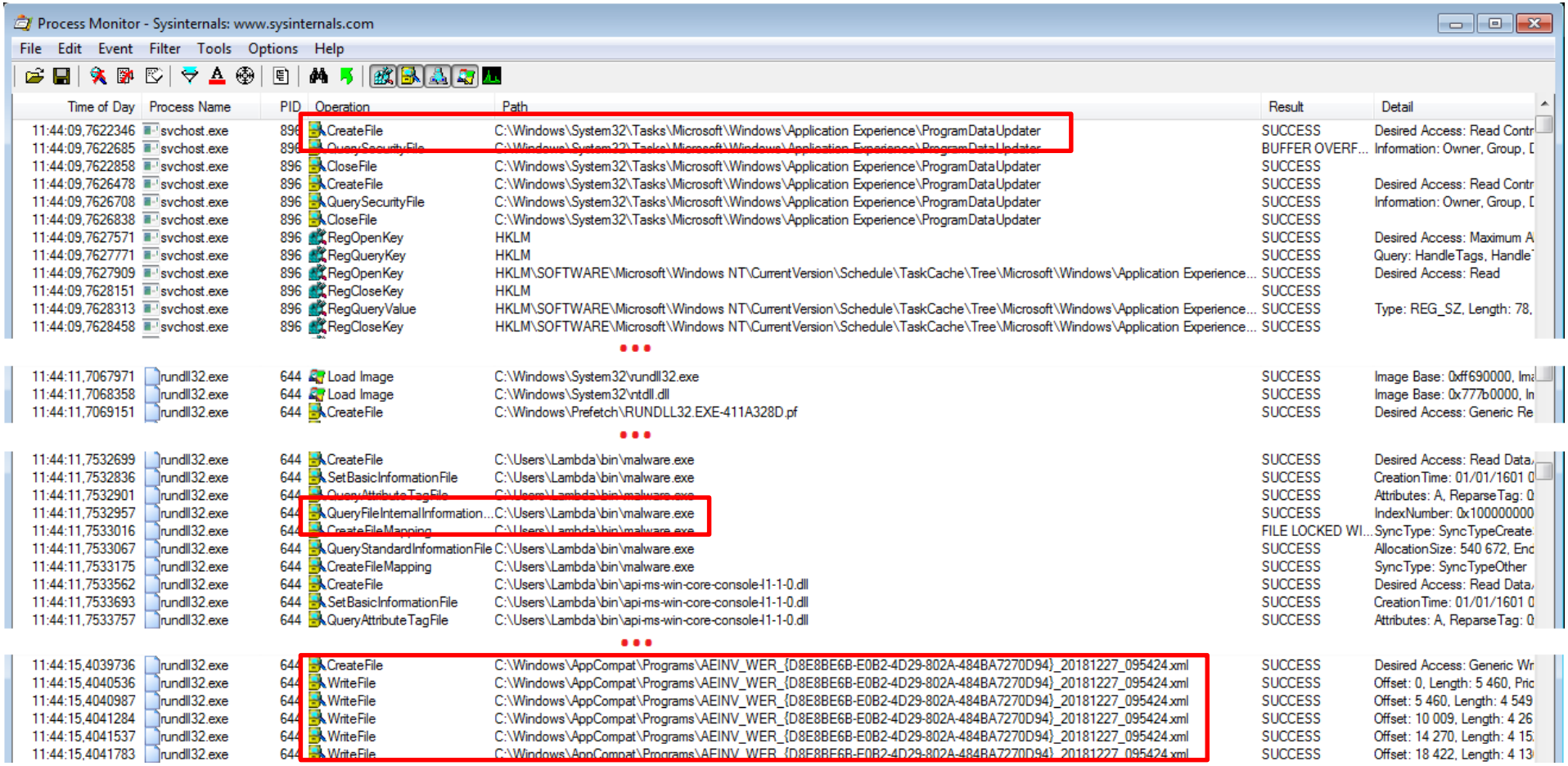
- DLL version: 6.1.7600

Windows 7*: PE execution



*DLL version: 6.1.7600

Windows 7*: Scheduled Task



*DLL version: 6.1.7600

Windows 7*

- PE execution:
  - C:\Windows\AppCompat\Programs\RecentFileCache.bcf
- Scheduled task : ProgramDataUpdater (00:30 every day)
  - Empties RecentFileCache.bcf
  - C:\Windows\AppCompat\Programs\AEINV_WER_{GUID}_YYYYMMDD_hhmm.xml

*DLL version: 6.1.7600

Windows 8

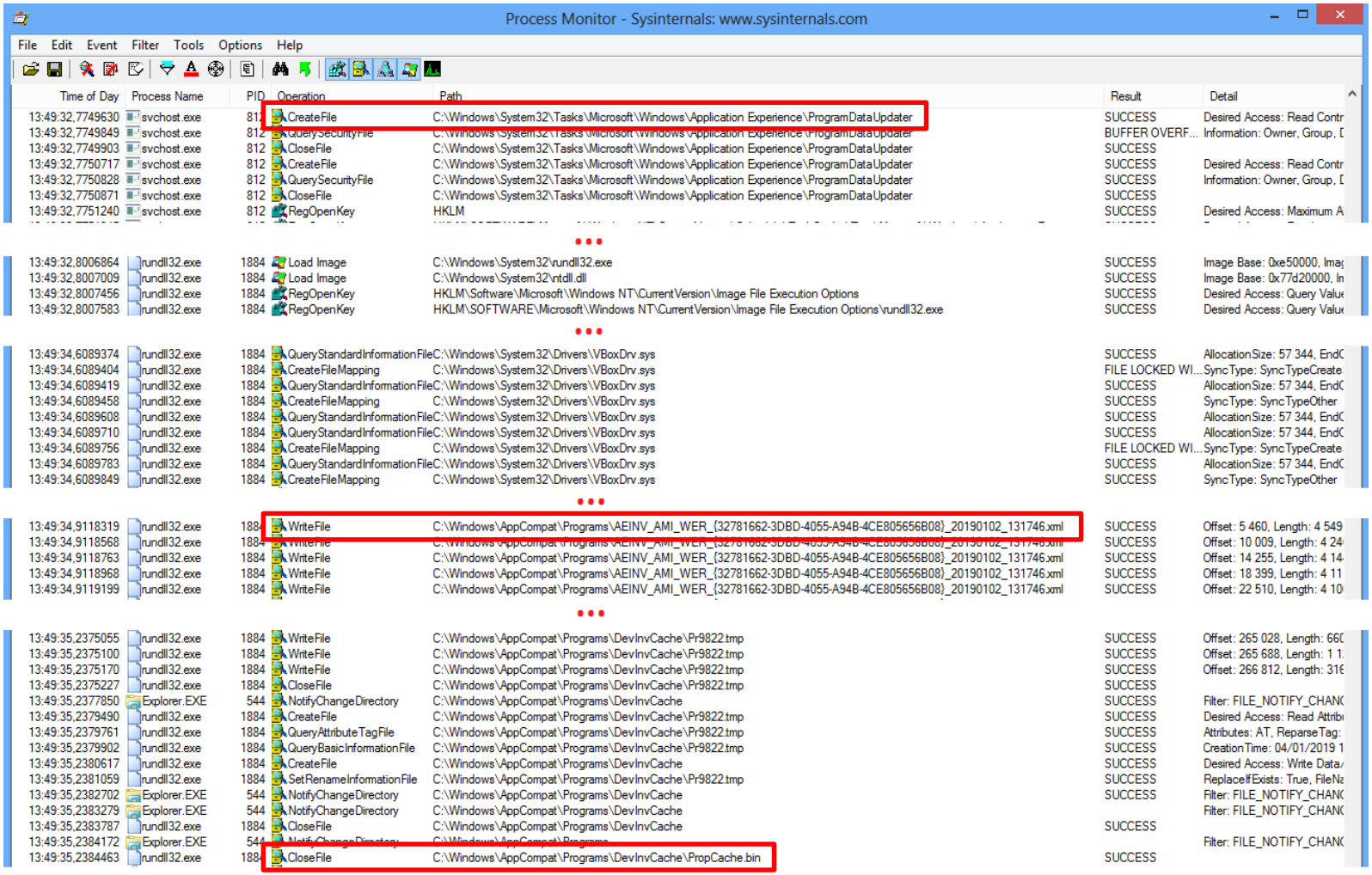
- DLL version: 6.2.9200

Windows 8*: PE execution

Time of Day	Process Name	PID	Operation	Path	Result	Detail
17:51:28,2721324	malware.exe	316	Load Image	C:\Users\Lambda\malware.exe	SUCCESS	Image Base: 0x400000, Ima
17:51:28,2721435	malware.exe	316	[illegible]	[illegible]	SUCCESS	Image Base: 0x7ff3e590000
17:51:28,2721543	malware.exe	3164	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77540000, Ir
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/Tı
17:51:28,2726778	malware.exe	3164	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attrib
...						
17:51:28,2850436	svchost.exe	864	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	AllocationSize: 524 288, En
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-3340-7fe81eec04d3}	SUCCESS	Hive Path: C:\Windows\Apı
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_COMI
17:51:28,2851956	svchost.exe	864	QueryStandardInformationFile	C:\Windows\AppCompat\Programs\Amcache.hve	SUCCESS	AllocationSize: 524 288, En
17:51:28,2852359	svchost.exe	864	[illegible]	[illegible]	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-DDB814F60820}	SUCCESS	
17:51:28,2854813	svchost.exe	864	[illegible]	[illegible]	SUCCESS	
17:51:28,2855925	svchost.exe	864	RegQueryKeySecurity	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}	SUCCESS	
17:51:28,2856845	svchost.exe	864	RegQueryKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}	SUCCESS	Query: HandleTags, Handle
...						
17:51:28,2869032	svchost.exe	864	RegQueryKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\Root\File	SUCCESS	Query: HandleTags, Handle
17:51:28,2869134	svchost.exe	864	RegOpenKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Desired Access: Read
17:51:28,2869299	svchost.exe	864	RegQueryKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\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-DDB814F60820}\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-DDB814F60820}\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	RegQueryKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\Root\File	SUCCESS	Query: HandleTags, Handle
17:51:28,2927365	svchost.exe	864	RegCreateKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	Desired Access: All Access,
17:51:28,2927461	svchost.exe	864	[illegible]	[illegible]	SUCCESS	Query: HandleTags, Handle
17:51:28,2927530	svchost.exe	864	RegCreateKey	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\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 Attrib
17:51:28,2928428	svchost.exe	864	QueryNetworkOpenInformati...	C:\Users\Lambda\malware.exe	SUCCESS	CreationTime: 21/12/2018 1
17:51:28,2928497	svchost.exe	864	CloseFile	C:\Users\Lambda\malware.exe	SUCCESS	
17:51:28,2928684	svchost.exe	864	[illegible]	[illegible]	SUCCESS	Type: REG_QWORD, Leng
17:51:28,2928777	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\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-DDB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963	SUCCESS	
17:51:28,2928927	svchost.exe	864	RegSetValue	\REGISTRY\A\{77A84288-FD92-1FE9-4ABE-DDB814F60820}\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-DDB814F60820}\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-DDB814F60820}\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-DDB814F60820}\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-DDB814F60820}\Root\File\18759901-866f-11e7-be66-806e6f6e6963\1000014a37\a	SUCCESS	Type: REG_QWORD, Leng

*DLL version: 6.2.9200

Windows 8*: Scheduled Task



*DLL version: 6.2.9200

Windows 8*: Scheduled Task

- PE execution:
  - C:\Windows\AppCompat\Programs\AmCache.hve
- Scheduled task: ProgramDataUpdater (~3:00 every 3 days)
  - Updates AmCache.hve
  - C:\Windows\AppCompat\Programs\AEINV_AMI_WER_{GUID}_YYYYMMDD_hhmm.xml
  - C:\Windows\AppCompat\Programs\DevInvCache\PropCache.bin

    (if PE is a driver)

*DLL version: 6.2.9200

Windows 10 Redstone 1

- DLL version: 10.0.14913

Windows 10 Redstone 1*

- PE execution:
  - C:\Windows\AppCompat\Programs\AmCache.hve
- Scheduled task: ProgramDataUpdater (~3:00 every 3 days)
  - Updates AmCache.hve
- Scheduled task: Microsoft Compatibility Appraiser (every day)
  - C:\Windows\AppCompat\Appraiser\APPRAISER_FileInventory.xml
  - Updates AmCache.hve

*DLL version: 10.0.14913

Windows 10 Redstone 3

- DLL version: 10.0.16299

Windows 10 Redstone 3*: PE execution

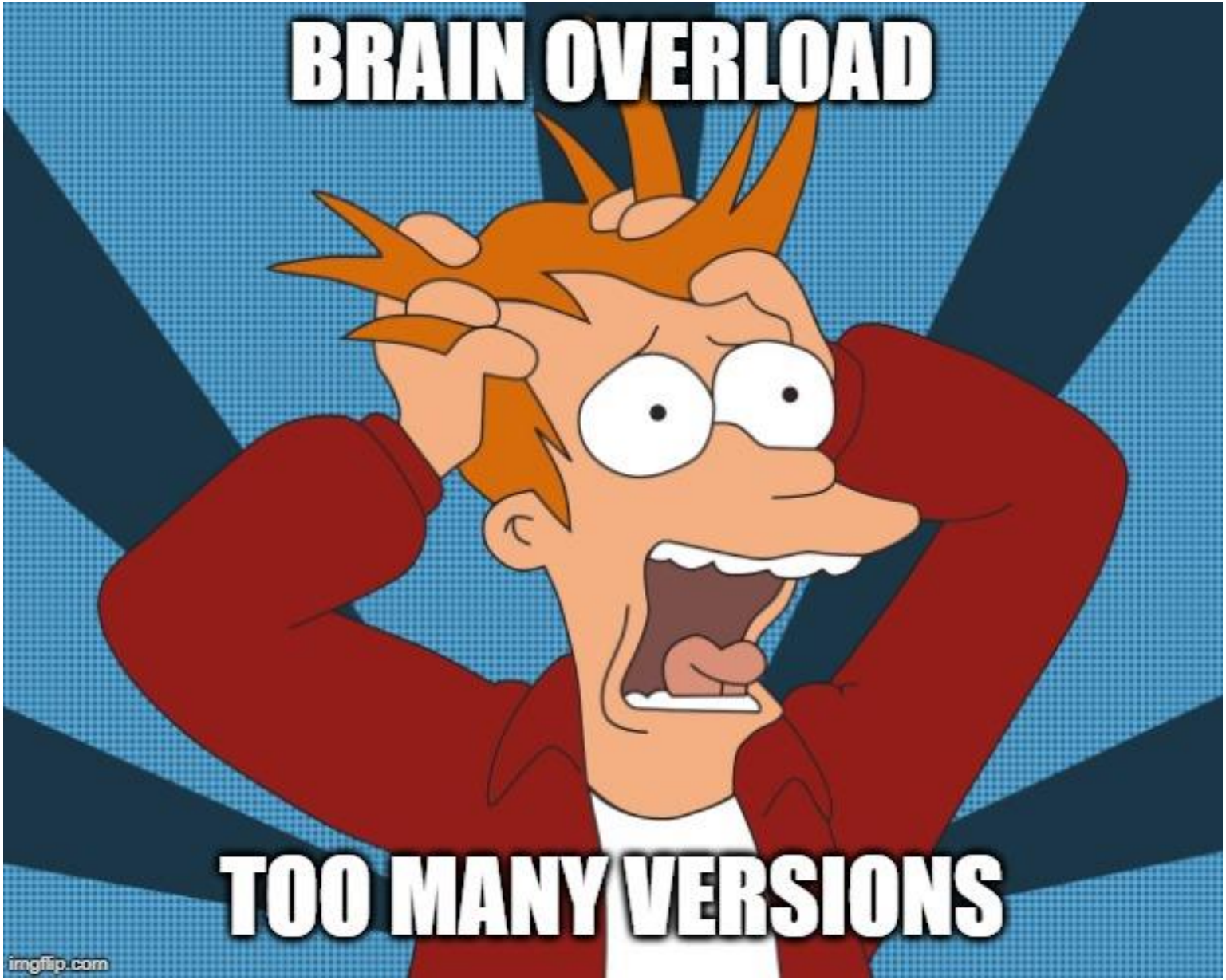
Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:19:21.5709543 AM	malware.exe	2396	Load Image	C:\Users\Lambda\malware.exe	SUCCESS	Image Base: 0x400...
9:19:21.5711666 AM	malware.exe	2396	CreateFile	C:\Windows\Prefetch\MALWARE.EXE-6C404B93.pf	NAME NOT FOU...	Desired Access: G...
9:19:21.5756005 AM	malware.exe	2396	CreateFile	C:\Users\Lambda\malware.exe	SUCCESS	Desired Access: R...
...						
9:19:35.4113140 AM	svchost.exe	1020	QueryBasicInformationFile	C:\Windows\appcompat\Programs\Amcache.hve	SUCCESS	CreationTime: 5/3/...
9:19:35.4113287 AM	svchost.exe	1020	CloseFile	C:\Windows\appcompat\Programs\Amcache.hve	SUCCESS	
9:19:35.4117286 AM	svchost.exe	1020	CreateFile	C:\Windows\appcompat\Programs\Amcache.hve	SUCCESS	Desired Access: R...
9:19:35.4117779 AM	svchost.exe	1020	QueryStandardInformationFile	C:\Windows\appcompat\Programs\Amcache.hve	SUCCESS	AllocationSize: 1,3...
9:19:35.4117964 AM	svchost.exe	1020	CloseFile	C:\Windows\appcompat\Programs\Amcache.hve	SUCCESS	
9:19:35.4118777 AM	svchost.exe	1020	RegLoadKey	\REGISTRY\A\{c73a0ba9-3b26-3677-385f-c6e195fe1a62}	SUCCESS	Hive Path: C:\Win...
...						
9:19:35.4247734 AM	svchost.exe	1020	QueryStandardInformationFile	C:\Users\Lambda\malware.exe	SUCCESS	AllocationSize: 36,...
9:19:35.4247927 AM	svchost.exe	1020	CreateFileMapping	C:\Users\Lambda\malware.exe	FILE LOCKED WI...	SyncType: SyncTy...
9:19:35.4248100 AM	svchost.exe	1020	QueryStandardInformationFile	C:\Users\Lambda\malware.exe	SUCCESS	AllocationSize: 36,...
9:19:35.4248325 AM	svchost.exe	1020	CreateFileMapping	C:\Users\Lambda\malware.exe	SUCCESS	SyncType: SyncTy...
9:19:35.4249389 AM	svchost.exe	1020	CloseFile	C:\Users\Lambda\malware.exe	SUCCESS	
9:19:35.4286806 AM	svchost.exe	1020	RegQueryValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\ProviderSyncId	SUCCESS	Type: REG_SZ, Le...
9:19:35.4287089 AM	svchost.exe	1020	RegOpenKey	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7	NAME NOT FOU...	Desired Access: All...
9:19:35.4287274 AM	svchost.exe	1020	RegCreateKey	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7	SUCCESS	Desired Access: All...
9:19:35.4288505 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\ProgramId	SUCCESS	Type: REG_SZ, Le...
9:19:35.4289655 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\FileId	SUCCESS	Type: REG_SZ, Le...
9:19:35.4290144 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\LowerCaseLongPath	SUCCESS	Type: REG_SZ, Le...
9:19:35.4290386 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\LongPathHash	SUCCESS	Type: REG_SZ, Le...
9:19:35.4290591 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\Name	SUCCESS	Type: REG_SZ, Le...
9:19:35.4290772 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\Publisher	SUCCESS	Type: REG_SZ, Le...
9:19:35.4290940 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\Version	SUCCESS	Type: REG_SZ, Le...
9:19:35.4291092 AM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{fe934a07-3532-3628-fbd3-7be18247a37a}\Root\InventoryApplicationFile\malware.exe\8cc074c7\BinFileVersion	SUCCESS	Type: REG_SZ, Le...

*DLL version: 10.0.16299

Windows 10 Redstone 3*

- PE execution:
  - C:\Windows\AppCompat\Programs\AmCache.hve
- Scheduled task: ProgramDataUpdater (~3:00 every 3 days)
  - Does not seem to write or update any file
- Scheduled task: Microsoft Compatibility Appraiser (every day)
  - Updates AmCache.hve

*DLL version: 10.0.16299


BRAIN OVERLOAD
TOO MANY VERSIONS
imgflip.com

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename								
File path								
SHA-1								
Program								
Install Directory								
Driver								
Driver path								

Plan

- Inner workings
- Scenario 1: « Welcome to the Hellmouth »
- Scenario 2: « Same Time, Same Place »
- Scenario 3: « The Killer in Me »

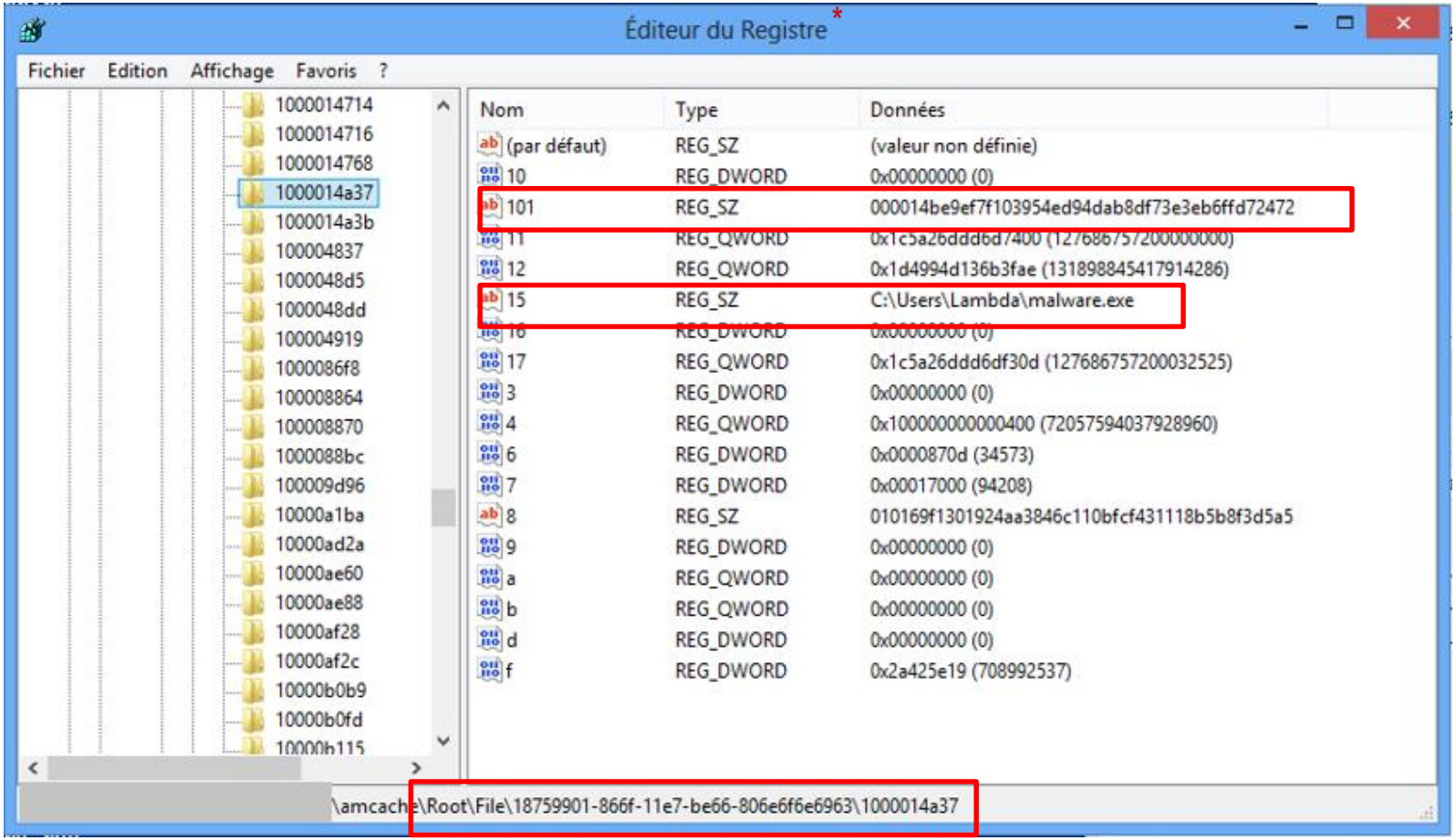
Welcome to the Hellmouth: Attacker

- An attacker compromises a user account: « Lambda » on a Windows 8 machine
- The attacker logs on as Lambda
- The attacker launches « C:\Users\Lambda\malware.exe »
- The attacker deletes the file

Welcome to the Hellmouth: Analyst

- Suspect behavior identified on a Windows 8 machine
- Several artifacts indicate the execution of « C:\Users\Lambda\malware.exe »
- But malware.exe is no longer on the system…

Welcome to the Hellmouth: Analyst

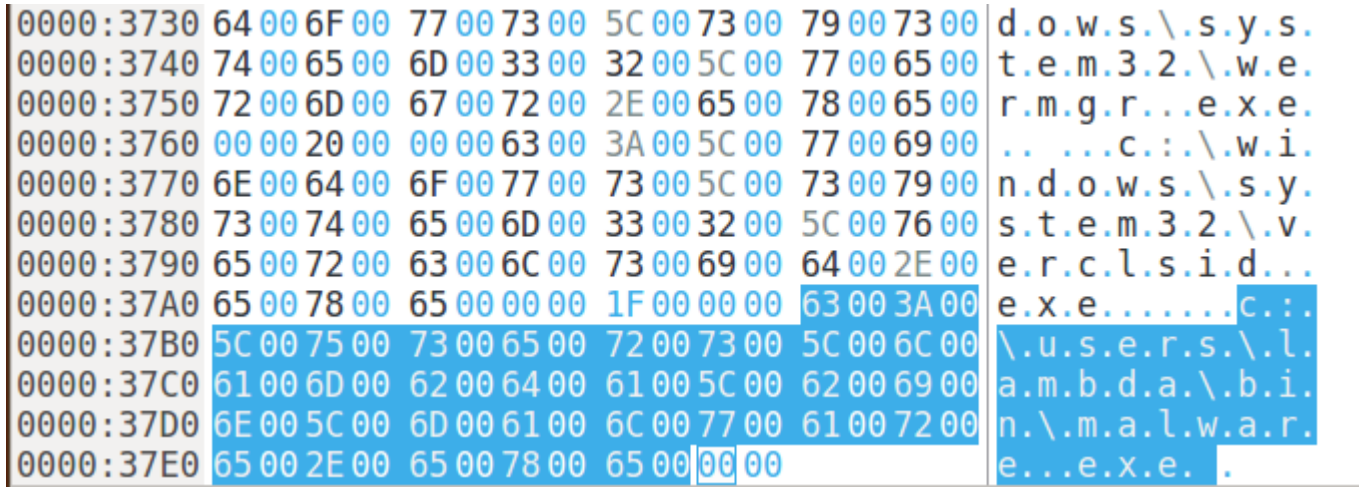


*** Hive mounted manually**

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFileCache.bcf	AEINV_WER.xml	AmCache.hve	AEINV_AMI.xml	PropCache.bin	AmCache.hve	APPRAISER_FileInventory.xml	AmCache.hve
Filename			X			X		X
File path			X			X		X
SHA-1			X			X		X
Program								
Install Directory								
Driver								
Driver path								

Welcome to the Hellmouth 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

Welcome to the Hellmouth 2: Analyst

- Limits of RecentFileCache.bcf :
  - Only the filename with its path
  - Not all executables are referenced in RecentFileCache.bcf :
    - Executions from an external media or from a network share are not recorded
    - Exceptions in C:\Users (empirical and non-exhaustive list) :
      - C:\Users\<username>\Downloads
      - C:\Users\<username>\Documents
      - Modification date of the binary > 12h
  - Content emptied every day at 00h30 by ProgramDataUpdater

Welcome to the Hellmouth 2: Scheduled Task

```
−<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

Welcome to the Hellmouth 2: Scheduled Task

<File Name="malware.exe" Id="0000c686bc8fcbeec14be0993ce74db89fa864975970"
SwitchBackContext="0x0100000000000501" Size="0x83200" SizeOfImage="0x87000"
PeHeaderHash="01013246bfaf67ffa917fc960cbd8581ddbf93a3f78b" 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

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename	X	X	X	X		X		X
File path	X		X			X		X
SHA-1		X	X	X		X		X
Program								
Install Directory								
Driver								
Driver path								

Plan

- Inner workings
- Scenario 1: « Welcome to the Hellmouth »
- Scenario 2: « Same Time, Same Place »
- Scenario 3: « The Killer in Me »

Same Time, Same Place: Attacker

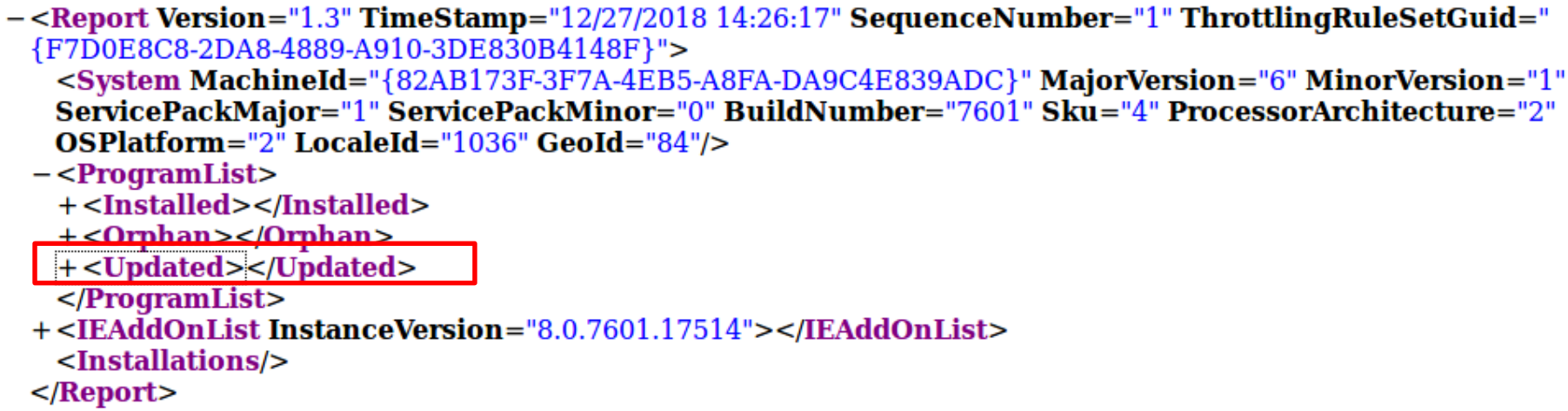
- An attacker compromises a user account « Lambda » on a Windows 7 machine
- The attacker logs on as Lambda
- The attacker hides a malicious binary « hidden-malware.exe » in C:\Program Files\7-Zip\

Same Time, Same Place: Analyst

- Threat hunting on the Windows 7 machine
- No specific lead


MIND YOUR HEAD

Same Time, Same Place: Analyst



AEINV_WER_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}_20181227_142615.xml

Aside: Inner workings

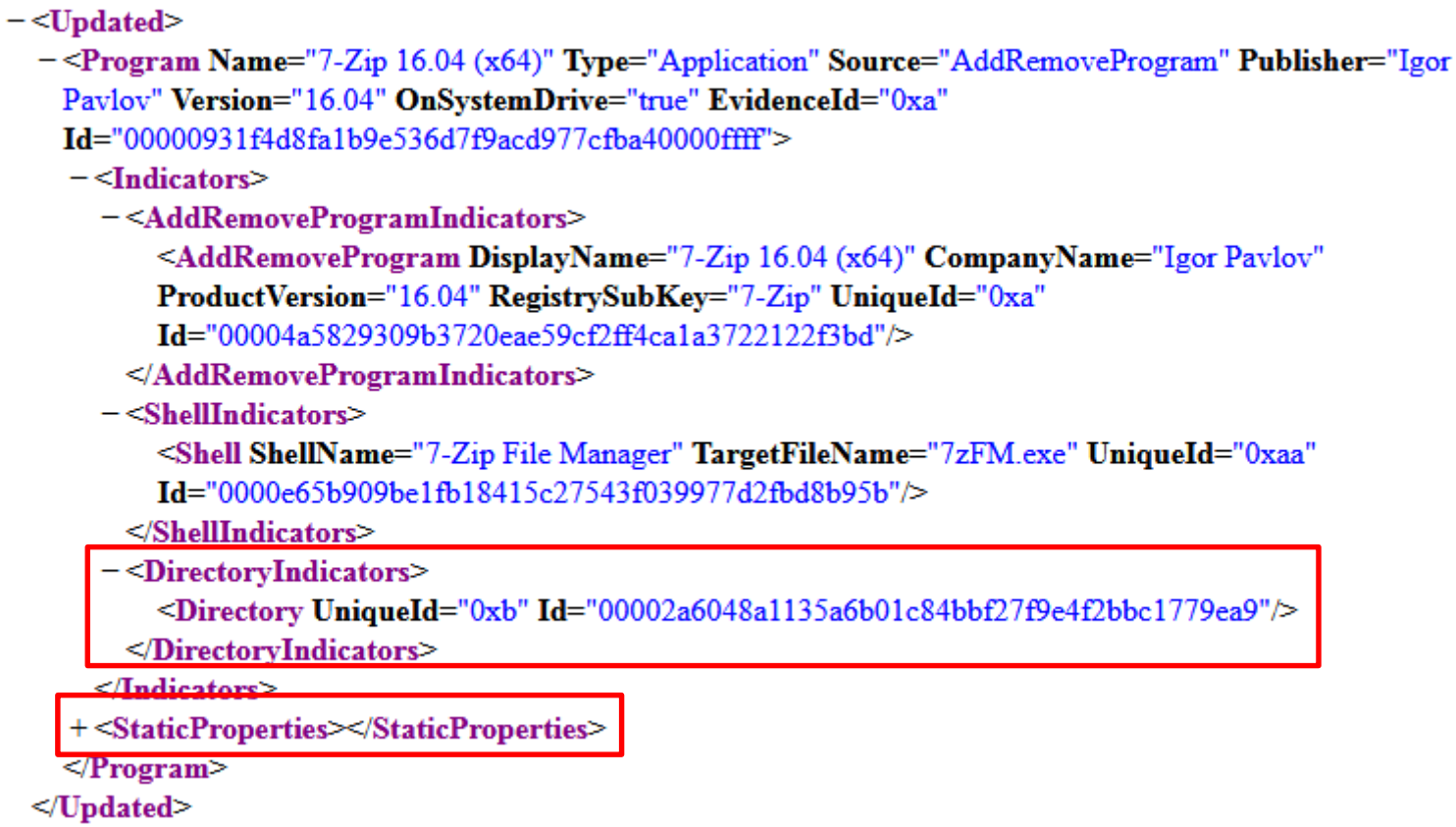
- In the AEINV, programs are defined by indicators:
  - RegistryIndicators ;
  - AddRemoveProgramIndicators ;
  - ShellIndicators ;
  - MsiIndicators ;
  - FileExtIndicators ;
  - DirectoryIndicators.
- Change in one of the indicator

  ➔ Entry in the Updated list

Same Time, Same Place: Inner workings

- Installation of 7-Zip:
  - ➔ Entry in Installed
- New PE file under C:\Program Files\7-Zip\:
  - ➔ Entry in Updated

Same Time, Same Place: Analyst



AEINV_WER_{82AB173F-3F7A-4EB5-A8FA-DA9C4E839ADC}_20181227_142615.xml

Same Time, Same Place: Analyst

```
<File Name="hidden-malware.exe"
Id="000014be9ef7f103954ed94dab8df73e3eb6ffd72472"
ShortName="HIDDEN~1.EXE"
SwitchBackContext="0x0100000000000400" 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

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename	X	X	X	X		X		X
File path	X		X	X		X		X
SHA-1		X	X	X		X		X
Program		X	X	X		X		X
Install Directory		X						
Driver								
Driver path								

Same Time, Same Place 2: Redstone 1

- AEINV_WER.xml no longer exists
- New scheduled task Microsoft Compatibility Appraiser which updates a new file: APPRAISER_FileInventory.xml

Same Time, Same Place 2: Redstone 1

```
−<PathEntry name="C:\Program Files">
    <File Name="7z.exe" BinaryType="PE64_AMD64" Created="06/28/2019 11:27:04" Modified="10/04/2016 14:51:30"
    Size="0x000000000006D200" LowerCaseLongPath="c:\program files\7-zip\7z.exe"
    LongPathHash="000045cabbdf328f98a10cf21e436497694856d0b54f"/>
    <File Name="7zFM.exe" BinaryType="PE64_AMD64" Created="06/28/2019 11:27:04" Modified="10/04/2016 14:54:28"
    Size="0x00000000000CCE00" LowerCaseLongPath="c:\program files\7-zip\7zfm.exe"
    LongPathHash="000040c5133c22925bf611129f46bcef893f9bcf4aca"/>
    <File Name="7zG.exe" BinaryType="PE64_AMD64" Created="06/28/2019 11:27:04" Modified="10/04/2016 14:55:15"
    Size="0x0000000000087400" LowerCaseLongPath="c:\program files\7-zip\7zg.exe"
    LongPathHash="00002f61fbf5af75fa62c1a356e11769a0df1ef10a99"/>
    <File Name="hidden-malware.exe" BinaryType="PE32_I386" Created="06/28/2019 11:30:41" Modified="08/16/2005 14:22:00"
    Size="0x000000000000870D" LowerCaseLongPath="c:\program files\7-zip\hidden-malware.exe"
    LongPathHash="0000add69fa4eb4d9c413eda8bab40408f1dc561a278"/>
```

APPRAISER_FileInventory.xml

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename	X	X	X	X		X	X	X
File path	X		X	X		X	X	X
SHA-1		X	X	X		X		X
Program		X	X	X		X		X
Install Directory		X					\	X
Driver								
Driver path								

Plan

- Inner workings
- Scenario 1: « Welcome to the Hellmouth »
- Scenario 2: « Same Time, Same Place »
- Scenario 3: « The Killer in Me »

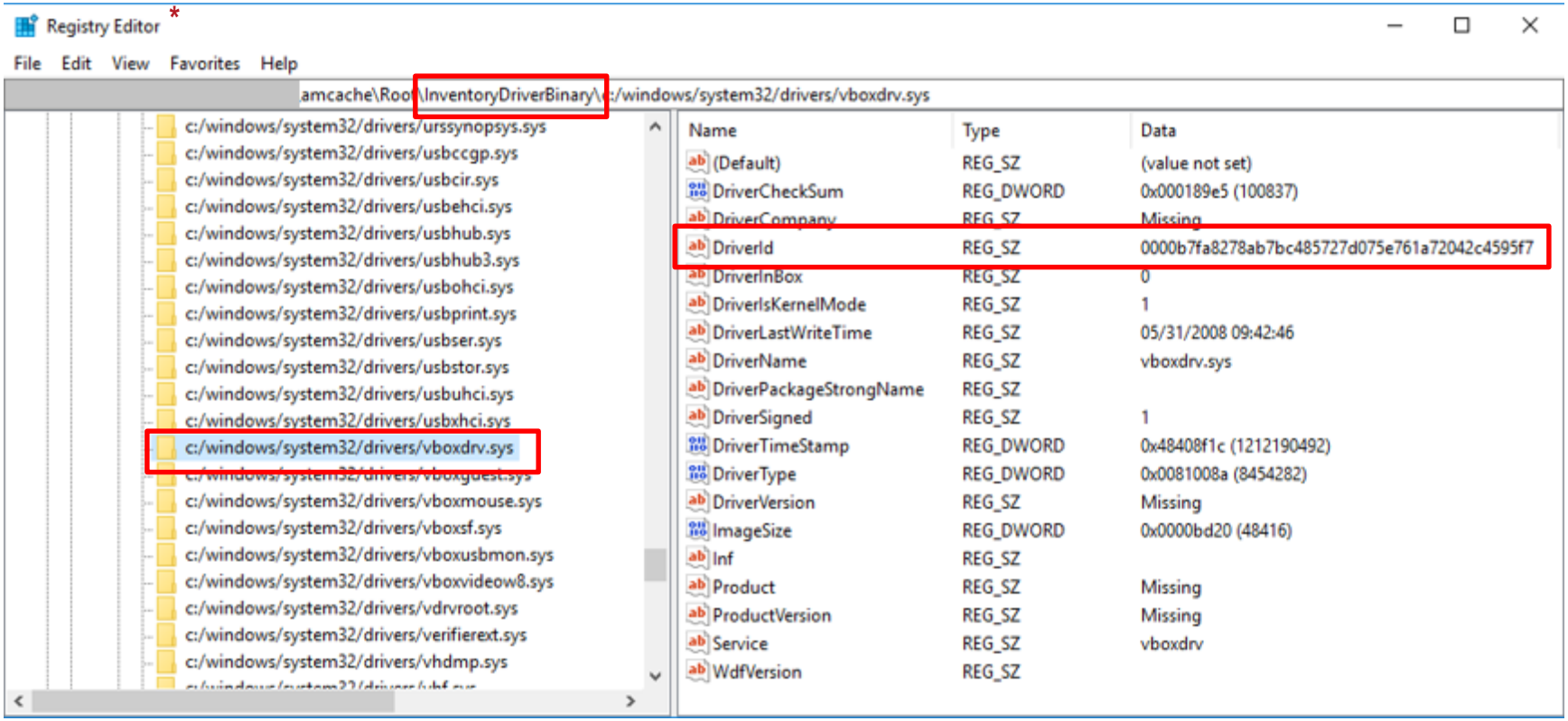
The Killer in Me: Attacker

- An attacker compromises a Windows 10 (Redstone 1) machine
- He uses a legitimate but vulnerable driver, « vboxdrv.sys » so that he can have a backdoor to do a privilege escalation.

The Killer in Me: Analyst

- Suspicious behavior identified on a Windows 10 machine
- Immediate response done
- Did the attacker leave anything else?

The Killer in Me: Analyst



* Hive mounted manually

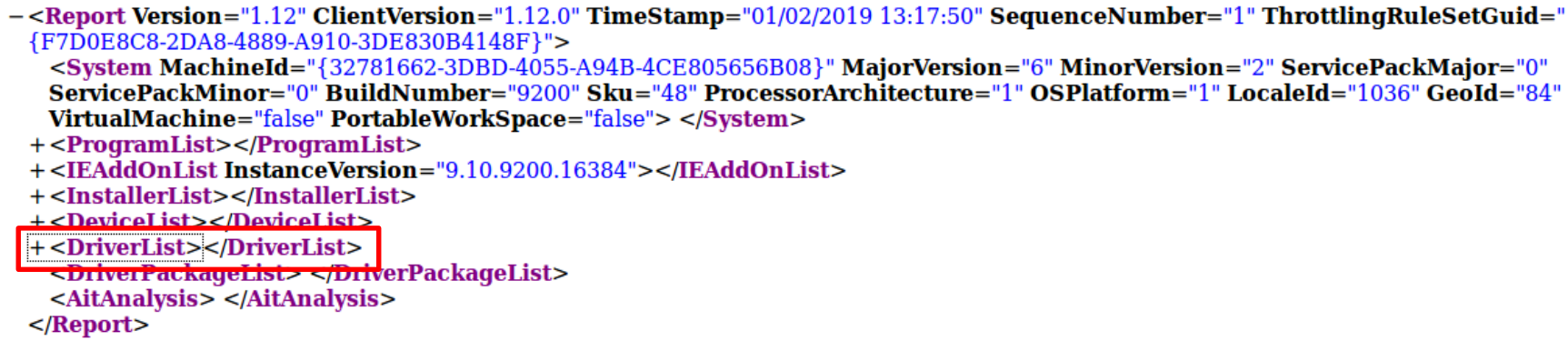
Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename	X	X	X	X		X	X	X
File path	X		X	X		X	X	X
SHA-1		X	X	X		X		X
Program		X	X	X		X		X
Install Directory		X					X	X
Driver						X		X
Driver path						X		X

The Killer in Me 2: Windows 8

- AmCache.hve does not record the drivers
- Scheduled task ProgramDataUpdater still exists…

The Killer in Me 2: Analyst



AEINV_AMI_WER[…].xml

The Killer in Me 2: Analyst

```
<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

The Killer in Me 2: Analyst

```
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  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

Summary of the artifacts found by OS (DLL version)

	Windows 7 (6.1.7600)		Windows 8 (6.2.9200)			Redstone 1 (10.0.14913)		Redstone 3 (10.0.16299)
	RecentFile Cache.bcf	AEINV _WER .xml	AmCache .hve	AEINV _AMI .xml	PropCache .bin	AmCache .hve	APPRAISER _FileInventory .xml	AmCache .hve
Filename	X	X	X	X		X	X	X
File path	X		X	X		X	X	X
SHA-1		X	X	X		X		X
Program		X	X	X		X		X
Install Directory		X					X	X
Driver				X	X	X		X
Driver path					X	X		X

Conclusion

- Artifact difficult to analyse:
  - Check the DLL version and not the OS!
  - Retrieve all the files!
- Be careful with your findings:
  - About the execution of the PE,
  - About the date of execution,
  - About the absence of a PE in the artifact.
- But the artifact is a precious asset in an investigation
- Technical analysis to help the analyst:

  ➔ https://www.ssi.gouv.fr/en/publication/amcache-analysis/

Questions?

> Contact:
- blanche.lagny@ssi.gouv.fr
- @moustik01

Execution date? – Example on Windows 8 (6.2.9200)

- If the PE is part of a program:
  - If the PE needed shimming and was executed before ProgramDataUpdater
    - ➔ Last modification date seems to be the execution date of the PE
  - Else if ProgramDataUpdater was executed since the program was installed
    - ➔ Last modification date seems to be the launch date of the scheduled task
  - Else
    - ➔ Last modification date seems to be the date the program was installed
- Else if the PE is the "installer" of a program:
  - If ProgramDataUpdater was executed since the program was installed
    - ➔ Last modification date seems to be the launch date of the scheduled task
  - Else
    - ➔ Last modification date seems to be the execution date of the PE
- Else:
  - If it is an "internal" PE
    - ➔ Last modification date is set after the execution date but could not be correlated with anything
  - Else if ProgramDataUpdater was executed since the PE was executed
    - ➔ Last modification date seems to be the launch date of ProgramDataUpdater
  - Else
    - ➔ Last modification date seems to be the execution date of the PE