Réponse à Incident

CONFIDENTIEL

Rapport d'analyse Forensic
23/09/2016

XXX

Préambule

Ce document présente de manière rapide les éléments de la réponse à incident du 30/06/2016

Vos interlocuteurs

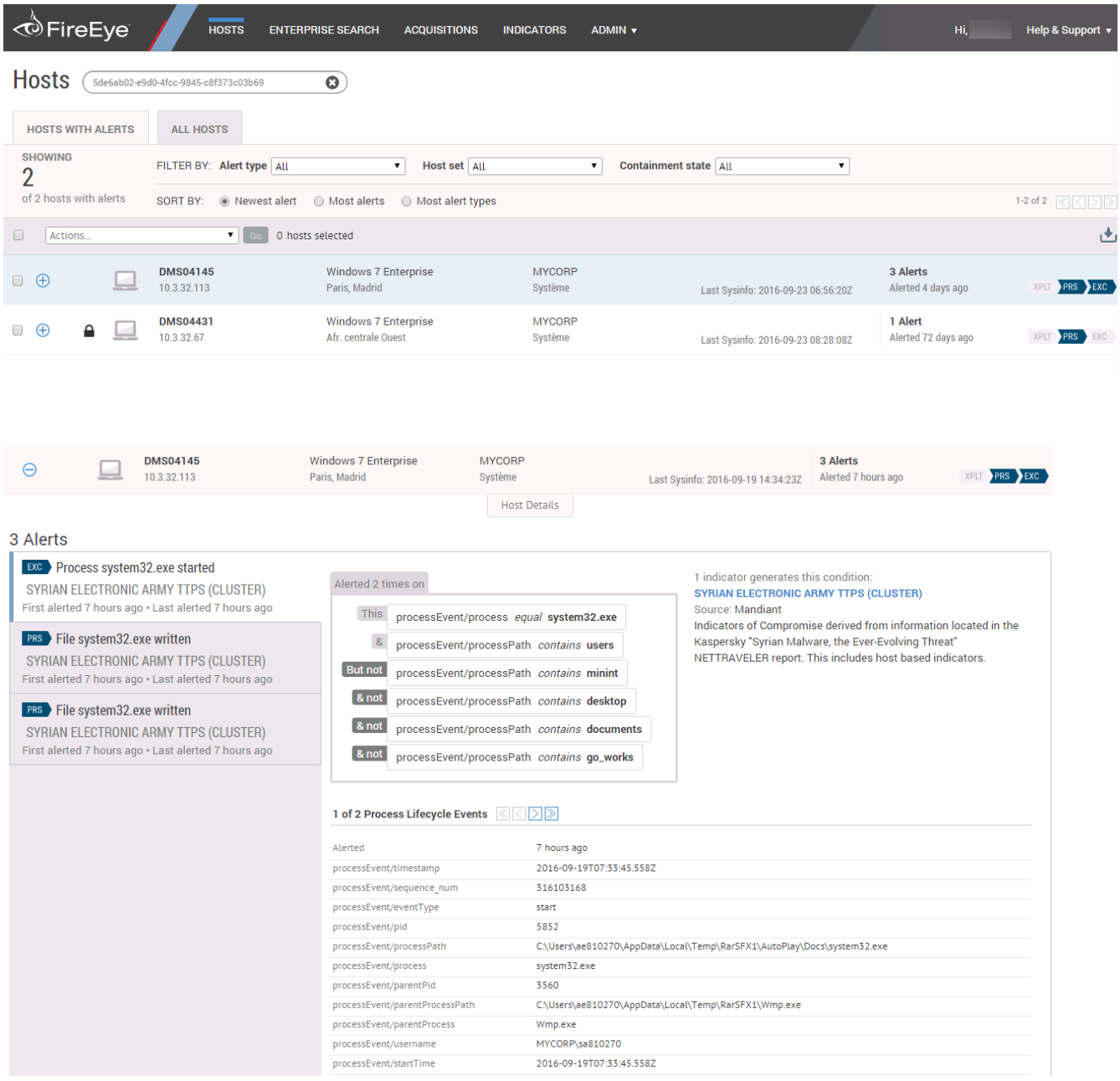
B. DUPONT	**Cybersecurity Expert – SOC Level 3/Forensic**
 +33 (0) 6 XX XX XX XX	E-mail : B.dupont@xxx.com
Florian CARFANTAN	**Analyste Forensic**
 +33 (0) 7 86 04 30 77	E-mail : florian.carfantan@xxx.com
R. DURANT	**Analyste Forensic**
 +33 (0) 6 XX XX XX XX	E-mail : r.durant@xxx.com
M. HENRY	**Analyste Forensic**
 +33 (0) 6 XX XX XX XX	E-mail : m.henry@xxx.com
D. CORDIN	**Manager de contrat**
 +33 6 XX XX XX XX	E-mail : d.cordin@xxx.com

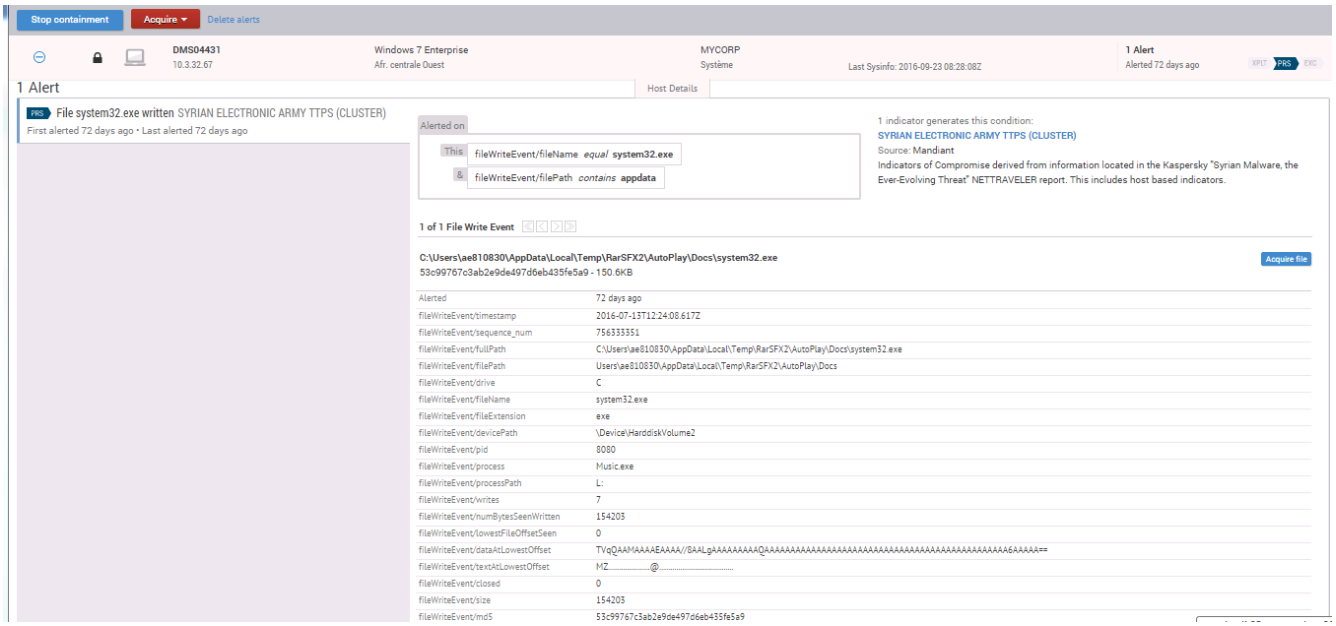
Sommaire

1. Contexte

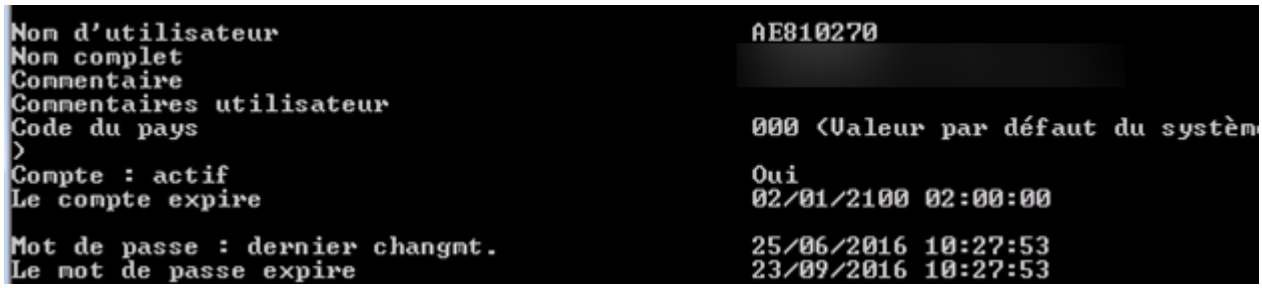
1.1. Rappel

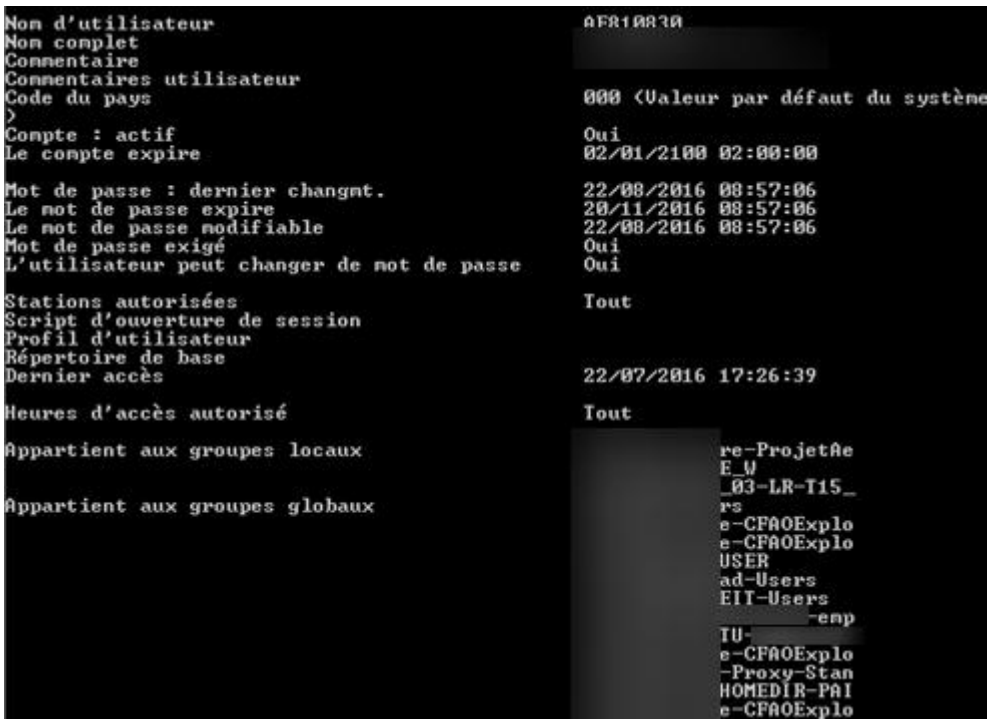
La console FireEye HX a détecté 2 postes (***DMS04145/DMS04431***) infectés par un malware et marqué ***Présence*** pour les deux et marqué ***Exécution*** pour le premier poste. L'indicateur ayant déclenché est « ***SYRIAN ELECTRONIC ARMY TTPS (CLUSTER)*** ».





Le fichier détecté est un exécutable « ***system32.exe*** » (Hash MD5 : ***53c99767c3ab2e9de497d6eb435fe5a9***) et lancé par l'utilisateur ***AE810270***.

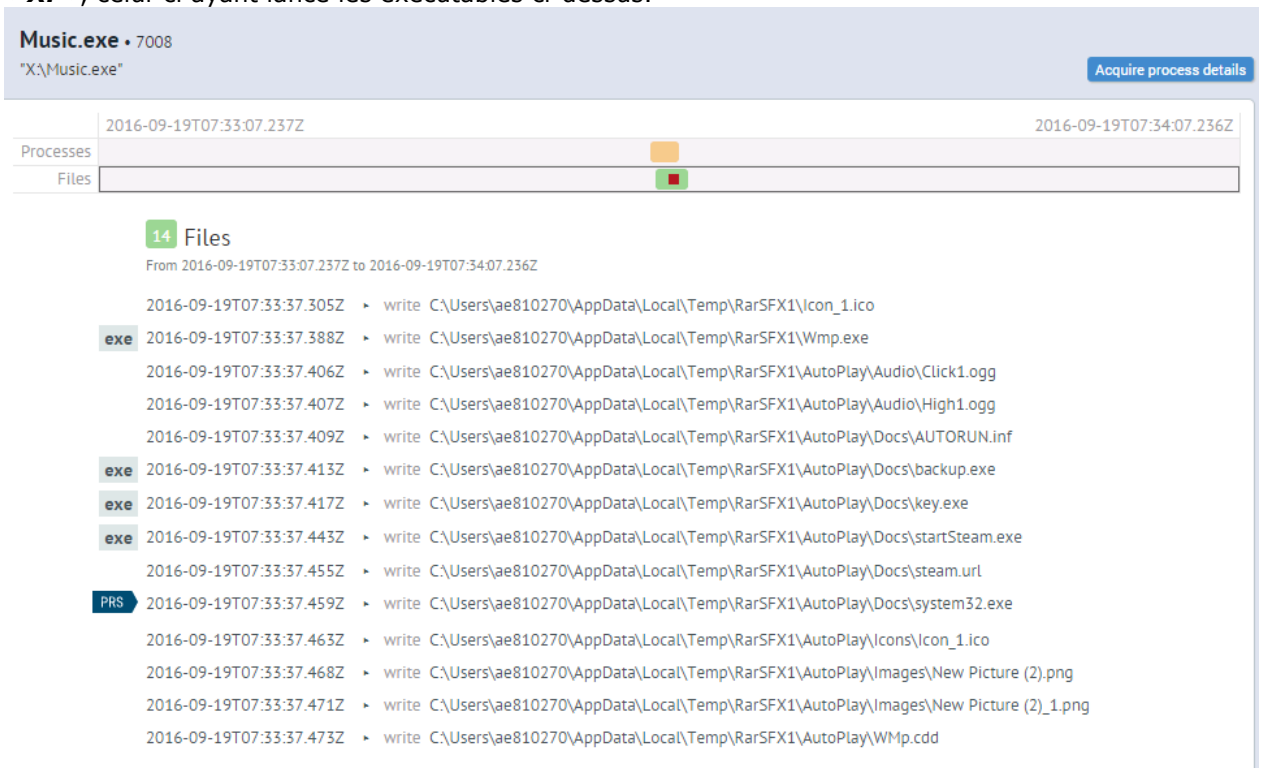




Les exécutables suivants ont également été détectés :

- ***backup.exe*** (***12255955f9ef37f663910d4deaf9cc86***)
- ***key.exe*** (***f4d627d2ef6fcd217774f2a915902d14***)
- ***startSteam.exe*** (***04c24c4d1958466ed17ff58dc7cd7c4d***)
- ***Wmp.exe*** (***2e5d84f170a33ed44a9eada85f58ed03***)

Les 5 exécutables sont situés dans le dossier « ***C:\users\ae810270\AppData\Local\Temp\RarSFX1\Docs*** » à l'exception de Wmp.exe qui lui est situé dans le répertoire « ***C:\users\ae810270\AppData\Local\Temp\RarSFX1*** ».
D'après la console HX, la source de ces exécutions serait un fichier « ***Music.exe*** » situé sur un lecteur « ***X:*** », celui-ci ayant lancé les exécutables ci-dessus.



Aucune trace de communication réseau n'a été détectée par le HX.

1.2. Nature de l'infection

1.2.1. Généralités

D'après notre analyse, le malware a le profil d'un virus qui s'autoréplique. Il décompresse des fichiers exécutables qu'il lance ensuite et écrit dans le registre afin d'être persistant. Il s'autoréplique en créant des fichiers autorun.inf sur les périphériques amovibles.

1.2.2. Détails techniques

L'arborescence caractéristique de ce malware est la suivante :

Création du répertoire « C:\Documents and Settings\$USER\Local Settings\Temp\RarSFX0\ » avec le contenu suivant :

```
│   Icon_1.ico (f546460510a77e4a4b616d12cf7a9ccb)
│   │
└───AutoPlay
    │   Wmp.cdd (1ac1e89a92f8d0f25572752d3e6a8dac)
    │
    ├───Audio
    │       Click1.ogg (93270c4fa492e4e4edee872a2b961dde)
    │       High1.ogg (fc2a595f574b1ead82a6dcf06492c985)
    │
    ├───Docs
    │           │           │           │       steam.url (6e3e4e19cf3d91dcb7f065d5c8627748)
    │       system32.exe (53c99767c3ab2e9de497d6eb435fe5a9)
    │
    ├───Icons
    │       Icon_1.ico (f546460510a77e4a4b616d12cf7a9ccb)
    │
    └───Images
            New Picture (2).png (f6a50ad48108259cea7f8278cfa7f241)
            New Picture (2)_1.png (59db4ed1e01b3c3f5c3f2a8ff3ed7f69)
```

Certaines clés de registres sont modifiées :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"system32"="C:\\Windows\\Branding\\key.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"steam"="C:\\Windows\\AppPatch\\taskmgr.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Steam"="\"C:\\Windows\\TVCS\\Steam Powerd.exe"
```

1.3. Évènements

1.3.1. Infection initiale

Music.exe est l'exécutable à l'origine des alertes qui ont provoqué cette investigation. Il était présent sur le partage réseau dédié aux utilisateurs (Home Directory) pour les deux attaques. La première a eu lieu le 13/07/2016 et la seconde a eu lieu le 19/09/2016.

Les partages réseau étant en dehors du périmètre de FireEye HX, il n'est pas possible de remonter plus loin en amont pour savoir ce qui a écrit ces fichiers Music.exe sur le partage réseau.

1.3.2. Incident utilisateur

Pour l'attaque du 13 juillet, l'utilisateur qui a exécuté Music.exe est sa810830. Le nom associé à ce login est Sophie BOULAIN. L'exécution s'est produite sur le poste DMS04145 à 7h33 et 37 secondes (GMT).

Pour l'attaque du 19 septembre, l'utilisateur qui a exécuté Music.exe est AE810270. Le nom associé à ce login est Pierre DOHERTY. L'exécution s'est produite sur le poste DMS04431 à 12h24 et 20 secondes (GMT).

2. Analyse du malware

Pour les 2 exécutions qui ont eu lieu, le malware n'a pu avoir un comportement malveillant réussi durant son exécution, car :

1. L'antivirus McAfee a bloqué l'exécution d'un des fichiers extraits de music.exe : backup.exe.
2. Le malware nécessite les droits d'administration pour avoir un comportement nominal
3. Le malware a des soucis pour s'exécuter sur Windows 7 et les 2 postes en question étaient sous cette distribution
4. Le serveur de C&C n'est à priori plus actif « http://storeysteampowered.tk/ »

2.1. Composition

2.1.1. Fichiers & Dépendances

Récapitulatif des différents fichiers détectés ainsi qu'une explication de son fonctionnement :

Music.exe (32745eb47462ebf97116e4f7bae1da66)	Installeur. À l'exécution, il crée aussi un fichier « AUTORUN.inf » (3ea55697a8ca3c6af0855cf45f007beb)qu'il maintient existant tant que le programme est résident (si suppression, il le recrée). cat AUTORUN.inf [AutoRun] action=Ouvrir le dossier pour afficher les fichiers ShellExecute=music.exe Shell\Open\Command=music.exe Shell\Explore\Command=music.exe open=music.exe https://www.virustotal.com/fr/file/fc0c59bdec71cab679f349fa1078cf03d0f65a57c48c85b1e9745eb7c8fe1c92/analysis/ Trojan.Win32.Agent2.fjnn

Wmp.exe
Steam.exe
 	
(2e5d84f170a33ed44a9eada85f58ed03)
	file Wmp.exe
	Wmp.exe: PE32 executable (GUI) Intel 80386, for MS Windows
	
	Version du fichier :
	  7.5.1004.0
	Description :
	  AutoPlay Application
	
	Copyright :
	  Runtime Engine Copyright © 2008 Indigo Rose Corporation (www.indigorose.com)
	
	https://www.virustotal.com/fr/file/f659ca020b97340542c45516fe8c3e97491a8adc769ec13602a3ace462a6e773/analysis/
	Probably harmless! There are strong indicators suggesting that this file is safe to use

Wmp.cdd (1ac1e89a92f8d0f25572752d3e6a8dac)	file WMp.cdd
	WMp.cdd: Zip archive data, at least v2.0 to extract
	
	unzip WMp.cdd
	Archive: WMp.cdd
	[WMp.cdd] _detect.dat password:
	  skipping: _detect.dat incorrect password
	  skipping: _proj.dat incorrect password
	  skipping: _fonts.dat incorrect password
	
	https://www.virustotal.com/fr/file/7641a4e3a156c3943091225bec5c4296f9477768a7edf04eb5ea83eca62d306b/analysis/
	Trojan.Win32.Agent2.fjnn

Click1.ogg (93270c4fa492e4e4edee872a2b961dde)	Ogg data, Vorbis audio, mono, 44100 Hz, ~128000 bps, created by: Xiphophorus libVorbis I (1.0 RC2) https://www.virustotal.com/fr/file/25d49cbbd65d48ad462455f1143f73ee997df8f747e7d2213daab18e321c028b/analysis/ Probably harmless! There are strong indicators suggesting that this file is safe to use
High1.ogg (fc2a595f574b1ead82a6dcf06492c985)	Ogg data, Vorbis audio, mono, 44100 Hz, ~128000 bps, created by: Xiphophorus libVorbis I (1.0 RC2) https://www.virustotal.com/fr/file/ee9a4903a8df90eff4c5b65a8073e564a3581cf73772a72eb82396e69932e769/analysis/ Probably harmless! There are strong indicators suggesting that this file is safe to use
backup.exe (12255955f9ef37f663910d4deaf9cc86)	unrar x backup.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../backup.exe Le commentaire ci-dessous contient des commandes pour script SFX Setup=REGEDIT /s system32.reg TempMode Silent=1 Overwrite=1 Extracting system32.reg OK All OK md5sum * 389370c7988842b5c65894569428a4d8 system32.reg https://www.virustotal.com/en/file/0f6923f61c7d7630794ff32b5681e14df3a584cca2154bddc679e0045569d68c/analysis/ Troj/Agent-AFBW

system32.reg (389370c7988842b5c65894569428a4d8)	cat system32.reg Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "system32"="C:\\Windows\\Branding\\key.exe"
key.exe (f4d627d2ef6fcd217774f2a915902d14)	unrar x key.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../key.exe Le commentaire ci-dessous contient des commandes pour script SFX Setup=REGEDIT /s key.reg TempMode Silent=1 Overwrite=1 Extracting key.reg OK All OK md5sum * 460a71bfe467e11fb3b3e14890062455 key.reg https://www.virustotal.com/fr/file/51bed171a4dd0fe614bb3164dd118ebf085d2d3fc9ce5c2d80c642666a6670d4/analysis/ Troj/Agent-AFBW

startSteam.exe (04c24c4d1958466ed17ff58dc7cd7c4d)	unrar x startSteam.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../startSteam.exe Le commentaire ci-dessous contient des commandes pour script SFX Path=C:\windows\TVCS\ Setup=REGEDIT /s key.reg Silent=1 Overwrite=1 Extracting key.reg OK Extracting Steam Powerd.exe OK All OK md5sum * 4f29658c17572469adadc00ef52010e3 key.reg 6addfe3f0ead8a876fbb5acaeb477a34 Steam Powerd.exe https://www.virustotal.com/en/file/85927a5c1ab1694b9e71eaf01188b9c77df4a5a73a1f4192f521925396bcee09/analysis/ Troj/Agent-AFBW
steam.url (6e3e4e19cf3d91dcb7f065d5c8627748)	cat steam.url [{000214A0-0000-0000-C000-000000000046}] Prop3=19,2 [InternetShortcut] URL=http://storeysteampowered.tk/ IDList=
system32.exe (53c99767c3ab2e9de497d6eb435fe5a9)	unrar x system32.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../system32.exe Le commentaire ci-dessous contient des commandes pour script SFX Path=C:\Windows\Branding Silent=1 Overwrite=1 Extracting key.exe OK All OK md5sum * 2c9ba2a957e34796558047459da5cd86 key.exe https://www.virustotal.com/en/file/619840381aebcd943571a13113c5d44aba19693c4a4eb6fdee3d4fad91fdffa3/analysis/ Troj/Agent-AFBY

Icon_1.ico (f546460510a77e4a4b616d12cf7a9ccb)	Icon_1.ico: MS Windows icon resource - 16 icons, 64x64, 16-colors https://www.virustotal.com/fr/file/832daf3c2f11a87cdb5fd606f3a15bd460f9849d3d46ce7eeb72c0c84f8151b2/analysis/ Probably harmless! There are strong indicators suggesting that this file is safe to use
New Picture (2).png (f6a50ad48108259cea7f8278cfa7f241)	New Picture (2).png: PNG image data, 1192 x 179, 8-bit/color RGBA, non-interlaced
New Picture (2)_1.png (59db4ed1e01b3c3f5c3f2a8ff3ed7f69)	New Picture (2)_1.png: PNG image data, 552 x 83, 8-bit/color RGBA, non-interlaced
C:\WINDOWS\Branding\key.exe (2c9ba2a957e34796558047459da5cd86)	unrar x key.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from key.exe Le commentaire ci-dessous contient des commandes pour script SFX Setup=REGEDIT /s key.reg TempMode Silent=1 Overwrite=1 Extracting key.reg OK All OK md5sum * 460a71bfe467e11fb3b3e14890062455 key.reg https://www.virustotal.com/fr/file/eb543fac82adb897cafbfecd9fc35d55996eee5cad659f93600e5efbdef1610e/analysis/ Troj/Agent-AFBW
C:\WINDOWS\TVC\Steam.exe (f6eb530e44b03398701d07f2587b1c81)	unrar x Steam.exe UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../Steam.exe Le commentaire ci-dessous contient des commandes pour script SFX Setup=Steam.exe TempMode Silent=1 Overwrite=1 Creating AutoPlay OK Creating AutoPlay/Audio OK Extracting AutoPlay/Audio/Click1.ogg OK Extracting AutoPlay/Audio/High1.ogg OK

	Creating AutoPlay/Icons OK Extracting AutoPlay/Icons/steam.ico OK Creating AutoPlay/Images OK Extracting AutoPlay/Images/achievementbg.jpg OK Extracting AutoPlay/Images/avatarBorderOffline.jpg OK Extracting AutoPlay/Images/clienttexture2.jpg OK Extracting AutoPlay/Images/logo6.jpg OK Extracting AutoPlay/Images/minithrobber04.jpg OK Extracting AutoPlay/Images/New Picture (1).png OK Extracting AutoPlay/Images/New Picture (2).png OK Extracting AutoPlay/Images/New Picture.png OK Extracting AutoPlay/Images/steam_logo_big.jpg OK Extracting AutoPlay/Steam.cdd OK Extracting Steam.exe OK Extracting steam.ico OK All OK find ./ -exec md5sum {} \; 2>/dev/null 2e5d84f170a33ed44a9eada85f58ed03 ./Steam.exe 05deb0e24e50a822345cc23de4f7d807 ./steam.ico d1b610eb5e6bf1c9960b9b31b23790fb ./AutoPlay/Steam.cdd 93270c4fa492e4e4edee872a2b961dde ./AutoPlay/Audio/Click1.ogg fc2a595f574b1ead82a6dcf06492c985 ./AutoPlay/Audio/High1.ogg 618fbd3682fccdf73800e8d09569d3c7 ./AutoPlay/Images/minithrobber04.jpg e931b007e9feb6de12e1742843fa5481 ./AutoPlay/Images/avatarBorderOffline.jpg a218f552cda0826d05c08cd6916aa877 ./AutoPlay/Images/logo6.jpg 59db4ed1e01b3c3f5c3f2a8ff3ed7f69 ./AutoPlay/Images/New Picture (2).png 7ffcb22a9206866a06551a7b19f0f83e ./AutoPlay/Images/New Picture (1).png b54918b3777a8b312ae1fd25cf396253 ./AutoPlay/Images/clienttexture2.jpg 50a8c32acb4a45fe356f9724c79ecd38 ./AutoPlay/Images/New Picture.png 0689e7bc4a7647a9bc1f9ee94880107e ./AutoPlay/Images/achievementbg.jpg 0b433071bdd7eb7575e2344aa70e7428 ./AutoPlay/Images/steam_logo_big.jpg 4adcb7e9abf32ad99183265e6587affd ./AutoPlay/Icons/steam.ico https://www.virustotal.com/fr/file/f271439a77ed8e3d58b8bf483d33022d81d89dfd2ce8031d9b898052edfc0d18/analysis/ Troj/Agent-AFBW
C:\WINDOWS\TVCS\key.reg (4f29658c17572469adadc00ef52010e3)	Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "Steam"="\"C:\\Windows\\TVCS\\Steam Powerd.exe"
./steam.ico (05deb0e24e50a822345cc23de4f7d807)	file steam.ico steam.ico: MS Windows icon resource - 4 icons, 32x32, 16-colors

./AutoPlay/Steam.cdd (d1b610eb5e6bf1c9960b9b31b23790fb)	file Steam.cdd Steam.cdd: Zip archive data, at least v2.0 to extract unzip ../Steam.cdd Archive: ../Steam.cdd [../Steam.cdd] _detect.dat password: skipping: _detect.dat incorrect password skipping: _proj.dat incorrect password https://www.virustotal.com/fr/file/54b8e333d52c3672effc28480575c00bc7ec7415fd8ffce5b56ca27dad02bab4/analysis/ Considered as safe but encrypted data ...
./AutoPlay/Images/minithrobber04.jpg (618fbd3682fccdf73800e8d09569d3c7)	minithrobber04.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Images/avatarBorderOffline.jpg (e931b007e9feb6de12e1742843fa5481)	avatarBorderOffline.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Images/logo6.jpg (a218f552cda0826d05c08cd6916aa877)	logo6.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Images/New Picture (1).png (7ffcb22a9206866a06551a7b19f0f83e)	New Picture (1).png: PNG image data, 159 x 83, 8-bit/color RGBA, non-interlaced
./AutoPlay/Images/clienttexture2.jpg (b54918b3777a8b312ae1fd25cf396253)	clienttexture2.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Images/New Picture.png (50a8c32acb4a45fe356f9724c79ecd38)	New Picture.png: PNG image data, 618 x 163, 8-bit/color RGBA, non-interlaced
./AutoPlay/Images/achievementbg.jpg (0689e7bc4a7647a9bc1f9ee94880107e)	achievementbg.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Images/steam_logo_big.jpg (0b433071bdd7eb7575e2344aa70e7428)	steam_logo_big.jpg: JPEG image data, JFIF standard 1.01
./AutoPlay/Icons/steam.ico (4adcb7e9abf32ad99183265e6587affd)	steam.ico: MS Windows icon resource - 1 icon
key.reg (460a71bfe467e11fb3b3e14890062455)	cat key.reg Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "steam"="C:\\Windows\\AppPatch\\taskmgr.exe"

C:\WINDOWS\TVCS\Steam Powerd.exe (6addfe3f0ead8a876fbb5acaeb477a34)	unrar x "Steam Powerd.exe" UNRAR 5.00 beta 8 freeware Copyright (c) 1993-2013 Alexander Roshal Extracting from ../Steam Powerd.exe Le commentaire ci-dessous contient des commandes pour script SFX Path=c:\windows\TVC\ Setup=Steam.exe Silent=1 Overwrite=1 Shortcut=D, Steam.exe, , "Steam client", Steam, Extracting Steam.exe OK All OK md5sum * f6eb530e44b03398701d07f2587b1c81 Steam.exe https://www.virustotal.com/fr/file/21441bc15b964541a6f88c14d27878c0433e673cb576ebf997cc096cab4c4aec/analysis/ Troj/Agent-AFBW

2.1.2. Détails de fonctionnement

L'installation ne se réalisant pas correctement si le poste est sous Windows 7, le test décrit ci-dessous a été effectué sous Windows XP.
(Entre parenthèse sont précisés les md5 des fichiers)

> Exécution de « Music.exe » (32745eb47462ebf97116e4f7bae1da66) :

Création du répertoire « C:\Documents and Settings\$USER\Local Settings\Temp\RarSFX0\ » avec le contenu suivant :

```
│   Icon_1.ico (f546460510a77e4a4b616d12cf7a9ccb)
│   Wmp.exe (2e5d84f170a33ed44a9eada85f58ed03)
│
└───AutoPlay
    │   Wmp.cdd (1ac1e89a92f8d0f25572752d3e6a8dac)
    │
    ├───Audio
    │       Click1.ogg (93270c4fa492e4e4edee872a2b961dde)
    │       High1.ogg (fc2a595f574b1ead82a6dcf06492c985)
    │
    ├───Docs
    │       backup.exe (12255955f9ef37f663910d4deaf9cc86)
    │       key.exe (f4d627d2ef6fcd217774f2a915902d14)
    │       startSteam.exe (04c24c4d1958466ed17ff58dc7cd7c4d)
    │       steam.url (6e3e4e19cf3d91dcb7f065d5c8627748)
    │       system32.exe (53c99767c3ab2e9de497d6eb435fe5a9)
    │
    ├───Icons
    │       Icon_1.ico (f546460510a77e4a4b616d12cf7a9ccb)
    │
    └───Images
            New Picture (2).png (f6a50ad48108259cea7f8278cfa7f241)
            New Picture (2)_1.png (59db4ed1e01b3c3f5c3f2a8ff3ed7f69)
```

Une fois les fichiers décompressés, « Wmp.exe » (aussi trouvé sous le nom de « Steam.exe ») sera exécuté ainsi que « backup.exe » et « system32.exe ».

- « backup.exe » créera une entrée dans la base de registre :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"system32"="C:\\Windows\\Branding\\key.exe"
```

- « system32.exe » créera le fichier « C:\Windows\Branding\key.exe » qui aura la fonction de créer suivante dans la base de registre :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"steam"="C:\\Windows\\AppPatch\\taskmgr.exe"
```

Cependant, « taskmgr.exe » n'a pas été trouvé

- « Wmp.exe » assurera l'installation du contenu Autoplay (voir https://www.indigorose.com/autoplay-media-studio/) qui était probablement développé pour « http://storeysteampowered.tk/ » (ce site n'existe plus)
Cet installateur créera aussi une entrée dans la base de registre afin d'exécuter l'application au démarrage du système:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Steam"="\"C:\\Windows\\TVCS\\Steam Powerd.exe"
```

Au final, les fichiers suivants sont installés dans des répertoires système :

C:\WINDOWS\AppPatch\Music.exe (32745eb47462ebf97116e4f7bae1da66)
C:\WINDOWS\Branding\key.exe (2c9ba2a957e34796558047459da5cd86)
C:\WINDOWS\TVC\Steam.exe (f6eb530e44b03398701d07f2587b1c81)
C:\WINDOWS\TVCS\key.reg (4f29658c17572469adadc00ef52010e3)
C:\WINDOWS\TVCS\Steam Powerd.exe (6addfe3f0ead8a876fbb5acaeb477a34)

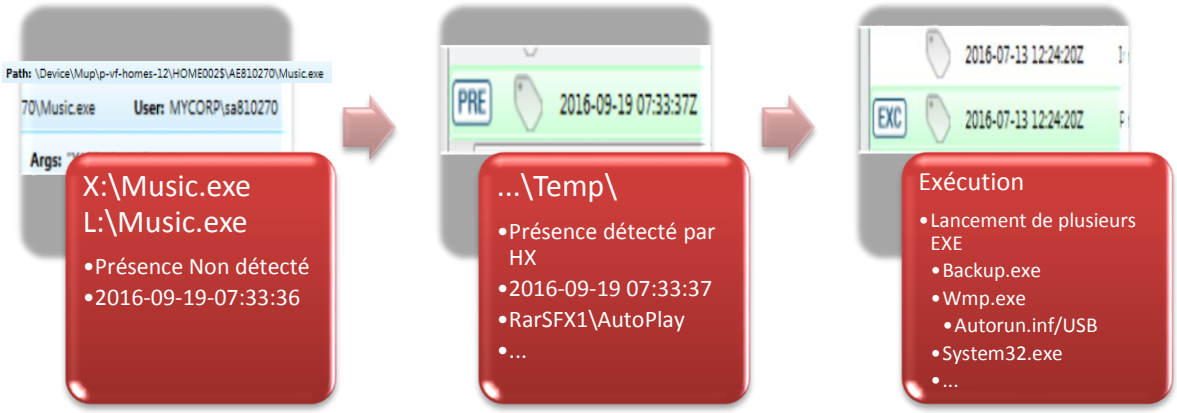
2.1.3. Déclenchement Réponse à Incident

La première attaque a été étiquetée dans le produit FireEye HX par le tag Présence, mais sans le tag exécution alors que dans Redline, le tag exécution est bien présent. Ce point est à remonter à l'éditeur afin de comprendre pourquoi cette erreur d'étiquetage a eu lieu.

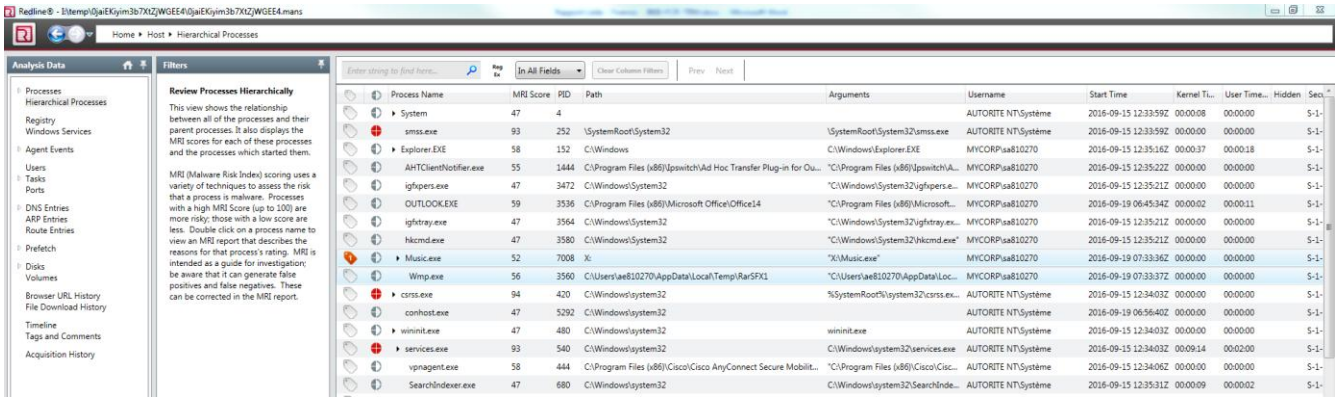
La seconde attaque a permis le déclenchement de la réponse à incident, car les alertes de FireEye HX sont remontées au SIEM Splunk, ce qui n'était pas le cas avec RSA EnVision.

2.1.4. Analyse Redline

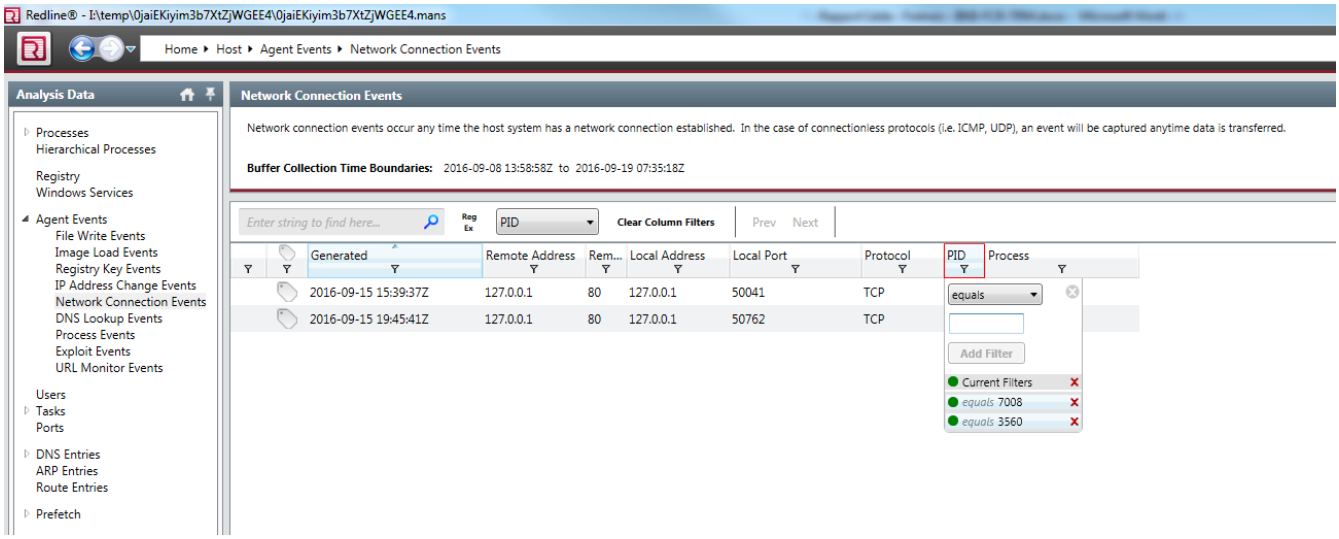
Après avoir analysé le triage récupéré par FireEye HX, nous avons pu établir l'enchaînement des évènements :



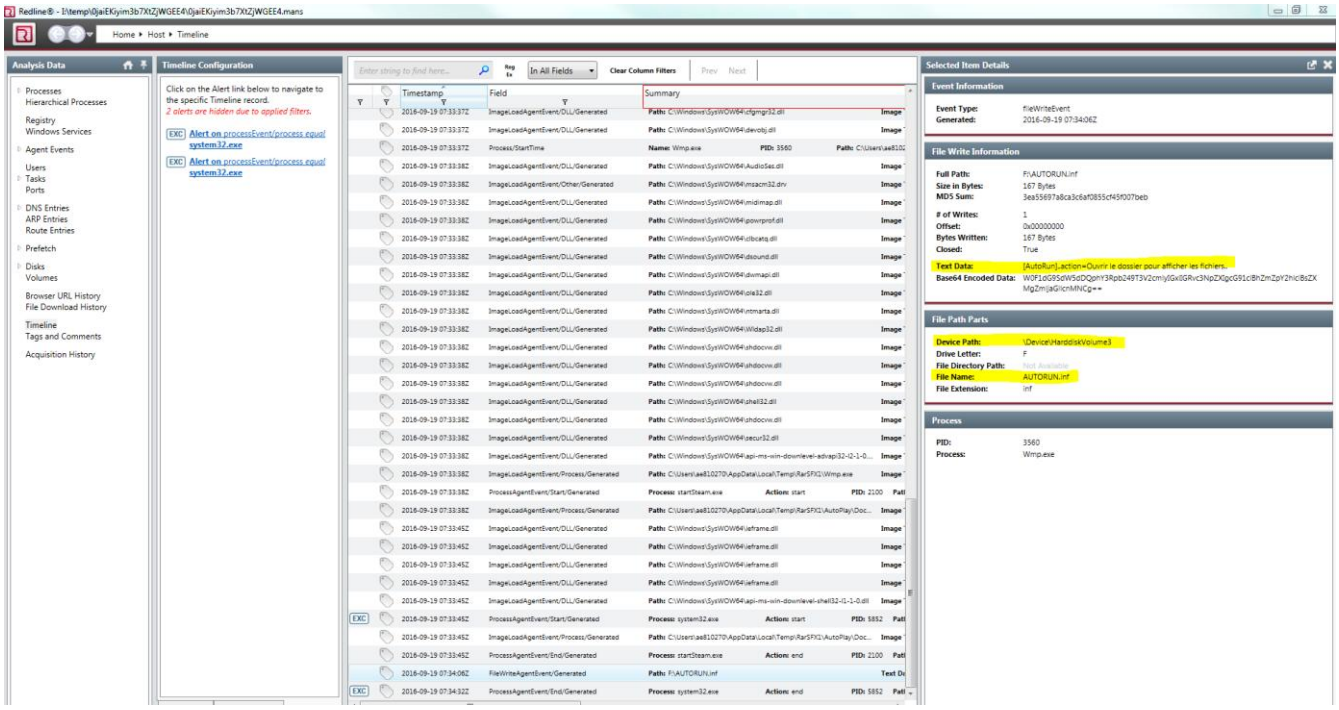
Nous avons aussi pu faire les liens entre plusieurs processus malveillants et comprendre leur hiérarchie.



De plus, nous avons vérifié ***qu'aucune*** communication n'a eu lieu entre les processus malveillants et l'extérieur à la date de l'infection.



Enfin, nous avons identifié le processus de la création d'un *Autorun.inf* qui se lancera lors du prochain branchement du périphérique USB externe.



2.2. Risques

Les risques liés au bon déroulement de l'exécution du malware sont considérés comme important, puisque que son comportement d'autoréplication et sa possibilité de recevoir des commandes depuis un C&C en font un élément dangereux. Il est important de noter que l'emplacement de ces exécutions sur le réseau (criticité du poste ou du réseau) est un facteur important sur la dangerosité de ce malware.

2.3. Impacts

2.3.1. Entreprise

À ce stade, nous n'avons pas d'éléments qui prouvent une sortie d'information via cette infection. Il sera néanmoins conseillé de vérifier l'occurrence des signatures de fichiers malveillants dans le réseau pour empêcher tout problème.

2.3.2. Utilisateur

Les périphériques amovibles qui ont été infectés durant les attaques ont pu permettre la propagation du malware par le branchement de ces périphériques sur d'autres postes.

2.3.3. Machine

Voici les impacts du malware sur la machine :

- L'extraction et l'exécution des exécutables sur les machines a eu lieu.
- Des fichiers autorun.inf ont été écrits sur des périphériques amovibles.
- Nous n'avons identifié aucune modification sur le registre qui vienne de ce malware.

3. Mesures préventives

3.1. Mesures de protection

3.1.1. Entreprise

Les mesures conseillées sont les suivantes :

- Mettre en place d'une sécurité sur le branchement de périphérique extérieur (Disable Autoruns)
- Amélioration de la détection de FireEye (EX/NX/HX) en les informant sur le comportement observé.
- Enregistrement des signatures non connues des fichiers malveillants dans les systèmes FireEye.
- Dans le cas où SEA est impliqué, nous recommandons de prendre des mesures de sécurité élevée. Notamment car la Tunisie fait partie des cibles de ce groupe.

3.1.2. Utilisateur

- Sensibilisation des utilisateurs sur les risques des infections similaires.
- Sensibilisation des utilisateurs sur l'exécution des fichiers avec un Issuer inconnu (Music.exe).
- Vérification des fichiers de l'utilisateur en termes d'intégrité et confidentialité.
- Interroger l'utilisateur pour vérifier ce qu'est devenu la clé USB qui contient ce malware.

3.1.3. Machine

- Formatage de la machine (avec l'option WIPE de préférence).
- Par rapport à la criticité des données, nous recommandons de garder une copie de la machine pour éviter le manque futur d'information afin de pouvoir mener une nouvelle investigation si de nouveaux éléments ou de nouvelles alertes mènent à une nouvelle suspicion.

4. Conclusions

À l'heure actuelle, il n'est pas possible d'affirmer ou d'infirmer que le groupe d'Hacktivistes SEA est à l'origine des 2 attaques de ce rapport. Il est cependant fortement probable qu'il ne soit pas lié vu le peu de ressemblance des preuves acquises durant cette investigation.

L'attribution de l'étiquette SEA par le produit FireEye HX est probablement un faux positif, il faudrait voir avec l'éditeur pour creuser ce point. Le produit se basant sur le comportement du malware et non sur signature, le comportement du malware a pu être considéré comme proche des attaques SEA par le passé.

Cette analyse Forensic permet de dire que c'est plutôt un malware commun, car :

- Il est connu
- Il n'est pas nouveau (apparition en 2012 sur Virus Total)
- L'attaque n'est pas ciblée (la charge utile ne s'est pas exécutée correctement à cause de nombreux facteurs montrant une méconnaissance de l'environnement où il a essayé de s'exécuter).