专注APT攻击与防御

https://micropoor.blogspot.com/

1.是否开启远程桌面，1表示关闭，0表示开启

EXEC master..xp\_regread 'HKEY\_LOCAL\_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server' ,'fDenyTSConnections'

2.读取远程桌面端口

EXEC master..xp\_regread 'HKEY\_LOCAL\_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp','PortNumber'

3.开启远程桌面

EXEC master.dbo.xp\_regwrite'HKEY\_LOCAL\_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG\_DWORD',0;

reg文件开启远程桌面：

Windows Registry Editor Version 5.00HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]"fDenyTSConnections"=dword:00000000[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]"PortNumber"=dword:00000d3d

////

保存micropoor.reg，并执行regedit /s micropoor.reg

注：如果第一次开启远程桌面，部分需要配置防火墙规则允许远程端口。

netsh advfirewall firewall add rule name="Remote Desktop" protocol=TCP dir=in localport=3389 action=allow

4.关闭远程桌面

EXEC master.dbo.xp\_regwrite'HKEY\_LOCAL\_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG\_DWORD',1;

Micropoor