

一分钟免杀cobaltstrike

原创 Kobefanss 小生观察室 前天

收录于话题

#cobaltstrike 1 #免杀 1 #渗透测试 48 #内网安全 3 #代码 2



小生观察室

本观察室仅个人做内容存档使用！

63篇原创内容

公众号

简要介绍

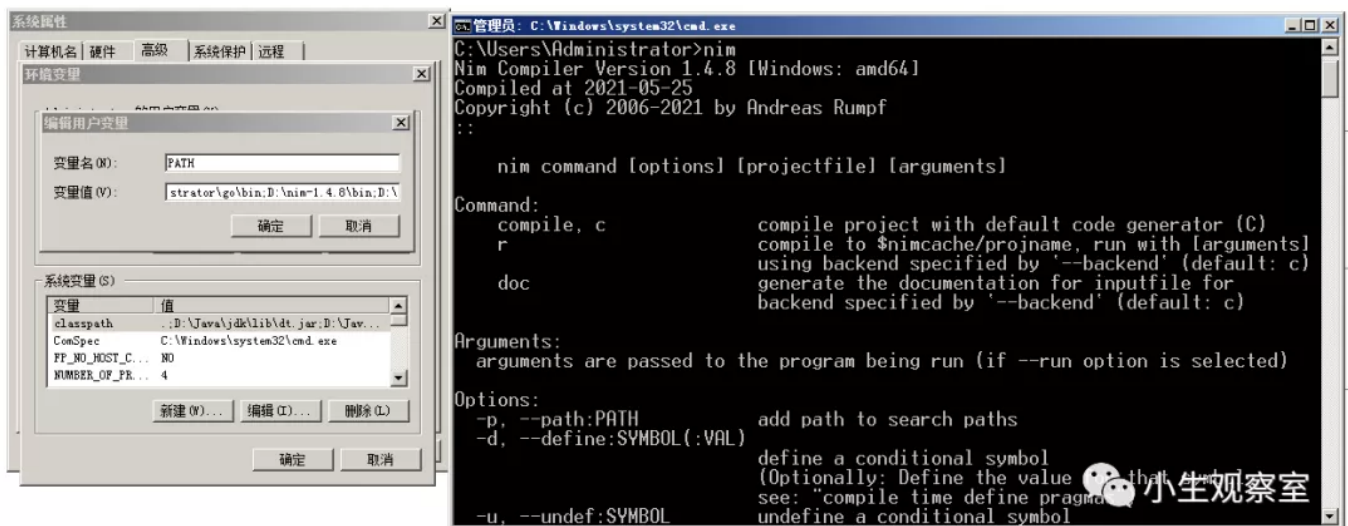
- 本次利用到的是Nim语言
1. Nim 是一门开源的编程语言
 2. Nim 的独到之处在于它可以编译成其他编程语言代码（主要是 C 语言和 JavaScript）
 3. 将 Nim 与 C 语言或 JavaScript 代码集成在一起可以获得最大的价值
 4. Nim 可以生成高质量的 C 语言代码，避免出现 C 语言的典型错误（如内存泄露和数组指针错误）

下载**Nim**安装包

<https://nim-lang.org/install.html>

官方提供Windows、Linux、Mac版本，根据自己的需求进行下载 本次使用Windows环境做演示

下载解压后需将 **bin** 目录添加到环境变量



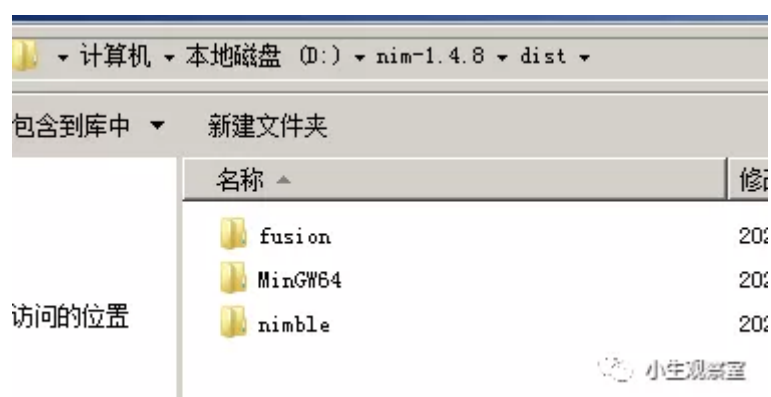
安装C、C++编译器

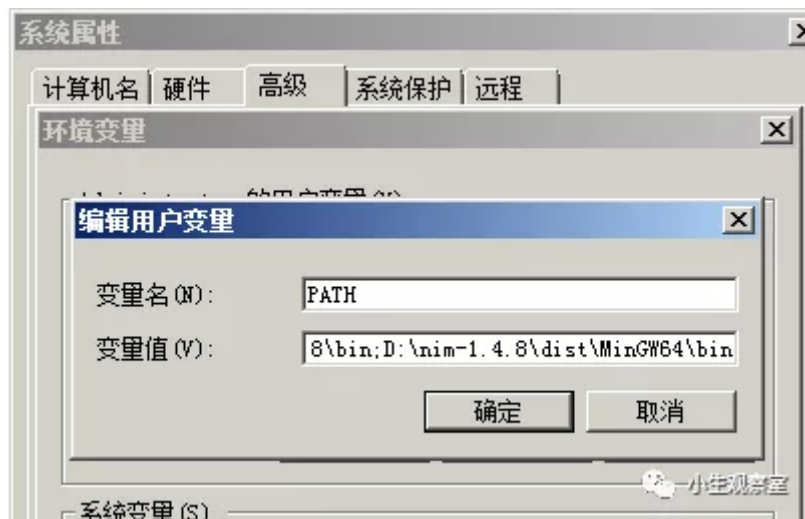
Nim编译器需要C编译器才能编译软件

下载地址

<https://github.com/GorvGoyl/MinGW64/releases>

将文件解压到nim目录的 **dist** 路径下，并将 **D:\nim-1.4.8\dist\MinGW64\bin** 添加至环境变量





encryption编译

下载地址

<https://github.com/aeveryj/NimShellCodeLoader/releases>

下载解压后进入 `NimShellCodeLoader_Winx64\NimShellCodeLoader\encryption` 目录，利用下面的代码进行编译

```
nim c -d:release --opt:size Tdea.nim
nim c -d:release --opt:size Caesar.nim
```

```
C:\Users\Administrator\Downloads\NimShellCodeLoader_Winx64\NimShellCodeLoader\en
cryption>nim c -d:release --opt:size Tdea.nim
Hint: used config file 'D:\nim-1.4.8\config\nim.cfg' [Conf]
Hint: used config file 'D:\nim-1.4.8\config\config.nims' [Conf]
.....CC: des
CC: stdlib_assertions.nim
CC: stdlib_widechars.nim
CC: stdlib_io.nim
CC: stdlib_system.nim
CC: stdlib_math.nim
CC: stdlib_dynlib.nim
CC: stdlib_winlean.nim
CC: stdlib_times.nim
CC: stdlib_random.nim
CC: stdlib_sequils.nim
CC: stdlib_os.nim
CC: stdlib_base64.nim
CC: Tdea.nim

Hint: [Link]
Hint: 44744 lines; 5.919s; 61.109MiB peakmem; Release build; proj: C:\Users\Admi
nistrator\Downloads\NimShellCodeLoader_Winx64\NimShellCodeLoader\encryption\Tdea
.nim; out: C:\Users\Administrator\Downloads\NimShellCodeLoader_Winx64\NimShellCo
deLoader\encryption\Tdea.exe [SuccessX]
```

```
C:\Users\Administrator\Downloads\NimShellCodeLoader_Winx64\NimShellCodeLoader\en
cryption>nim c -d:release --opt:size Caesar.nim
Hint: used config file 'D:\nim-1.4.8\config\nim.cfg' [Conf]
Hint: used config file 'D:\nim-1.4.8\config\config.nims' [Conf]
.....CC: stdlib_assertions.nim
CC: stdlib_widechars.nim
CC: stdlib_io.nim
CC: stdlib_system.nim
CC: stdlib_sequtils.nim
CC: stdlib_math.nim
CC: stdlib_dynlib.nim
CC: stdlib_winlean.nim
CC: stdlib_times.nim
CC: stdlib_random.nim
CC: stdlib_os.nim
CC: stdlib_base64.nim
CC: Caesar.nim

Hint: [Link]
Hint: 44739 lines; 3.344s; 61.184MiB peakmem; Release build; proj: C:\Users\Admi
nistrator\Downloads\NimShellCodeLoader_Winx64\NimShellCodeLoader\encryption\Caes
ar.nim; out: C:\Users\Administrator\Downloads\NimShellCodeLoader_Winx64\NimShell
CodeLoader\encryption\Caesar.exe [SuccessX]
```

免杀详情

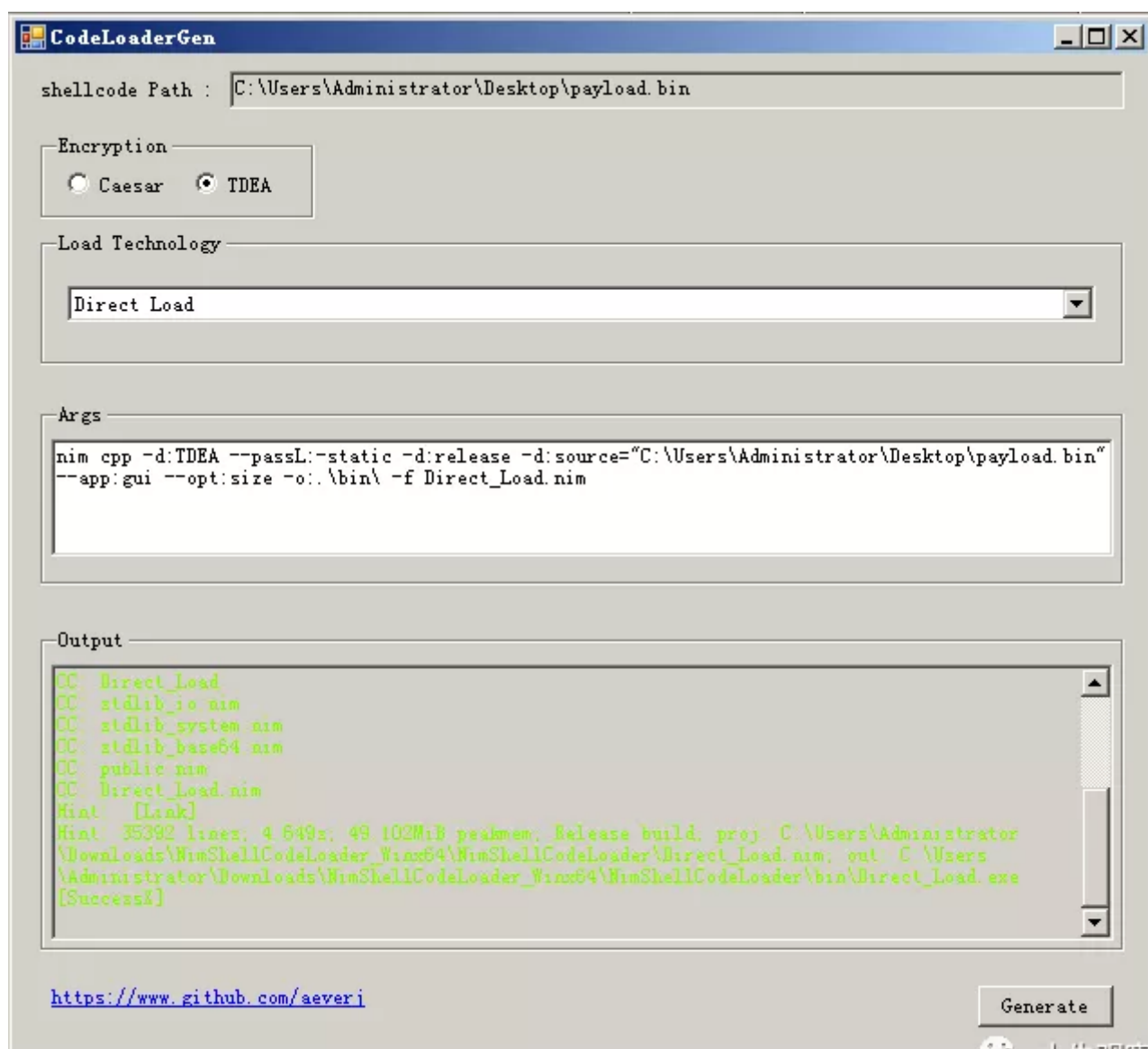
利用 **Nim+NimShellCodeLoader** 可以有10多种免杀方式绕过全网杀软，这里演示其中一种

cobaltstrike生成 raw 格式 64位 的 **payload.bin** 文件

打开 **codeLoader.exe** 图形化界面，将 **payload.bin** 直接拖进来

这里选择的是直接加载 **TDEA -- Direct Load**

选好加载方式和加密方式，点击 **generate** 即可导出



小生观察室

输出生成的可执行文件在 `NimShellCodeLoader_Winx64\NimShellCodeLoader\bin` 目录

最终效果

本地测试火绒、360、管家等均可免杀，并附上VT和CS正常上线结果

external	internal	listener	user	computer	note	process	pid	arch	last
	192.168.2.23	cs4.1		960791		1.exe	7076	x64	02m9

4

166

?

Community Score

① 4 security vendors flagged this file as malicious

02af4be43a8408037ba2a06c7b6415d912fe8876d172a7c0b34291e43d1a7f6

Lexa

64bits assembly overlay peexe

586.26 KB

Size

2021-09-24 06:59:01 UTC

1 minute ago

EXE

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX	① Malicious	Elastic	① Malicious (high Confidence)
ESET-NOD32	① A Variant Of Win64/Injector.FZ	Malwarebytes	① Malware.AI.3139776187
Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClimAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	CrowdStrike Falcon	✓ Undetected

微信搜一搜

Q 小生观察室

小生观察室

喜欢此内容的人还喜欢

【Flink】第二十六篇：源码角度分析Task执行过程

章鱼沉思录

2021年vue和react如何选择

程序那些事儿

springboot 项目敏感信息脱敏实践

地道程序员