

TG 下的 C2 创建过程

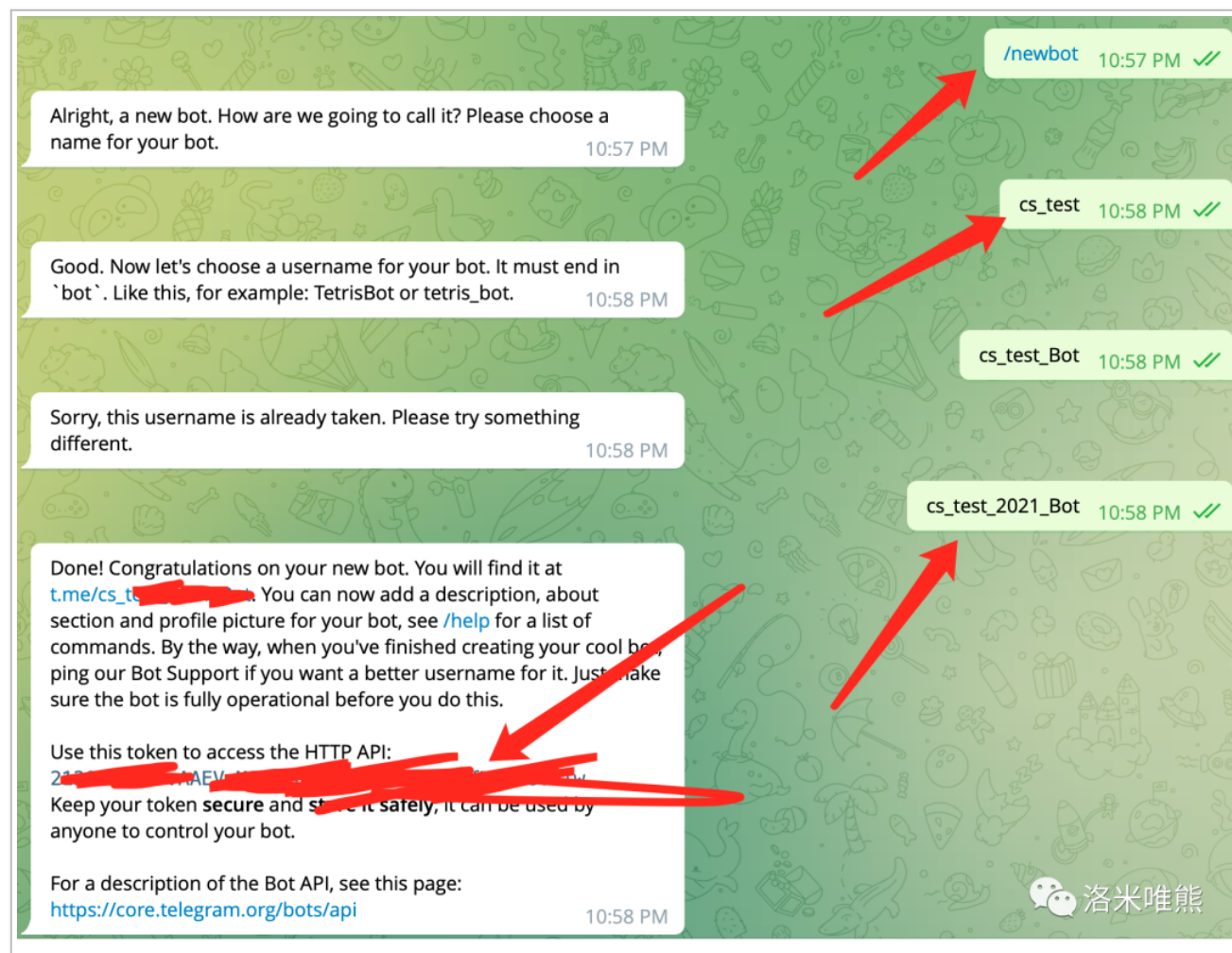
0x00: 简介

没啥新技术，基本就是老技术。我这里只是做笔记，仅供学习。

0x01: 环境部署过程

1、申请 TG token

```
https://telegram.me/botfather
```



这里有 api 的调用文档

<https://core.telegram.org/bots/api>

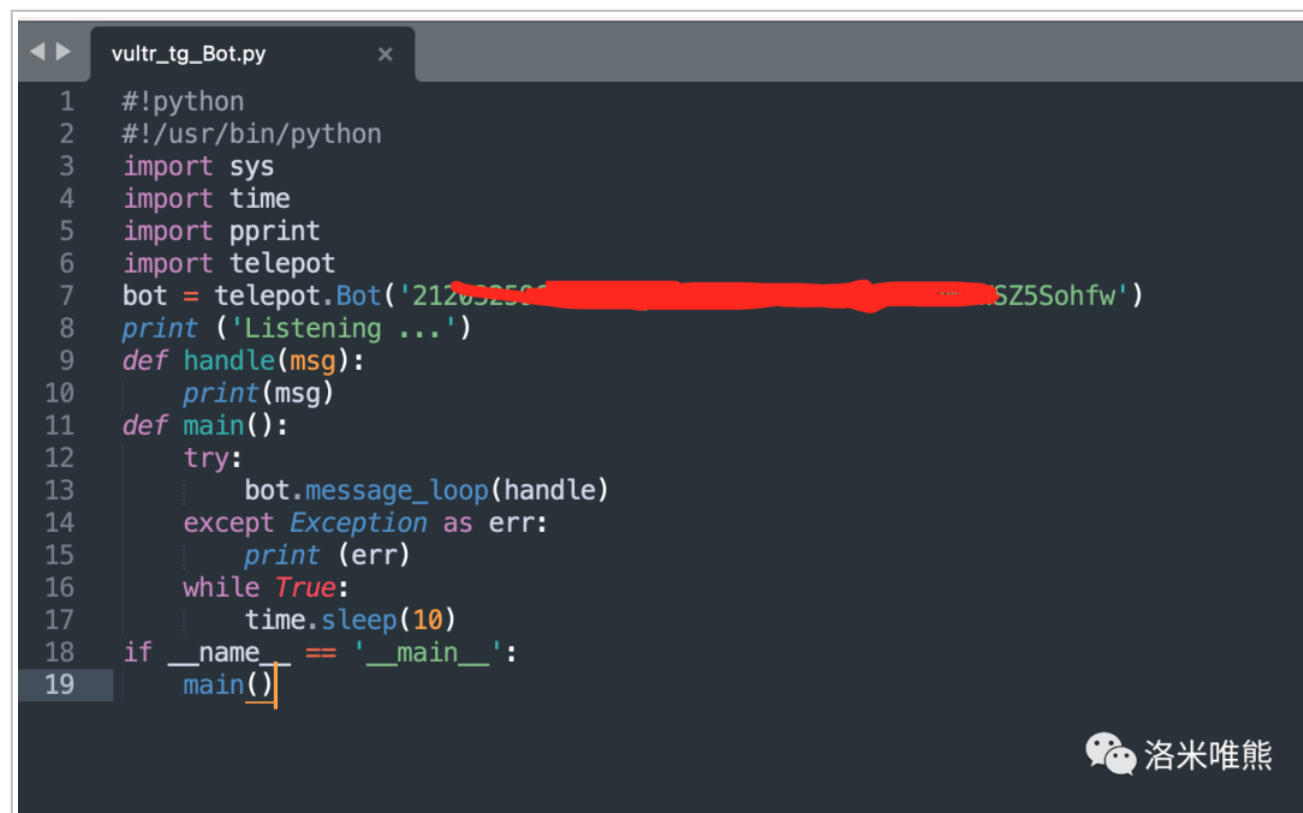
<https://core.telegram.org/bots/api>

2、利用 python 调用

```
#!/python
#!/usr/bin/python
import sys
import time
import pprint
import telepot
bot = telepot.Bot('you-token')
print ('Listening ...')
def handle(msg):
    print(msg)
def main():
    try:
        bot.message_loop(handle)
    except Exception as err:
        print (err)
    while True:
        time.sleep(10)
if __name__ == '__main__':
    main()
```

3、测试 token 调用效果

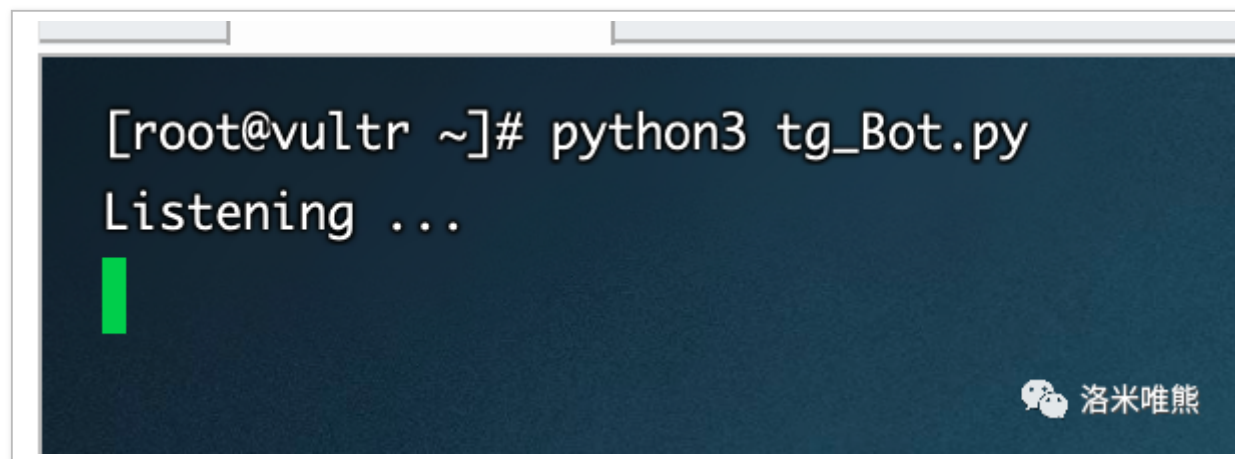
(记得要国外服务器的运行脚本，不然运行没结果。我自己的没结果)



```
1  #!python
2  #!/usr/bin/python
3  import sys
4  import time
5  import pprint
6  import telepot
7  bot = telepot.Bot('21203250' 'SZ5Sohfw')
8  print ('Listening ...')
9  def handle(msg):
10     print(msg)
11  def main():
12     try:
13         bot.message_loop(handle)
14     except Exception as err:
15         print (err)
16     while True:
17         time.sleep(10)
18  if __name__ == '__main__':
19     main()
```

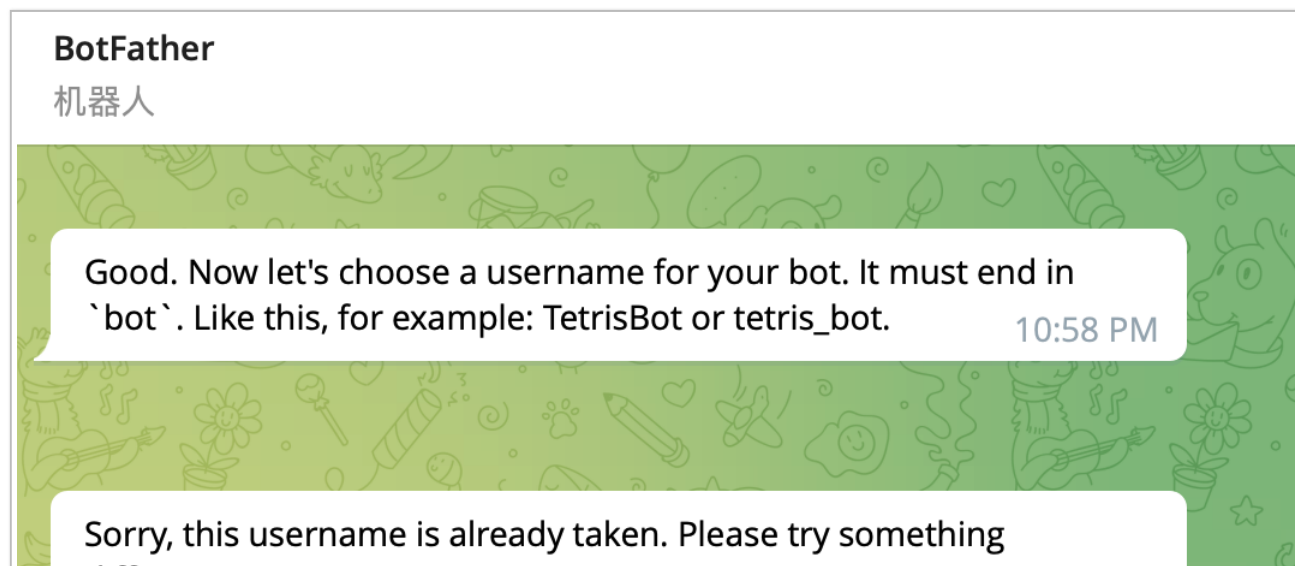
服务器上运行

```
[root@vultr ~]# python3 tg_Bot.py
Listening ...
```

A terminal window with a dark blue background. The prompt is [root@vultr ~]#. The command python3 tg_Bot.py has been executed, and the output is Listening ... followed by a green cursor bar. In the bottom right corner, there is a small logo of a bear and the text 洛米唯熊.

洛米唯熊

到 TG 上去对你的机器人说话



different.

10:58 PM



Done! Congratulations on your new bot. You will find it at t.me/your_bot. You can now add a description, about section and profile picture for your bot, see [/help](#) for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:

21205[REDACTED]

Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page:

<https://core.telegram.org/bots/api>

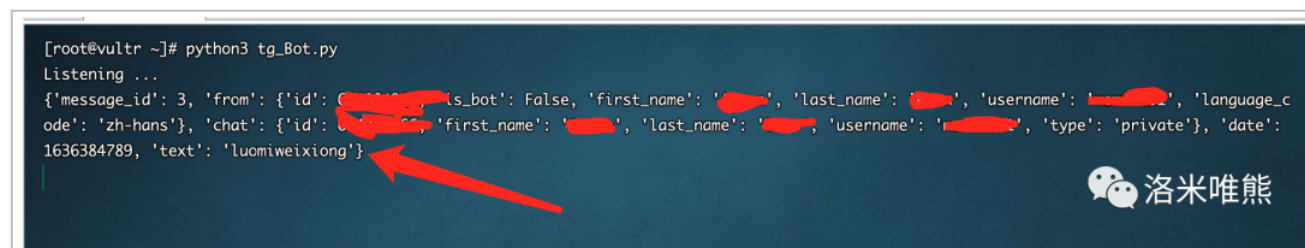
10:58 PM

洛米唯熊



Python 脚本看到你的消息

```
[root@vultr ~]# python3 tg_Bot.py
Listening ...
{'message_id': 3, 'from': {'id': '123456789', 'is_bot': False, 'first_name': '洛米', 'last_name': '唯熊', 'username': 'luomiweixiong', 'language_code': 'zh-hans'}, 'chat': {'id': '123456789', 'first_name': '洛米', 'last_name': '唯熊', 'username': 'luomiweixiong', 'type': 'private'}, 'date': 1636384789, 'text': 'luomiweixiong'}
```



4、服务端到客户端

PS: 建议看一下 API 文档在来看

提取文字消息

使用 glance() 可以从接收的消息中提取一个元组

-

```
(content_type, chat_type, chat_id)
```

content_type 包括

```
text, audio, document, photo, sticker, video, voice, contact, location, venue, new_chat_member, left_chat_member, etc.
```

chat_type 包括

```
private, group, or channel.
```

所以我们可以使用 glance() 把接收的文字消息提取出来，代码如下：

```
#!/python
#!/usr/bin/python
import sys
import time
import pprint
import telepot
bot = telepot.Bot('you-token')
print ('Listening ...')
def handle(msg):
    content_type, chat_type, chat_id = telepot.glance(msg)

    if content_type == 'text':
        received_command = msg['text']
        print (received_command)
    else:
        print (content_type, chat_type, chat_id)
        return
def main():
    try:
        bot.message_loop(handle)
    except Exception as err:
        print (err)
    while True:
        time.sleep(10)

if __name__ == '__main__':
    main()
```

The image shows a Telegram bot interface on the left and a terminal window on the right. The Telegram bot interface, titled 'cs_test 机器人', displays a chat history with messages: '/start 10:58 PM', 'Jaky 11:12 PM', 'luomiweixiong 11:19 PM', 'demo 11:24 PM', 'hello jaky 11:32 PM', and 'hello jaky 11:37 PM'. A red arrow points from the 'hello jaky 11:37 PM' message to the terminal window. The terminal window, titled '1 vultr', shows the command '[root@vultr ~]# python3 tg_Bot_cs.py' and the output 'Listening ...' and 'hello jaky'. A red arrow points from the 'hello jaky' output to the Telegram chat history. The terminal also displays system information: '运行 31 分', '负载 0.02, 0.09, 0.12', 'CPU 7%', '内存 30% 293M/990M', '交换 0% 0/0', and a table of running processes.

内存	CPU	命令
5.9M	1	sshd
2.9M	0.3	top
16M	0.3	python3
6.5M	0	systemd

The terminal also shows a file system tree for the root directory:

路径	可用/大小
/dev	485M/485M
/dev/shm	495M/495M
/run	482M/495M
/sys/fs/cgroup	495M/495M
/	20.4G/23.4G
/run/user/0	99M/99M

The terminal also shows a file system tree for the root directory:

文件名
.pki
.bash_logo
.bash_profi
.bashrc
cshrc
cs.py
tg_Bot_cs.py
tg_Bot.py

接收文件

执行接收消息的 python 代码，可获得接收文件的消息格式.

下载文件需要使用

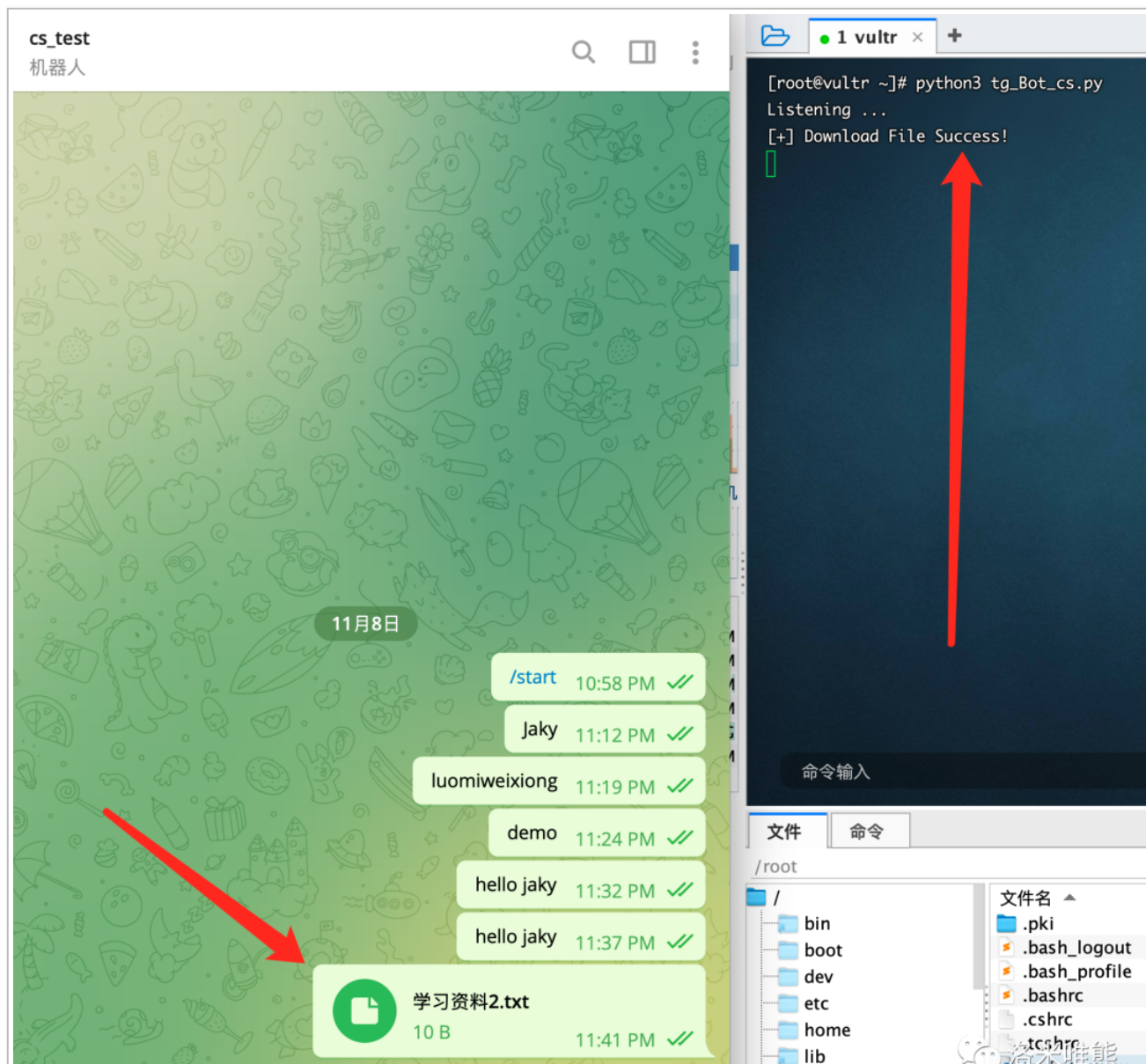
```
bot.download_file(file_id, filename)
```

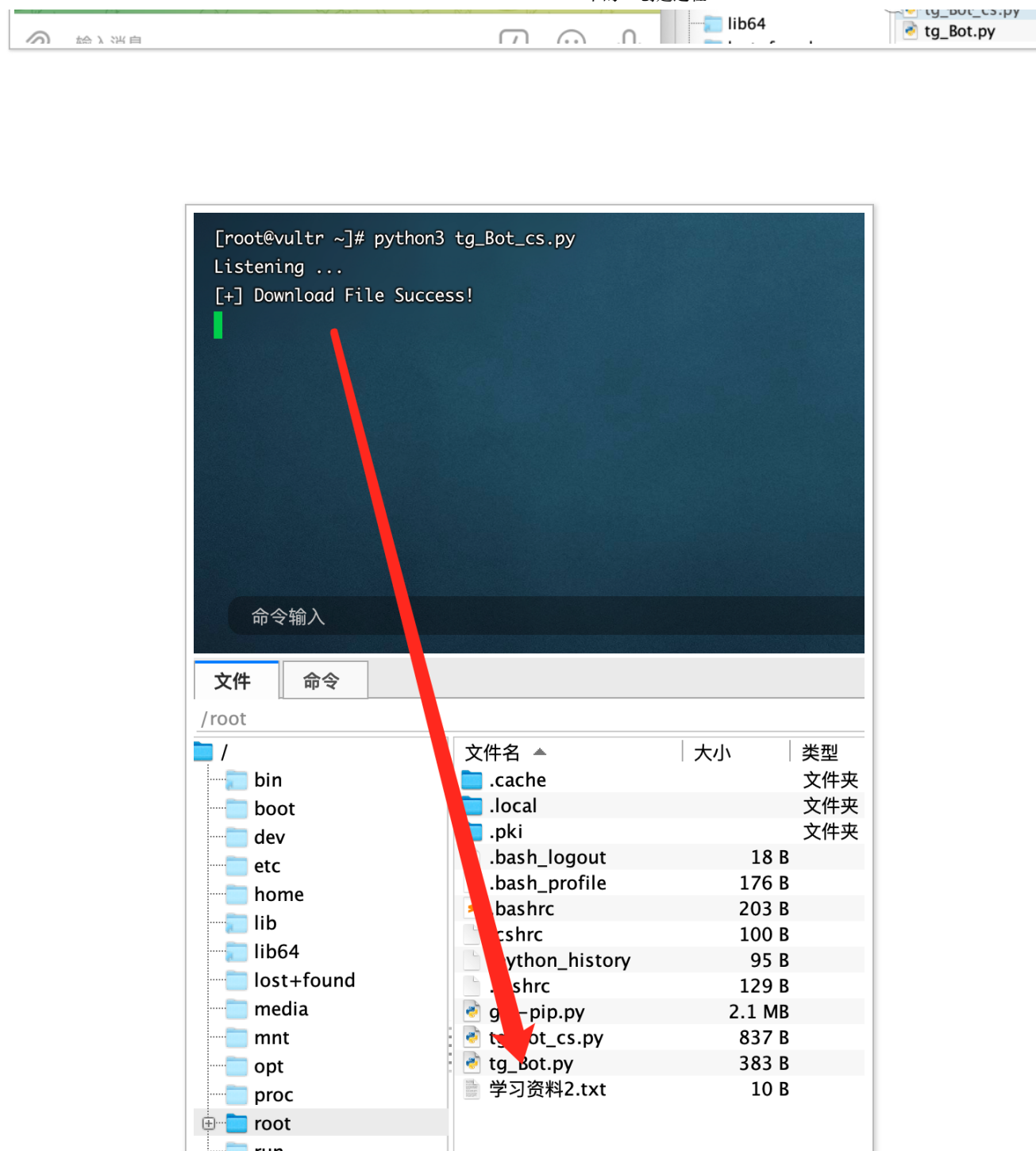
```
#!/python
#!/usr/bin/python
import sys
import time
import pprint
import telepot
bot = telepot.Bot('you-token')
print ('Listening ...')
def handle(msg):
    content_type, chat_type, chat_id = telepot.glance(msg)

    if content_type == 'text':
        received_command = msg['text']
        print (received_command)
    elif content_type == 'document':
        file_id = msg['document']['file_id']
        filename = msg['document']['file_name']
        bot.download_file(file_id, filename)
        print ("[+] Download File Success!")
    else:
        print (content_type, chat_type, chat_id)
        return
def main():
    try:
        bot.message_loop(handle)
    except Exception as err:
        print (err)
```

```
while True:
    time.sleep(10)

if __name__ == '__main__':
    main()
```







5、客户端到服务端

发送消息使用

```
bot.sendMessage(chat_id, message)
```

向 Server 端发送一条消息，代码如下

```
#!/python
import telepot
from pprint import pprint
bot = telepot.Bot('you-token')
bot.sendMessage(id, 'Hello C2 Server Jaky')
```

id 换成你自己的 ID



The screenshot displays a remote terminal interface with three main sections:

- Left Panel (cs_test 机器人):** Contains a green patterned background. A red arrow points to the bottom of this panel.
- Top Right Panel (System Information):** Displays system status for 'cs_test 机器人'.
 - 同步状态: ●
 - IP: [redacted] 复制
 - 系统信息
 - 运行 42 分
 - 负载 0.07, 0.10, 0.13
 - CPU: 9%
 - 内存: 29% 282M/990M
 - 交换: 0% 0/0
 - Table of running processes:

内存	CPU	命令
5.9M	1	sshd
0	0.3	kworker/0:3
6.5M	0	systemd
0	0	kthreadd

- Network graph for eth0 showing 8K upload and 4K download.

- Right Panel (Terminal):** Shows a terminal window with the command `python3 tg_Bot_server.py` being executed. A red arrow points to the command. Below the terminal is a file explorer showing the root directory with various files and folders.



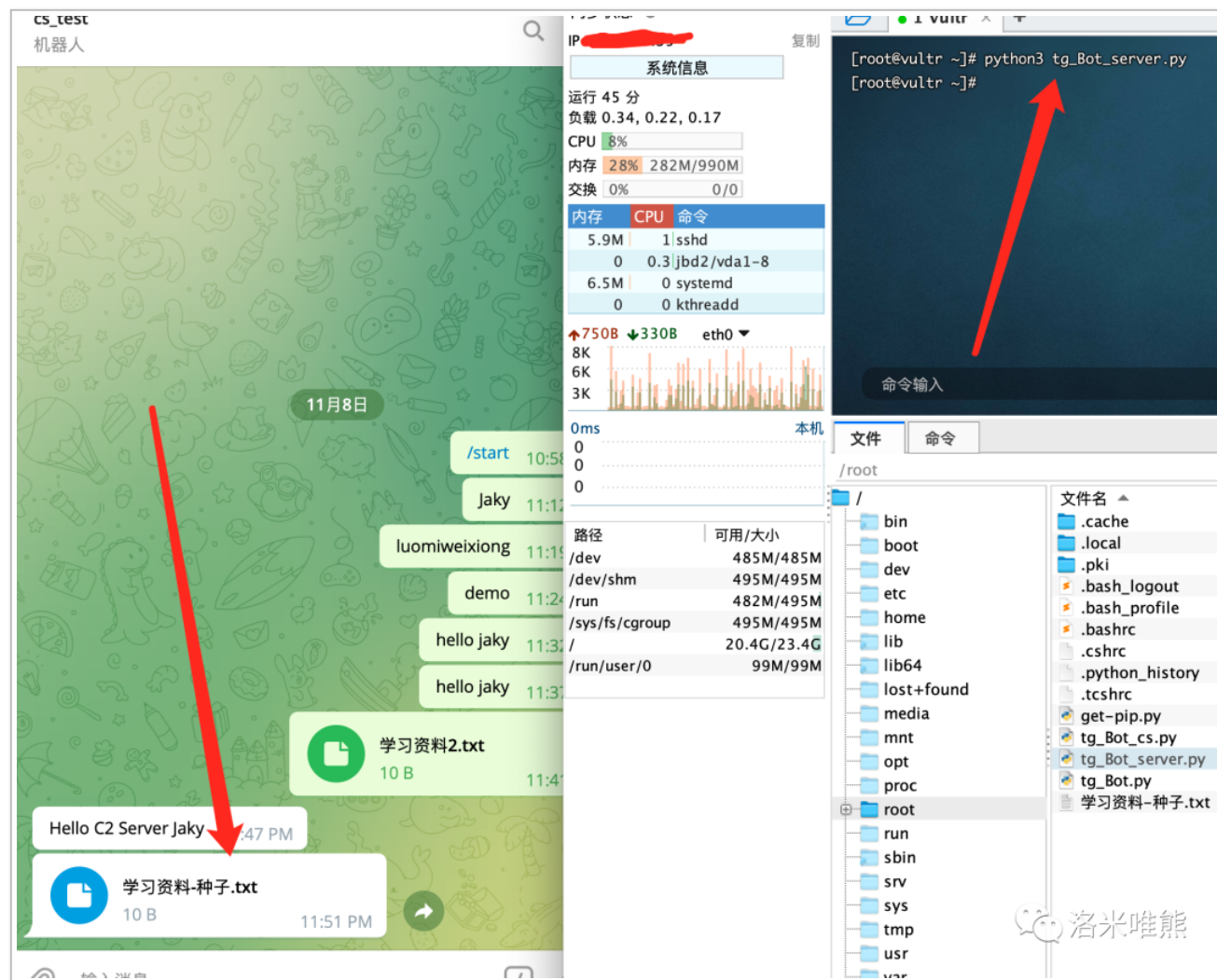
发送文件使用

```
bot.sendDocument(chat_id,file)
```

代码如下：

```
#!/python
import telepot
from pprint import pprint
bot = telepot.Bot('you-token')
f = open('/root/学习资料-种子.txt', 'rb')
bot.sendDocument(id, f)
```

id 换成你自己的 ID



0x02: 环境测试过程

1、搭建 C2 Server

```
git clone https://github.com/blazeinfosec/bt2.git
```

2、编辑参数

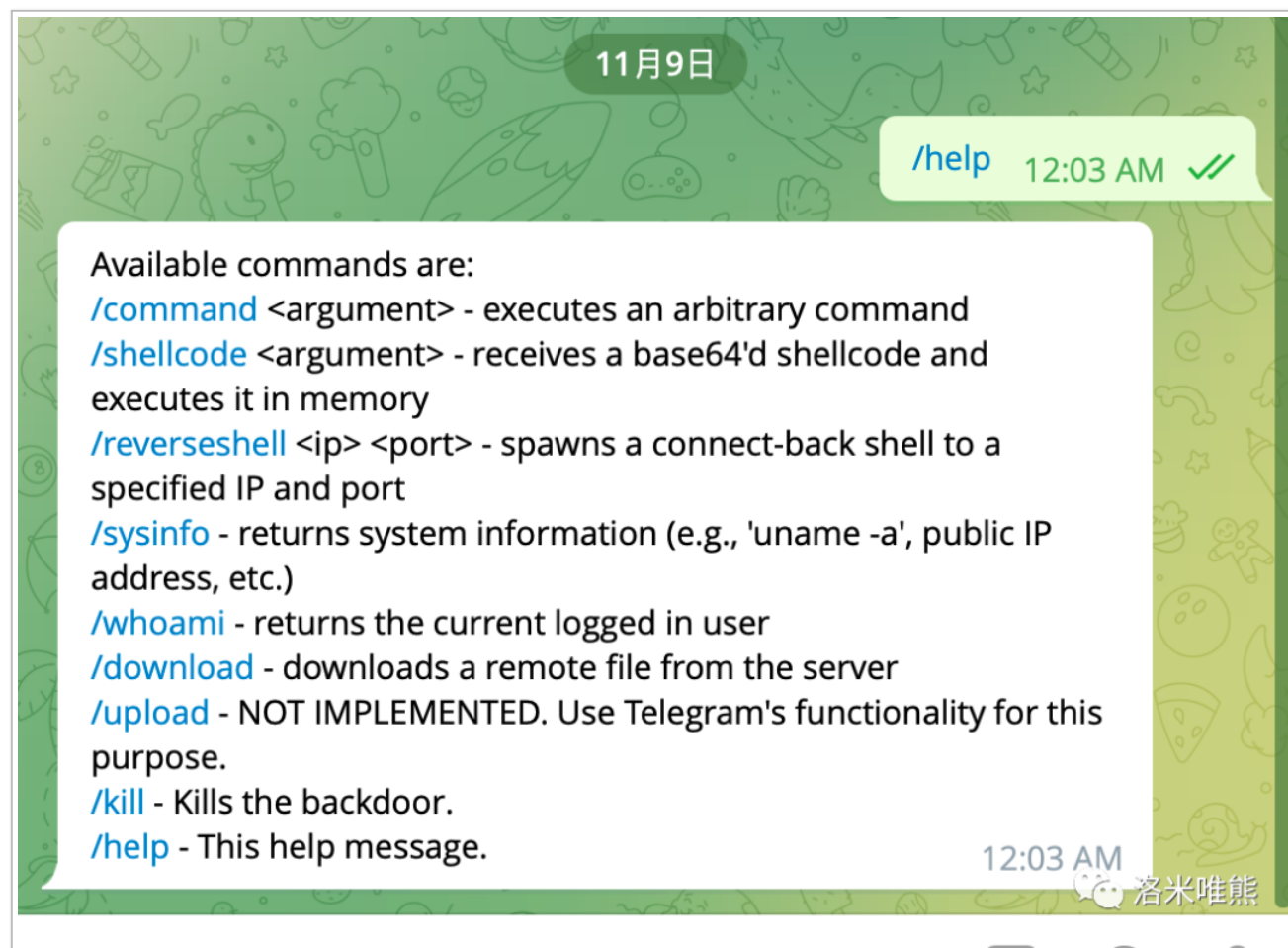
编辑 **bt2.py**

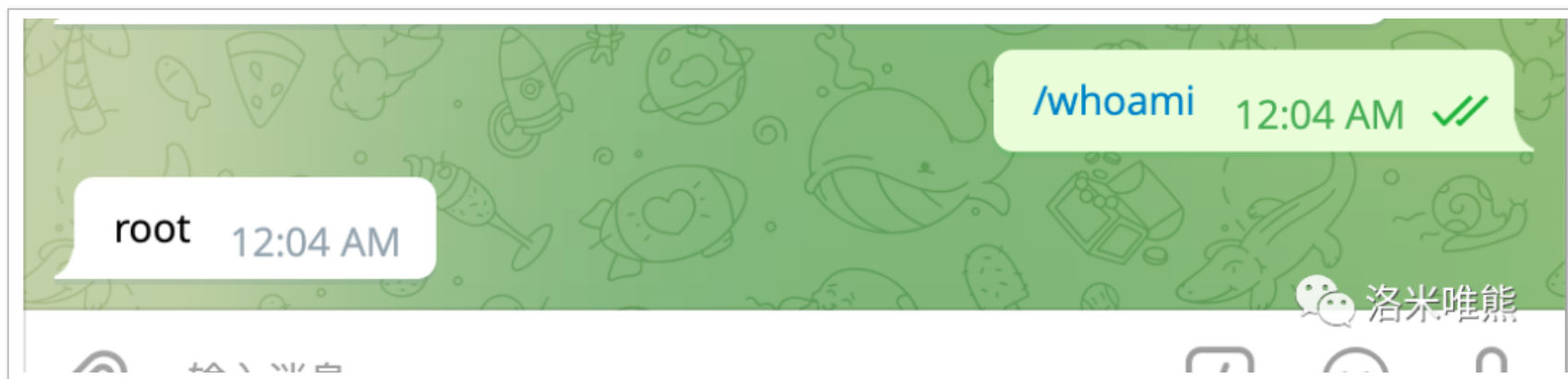
设置以下参数

```
API_TOKEN: token  
BOTMASTER_ID: 自己帐号的id
```

A terminal window with a dark blue background and white text. The prompt is [root@vultr bt2]#. The command entered is python bt2.py. To the right of the command, there is a small circular icon with a skull and crossbones, followed by the text 洛米唯熊.

```
[root@vultr bt2]# python bt2.py 洛米唯熊
```





接下来就可以去 python 代码里扩展 CS 上线了