Hunting malware with a chatbot

Rémi Chipaux, @futex90

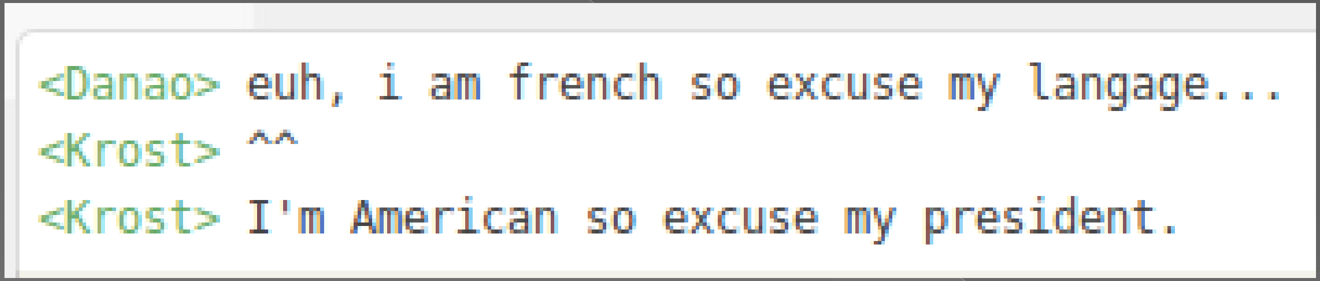
BSIDES LUXEMBOURG

$ whoami

- Security consultant at itrust consulting (itrust.lu/malware.lu)
- Malware analyst
- Penetration tester
- CTF player
- Zythologue

$ Cocoricoo

- Soriz hi'm franch



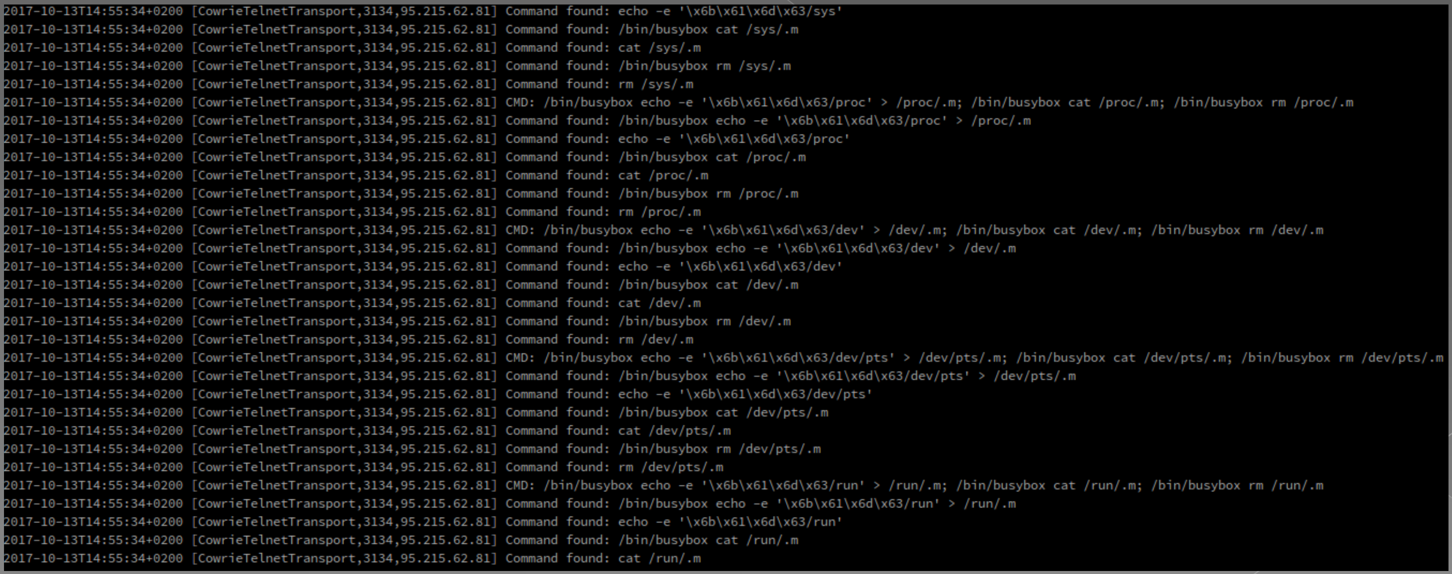
```
<Danao> euh, i am french so excuse my langage...
<Krost> ^^
<Krost> I'm American so excuse my president.
```

$ Hunting malware

- For fun and curiosity
- Understand what attackers are doing
- Following the attacks
- Find new stuff

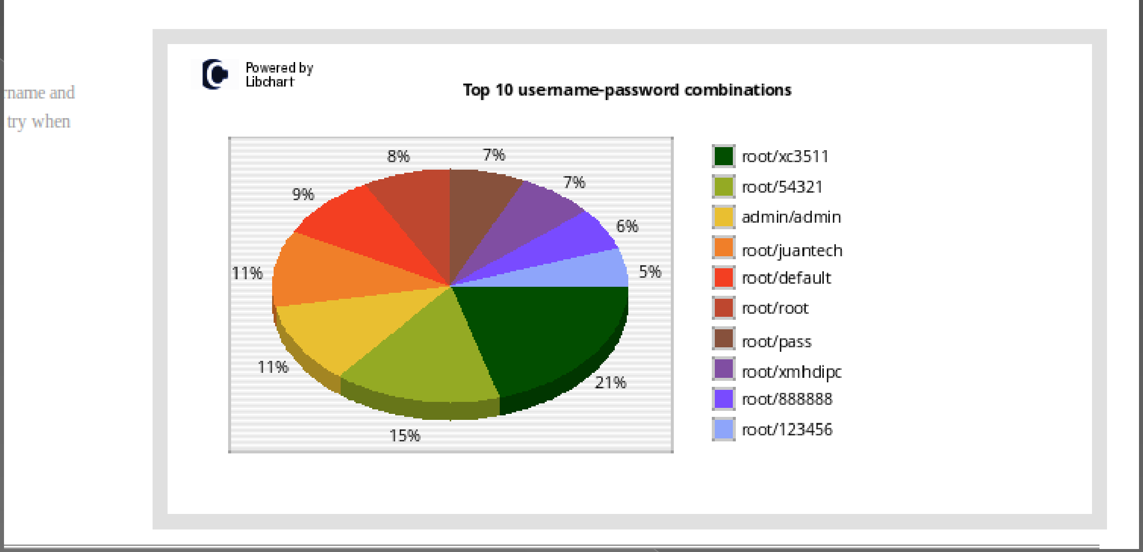
$ Honeypots

- A RaspberryPI
- Cowrie SSH/Telnet Honeypots
- Capture commands and malwares



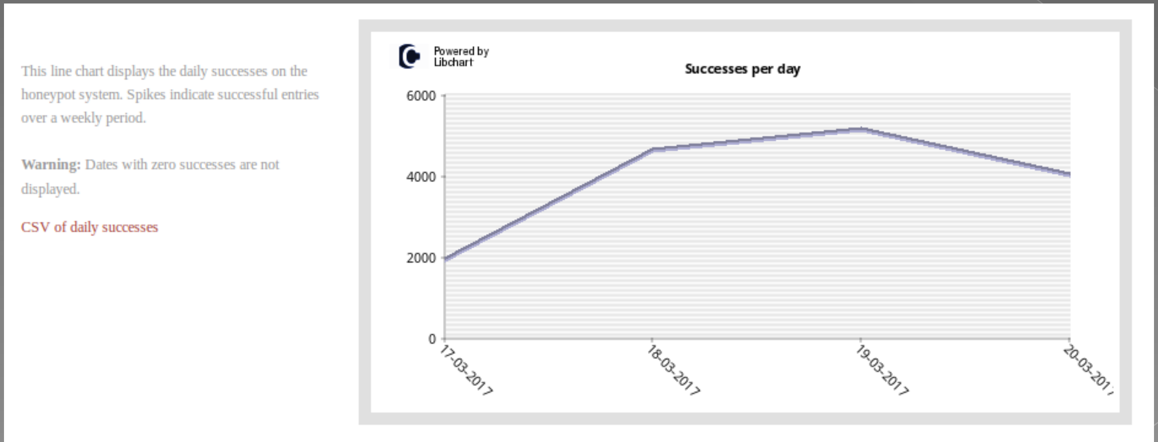
```
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: echo -e '\x6b\x61\x6d\x63/sys'
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox cat /sys/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: cat /sys/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox rm /sys/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: rm /sys/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] CMD: /bin/busybox echo -e '\x6b\x61\x6d\x63/proc' > /proc/.m; /bin/busybox cat /proc/.m; /bin/busybox rm /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox echo -e '\x6b\x61\x6d\x63/proc' > /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: echo -e '\x6b\x61\x6d\x63/proc'
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox cat /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: cat /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox rm /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: rm /proc/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] CMD: /bin/busybox echo -e '\x6b\x61\x6d\x63/dev' > /dev/.m; /bin/busybox cat /dev/.m; /bin/busybox rm /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox echo -e '\x6b\x61\x6d\x63/dev' > /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: echo -e '\x6b\x61\x6d\x63/dev'
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox cat /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: cat /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox rm /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: rm /dev/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] CMD: /bin/busybox echo -e '\x6b\x61\x6d\x63/dev/pts' > /dev/pts/.m; /bin/busybox cat /dev/pts/.m; /bin/busybox rm /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox echo -e '\x6b\x61\x6d\x63/dev/pts' > /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: echo -e '\x6b\x61\x6d\x63/dev/pts'
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox cat /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: cat /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox rm /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: rm /dev/pts/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] CMD: /bin/busybox echo -e '\x6b\x61\x6d\x63/run' > /run/.m; /bin/busybox cat /run/.m; /bin/busybox rm /run/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox echo -e '\x6b\x61\x6d\x63/run' > /run/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: echo -e '\x6b\x61\x6d\x63/run'
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: /bin/busybox cat /run/.m
2017-10-13T14:55:34+0200 [CowrieTelnetTransport,3134,95.215.62.81] Command found: cat /run/.m
```

$ Kippo graph



name and

try when

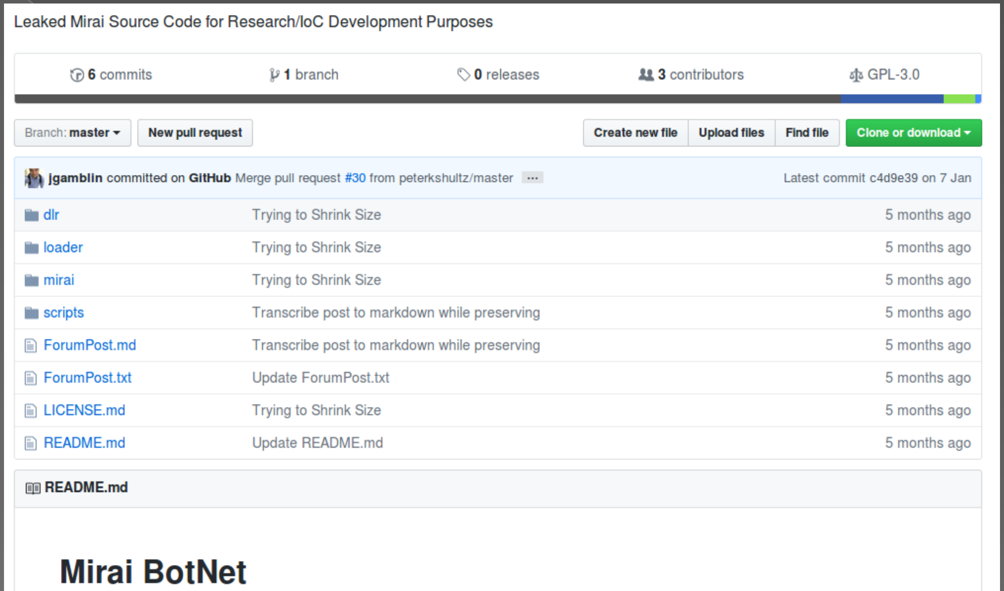


This line chart displays the daily successes on the honeypot system. Spikes indicate successful entries over a weekly period.

Warning: Dates with zero successes are not displayed.

CSV of daily successes

$ Mirai, XorDDos, Gafgyt..



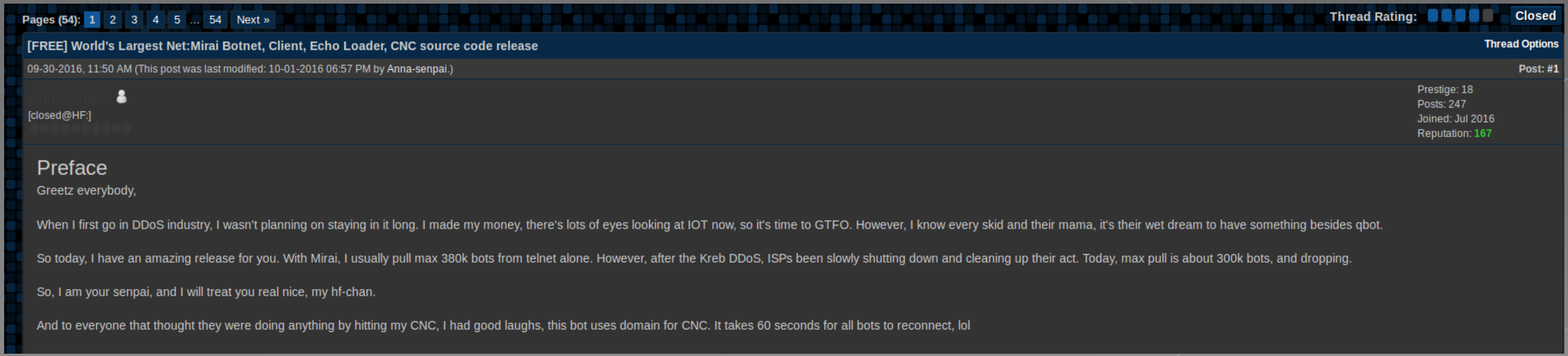
Leaked Mirai Source Code for Research/IoC Development Purposes

jgamblin committed on GitHub Merge pull request #30 from peterkshultz/master … Latest commit c4d9e39 on 7 Jan

dlr	Trying to Shrink Size	5 months ago
loader	Trying to Shrink Size	5 months ago
mirai	Trying to Shrink Size	5 months ago
scripts	Transcribe post to markdown while preserving	5 months ago
ForumPost.md	Transcribe post to markdown while preserving	5 months ago
ForumPost.txt	Update ForumPost.txt	5 months ago
LICENSE.md	Trying to Shrink Size	5 months ago
README.md	Update README.md	5 months ago

README.md

Mirai BotNet



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

09-30-2016, 11:50 AM (This post was last modified: 10-01-2016 06:57 PM by Anna-senpai.)

Post: #1

Anna-senpai
[closed@HF:]

Prestige: 18
Posts: 247
Joined: Jul 2016
Reputation: 167

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's time to GTFO. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISPs been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

And to everyone that thought they were doing anything by hitting my CNC, I had good laughs, this bot uses domain for CNC. It takes 60 seconds for all bots to reconnect, lol

$ Limitations

- One honeypot is small
- But more, can be hard to follow
- Linux malware is easy to reverse (become boring)
- A lot of malware to analyse, so it must be automated

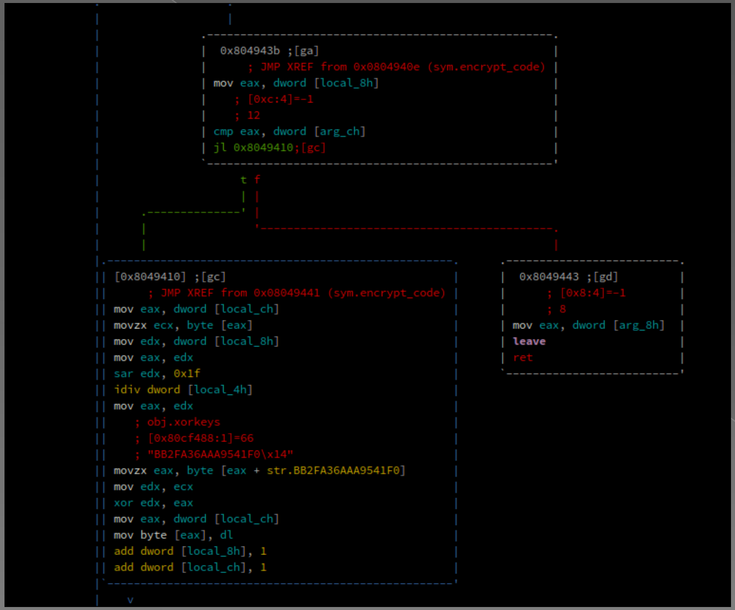
$ Radare2

- Reverse engineering framework
- x86, amd64, arm, mips, *.*
- Exploits
- Malware analysis
- Run on Windows, Linux, Mac
- Scripts in python (r2pipe module)

```
Megabeets$ r2 -
-- Welcome to IDA 10.0.
```

$ Automatisation

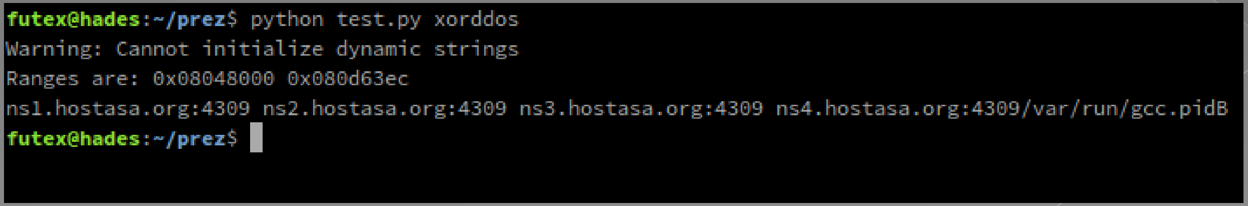
- XorDDOS encrypt is c&c address with a hardcoded xor key



```
 0x804943b ;[ga]
     ; JMP XREF from 0x0804940e (sym.encrypt_code)
mov eax, dword [local_8h]
   ; [0xc:4]=-1
   ; 12
cmp eax, dword [arg_ch]
jl 0x8049410;[gc]
```

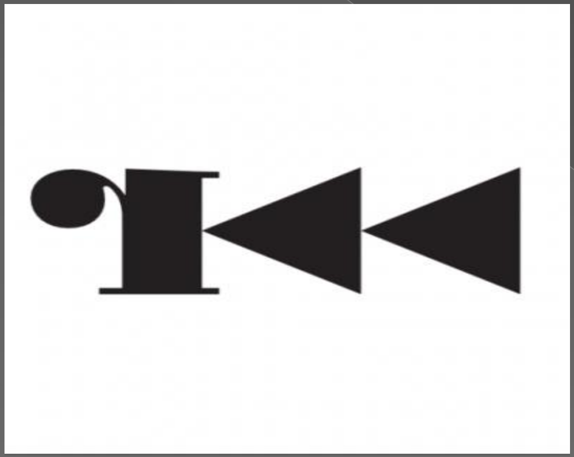
```
[0x8049410] ;[gc]
     ; JMP XREF from 0x08049441 (sym.encrypt_code)
mov eax, dword [local_ch]
movzx ecx, byte [eax]
mov edx, dword [local_8h]
mov eax, edx
sar edx, 0x1f
idiv dword [local_4h]
mov eax, edx
   ; obj.xorkeys
   ; [0x80cf488:1]=66
   ; "BB2FA36AAA9541F0\x14"
movzx eax, byte [eax + str.BB2FA36AAA9541F0]
mov edx, ecx
xor edx, eax
mov eax, dword [local_ch]
mov byte [eax], dl
add dword [local_8h], 1
add dword [local_ch], 1
```

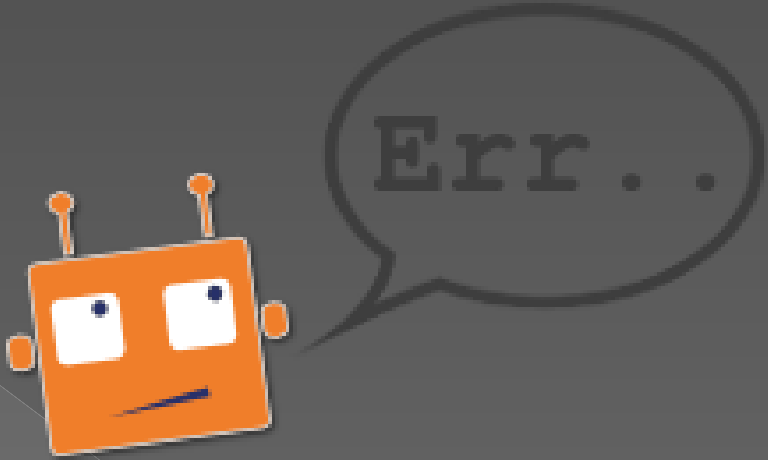
```
 0x8049443 ;[gd]
     ; [0x8:4]=-1
     ; 8
mov eax, dword [arg_8h]
leave
ret
```



```
futex@hades:~/prez$ python test.py xorddos
Warning: Cannot initialize dynamic strings
Ranges are: 0x08048000 0x080d63ec
ns1.hostasa.org:4309 ns2.hostasa.org:4309 ns3.hostasa.org:4309 ns4.hostasa.org:4309/var/run/gcc.pidB
futex@hades:~/prez$
```

$ Make Bots Great Again



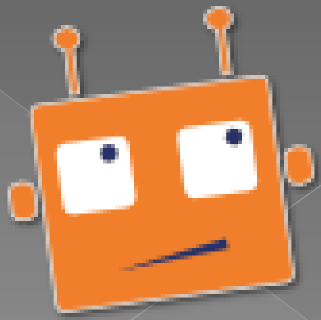


$ First create the bot

- You have to deal with @BotFather
- Send /newbot command, you will receive a token

$Errbot

- Easy to install
- Easy to develop plugins in python3
- Supports a lot of chat protocols
  - Telegram
  - IRC
  - HipChat
  - Slack
  - XMPP
  - Gitter …



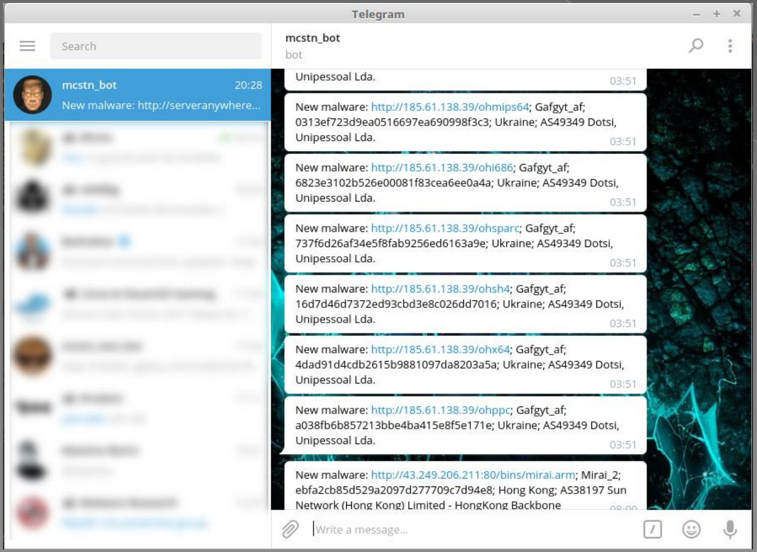
$ Errbot installation

- sudo pip3 install errbot && pip3 install python-telegram-bot && errbot --init
- Config file config.py

```
BACKEND = 'Telegram‘

ID = ‘BOT_ID’

BOT_DATA_DIR = r'/home/futex/errbot/data'
BOT_EXTRA_PLUGIN_DIR = '/home/futex/errbot/plugins'

BOT_LOG_FILE = r'/home/futex/errbot/errbot.log'
BOT_LOG_LEVEL = logging.DEBUG

BOT_ADMINS = (‘MY_TELEGRAM_ID’, )

BOT_IDENTITY = {
    'token': ID,
}

BOT_PREFIX = "/"
```

$ Telegram

- Each new sample is notified by the bot
- Dowloaded through tor
- Automatically uploaded to VirusTotal and linux.huntingmalware.com



Unipessoal Lda. 03:51

New malware: http://185.61.138.39/ohmips64; Gafgyt_af; 0313ef723d9ea0516697ea690998f3c3; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

New malware: http://185.61.138.39/ohi686; Gafgyt_af; 6823e3102b526e00081f83cea6ee0a4a; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

New malware: http://185.61.138.39/ohsparc; Gafgyt_af; 737f6d26af34e5f8fab9256ed6163a9e; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

New malware: http://185.61.138.39/ohsh4; Gafgyt_af; 16d7d46d7372ed93cbd3e8c026dd7016; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

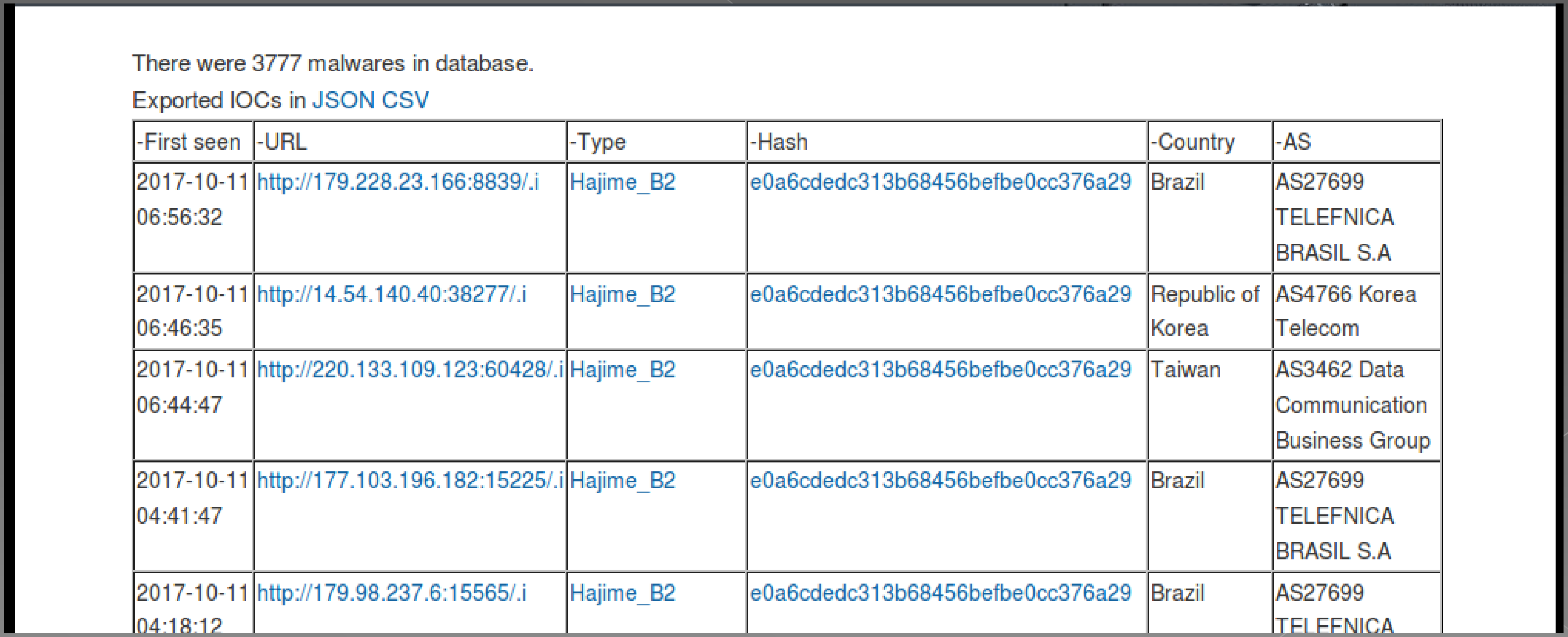
New malware: http://185.61.138.39/ohx64; Gafgyt_af; 4dad91d4cdb2615b9881097da8203a5a; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

New malware: http://185.61.138.39/ohppc; Gafgyt_af; a038fb6b857213bbe4ba415e8f5e171e; Ukraine; AS49349 Dotsi, Unipessoal Lda. 03:51

New malware: http://43.249.206.211:80/bins/mirai.arm; Mirai_2; ebfa2cb85d529a2097d277709c7d94e8; Hong Kong; AS38197 Sun Network (Hong Kong) Limited - HongKong Backbone 08:00

$ Tracker

- https://futex.re/tracker/index.php
- IOC are exported in JSON and CSV format



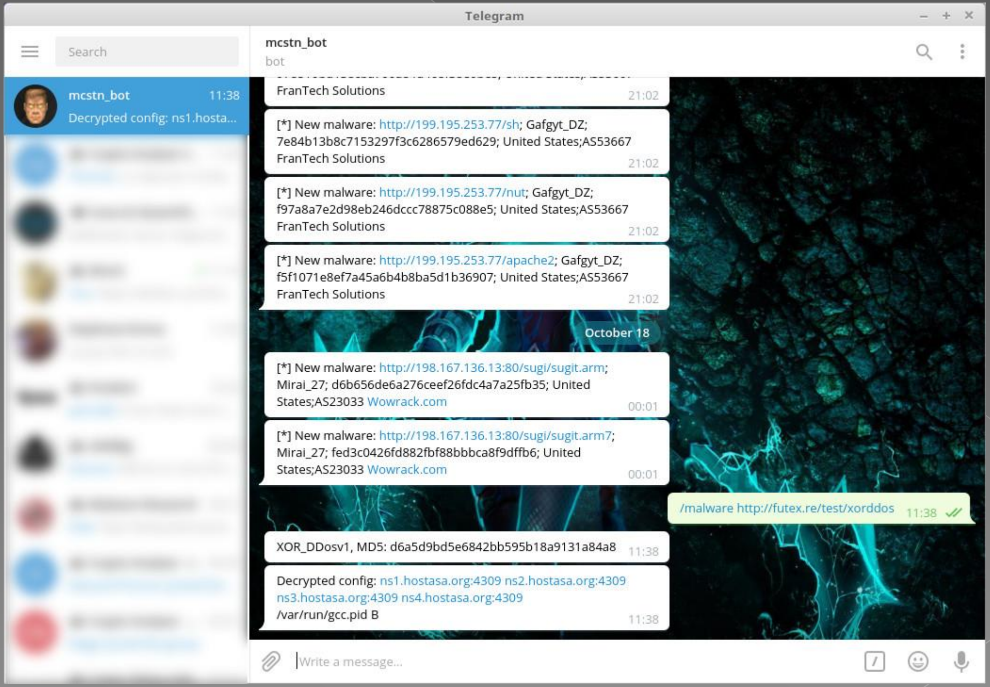
There were 3777 malwares in database.

Exported IOCs in JSON CSV

-First seen	-URL	-Type	-Hash	-Country	-AS
2017-10-11 06:56:32	http://179.228.23.166:8839/.i	Hajime_B2	e0a6cdedc313b68456befbe0cc376a29	Brazil	AS27699 TELEFNICA BRASIL S.A
2017-10-11 06:46:35	http://14.54.140.40:38277/.i	Hajime_B2	e0a6cdedc313b68456befbe0cc376a29	Republic of Korea	AS4766 Korea Telecom
2017-10-11 06:44:47	http://220.133.109.123:60428/.i	Hajime_B2	e0a6cdedc313b68456befbe0cc376a29	Taiwan	AS3462 Data Communication Business Group
2017-10-11 04:41:47	http://177.103.196.182:15225/.i	Hajime_B2	e0a6cdedc313b68456befbe0cc376a29	Brazil	AS27699 TELEFNICA BRASIL S.A
2017-10-11 04:18:12	http://179.98.237.6:15565/.i	Hajime_B2	e0a6cdedc313b68456befbe0cc376a29	Brazil	AS27699 TELEFNICA

$ Malware reversing

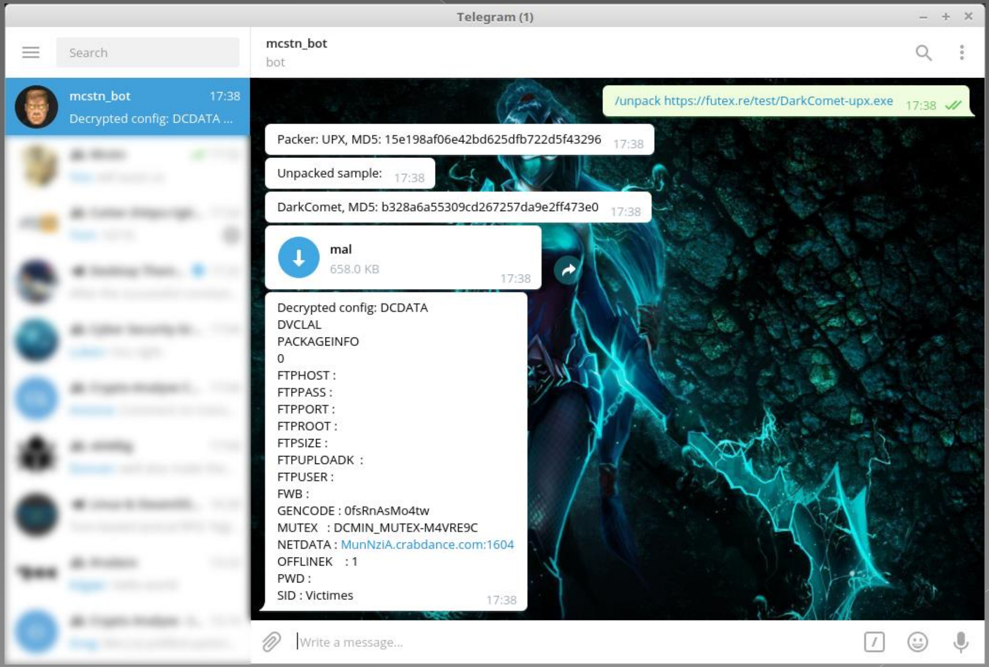
- Malware plugin can identify and reverse some samples
- Easy to add new malwares supported



```
FranTech Solutions 21:02

[*] New malware: http://199.195.253.77/sh; Gafgyt_DZ;
7e84b13b8c7153297f3c6286579ed629; United States;AS53667
FranTech Solutions 21:02

[*] New malware: http://199.195.253.77/nut; Gafgyt_DZ;
f97a8a7e2d98eb246dccc78875c088e5; United States;AS53667
FranTech Solutions 21:02

[*] New malware: http://199.195.253.77/apache2; Gafgyt_DZ;
f5f1071e8ef7a45a6b4b8ba5d1b36907; United States;AS53667
FranTech Solutions 21:02

October 18

[*] New malware: http://198.167.136.13:80/sugi/sugit.arm;
Mirai_27; d6b656de6a276ceef26fdc4a7a25fb35; United
States;AS23033 Wowrack.com 00:01

[*] New malware: http://198.167.136.13:80/sugi/sugit.arm7;
Mirai_27; fed3c0426fd882fbf88bbbca8f9dffb6; United
States;AS23033 Wowrack.com 00:01

/malware http://futex.re/test/xorddos 11:38

XOR_DDosv1, MD5: d6a5d9bd5e6842bb595b18a9131a84a8 11:38

Decrypted config: ns1.hostasa.org:4309 ns2.hostasa.org:4309
ns3.hostasa.org:4309 ns4.hostasa.org:4309
/var/run/gcc.pid B 11:38
```

$ Unpacking

- Unpack plugin can extract the sample
- Easy to add new packer supported (but can be hard to code and detect …)



```
/unpack https://futex.re/test/DarkComet-upx.exe 17:38

Packer: UPX, MD5: 15e198af06e42bd625dfb722d5f43296 17:38

Unpacked sample: 17:38

DarkComet, MD5: b328a6a55309cd267257da9e2ff473e0 17:38

mal
658.0 KB 17:38

Decrypted config: DCDATA
DVCLAL
PACKAGEINFO
0
FTPHOST :
FTPPASS :
FTPPORT :
FTPROOT :
FTPSIZE :
FTPUPLOADK  :
FTPUSER :
FWB :
GENCODE : 0fsRnAsMo4tw
MUTEX   : DCMIN_MUTEX-M4VRE9C
NETDATA : MunNziA.crabdance.com:1604
OFFLINEK    : 1
PWD :
SID : Victimes 17:38
```

$ Functionalities

Command	Description
/malware	Extract malware configuration
/unpack	Unpack the sample
/yara	Yara check
/shodan	Shodan search
/ip	Give informations about the IP
/vt	Return virustotal results
/urlquery	Urlquery search
/gse_find	Google custom engine search
/unshorten	Unshorten a URL

$ To improve

- Download directly from the chat room
- More supported packers and malware
- Autoreversing through a Windows VM
- Integrating into a SIEM?
- Sharing samples to MISP

$ Ideas, questions ?

$ End

- Thanks to Maxime Morin @maijin and radare errbot cowrie dev teams
- And you

$ references

- https://github.com/micheloosterhof/cowrie
- https://github.com/errbotio/errbot
- https://github.com/radare/radare2
- https://github.com/radareorg/cutter