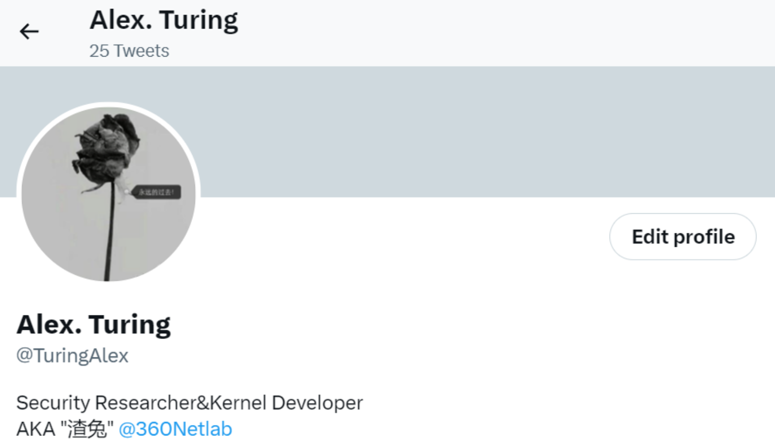
The Fodcha Botnet We Watched

Lingming Tu
Wenji Qu
Network Security Research Lab
Qihoo 360 Technology Co. Ltd.

Who are we?

- Alex Turing



Alex. Turing
25 Tweets

Alex. Turing
@TuringAlex

Security Researcher&Kernel Developer
AKA "渣兔" @360Netlab

- Wenji Qu

https://github.com/rootkiter

- 360 Netlab

- Blog

https://blog.netlab.360.com

Outline

- **About Fodcha botnet’s Details, including:**
  - ☐ Timeline
  - ☐ Similarities and differences with Mirai botnet
  - ☐ **C2 source code, Panel, Customer**
  - ☐ Tracking
- **About Fodcha botnet’s Statistics, including:**
  - ☐ Targets
  - ☐ Exploits
  - ☐ DDoS Vectors
  - ☐ Bot scales, distribution
- **About Fodcha botnet’s campaigns**
  - ☐ we can’t say in detail
  - ☐ **we can say**

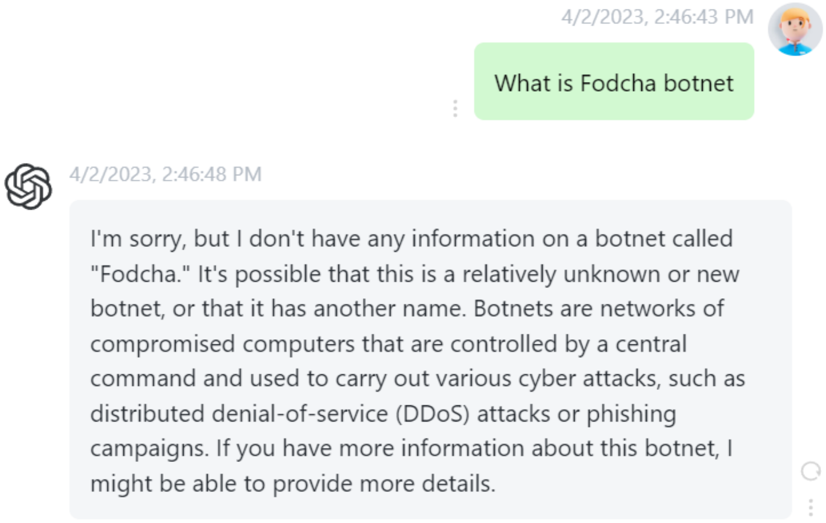
Bot: What is Fodcha

- **Published:**

  https://blog.netlab.360.com/fodcha-a-new-ddos-botnet

  https://blog.netlab.360.com/fodcha-is-coming-back-with-rddos

- **ChatGPT: ???**



4/2/2023, 2:46:43 PM

What is Fodcha botnet

4/2/2023, 2:46:48 PM

I'm sorry, but I don't have any information on a botnet called "Fodcha." It's possible that this is a relatively unknown or new botnet, or that it has another name. Botnets are networks of compromised computers that are controlled by a central command and used to carry out various cyber attacks, such as distributed denial-of-service (DDoS) attacks or phishing campaigns. If you have more information about this botnet, I might be able to provide more details.

- **Brief Intro**

Fodcha is a botnet that first appeared in 2022, mainly targeting IoT devices.

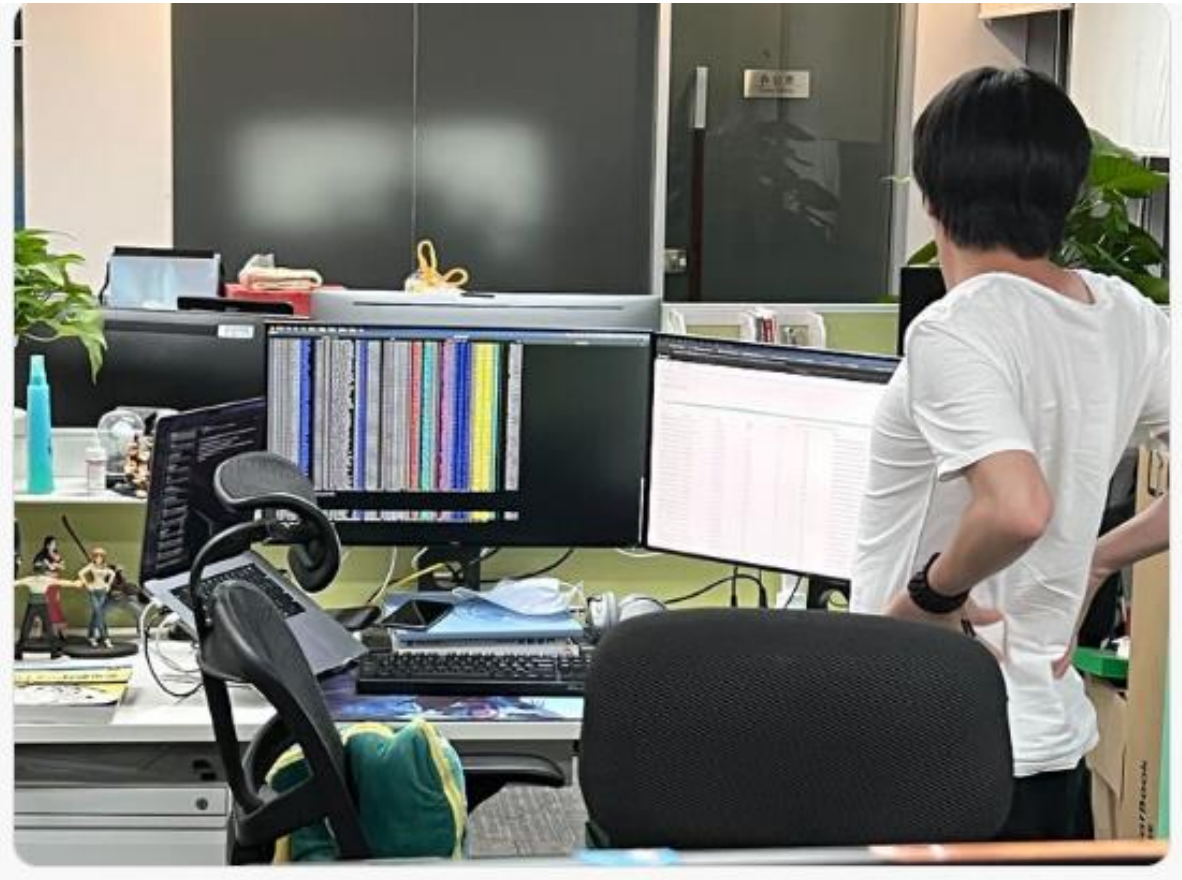
During the development, it absorbs some features of mirai botnet.

Also it has its own characteristic, such as using xxtea and chacha20 algorithms to protect sensitive resources, network communication, etc.

Bot: First Seen & Track

2022.01.12 captured by honeypot

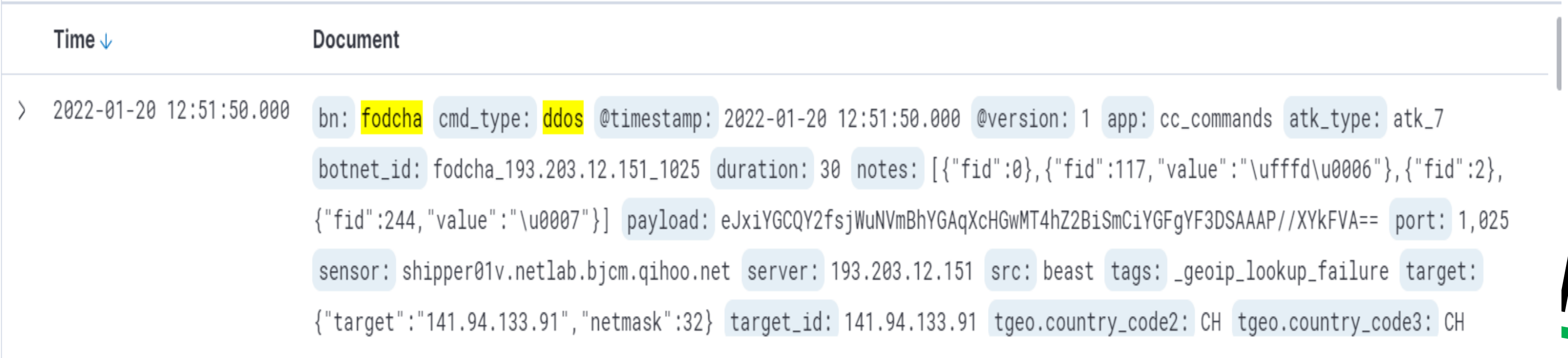
2022.01.13 tracked by Hui Wang



Bot: Timeline

2022.01.20

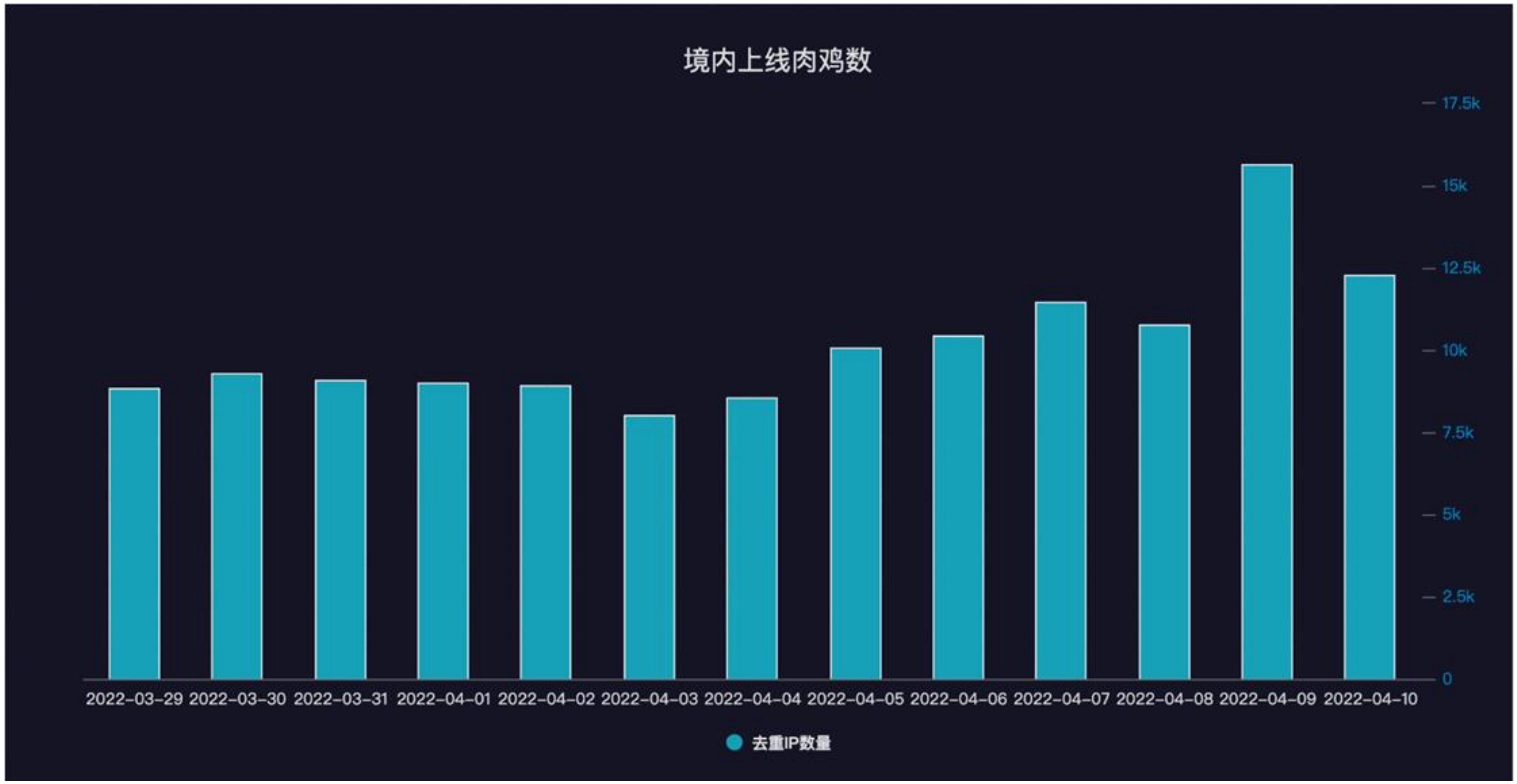
First time tracked DDoS record successfully



```
Time ↓                     Document

> 2022-01-20 12:51:50.000  bn: fodcha cmd_type: ddos @timestamp: 2022-01-20 12:51:50.000 @version: 1 app: cc_commands atk_type: atk_7
                           botnet_id: fodcha_193.203.12.151_1025 duration: 30 notes: [{"fid":0},{"fid":117,"value":"\ufffd\u0006"},{"fid":2},
                           {"fid":244,"value":"\u0007"}] payload: eJxiYGCQY2fsjWuNVmBhYGAqXcHGwMT4hZ2BiSmCiYGFgYF3DSAAAP//XYkFVA== port: 1,025
                           sensor: shipper01v.netlab.bjcm.qihoo.net server: 193.203.12.151 src: beast tags: _geoip_lookup_failure target:
                           {"target":"141.94.133.91","netmask":32} target_id: 141.94.133.91 tgeo.country_code2: CH tgeo.country_code3: CH
```

Bot: Timeline-Event

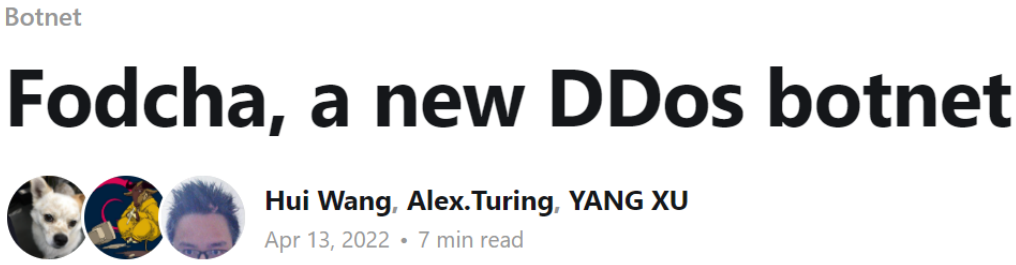
Bots in China From 03.20 – 04.10



Bot: Timeline

2022.04.13

Disclosure of the Fodcha botnet, containing version V1, V2 with CNCERT

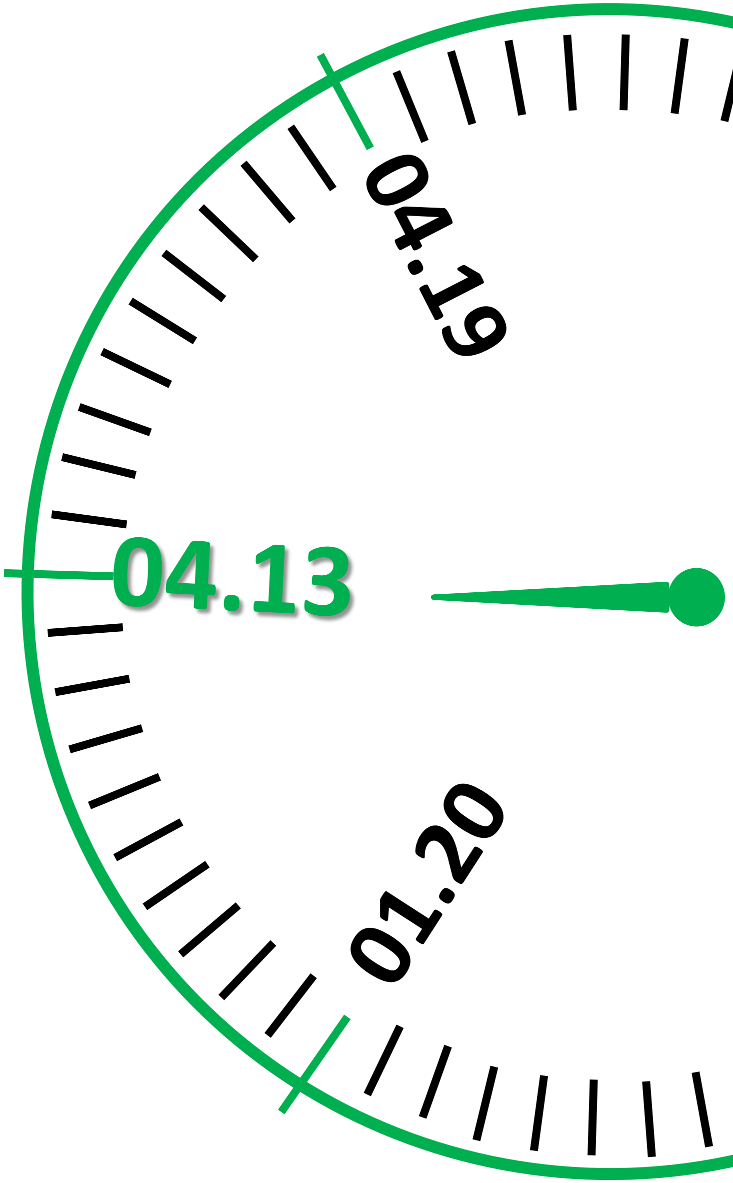


Botnet

Fodcha, a new DDos botnet

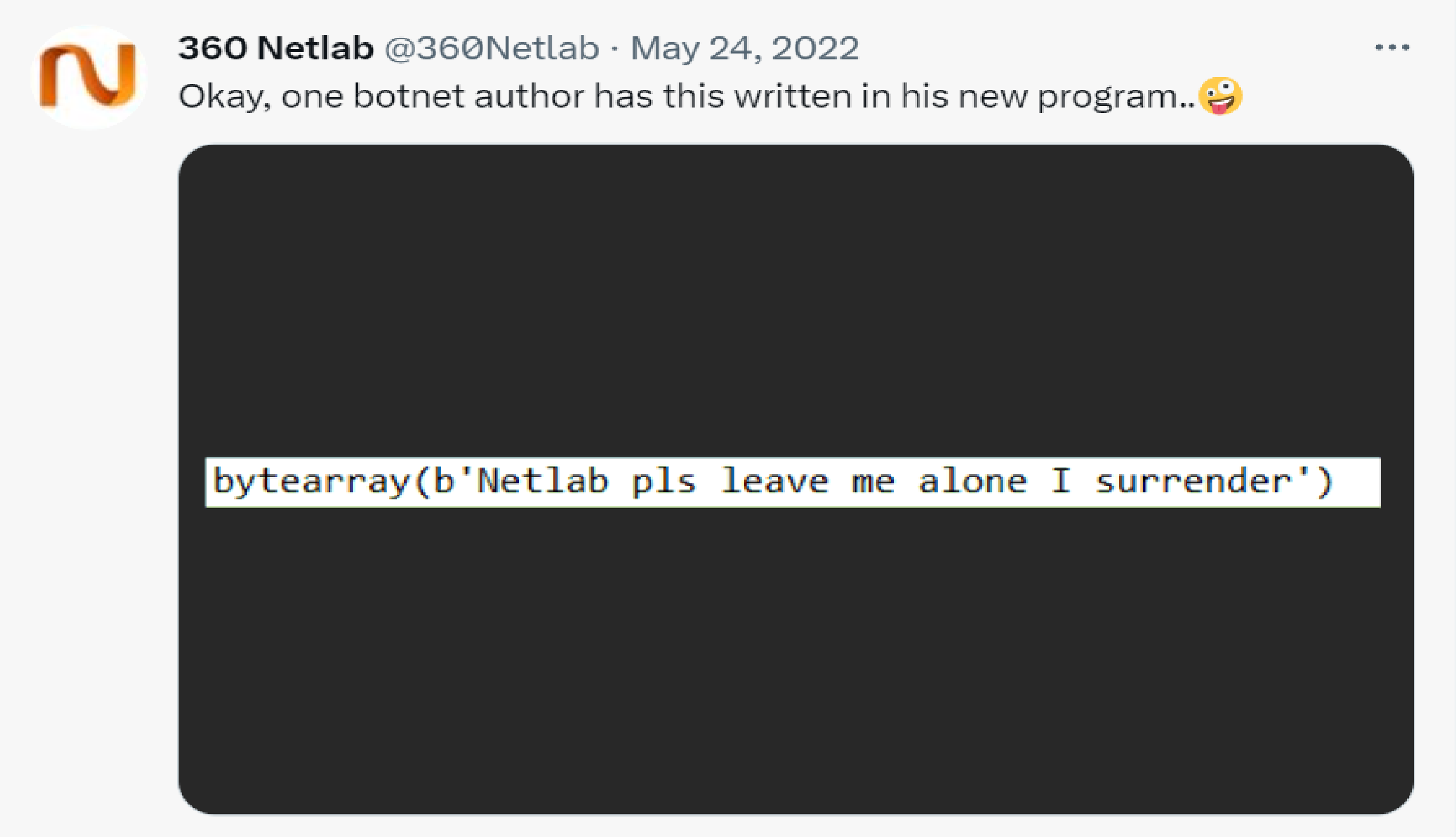
Hui Wang, Alex.Turing, YANG XU

Apr 13, 2022 • 7 min read



Bot: Timeline-Event

MSG1 leaved by the author



360 Netlab @360Netlab · May 24, 2022

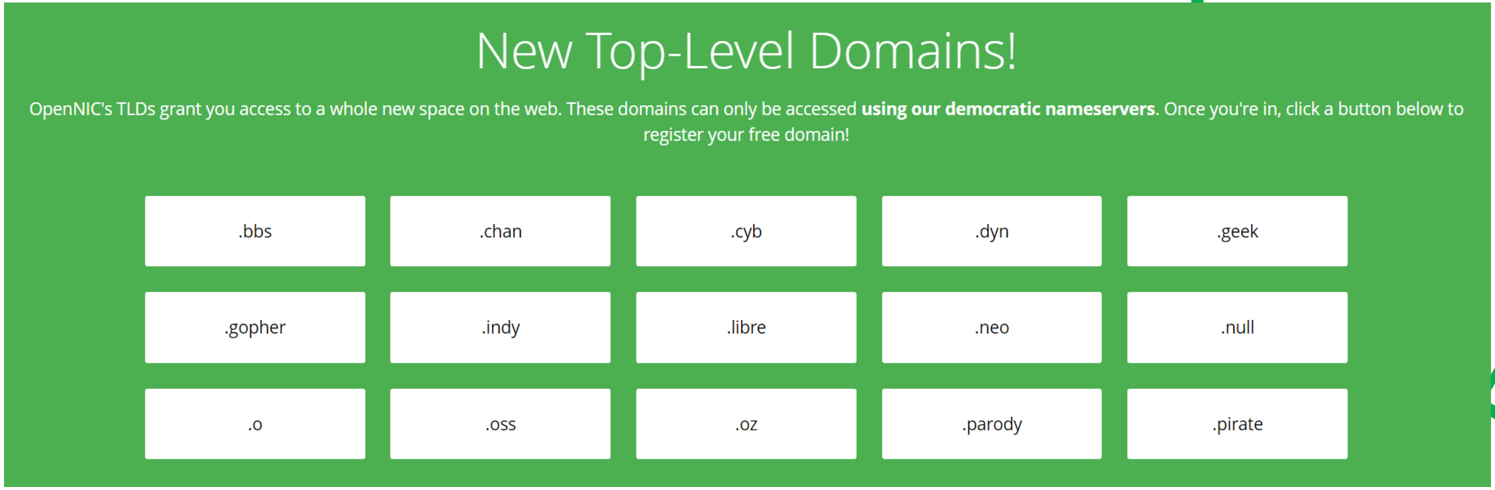
Okay, one botnet author has this written in his new program..🤪

```
bytearray(b'Netlab pls leave me alone I surrender')
```

Bot: Timeline

2022.04.19

Captured version v2.x,using OpenNIC's TLDs Style C2



New Top-Level Domains!

OpenNIC's TLDs grant you access to a whole new space on the web. These domains can only be accessed **using our democratic nameservers**. Once you're in, click a button below to register your free domain!

Bot: Timeline

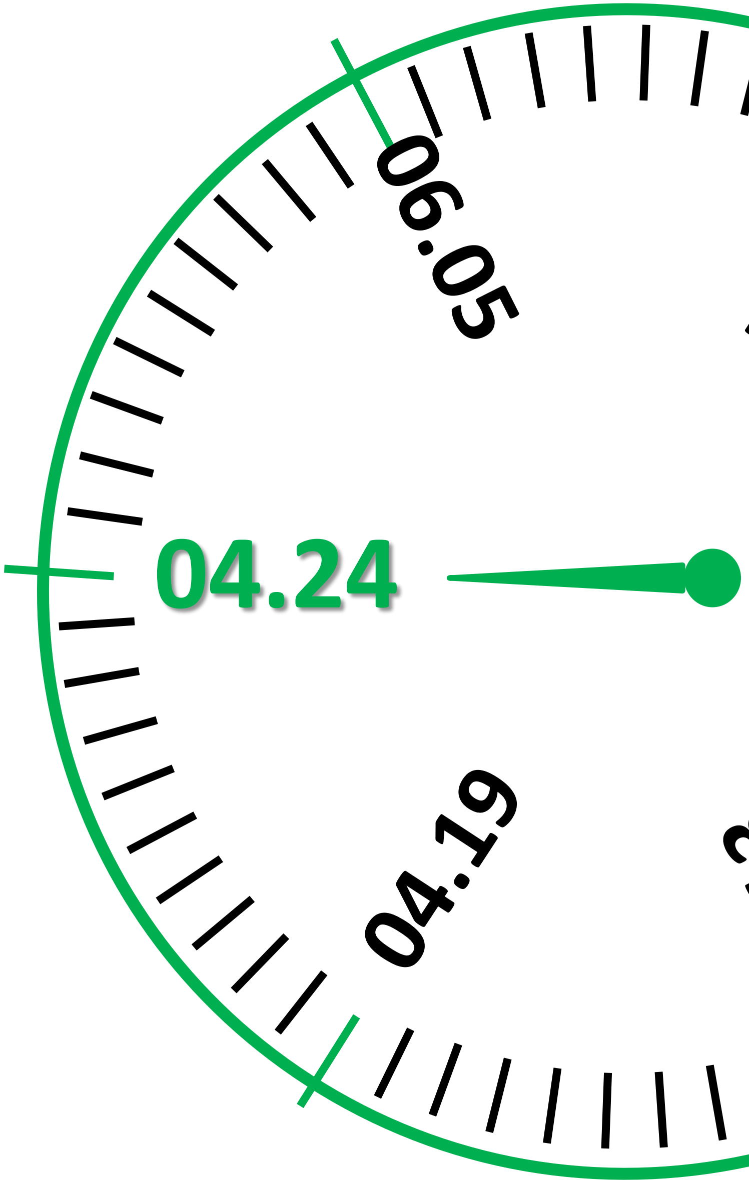
2022.04.24

Captured version v3

Using xxtea to encrypt configuration

Adding anti-sandbox & anti-debugging mechanism

Adopting ICANN domain as backup C2



Bot: Timeline

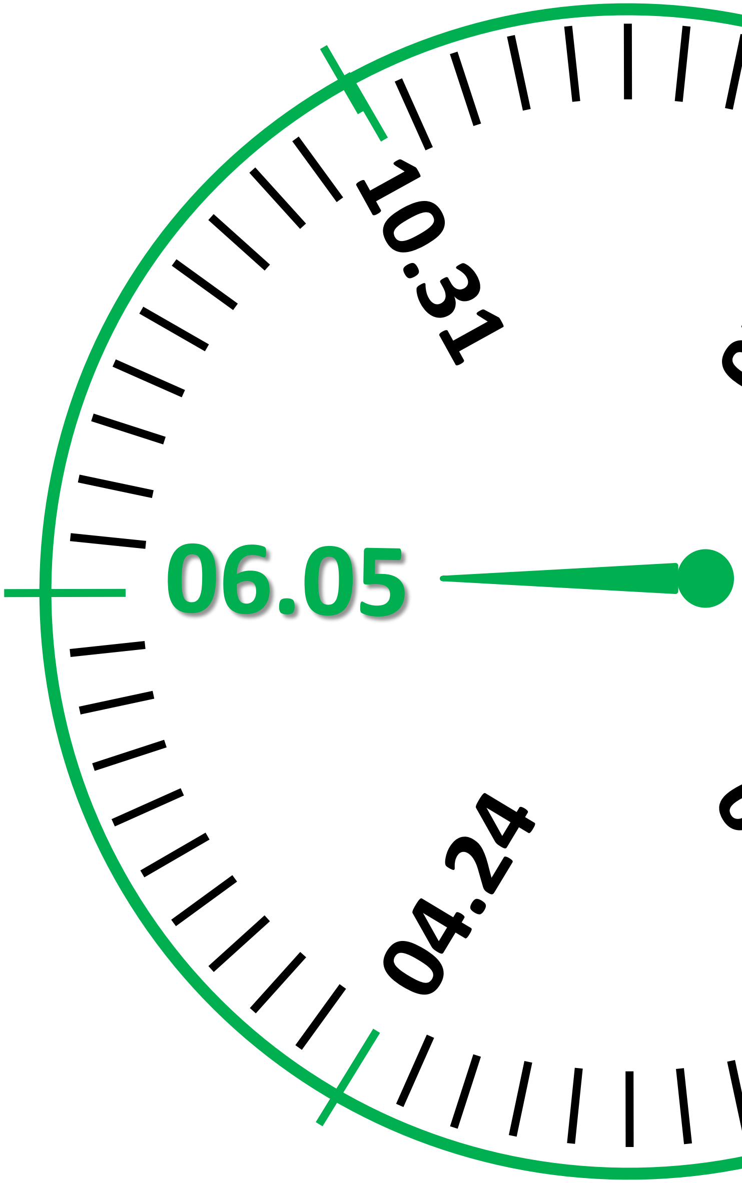
2022.06.05

☐ Captured version v4

☐ Using structured configuration

☐ Removing anti-sandboxing, anti-debugging mechanism

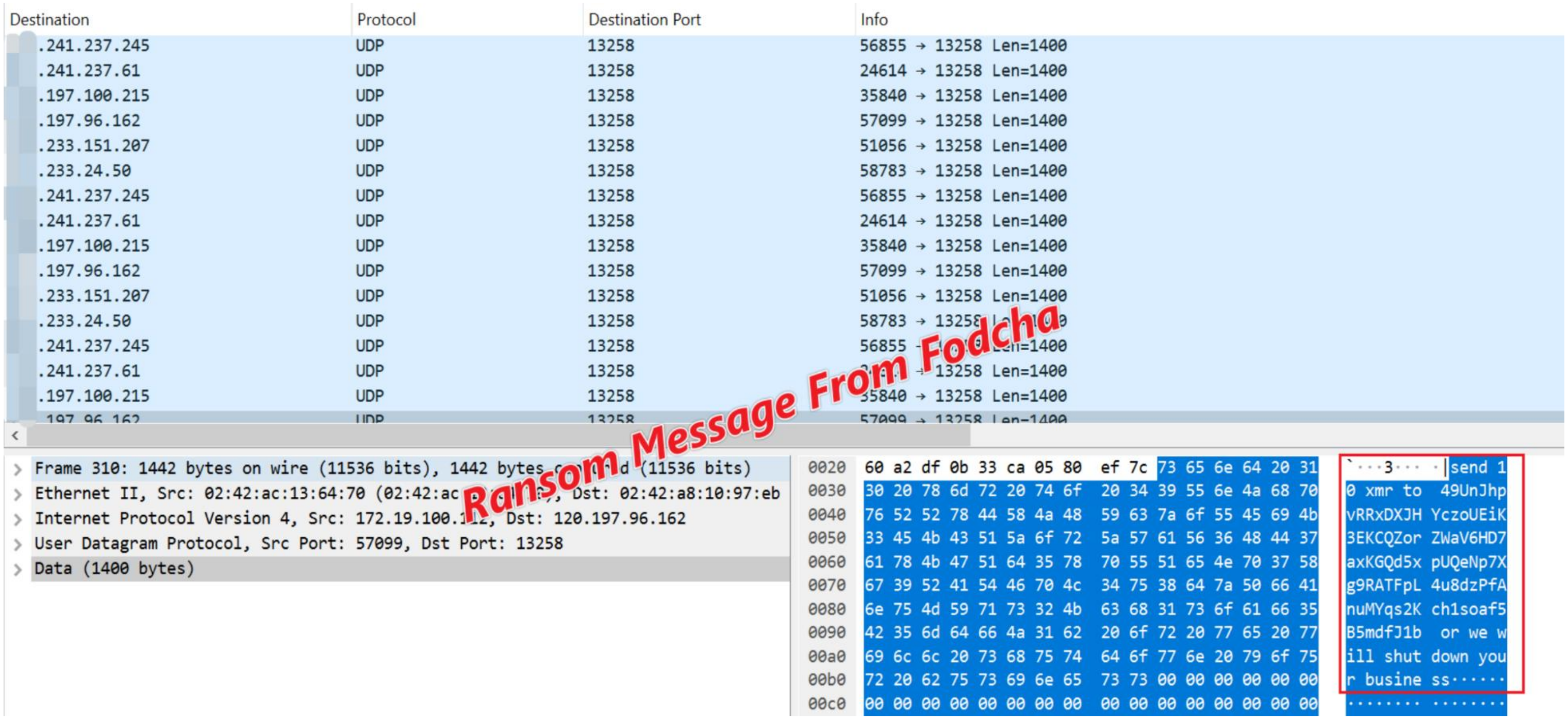
☐ Ransom DDoS



Bot: Timeline-Event

360 INTERNET SECURITY CENTER

Ransom DDoS



Destination	Protocol	Destination Port	Info
.241.237.245	UDP	13258	56855 → 13258 Len=1400
.241.237.61	UDP	13258	24614 → 13258 Len=1400
.197.100.215	UDP	13258	35840 → 13258 Len=1400
.197.96.162	UDP	13258	57099 → 13258 Len=1400
.233.151.207	UDP	13258	51056 → 13258 Len=1400
.233.24.50	UDP	13258	58783 → 13258 Len=1400
.241.237.245	UDP	13258	56855 → 13258 Len=1400
.241.237.61	UDP	13258	24614 → 13258 Len=1400
.197.100.215	UDP	13258	35840 → 13258 Len=1400
.197.96.162	UDP	13258	57099 → 13258 Len=1400
.233.151.207	UDP	13258	51056 → 13258 Len=1400
.233.24.50	UDP	13258	58783 → 1325[illegible]0
.241.237.245	UDP	13258	56855 [illegible]=1400
.241.237.61	UDP	13258	[illegible] → 13258 Len=1400
.197.100.215	UDP	13258	35840 → 13258 Len=1400
.197.96.162	UDP	13258	57099 → 13258 Len=1400

```
> Frame 310: 1442 bytes on wire (11536 bits), 1442 bytes [illegible]d (11536 bits)
> Ethernet II, Src: 02:42:ac:13:64:70 (02:42:ac[illegible]), Dst: 02:42:a8:10:97:eb
> Internet Protocol Version 4, Src: 172.19.100.1[illegible], Dst: 120.197.96.162
> User Datagram Protocol, Src Port: 57099, Dst Port: 13258
> Data (1400 bytes)
```

```
0020  60 a2 df 0b 33 ca 05 80  ef 7c 73 65 6e 64 20 31   `···3··· ·|send 1
0030  30 20 78 6d 72 20 74 6f  20 34 39 55 6e 4a 68 70   0 xmr to  49UnJhp
0040  76 52 52 78 44 58 4a 48  59 63 7a 6f 55 45 69 4b   vRRxDXJH YczoUEiK
0050  33 45 4b 43 51 5a 6f 72  5a 57 61 56 36 48 44 37   3EKCQZor ZWaV6HD7
0060  61 78 4b 47 51 64 35 78  70 55 51 65 4e 70 37 58   axKGQd5x pUQeNp7X
0070  67 39 52 41 54 46 70 4c  34 75 38 64 7a 50 66 41   g9RATFpL 4u8dzPfA
0080  6e 75 4d 59 71 73 32 4b  63 68 31 73 6f 61 66 35   nuMYqs2K ch1soaf5
0090  42 35 6d 64 66 4a 31 62  20 6f 72 20 77 65 20 77   B5mdfJ1b  or we w
00a0  69 6c 6c 20 73 68 75 74  64 6f 77 6e 20 79 6f 75   ill shut down you
00b0  72 20 62 75 73 69 6e 65  73 73 00 00 00 00 00 00   r busine ss······
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

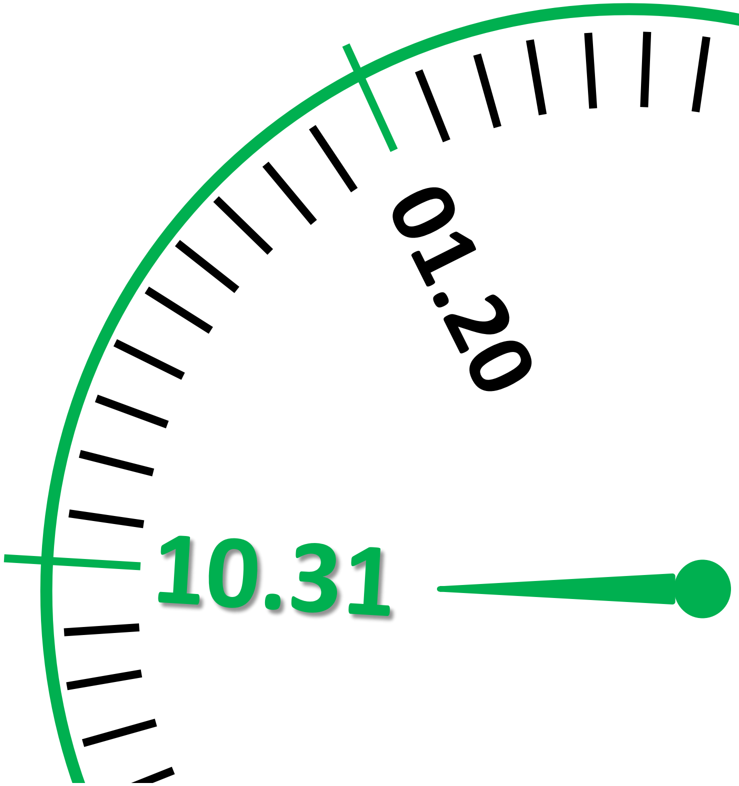
Ransom Message From Fodcha

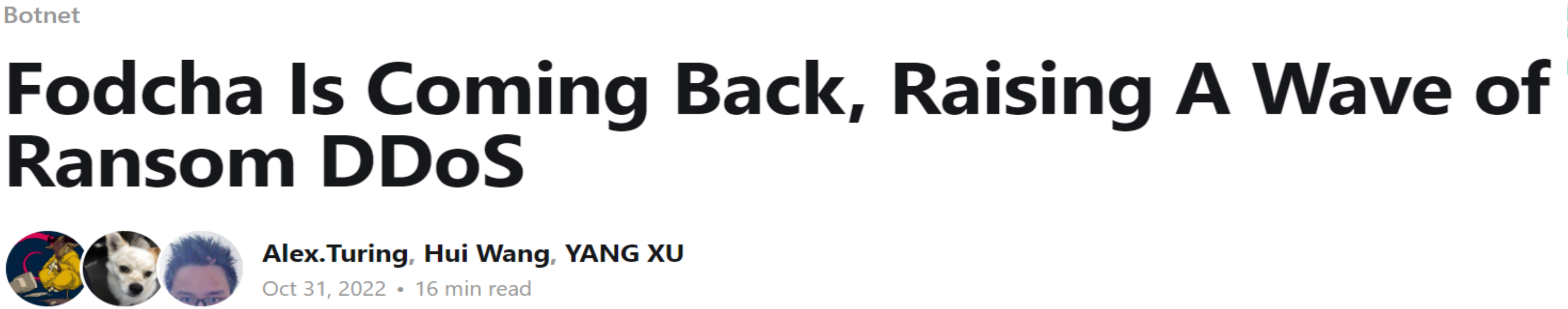
Bot: Timeline

"N3t1@bG@Y"

2022.10.31

Disclosure of the updated Fodcha botnet, containing version V3, V4





Botnet

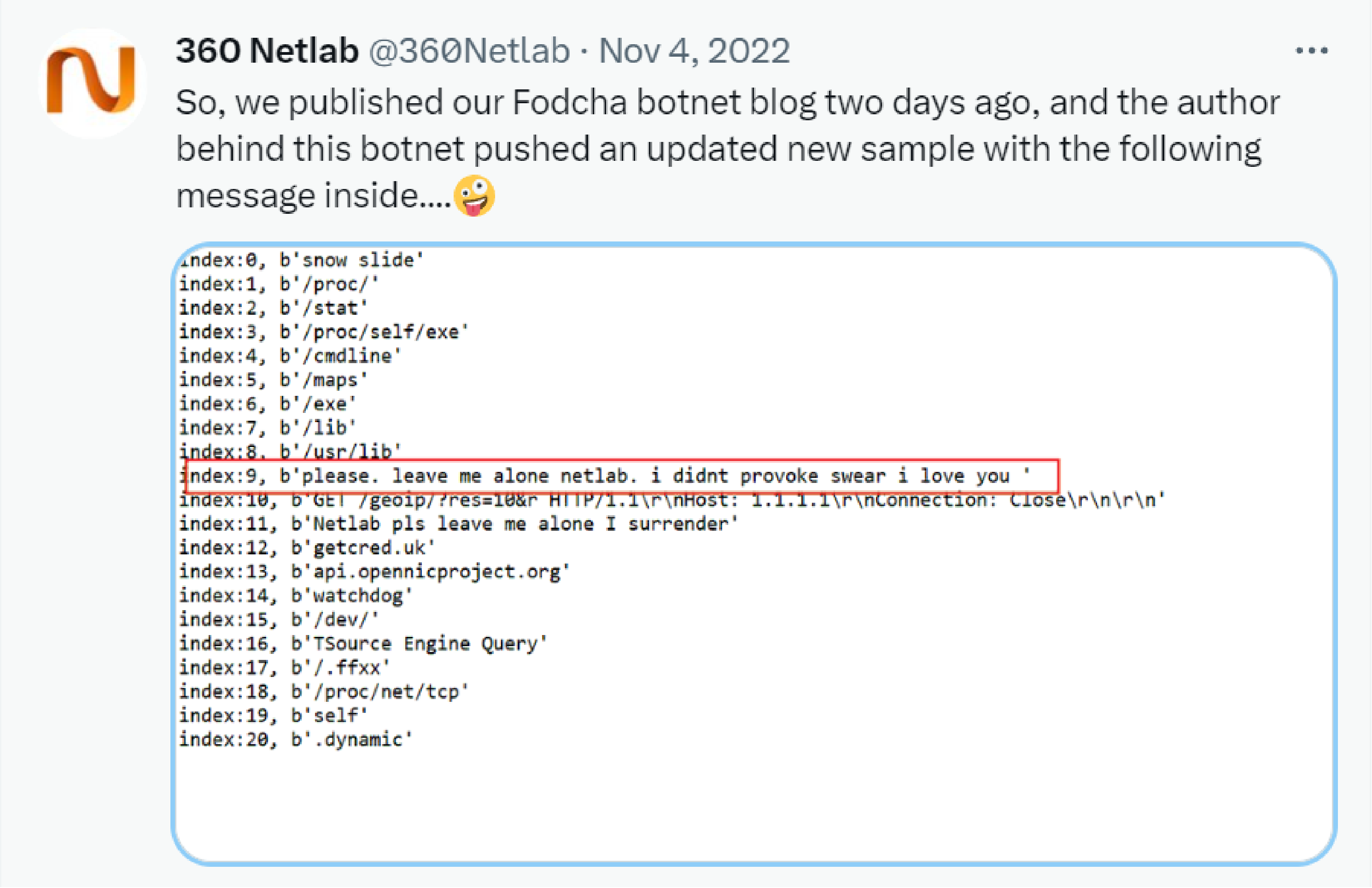
Fodcha Is Coming Back, Raising A Wave of Ransom DDoS

Alex.Turing, Hui Wang, YANG XU

Oct 31, 2022 • 16 min read

Bot: Timeline-Event

MSG2 leaved by the author



360 Netlab @360Netlab · Nov 4, 2022

So, we published our Fodcha botnet blog two days ago, and the author behind this botnet pushed an updated new sample with the following message inside....🤪

```
index:0, b'snow slide'
index:1, b'/proc/'
index:2, b'/stat'
index:3, b'/proc/self/exe'
index:4, b'/cmdline'
index:5, b'/maps'
index:6, b'/exe'
index:7, b'/lib'
index:8, b'/usr/lib'
index:9, b'please. leave me alone netlab. i didnt provoke swear i love you '
index:10, b'GET /geoip/?res=10&r HTTP/1.1\r\nHost: 1.1.1.1\r\nConnection: Close\r\n\r\n'
index:11, b'Netlab pls leave me alone I surrender'
index:12, b'getcred.uk'
index:13, b'api.opennicproject.org'
index:14, b'watchdog'
index:15, b'/dev/'
index:16, b'TSource Engine Query'
index:17, b'/.ffxx'
index:18, b'/proc/net/tcp'
index:19, b'self'
index:20, b'.dynamic'
```

Bot: Mirai vs Fodcha

Similarity

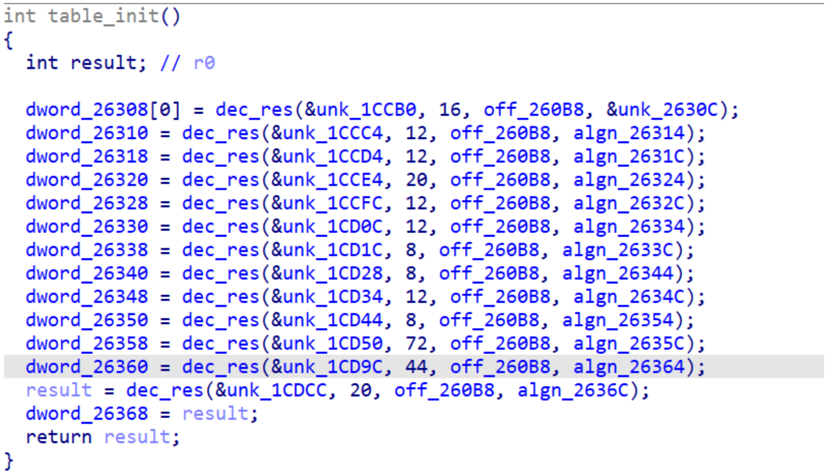
- ☐Host Behavior
- ☐DDoS Vectors
- ☐Cipher text Structure

Difference

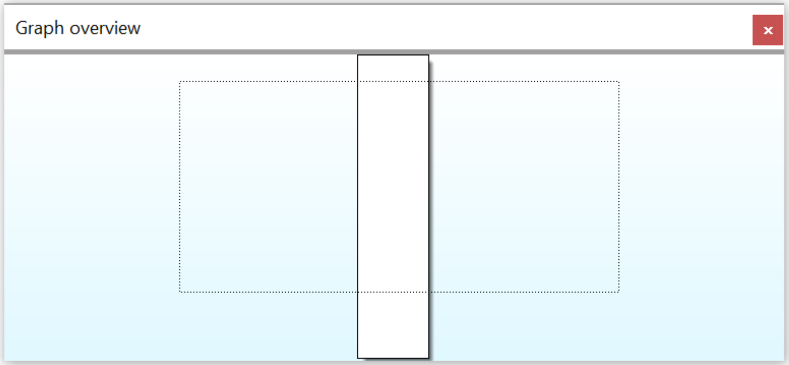
- ☐Encryption scheme
- ☐C2 protocol
- ☐OpenNIC C2
- ☐Anti sandbox/emulation/debugging

Bot: Learn from Mirai

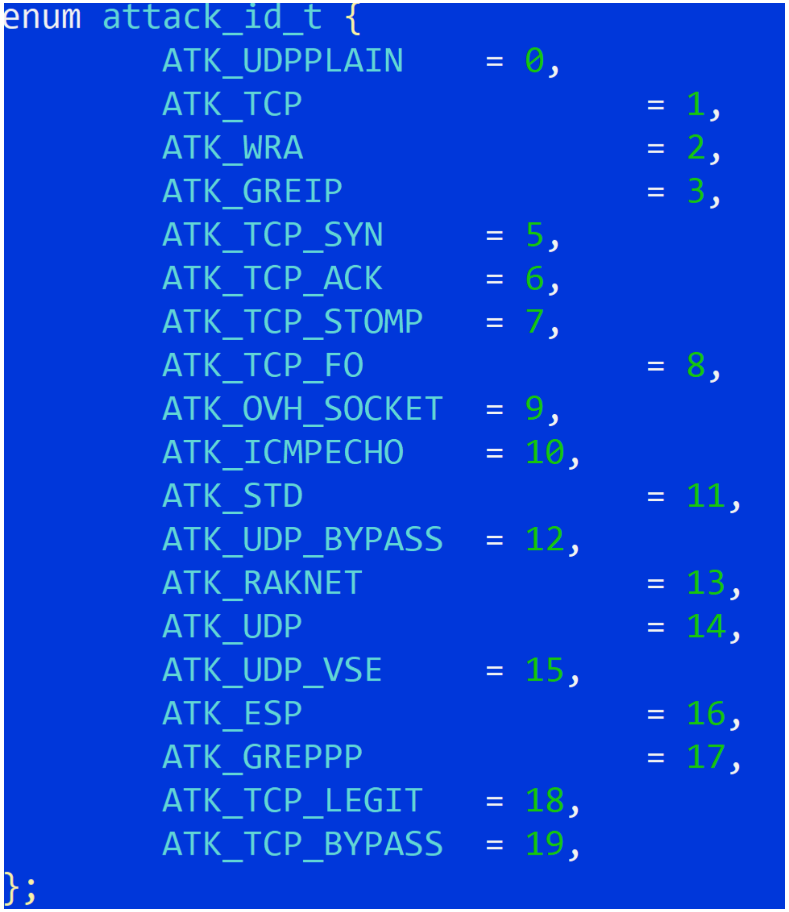
table_init



```
int table_init()
{
  int result; // r0

  dword_26308[0] = dec_res(&unk_1CCB0, 16, off_260B8, &unk_2630C);
  dword_26310 = dec_res(&unk_1CCC4, 12, off_260B8, algn_26314);
  dword_26318 = dec_res(&unk_1CCD4, 12, off_260B8, algn_2631C);
  dword_26320 = dec_res(&unk_1CCE4, 20, off_260B8, algn_26324);
  dword_26328 = dec_res(&unk_1CCFC, 12, off_260B8, algn_2632C);
  dword_26330 = dec_res(&unk_1CD0C, 12, off_260B8, algn_26334);
  dword_26338 = dec_res(&unk_1CD1C, 8, off_260B8, algn_2633C);
  dword_26340 = dec_res(&unk_1CD28, 8, off_260B8, algn_26344);
  dword_26348 = dec_res(&unk_1CD34, 12, off_260B8, algn_2634C);
  dword_26350 = dec_res(&unk_1CD44, 8, off_260B8, algn_26354);
  dword_26358 = dec_res(&unk_1CD50, 72, off_260B8, algn_2635C);
  dword_26360 = dec_res(&unk_1CD9C, 44, off_260B8, algn_26364);
  result = dec_res(&unk_1CDCC, 20, off_260B8, algn_2636C);
  dword_26368 = result;
  return result;
}
```



DDoS Vector



```
enum attack_id_t {
        ATK_UDPPLAIN    = 0,
        ATK_TCP                 = 1,
        ATK_WRA                 = 2,
        ATK_GREIP               = 3,
        ATK_TCP_SYN     = 5,
        ATK_TCP_ACK     = 6,
        ATK_TCP_STOMP   = 7,
        ATK_TCP_FO              = 8,
        ATK_OVH_SOCKET  = 9,
        ATK_ICMPECHO    = 10,
        ATK_STD                 = 11,
        ATK_UDP_BYPASS  = 12,
        ATK_RAKNET              = 13,
        ATK_UDP                 = 14,
        ATK_UDP_VSE     = 15,
        ATK_ESP                 = 16,
        ATK_GREPPP              = 17,
        ATK_TCP_LEGIT   = 18,
        ATK_TCP_BYPASS  = 19,
};
```

Bot: own characteristics

Algorithms used by Fodcha

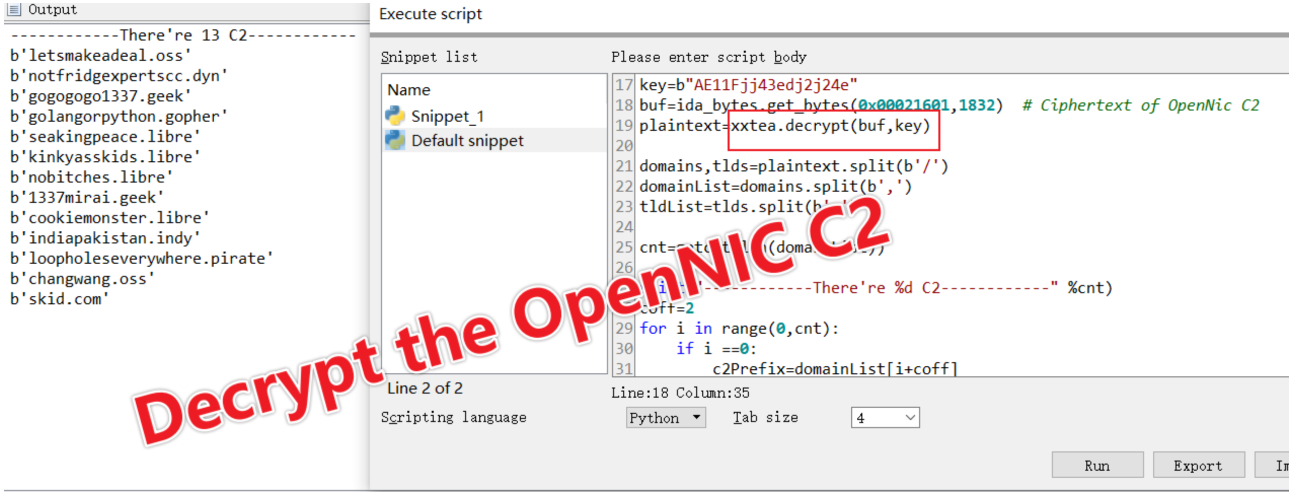
xxtea

Protect sensitive resources, including:

- ☐ Slogan,reporter,etc
- ☐ OpenNIC/ICANN C2
- ☐ Chacha20 key/nonce delivered by C2

chacha20

Protect communication from Stage 2 and on



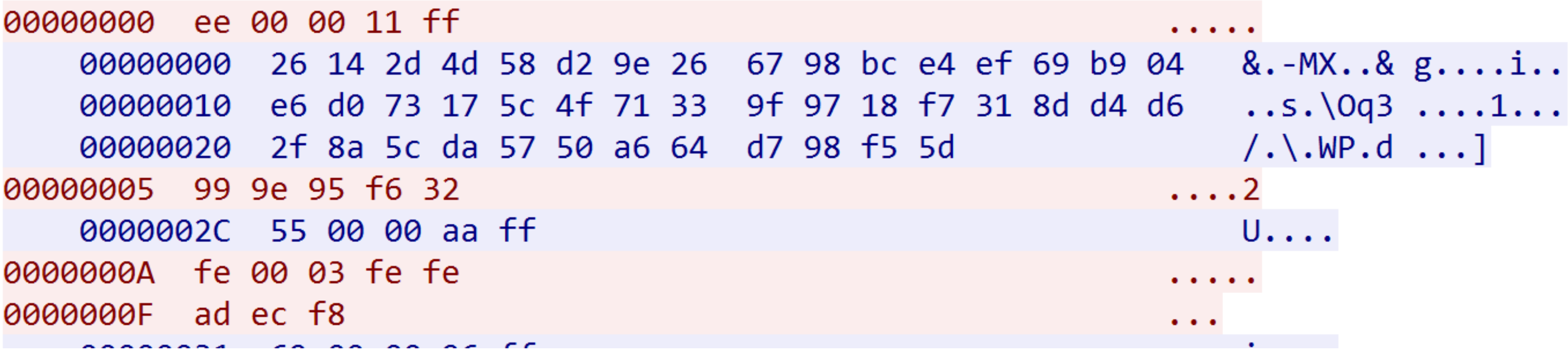
```
------------There're 13 C2------------
b'letsmakeadeal.oss'
b'notfridgexpertscc.dyn'
b'gogogogo1337.geek'
b'golangorpython.gopher'
b'seakingpeace.libre'
b'kinkyasskids.libre'
b'nobitches.libre'
b'1337mirai.geek'
b'cookiemonster.libre'
b'indiapakistan.indy'
b'loopholeseverywhere.pirate'
b'changwang.oss'
b'skid.com'
```

```
key=b"AE11Fjj43edj2j24e"
buf=ida_bytes.get_bytes(0x00021601,1832)  # Ciphertext of OpenNic C2
plaintext=xxtea.decrypt(buf,key)

domains,tlds=plaintext.split(b'/')
domainList=domains.split(b',')
tldList=tlds.split(b[illegible]

cnt=[illegible](doma[illegible])

[illegible]"------------There're %d C2------------" %cnt)
coff=2
for i in range(0,cnt):
    if i ==0:
        c2Prefix=domainList[i+coff]
```

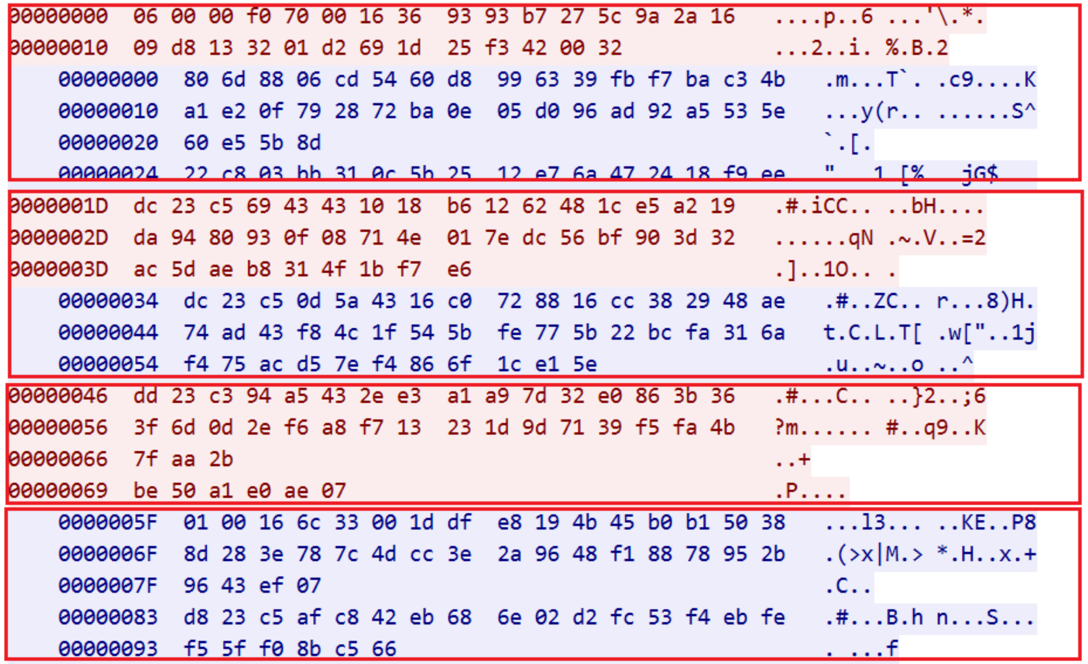
Line:18 Column:35

Bot: own characteristics

C2 Protocol used by V2 vs V3 & V4



```
00000000  ee 00 00 11 ff                                     .....
    00000000  26 14 2d 4d 58 d2 9e 26  67 98 bc e4 ef 69 b9 04   &.-MX..& g....i..
    00000010  e6 d0 73 17 5c 4f 71 33  9f 97 18 f7 31 8d d4 d6   ..s.\Oq3 ....1...
    00000020  2f 8a 5c da 57 50 a6 64  d7 98 f5 5d              /.\.WP.d ...]
00000005  99 9e 95 f6 32                                     ....2
    0000002C  55 00 00 aa ff                                 U....
0000000A  fe 00 03 fe fe                                     .....
0000000F  ad ec f8                                           ...
```



```
00000000  06 00 00 f0 70 00 16 36  93 93 b7 27 5c 9a 2a 16   ....p..6 ...'\.*.
00000010  09 d8 13 32 01 d2 69 1d  25 f3 42 00 32            ...2..i. %.B.2
    00000000  80 6d 88 06 cd 54 60 d8  99 63 39 fb f7 ba c3 4b   .m...T`. .c9....K
    00000010  a1 e2 0f 79 28 72 ba 0e  05 d0 96 ad 92 a5 53 5e   ...y(r.. ......S^
    00000020  60 e5 5b 8d                                    `.[.
    00000024  22 c8 03 bb 31 0c 5b 25  12 e7 6a 47 24 18 f9 ee   "   1 [%   jG$
0000001D  dc 23 c5 69 43 43 10 18  b6 12 62 48 1c e5 a2 19   .#.iCC.. ..bH....
0000002D  da 94 80 93 0f 08 71 4e  01 7e dc 56 bf 90 3d 32   ......qN .~.V..=2
0000003D  ac 5d ae b8 31 4f 1b f7  e6                        .]..1O.. .
    00000034  dc 23 c5 0d 5a 43 16 c0  72 88 16 cc 38 29 48 ae   .#..ZC.. r...8)H.
    00000044  74 ad 43 f8 4c 1f 54 5b  fe 77 5b 22 bc fa 31 6a   t.C.L.T[ .w["..1j
    00000054  f4 75 ac d5 7e f4 86 6f  1c e1 5e                .u..~..o ..^
00000046  dd 23 c3 94 a5 43 2e e3  a1 a9 7d 32 e0 86 3b 36   .#...C.. ..}2..;6
00000056  3f 6d 0d 2e f6 a8 f7 13  23 1d 9d 71 39 f5 fa 4b   ?m...... #..q9..K
00000066  7f aa 2b                                           ..+
00000069  be 50 a1 e0 ae 07                                  .P....
    0000005F  01 00 16 6c 33 00 1d df  e8 19 4b 45 b0 b1 50 38   ...l3... ..KE..P8
    0000006F  8d 28 3e 78 7c 4d cc 3e  2a 96 48 f1 88 78 95 2b   .(>x|M.> *.H..x.+
    0000007F  96 43 ef 07                                    .C..
    00000083  d8 23 c5 af c8 42 eb 68  6e 02 d2 fc 53 f4 eb fe   .#...B.h n...S...
    00000093  f5 5f f0 8b c5 66                              .  ...f
```

Stage 1

Stage 2

Stage 3

CMD

Bot: own characteristics

C2 protocol

1. Negotiate chacha20 key/nonce
2. Identity authentication
3. Beacon
4. Cmds

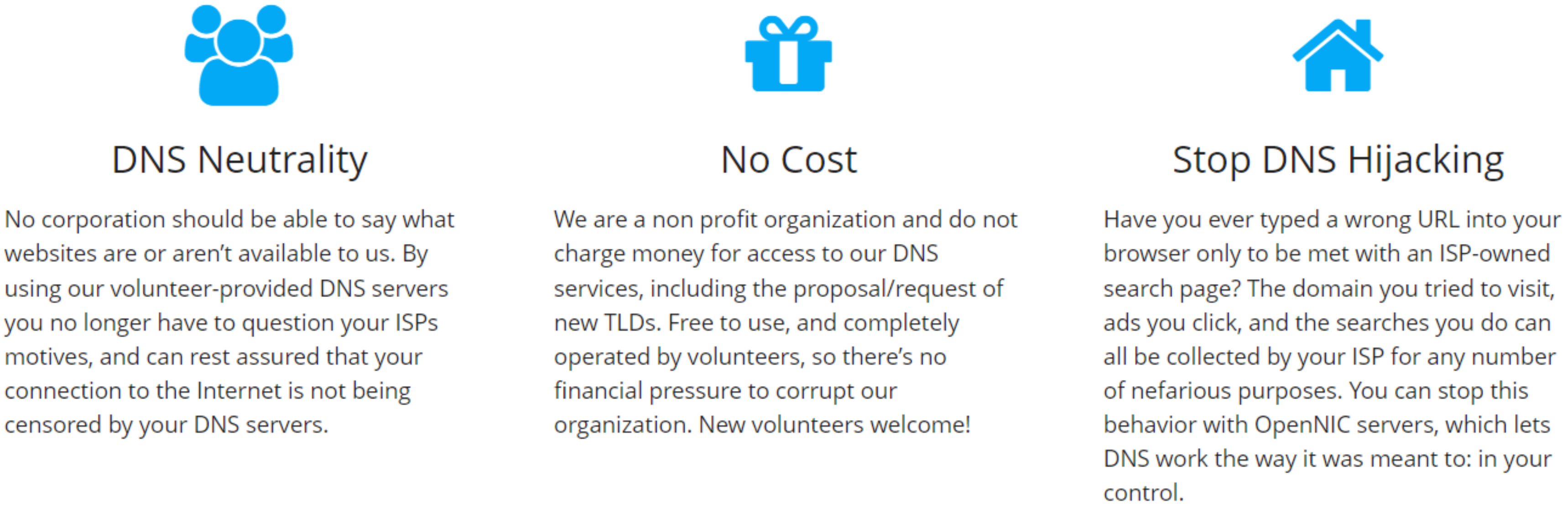
V2 vs V3&V4

- ☐ V2: no padding, chacha20 stuff are plaintext
- ☐ V3&V4: contains padding, chacha20 stuff are ciphertext

Bot: own characteristics

OpenNIC C2 Infrastructure Advantage

☐ DNS Neutrality
☐ No Cost
☐ Stop DNS Hijacking



DNS Neutrality

No corporation should be able to say what websites are or aren't available to us. By using our volunteer-provided DNS servers you no longer have to question your ISPs motives, and can rest assured that your connection to the Internet is not being censored by your DNS servers.

No Cost

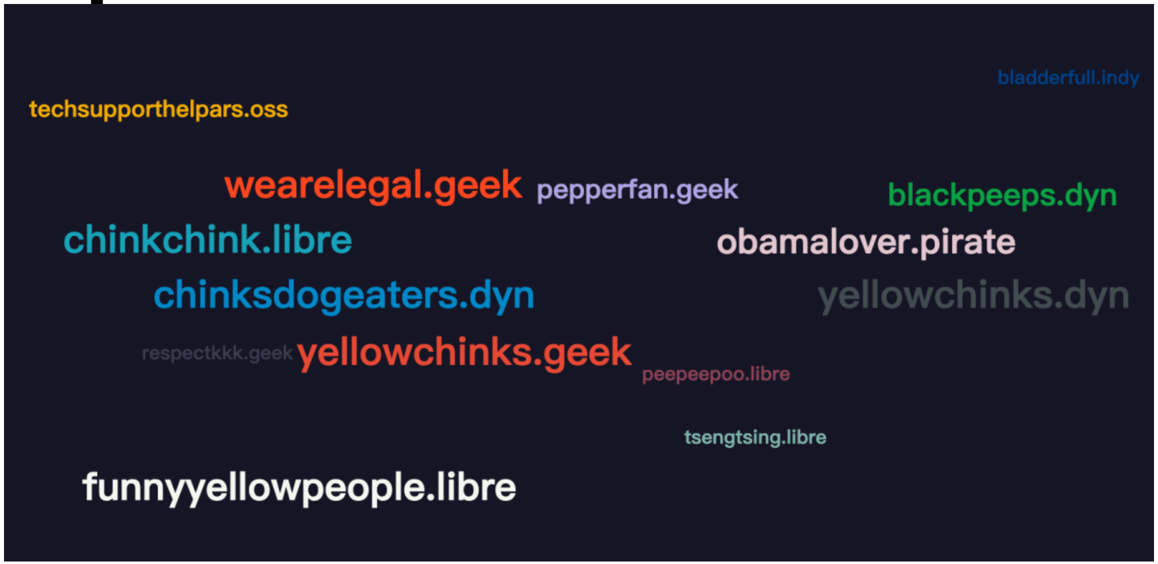
We are a non profit organization and do not charge money for access to our DNS services, including the proposal/request of new TLDs. Free to use, and completely operated by volunteers, so there's no financial pressure to corrupt our organization. New volunteers welcome!

Stop DNS Hijacking

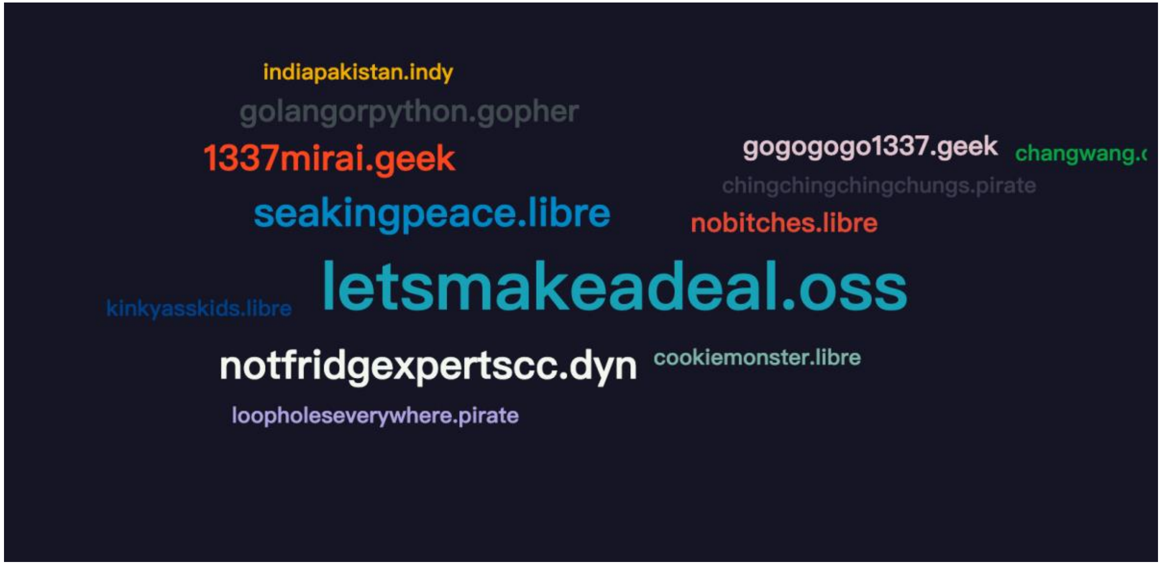
Have you ever typed a wrong URL into your browser only to be met with an ISP-owned search page? The domain you tried to visit, ads you click, and the searches you do can all be collected by your ISP for any number of nefarious purposes. You can stop this behavior with OpenNIC servers, which lets DNS work the way it was meant to: in your control.

Bot: own characteristics

OpenNIC C2 Infrastructure



bladderfull.indy
techsupporthelpars.oss
wearelegal.geek
pepperfan.geek
blackpeeps.dyn
chinkchink.libre
obamalover.pirate
chinksdogeaters.dyn
yellowchinks.dyn
respectkkk.geek
yellowchinks.geek
peepeepoo.libre
tsengtsing.libre
funnyyellowpeople.libre



indiapakistan.indy
golangorpython.gopher
1337mirai.geek
gogogogo1337.geek
changwang.
chingchingchingchungs.pirate
seakingpeace.libre
nobitches.libre
kinkyasskids.libre
letsmakeadeal.oss
notfridgexpertscc.dyn
cookiemonster.libre
loopholeseverywhere.pirate

Bot: own characteristics

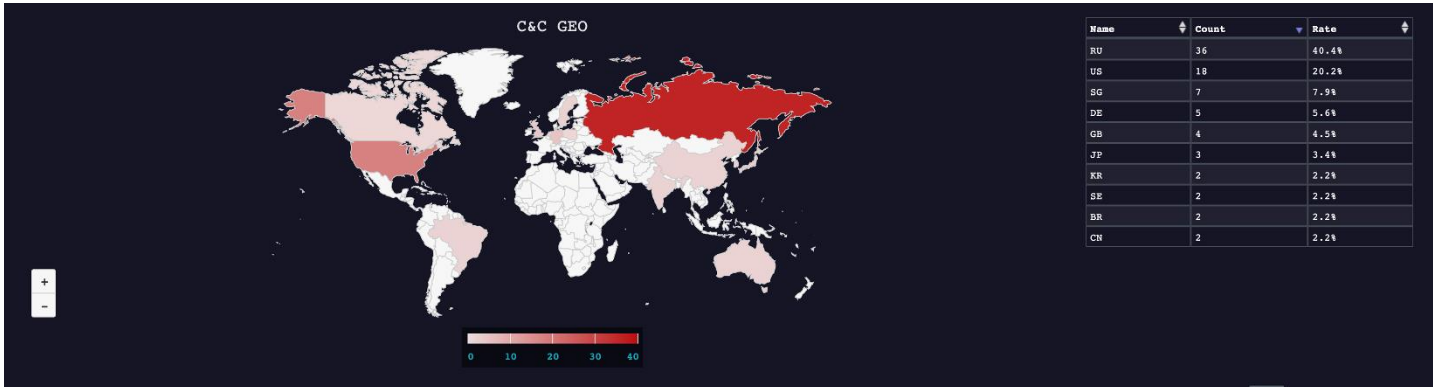
360 INTERNET SECURITY CENTER

OpenNIC Domain → IP

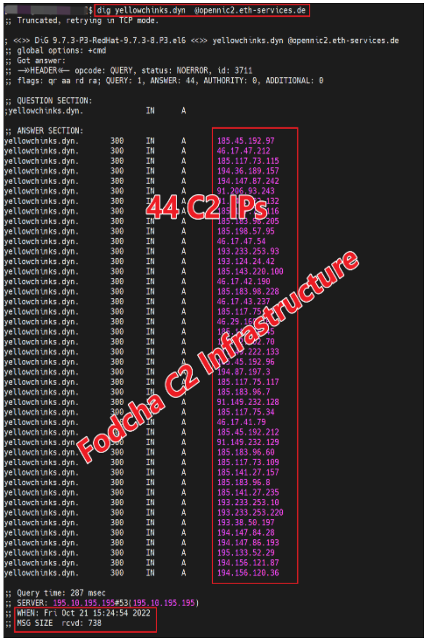
Just dig it with specific DNS resolver

Hard to take Fodcha down

- ☐ 13 domains, 90 ips,
- ☐ 10 countries, 10+ provider



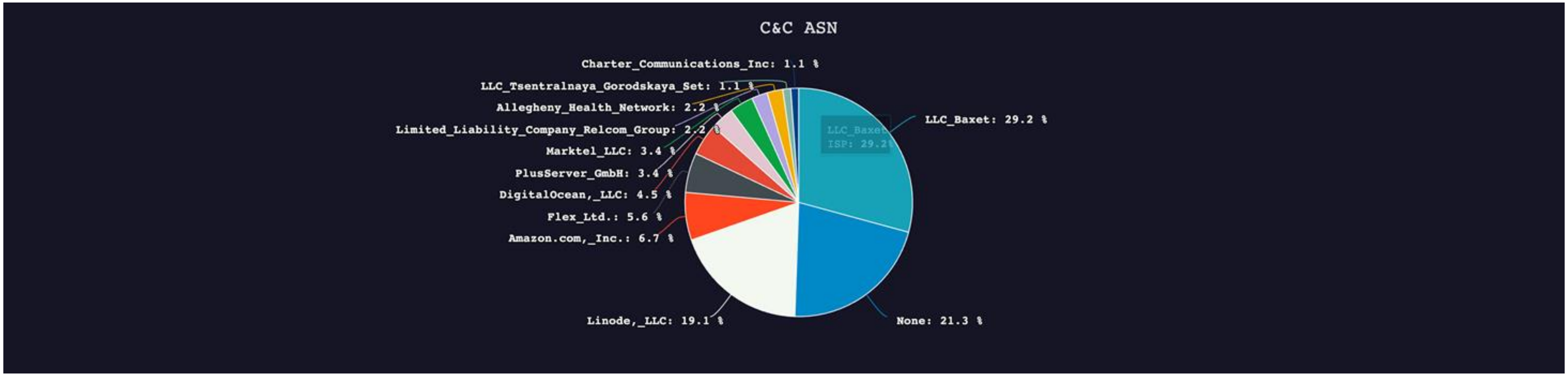
Name	Count	Rate
RU	36	40.4%
US	18	20.2%
SG	7	7.9%
DE	5	5.6%
GB	4	4.5%
JP	3	3.4%
KR	2	2.2%
SE	2	2.2%
BR	2	2.2%
CN	2	2.2%



```
[[redacted]]$ dig yellowchinks.dyn  @opennic2.eth-services.de
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6 <<>> yellowchinks.dyn @opennic2.eth-services.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3711
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 44, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;yellowchinks.dyn.              IN      A

;; ANSWER SECTION:
yellowchinks.dyn.       300     IN      A       185.45.192.97
yellowchinks.dyn.       300     IN      A       46.17.47.212
yellowchinks.dyn.       300     IN      A       185.117.73.115
yellowchinks.dyn.       300     IN      A       194.36.189.157
yellowchinks.dyn.       300     IN      A       194.147.87.242
yellowchinks.dyn.       300     IN      A       91.206.93.243
yellowchinks.dyn.       300     IN      A       91.[illegible].132
yellowchinks.dyn.       300     IN      A       185.[illegible].116
yellowchinks.dyn.       300     IN      A       185.183.98.205
yellowchinks.dyn.       300     IN      A       185.198.57.95
yellowchinks.dyn.       300     IN      A       46.17.47.54
yellowchinks.dyn.       300     IN      A       193.233.253.93
yellowchinks.dyn.       300     IN      A       193.124.24.42
yellowchinks.dyn.       300     IN      A       185.143.220.100
yellowchinks.dyn.       300     IN      A       46.17.42.190
yellowchinks.dyn.       300     IN      A       185.183.98.228
yellowchinks.dyn.       300     IN      A       46.17.43.237
yellowchinks.dyn.       300     IN      A       185.117.75.[illegible]
yellowchinks.dyn.       300     IN      A       46.29.16[illegible]
yellowchinks.dyn.       300     IN      A       185.1[illegible]45
yellowchinks.dyn.       300     IN      A       1[illegible]2.70
yellowchinks.dyn.       300     IN      A       [illegible]49.222.133
yellowchinks.dyn.       300     IN      A       [illegible]5.45.192.96
yellowchinks.dyn.       300     IN      A       194.87.197.3
yellowchinks.dyn.       300     IN      A       185.117.75.117
yellowchinks.dyn.       300     IN      A       185.183.96.7
yellowchinks.dyn.       300     IN      A       91.149.232.128
yellowchinks.dyn.       300     IN      A       185.117.75.34
yellowchinks.dyn.       300     IN      A       46.17.41.79
yellowchinks.dyn.       300     IN      A       185.45.192.212
yellowchinks.dyn.       300     IN      A       91.149.232.129
yellowchinks.dyn.       300     IN      A       185.183.96.60
yellowchinks.dyn.       300     IN      A       185.117.73.109
yellowchinks.dyn.       300     IN      A       185.141.27.157
yellowchinks.dyn.       300     IN      A       185.183.96.8
yellowchinks.dyn.       300     IN      A       185.141.27.235
yellowchinks.dyn.       300     IN      A       193.233.253.10
yellowchinks.dyn.       300     IN      A       193.233.253.220
yellowchinks.dyn.       300     IN      A       193.38.50.197
yellowchinks.dyn.       300     IN      A       194.147.84.28
yellowchinks.dyn.       300     IN      A       194.147.86.193
yellowchinks.dyn.       300     IN      A       195.133.52.29
yellowchinks.dyn.       300     IN      A       194.156.121.87
yellowchinks.dyn.       300     IN      A       194.156.120.36

;; Query time: 287 msec
;; SERVER: 195.10.195.195#53(195.10.195.195)
;; WHEN: Fri Oct 21 15:24:54 2022
;; MSG SIZE  rcvd: 738
```

44 C2 IPs

Fodcha C2 Infrastructure



C2: Source Code

How do we get the Fodcha C2 source code?

☐ 2022.11.09, Anonymous Source From telegram

☐ Has his own botnet

☐ Just want to be rich

☐ Just want to **take Fodcha down**

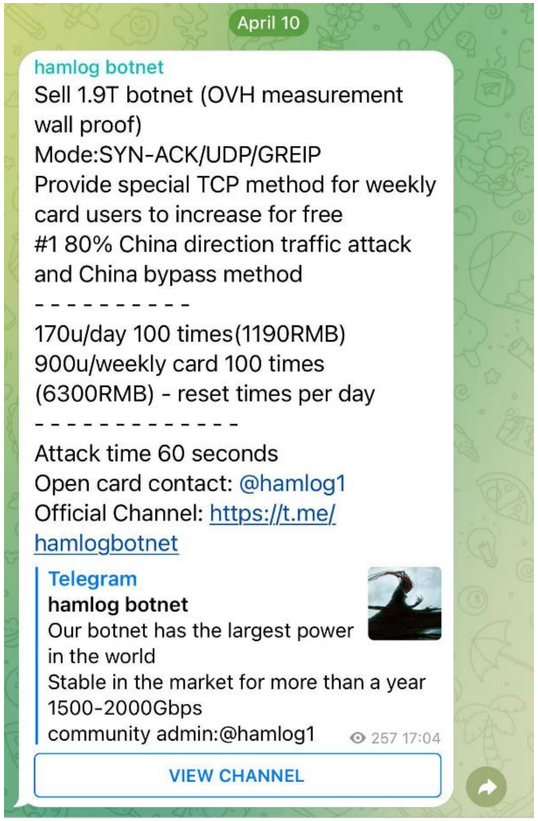
☐ **Source code & access to a control terminal**

Some other info(not verified)

☐ **Hamlog, aka LightTheLeafeon**

☐ **4 people**

☐ **brickerbot**



April 10

hamlog botnet

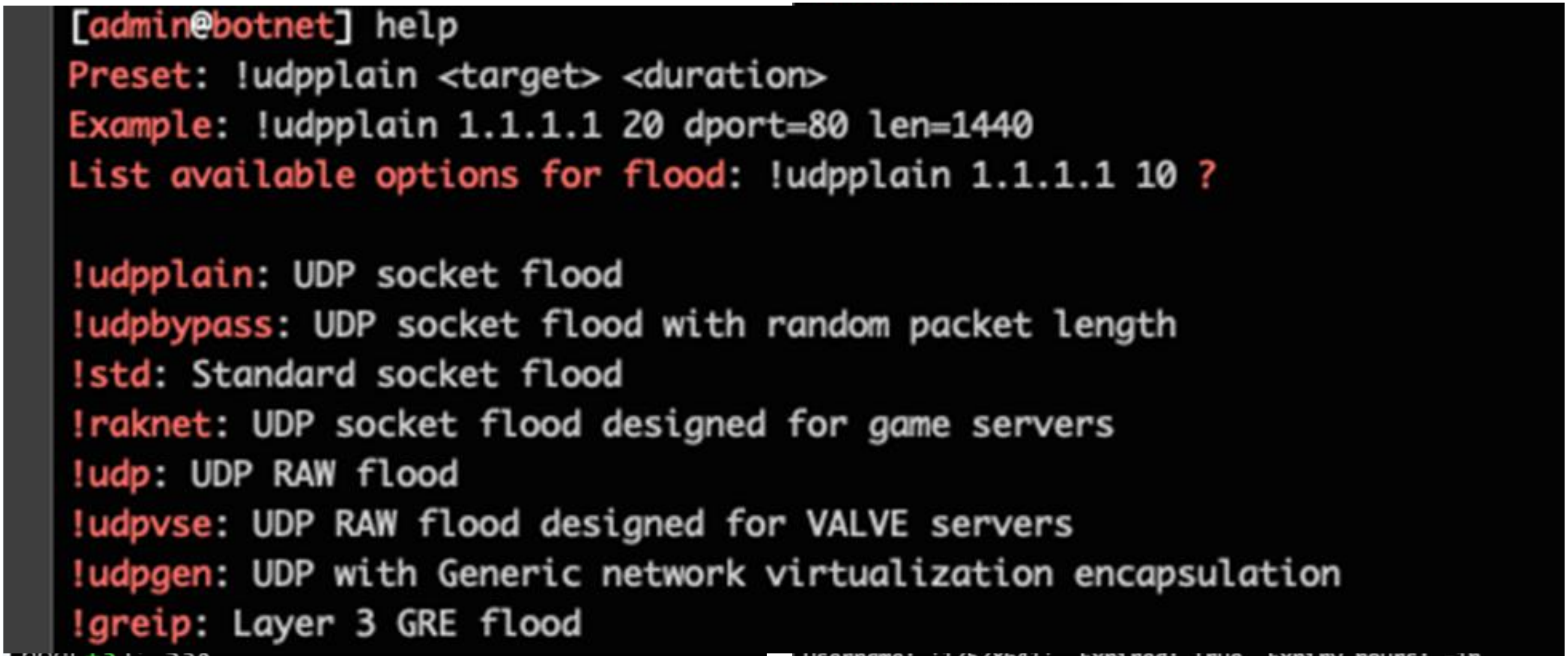
Sell 1.9T botnet (OVH measurement wall proof)
Mode:SYN-ACK/UDP/GREIP
Provide special TCP method for weekly card users to increase for free
#1 80% China direction traffic attack and China bypass method
- - - - - - - - - - -
170u/day 100 times(1190RMB)
900u/weekly card 100 times (6300RMB) - reset times per day
- - - - - - - - - - - - - -
Attack time 60 seconds
Open card contact: @hamlog1
Official Channel: https://t.me/hamlogbotnet

Telegram
hamlog botnet
Our botnet has the largest power in the world
Stable in the market for more than a year
1500-2000Gbps
community admin:@hamlog1

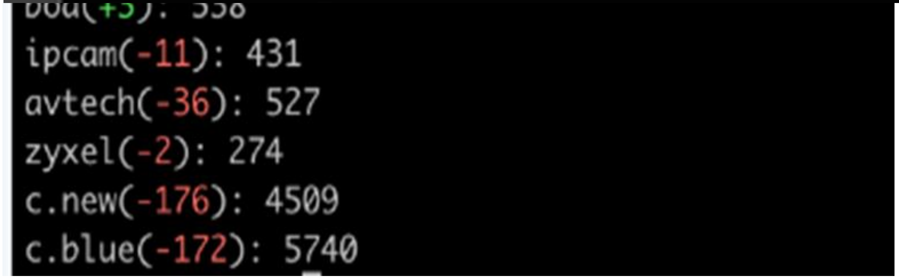
257 17:04

C2: Panel

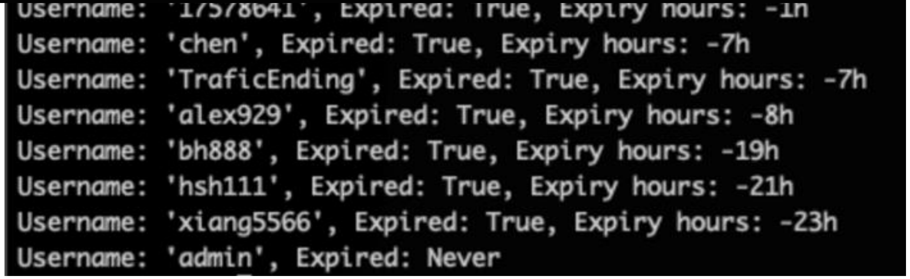
telnet 17x.18x.19x.2xx 1xx6



```
[admin@botnet] help
Preset: !udpplain <target> <duration>
Example: !udpplain 1.1.1.1 20 dport=80 len=1440
List available options for flood: !udpplain 1.1.1.1 10 ?

!udpplain: UDP socket flood
!udpbypass: UDP socket flood with random packet length
!std: Standard socket flood
!raknet: UDP socket flood designed for game servers
!udp: UDP RAW flood
!udpvse: UDP RAW flood designed for VALVE servers
!udpgen: UDP with Generic network virtualization encapsulation
!greip: Layer 3 GRE flood
```

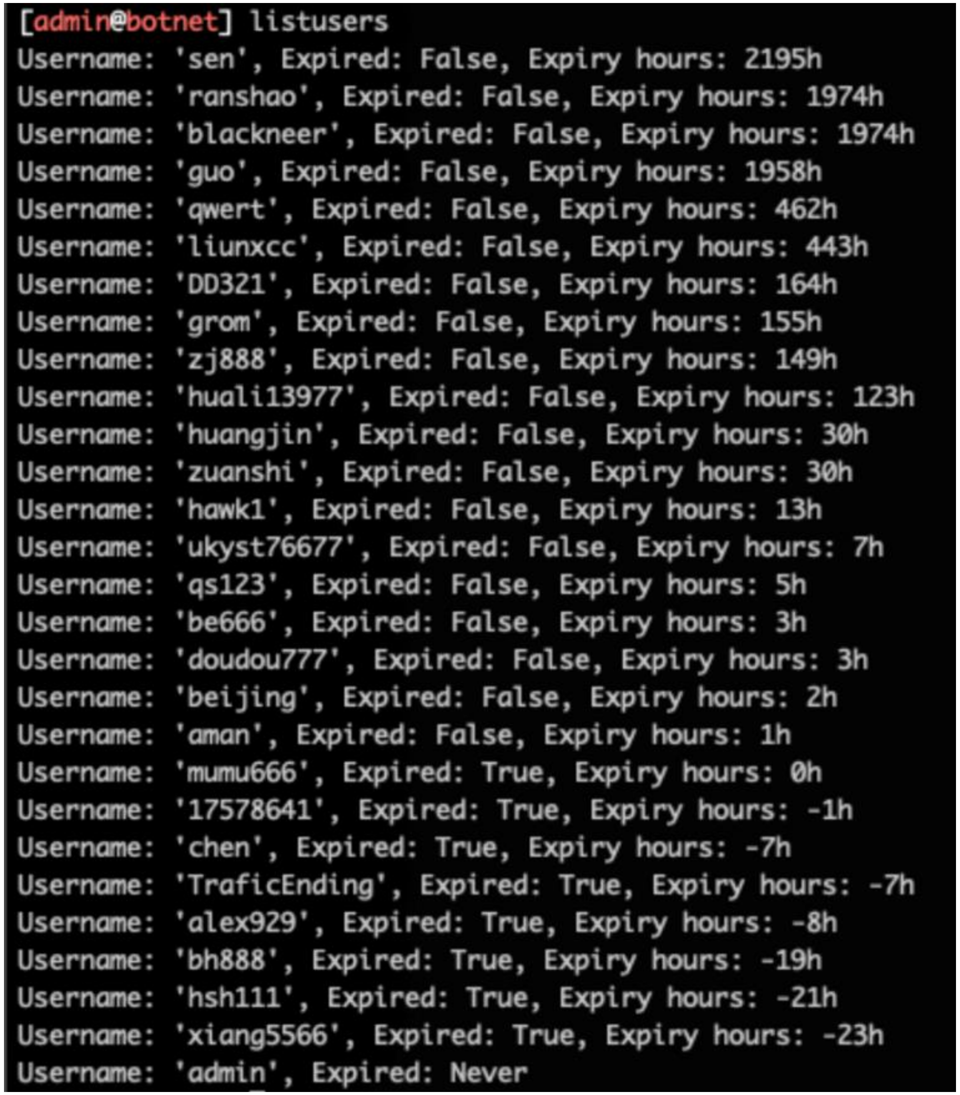


```
ipcam(-11): 431
avtech(-36): 527
zyxel(-2): 274
c.new(-176): 4509
c.blue(-172): 5740
```



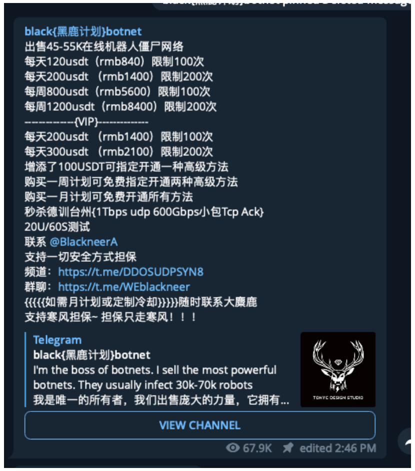
```
Username: '17578641', Expired: True, Expiry hours: -1h
Username: 'chen', Expired: True, Expiry hours: -7h
Username: 'TraficEnding', Expired: True, Expiry hours: -7h
Username: 'alex929', Expired: True, Expiry hours: -8h
Username: 'bh888', Expired: True, Expiry hours: -19h
Username: 'hsh111', Expired: True, Expiry hours: -21h
Username: 'xiang5566', Expired: True, Expiry hours: -23h
Username: 'admin', Expired: Never
```

C2: Panel



```
[admin@botnet] listusers
Username: 'sen', Expired: False, Expiry hours: 2195h
Username: 'ranshao', Expired: False, Expiry hours: 1974h
Username: 'blackneer', Expired: False, Expiry hours: 1974h
Username: 'guo', Expired: False, Expiry hours: 1958h
Username: 'qwert', Expired: False, Expiry hours: 462h
Username: 'liunxcc', Expired: False, Expiry hours: 443h
Username: 'DD321', Expired: False, Expiry hours: 164h
Username: 'grom', Expired: False, Expiry hours: 155h
Username: 'zj888', Expired: False, Expiry hours: 149h
Username: 'huali13977', Expired: False, Expiry hours: 123h
Username: 'huangjin', Expired: False, Expiry hours: 30h
Username: 'zuanshi', Expired: False, Expiry hours: 30h
Username: 'hawk1', Expired: False, Expiry hours: 13h
Username: 'ukyst76677', Expired: False, Expiry hours: 7h
Username: 'qs123', Expired: False, Expiry hours: 5h
Username: 'be666', Expired: False, Expiry hours: 3h
Username: 'doudou777', Expired: False, Expiry hours: 3h
Username: 'beijing', Expired: False, Expiry hours: 2h
Username: 'aman', Expired: False, Expiry hours: 1h
Username: 'mumu666', Expired: True, Expiry hours: 0h
Username: '17578641', Expired: True, Expiry hours: -1h
Username: 'chen', Expired: True, Expiry hours: -7h
Username: 'TraficEnding', Expired: True, Expiry hours: -7h
Username: 'alex929', Expired: True, Expiry hours: -8h
Username: 'bh888', Expired: True, Expiry hours: -19h
Username: 'hsh111', Expired: True, Expiry hours: -21h
Username: 'xiang5566', Expired: True, Expiry hours: -23h
Username: 'admin', Expired: Never
```

Blackneer
Ranshao
Mumu666

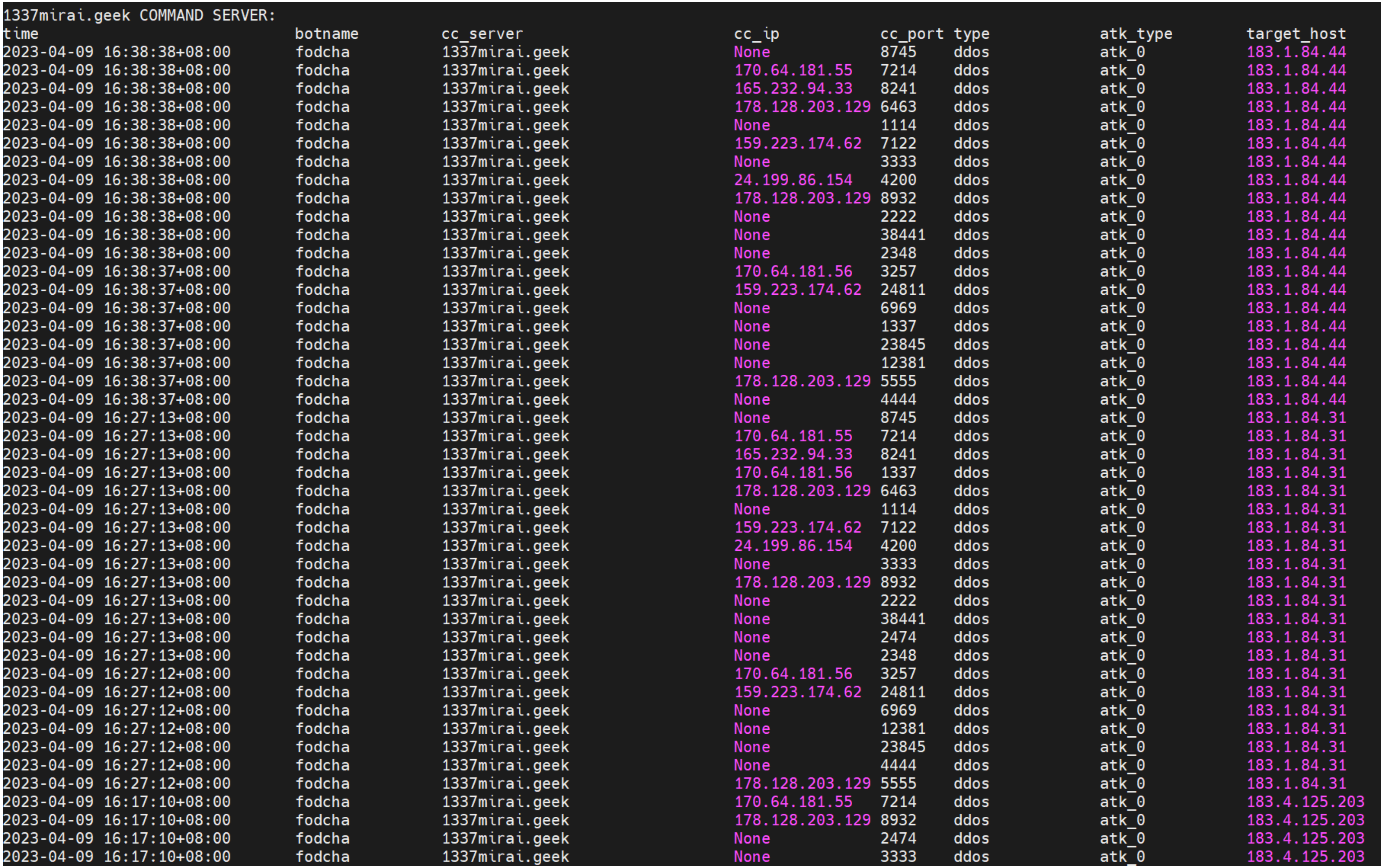


black{黑鹿计划}botnet
出售45-55K在线机器人僵尸网络
每天120usdt（rmb840）限制100次
每天200usdt （rmb1400）限制200次
每周800usdt（rmb5600）限制100次
每周1200usdt（rmb8400）限制200次
------------{VIP}------------
每天200usdt （rmb1400）限制100次
每天300usdt （rmb2100）限制200次
增添了100USDT可指定开通一种高级方法
购买一周计划可免费指定开通两种高级方法
购买一月计划可免费开通所有方法
秒杀德训台州{1Tbps udp 600Gbps小包Tcp Ack}
20U/60S测试
联系 @BlackneerA
支持一切安全方式担保
频道：https://t.me/DDOSUDPSYN8
群聊：https://t.me/WEblackneer
{{{{{如需月计划或定制冷却}}}}}随时联系大麋鹿
支持寒风担保~ 担保只走寒风！！！

Telegram
black{黑鹿计划}botnet
I'm the boss of botnets. I sell the most powerful botnets. They usually infect 30k-70k robots
我是唯一的所有者，我们出售庞大的力量，它拥有...

huangjin
zuanshi
huali13977
beijing
xiang5566
guo

Tracking: Example



```
1337mirai.geek COMMAND SERVER:
time                            botname         cc_server                       cc_ip           cc_port type            atk_type        target_host
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            8745    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  170.64.181.55   7214    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  165.232.94.33   8241    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  178.128.203.129 6463    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            1114    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  159.223.174.62  7122    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            3333    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  24.199.86.154   4200    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  178.128.203.129 8932    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            2222    ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            38441   ddos            atk_0           183.1.84.44
2023-04-09 16:38:38+08:00       fodcha          1337mirai.geek                  None            2348    ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  170.64.181.56   3257    ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  159.223.174.62  24811   ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  None            6969    ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  None            1337    ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  None            23845   ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  None            12381   ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  178.128.203.129 5555    ddos            atk_0           183.1.84.44
2023-04-09 16:38:37+08:00       fodcha          1337mirai.geek                  None            4444    ddos            atk_0           183.1.84.44
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            8745    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  170.64.181.55   7214    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  165.232.94.33   8241    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  170.64.181.56   1337    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  178.128.203.129 6463    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            1114    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  159.223.174.62  7122    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  24.199.86.154   4200    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            3333    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  178.128.203.129 8932    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            2222    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            38441   ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            2474    ddos            atk_0           183.1.84.31
2023-04-09 16:27:13+08:00       fodcha          1337mirai.geek                  None            2348    ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  170.64.181.56   3257    ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  159.223.174.62  24811   ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  None            6969    ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  None            12381   ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  None            23845   ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  None            4444    ddos            atk_0           183.1.84.31
2023-04-09 16:27:12+08:00       fodcha          1337mirai.geek                  178.128.203.129 5555    ddos            atk_0           183.1.84.31
2023-04-09 16:17:10+08:00       fodcha          1337mirai.geek                  170.64.181.55   7214    ddos            atk_0           183.4.125.203
2023-04-09 16:17:10+08:00       fodcha          1337mirai.geek                  178.128.203.129 8932    ddos            atk_0           183.4.125.203
2023-04-09 16:17:10+08:00       fodcha          1337mirai.geek                  None            2474    ddos            atk_0           183.4.125.203
2023-04-09 16:17:10+08:00       fodcha          1337mirai.geek                  None            3333    ddos            atk_0           183.4.125.203
```

Tracking: Method

Method A:

Contacting C&C servers with fake bots which re-implement the C&C protocols.

- C&C syntax and semantics are obtained by reverse engineering
- Having better control, while not taking part in the DDoS attacks

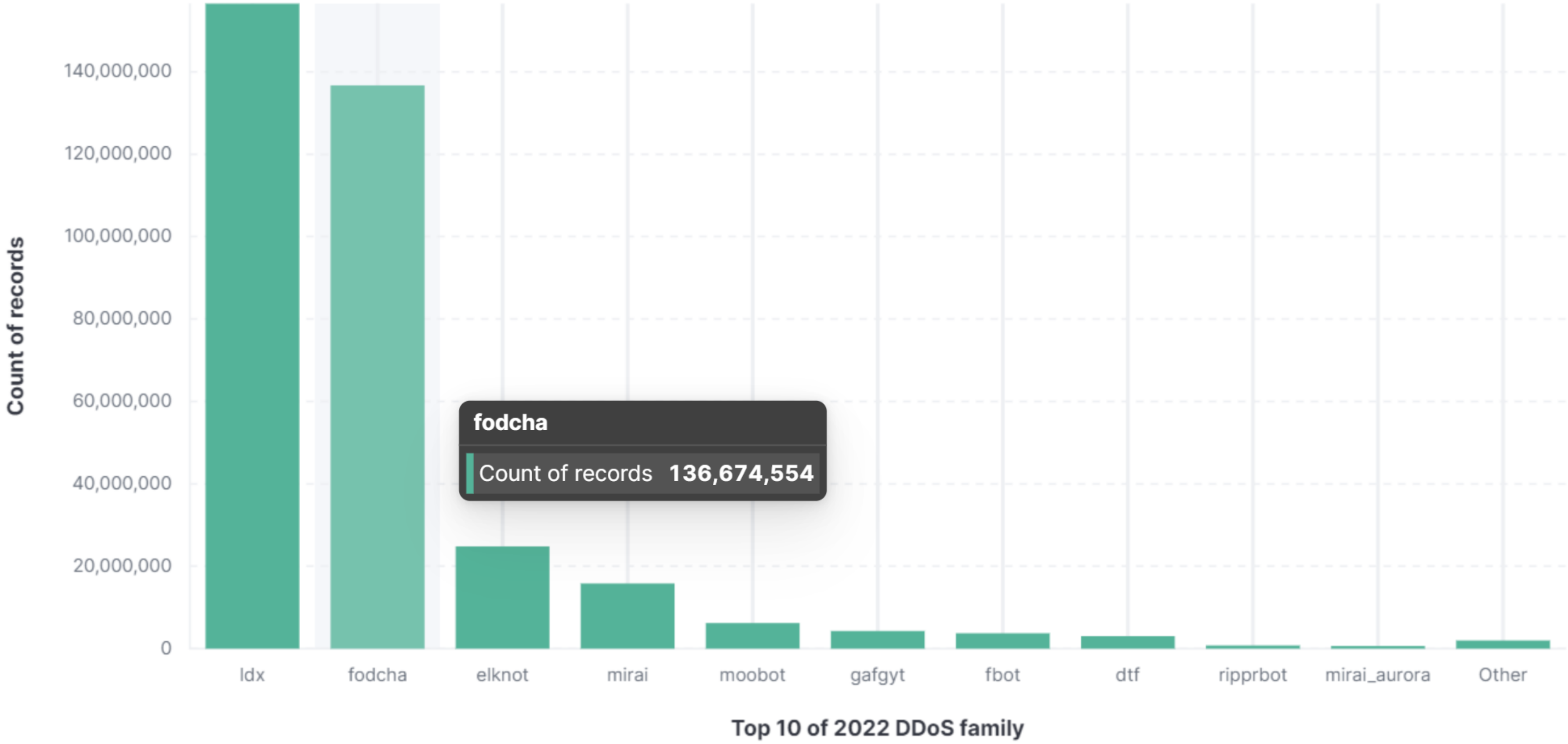
Method B:

Bots farm

Tracking: Fodcha Harvest

360 INTERNET SECURITY CENTER

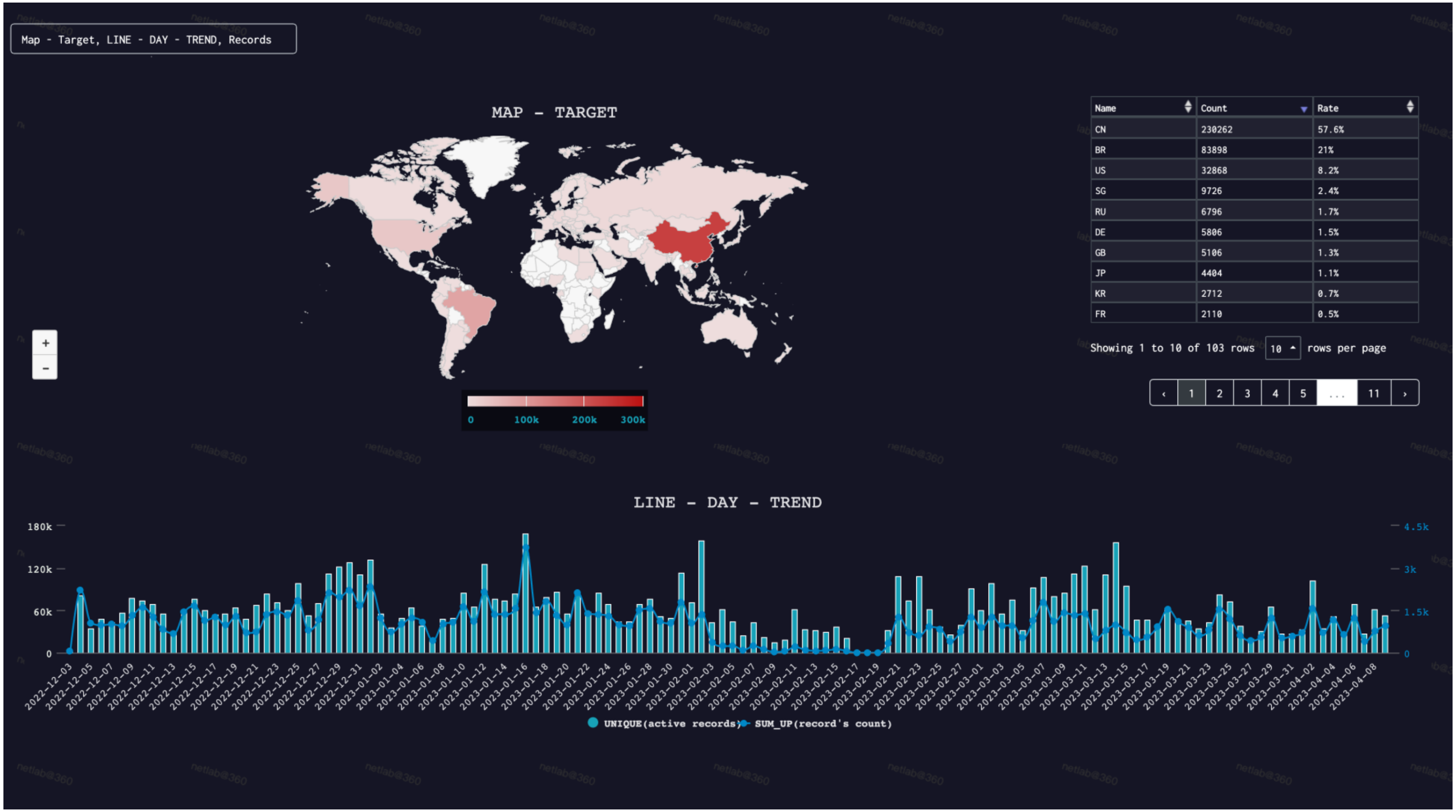
The most active new DDoS family in our sights



Statistics: Fodcha Overview

360 INTERNET SECURITY CENTER

Launching DDoS attacks like there is no tomorrow



Map - Target, LINE - DAY - TREND, Records

Name	Count	Rate
CN	230262	57.6%
BR	83898	21%
US	32868	8.2%
SG	9726	2.4%
RU	6796	1.7%
DE	5806	1.5%
GB	5106	1.3%
JP	4404	1.1%
KR	2712	0.7%
FR	2110	0.5%

Showing 1 to 10 of 103 rows 10 rows per page

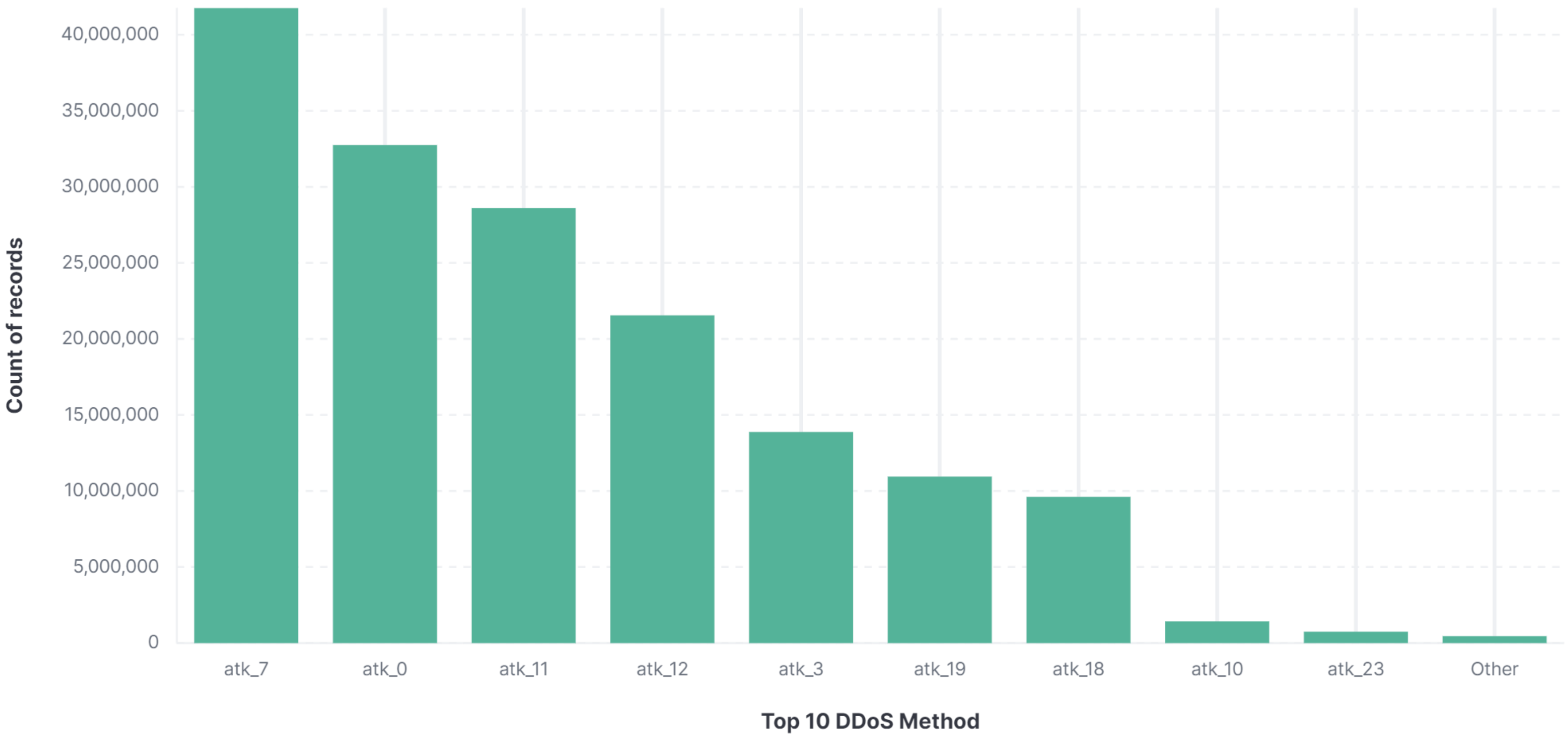
‹ 1 2 3 4 5 ... 11 ›

Statistics: Fodcha Overview

Launching DDoS attacks like there is no tomorrow

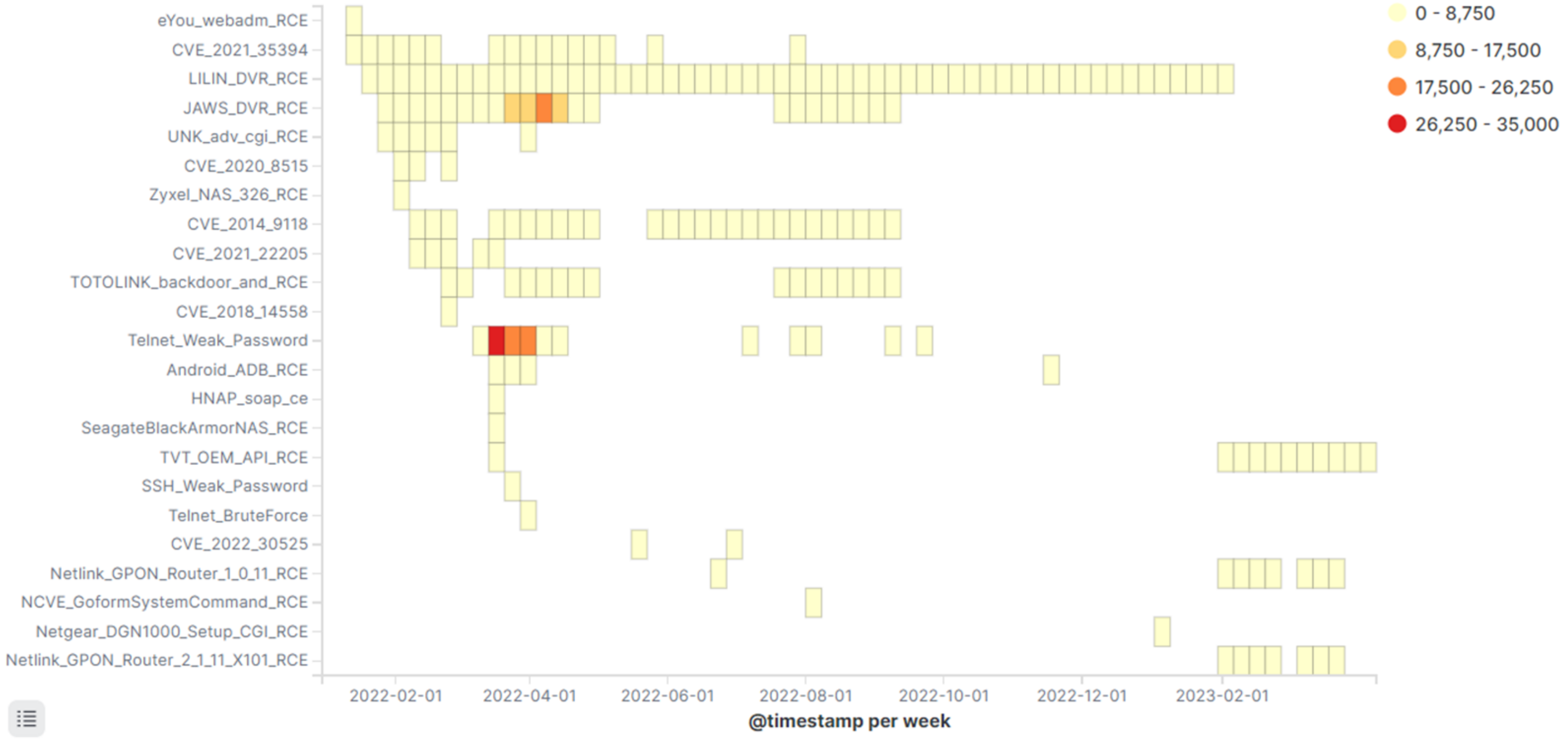
- 160,902,255 DDoS records, 7* 24
- 53,807 targets, all over the world
- Average 1k targets per day
- Peak 4014
- 38000+ bots

Statistics: DDoS Vectors



Statistics: Exploits

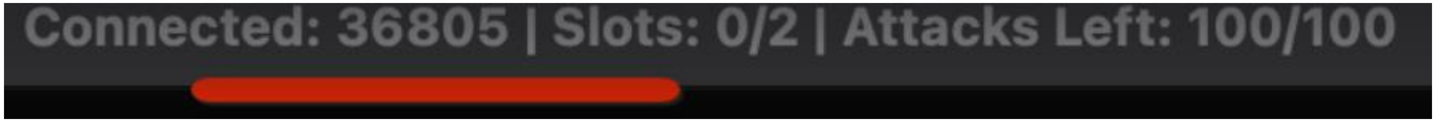
Exploits have been used by Fodcha which captured by honeypot



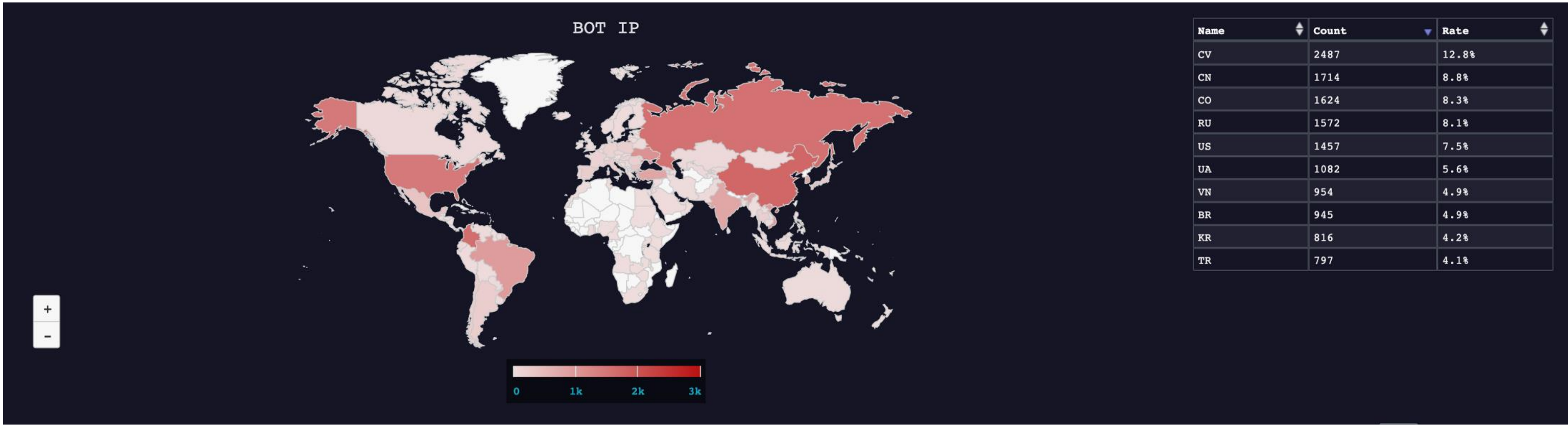
Statistics: Bot Scale

How do we measure the scale of the Fodcha botnet?

- ☐ under help of CNCERT (limited)
- ☐ use the bots info from panel,36805
- ☐ use the attack cmd from panel,19472 (limited)



Connected: 36805 | Slots: 0/2 | Attacks Left: 100/100



Name	Count	Rate
CV	2487	12.8%
CN	1714	8.8%
CO	1624	8.3%
RU	1572	8.1%
US	1457	7.5%
UA	1082	5.6%
VN	954	4.9%
BR	945	4.9%
KR	816	4.2%
TR	797	4.1%

Campaigns: No more details

2022.06.07-2022.06.08

It was monitored that Fodcha launched a DDoS attack on a health code organization of X Province

Campaigns: No more details

2022.09. xx

During the process of assisting a law enforcement agency to fix the evidence chain of a company's voice business being attacked by DDoS, it was found that Fodcha was behind the attack

Campaigns: No more details

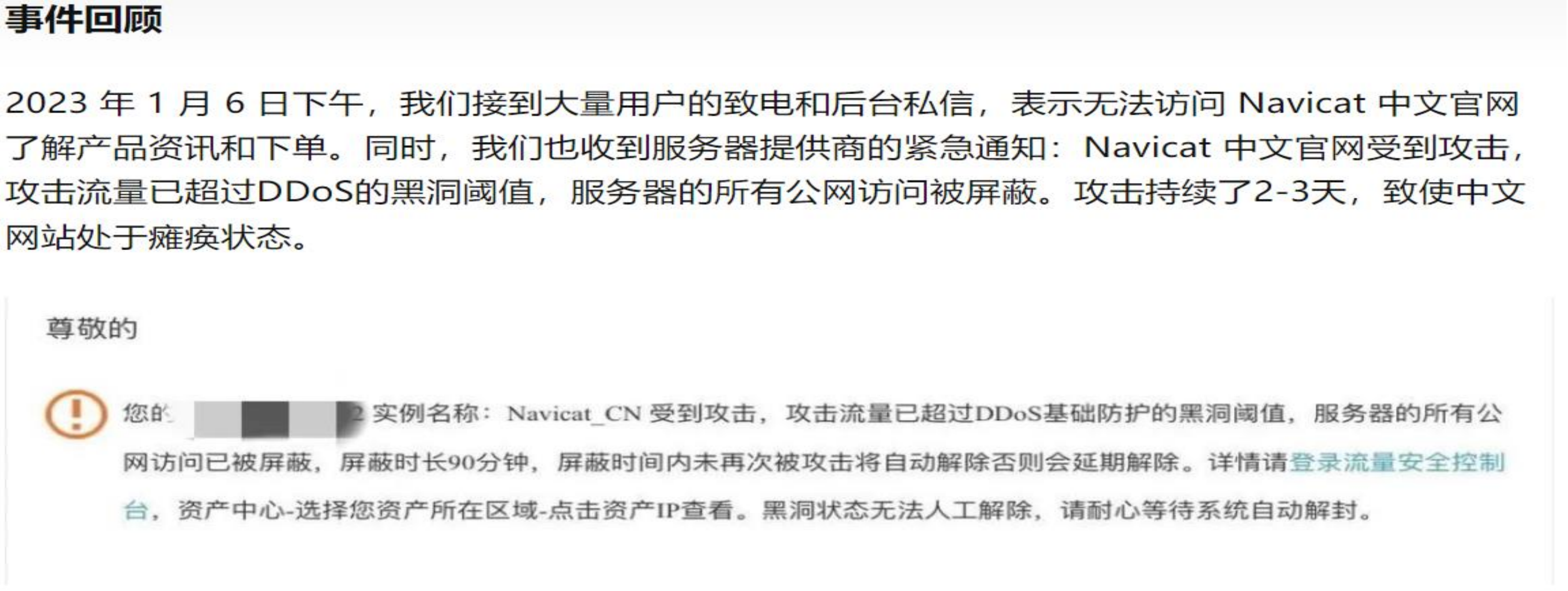
2022.09. 21

a well-known cloud service provider consulted us about an attack event with traffic exceeding 1Tbps. After cross-comparison of data, it was determined that the attacker was Fodcha.

Campaigns: Navicat

360 INTERNET SECURITY CENTER

Navicat.com.cn was attacked



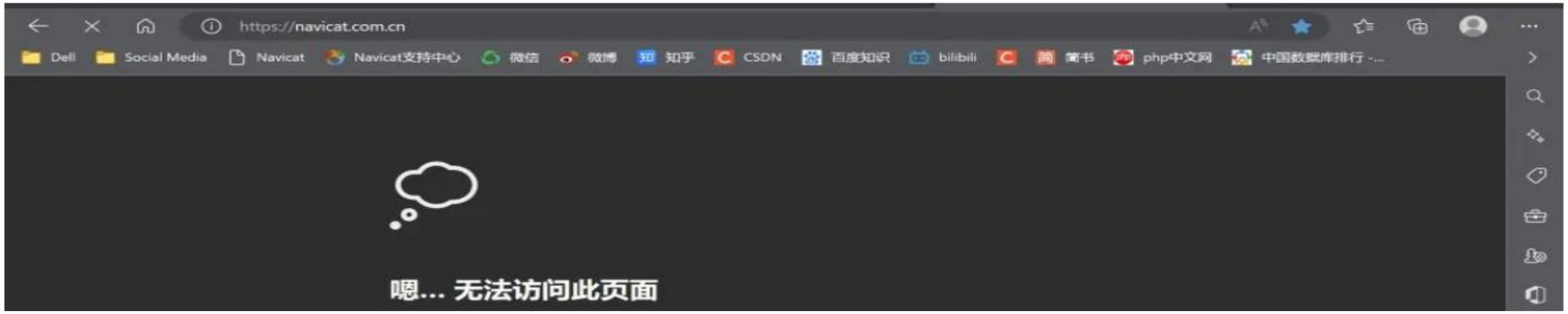
事件回顾

2023 年 1 月 6 日下午，我们接到大量用户的致电和后台私信，表示无法访问 Navicat 中文官网了解产品资讯和下单。同时，我们也收到服务器提供商的紧急通知：Navicat 中文官网受到攻击，攻击流量已超过DDoS的黑洞阈值，服务器的所有公网访问被屏蔽。攻击持续了2-3天，致使中文网站处于瘫痪状态。

尊敬的

您的 [redacted] 实例名称：Navicat_CN 受到攻击，攻击流量已超过DDoS基础防护的黑洞阈值，服务器的所有公网访问已被屏蔽，屏蔽时长90分钟，屏蔽时间内未再次被攻击将自动解除否则会延期解除。详情请登录流量安全控制台，资产中心-选择您资产所在区域-点击资产IP查看。黑洞状态无法人工解除，请耐心等待系统自动解封。

收到攻击的提醒邮件



https://navicat.com.cn

嗯… 无法访问此页面

Campaigns: Navicat

Allies

All we saw was the participation of the **Mirai botnet.**

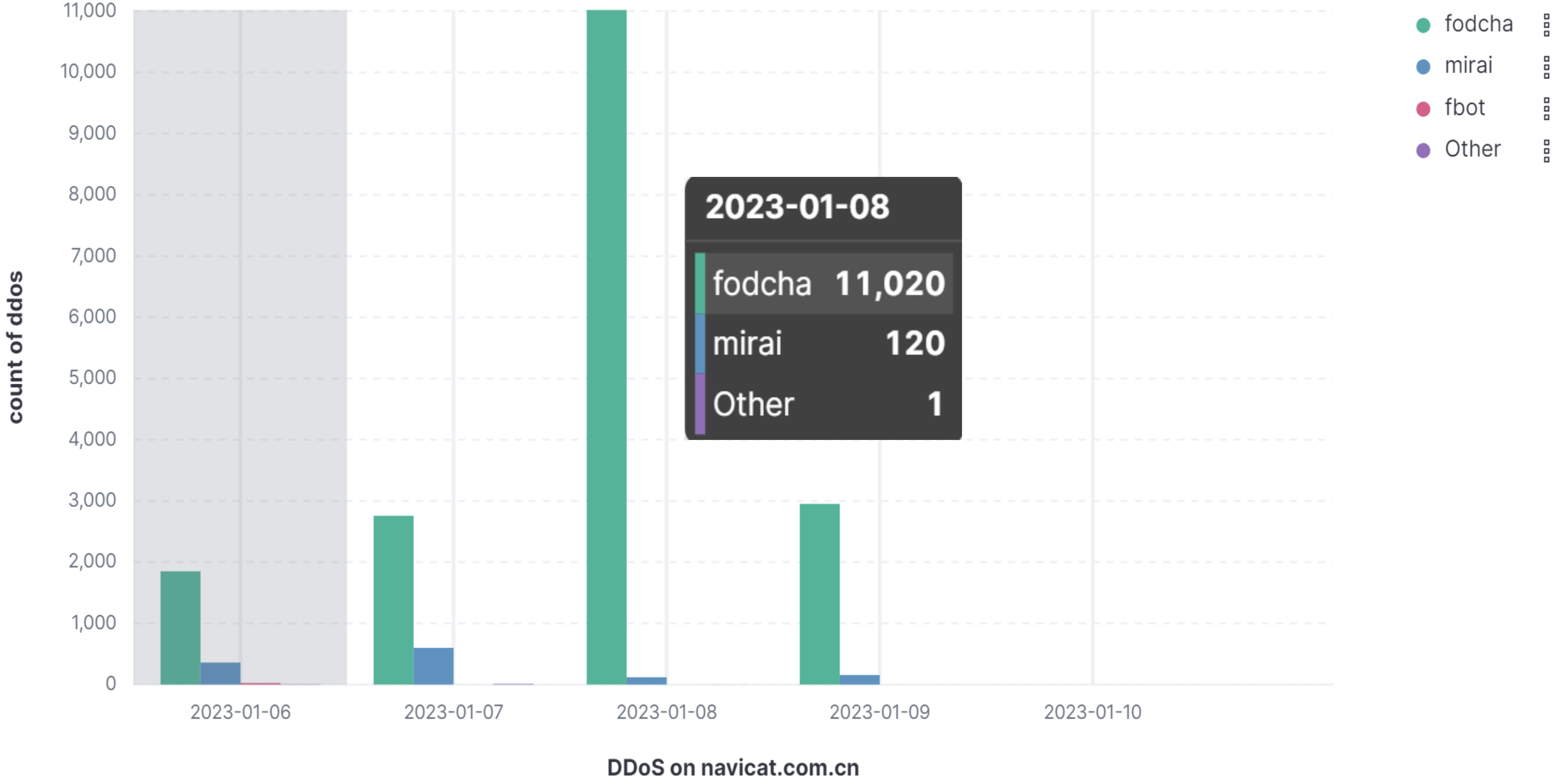
The peak of the attack occurred in more than 3 hours from 23:35 on January 6, 2023 to 02:45 on January 7, 2023

360Netlab

- ☐ Fodcha, Mirai, Fbot
- ☐ Fodcha 6-100x times bigger than Mirai
- ☐ 2022.01.08 reached the peak

Campaigns: Navicat

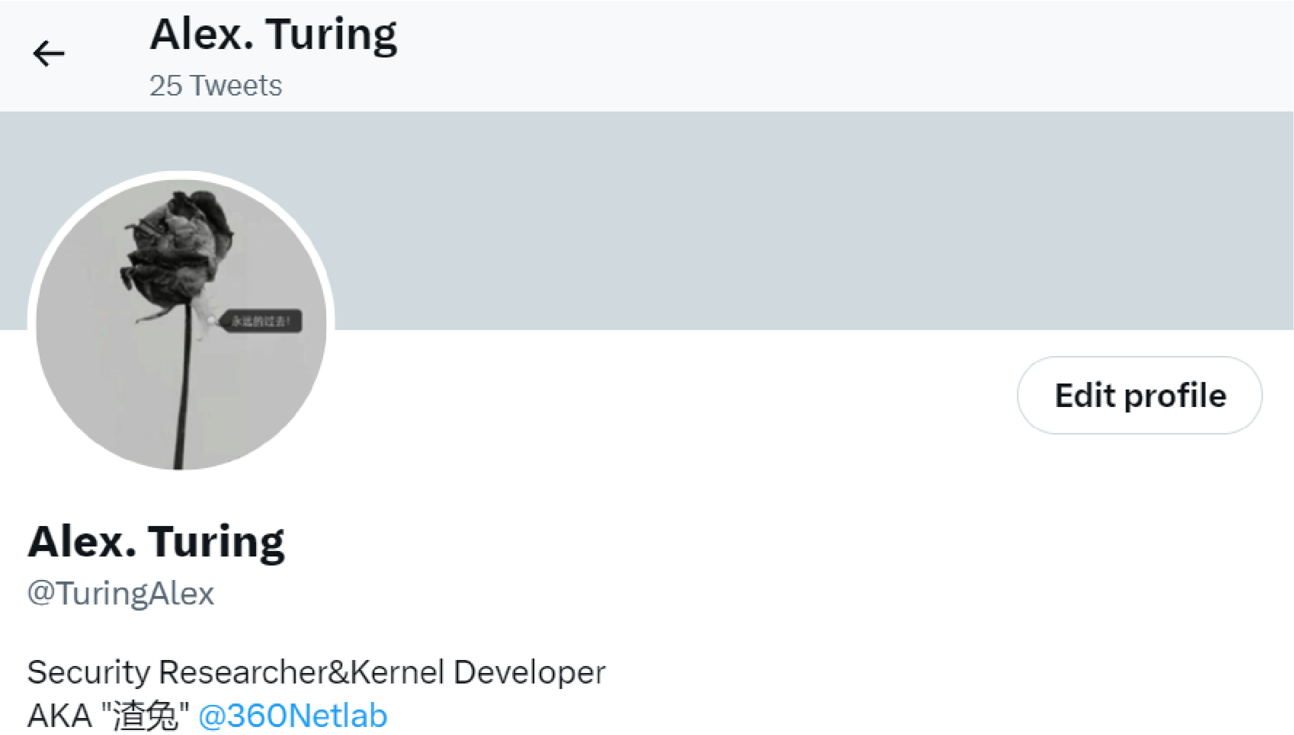
360 INTERNET SECURITY CENTER



Conclusions

- The Fodcha botnet infects the devices , attacks the targets located all over the world, sells its ability to customers.
- No specific country, Just Money-Driven
- The Fodcha botnet *is quite simple, there are a lot of botnets like* Fodcha over there, just keep fighting.
- Blog sometimes works!!!
- Botnet was like a box of chocolates, you never know what you’re gonna meet

Q&A



Alex. Turing

25 Tweets

Alex. Turing

@TuringAlex

Security Researcher&Kernel Developer
AKA "渣兔" @360Netlab