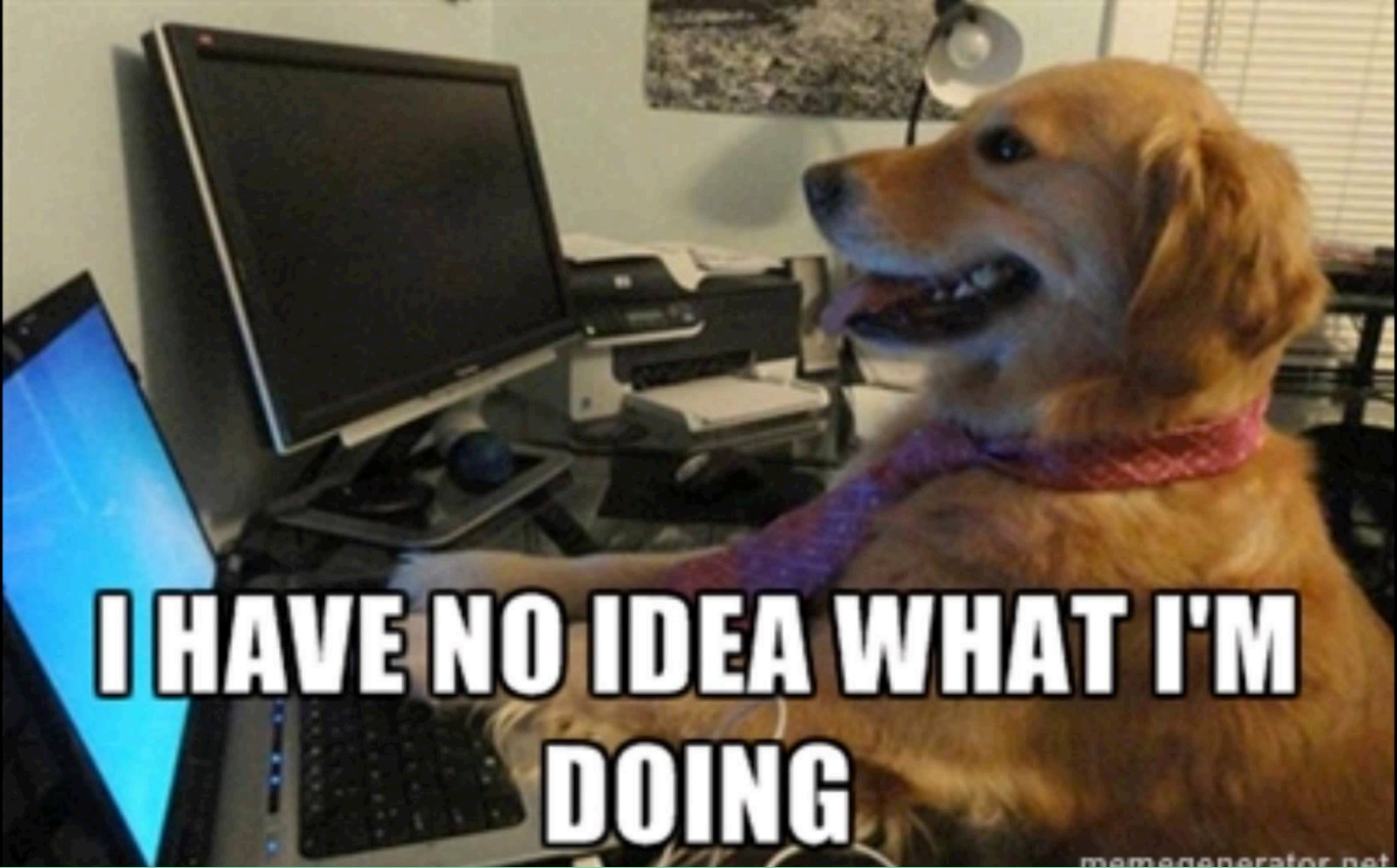
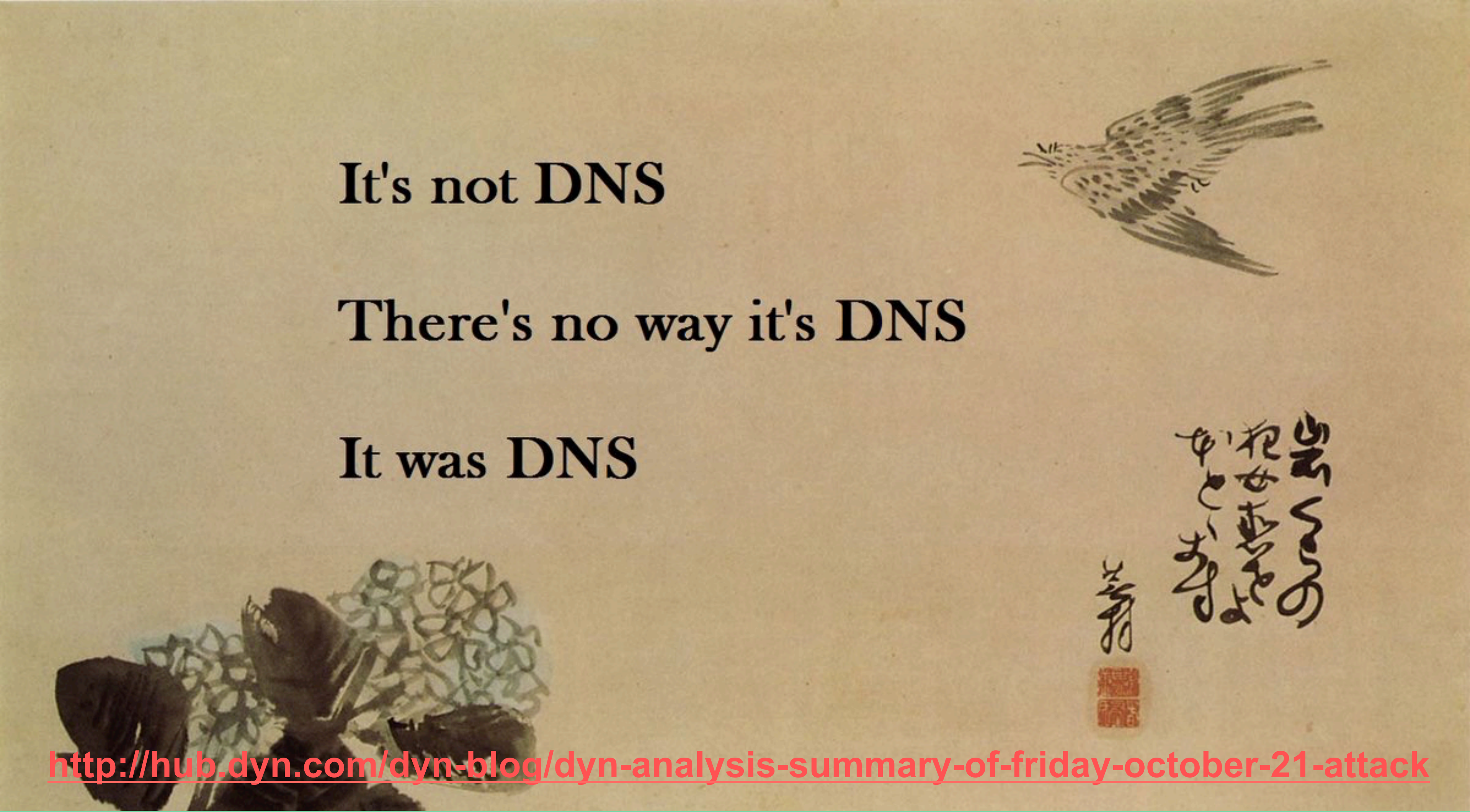
Mirai will ruin your day

Leslie Carr
Clover Health/SFMIX


I HAVE NO IDEA WHAT I'M DOING
memegenerator.net



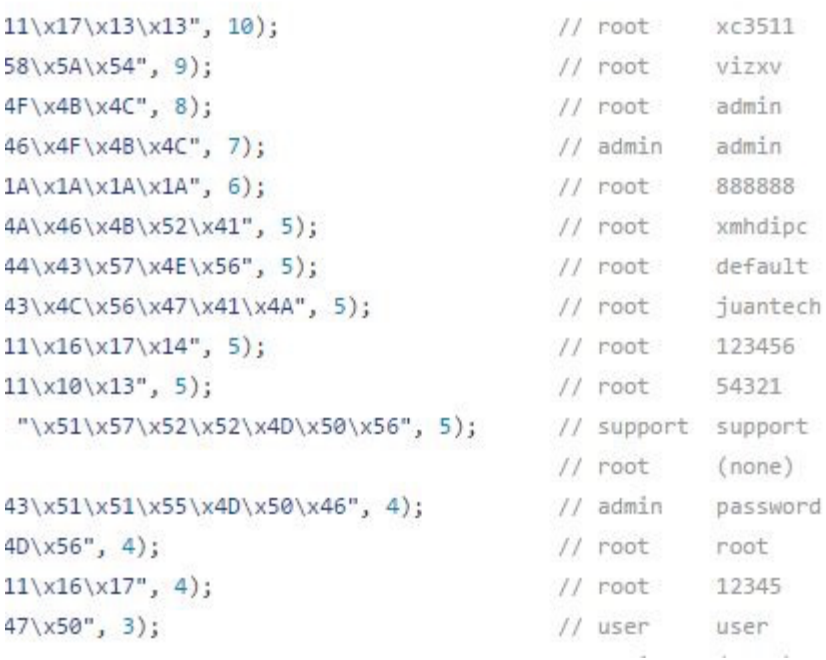
It's not DNS

There's no way it's DNS

It was DNS

http://hub.dyn.com/dyn-blog/dyn-analysis-summary-of-friday-october-21-attack

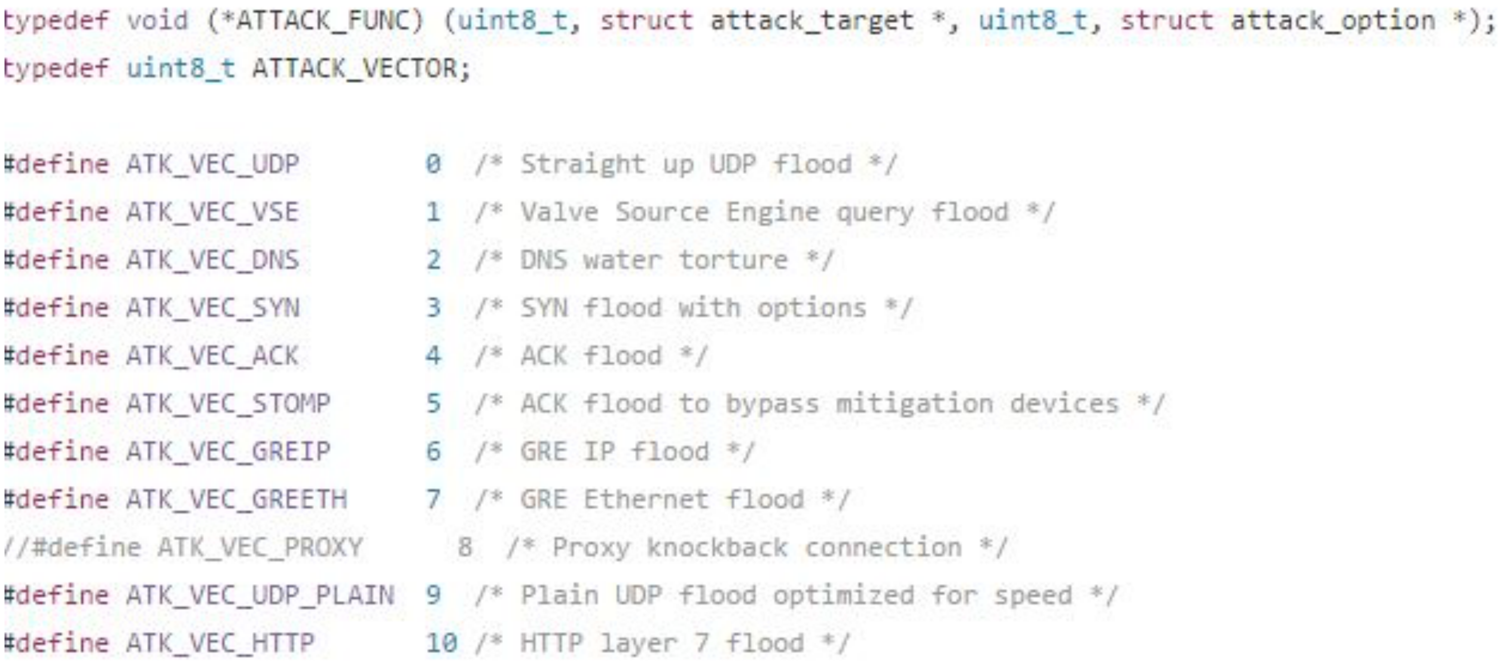
I can’t change my password!



```
11\x17\x13\x13", 10);                      // root     xc3511
58\x5A\x54", 9);                           // root     vizxv
4F\x4B\x4C", 8);                           // root     admin
46\x4F\x4B\x4C", 7);                       // admin    admin
1A\x1A\x1A\x1A", 6);                       // root     888888
4A\x46\x4B\x52\x41", 5);                   // root     xmhdipc
44\x43\x57\x4E\x56", 5);                   // root     default
43\x4C\x56\x47\x41\x4A", 5);               // root     juantech
11\x16\x17\x14", 5);                       // root     123456
11\x10\x13", 5);                           // root     54321
 "\x51\x57\x52\x52\x4D\x50\x56", 5);       // support  support
                                           // root     (none)
43\x51\x51\x55\x4D\x50\x46", 4);           // admin    password
4D\x56", 4);                               // root     root
11\x16\x17", 4);                           // root     12345
47\x50", 3);                               // user     user
```

http://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/

Multiple types of attack



```
typedef void (*ATTACK_FUNC) (uint8_t, struct attack_target *, uint8_t, struct attack_option *);
typedef uint8_t ATTACK_VECTOR;

#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP       10 /* HTTP layer 7 flood */
```

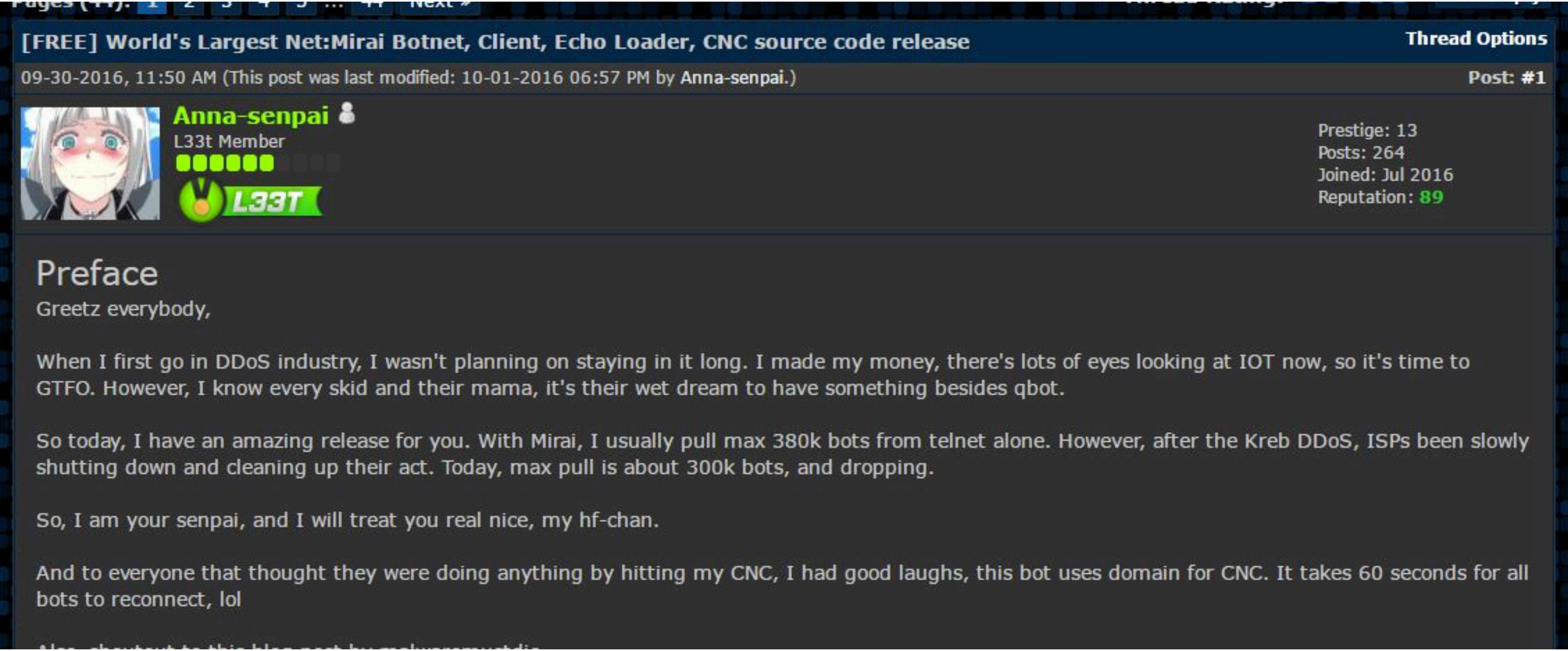
Controller uses load balancing!

DNS load balancing… to kill DNS?

TCP/103 is the control port

https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/

Free, like the wind!



[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.)

Anna-senpai
L33t Member

Prestige: 13
Posts: 264
Joined: Jul 2016
Reputation: 89

Preface

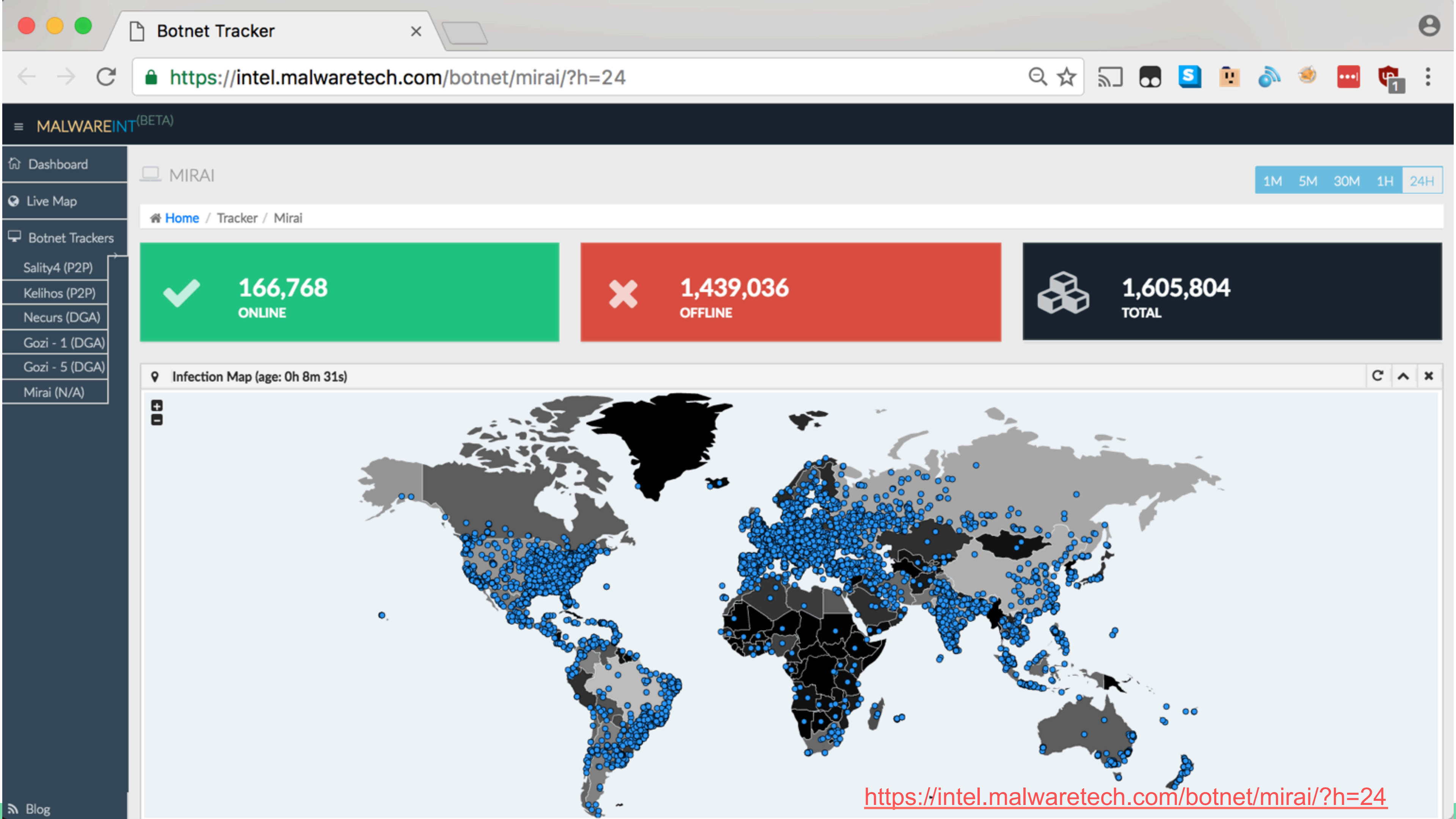
Greetz everybody,

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



https://intel.malwaretech.com/botnet/mirai/?h=24

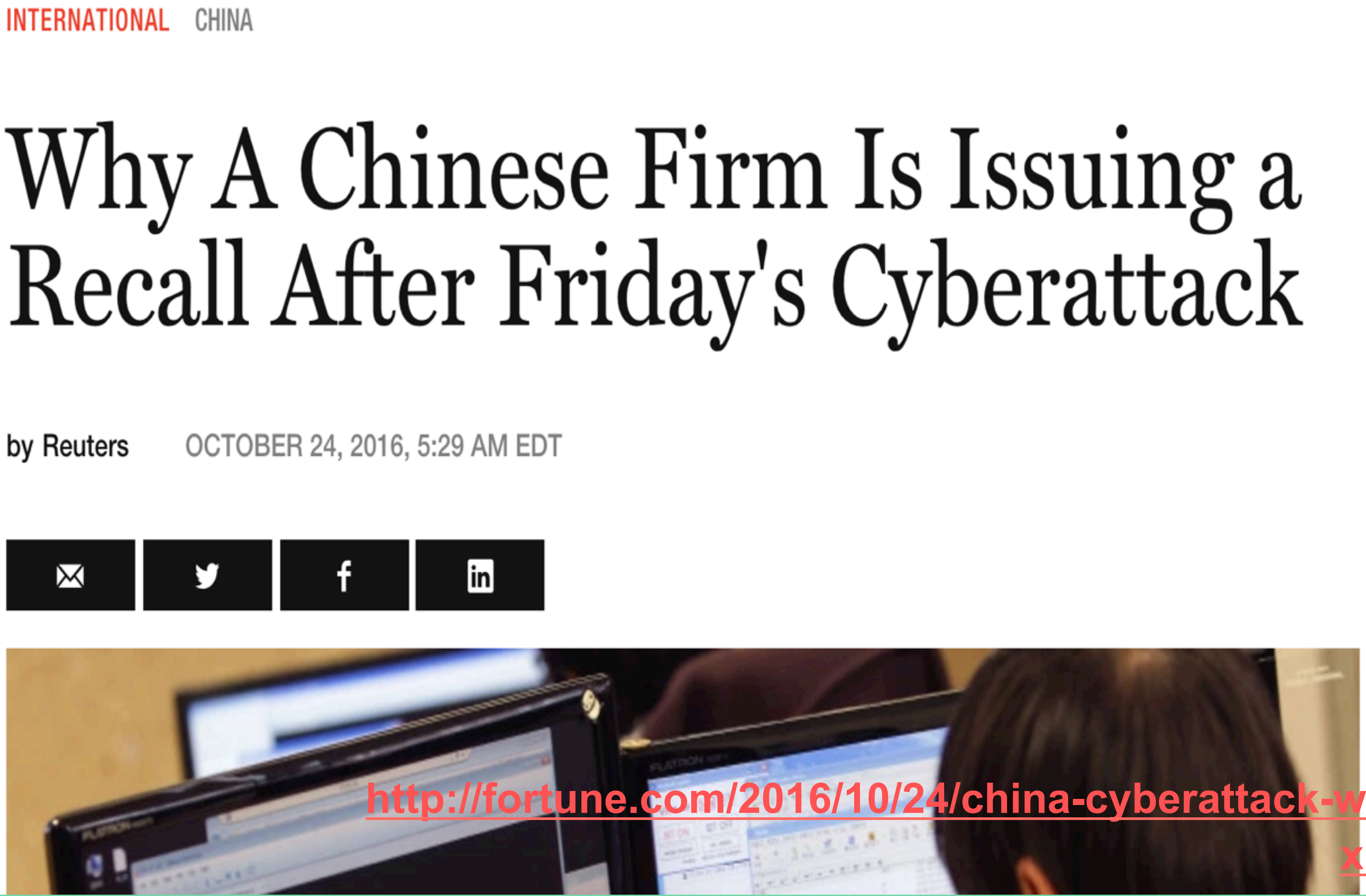
166,768 ONLINE

1,439,036 OFFLINE

1,605,804 TOTAL

Infection Map (age: 0h 8m 31s)

https://intel.malwaretech.com/botnet/mirai/?h=24



INTERNATIONAL CHINA

Why A Chinese Firm Is Issuing a Recall After Friday's Cyberattack

by Reuters OCTOBER 24, 2016, 5:29 AM EDT

http://fortune.com/2016/10/24/china-cyberattack-webcams-xiongmai/

Questions?

Leslie Carr

@lesliegeek