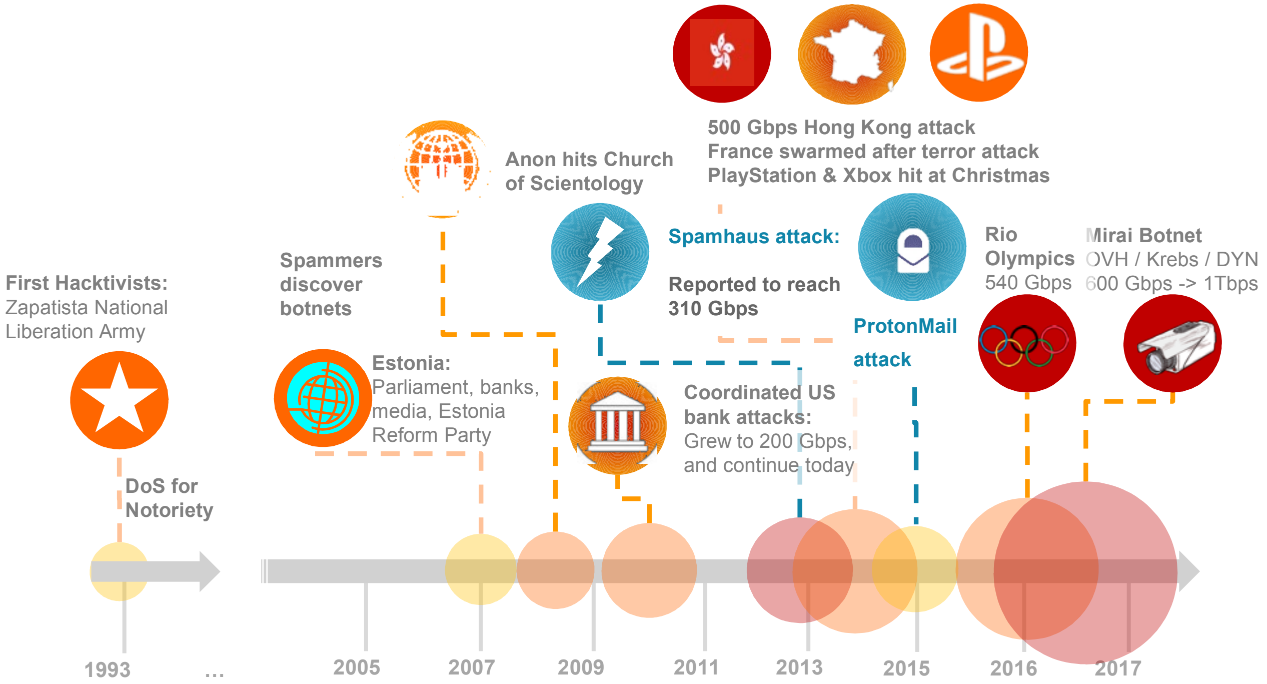
IoT as an Attack Vector

The DDoS Game Changer!

Sean Newman
Director Product Management

IoT-Based DDoS Dominates the Headlines!...



First Hacktivists:
Zapatista National
Liberation Army

DoS for Notoriety

Spammers discover botnets

Estonia:
Parliament, banks,
media, Estonia
Reform Party

Anon hits Church of Scientology

Spamhaus attack:

Reported to reach 310 Gbps

Coordinated US bank attacks:
Grew to 200 Gbps,
and continue today

500 Gbps Hong Kong attack
France swarmed after terror attack
PlayStation & Xbox hit at Christmas

ProtonMail attack

Rio Olympics
540 Gbps

Mirai Botnet
OVH / Krebs / DYN
600 Gbps -> 1Tbps

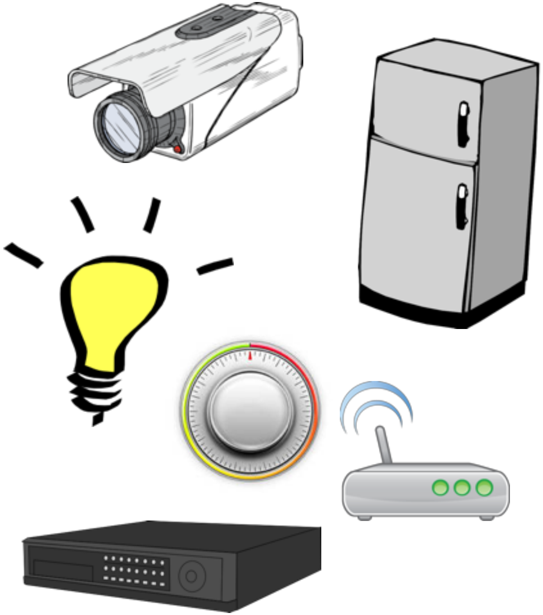
DDoS Evolving - “DoT” ups the Challenge

- Gartner, Inc. forecasts that Internet connected things will exceed 20 billion by 2020.

- Mirai malware code made public in Oct 2016 spreads to devices with factory default or hard-coded usernames and passwords

- Countless attack vectors and attack types out in the wild - Newly discovered ELF_IMEIJ.A and Amnesia malware

- New techniques, multi-vector attacks, DDoS-for-hire services, coupled with unlimited motivations create a volatile DDoS landscape



Friend or Foe?

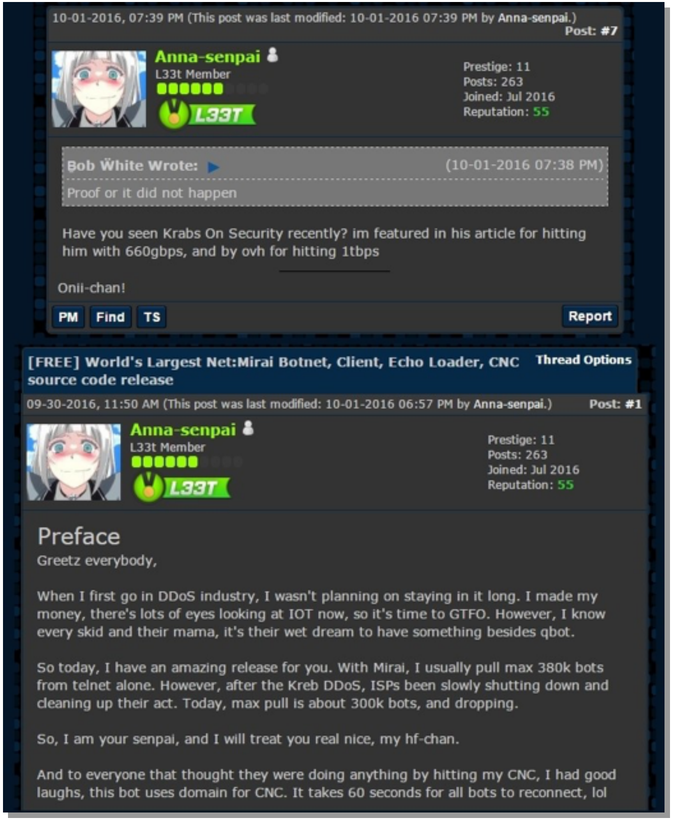
http://www.gartner.com/newsroom/id/3165317

Mirai - The Game Changer

- Hacker forum confirms Mirai link to attacks that started this DDoS revolution

- And announcement of the source code being published online, enabling many of the Mirai attacks and derivatives seen since!

- Lightbulb moment that inspired a whole new generation and scale
of DDoS attacks



10-01-2016, 07:39 PM (This post was last modified: 10-01-2016 07:39 PM by Anna-senpai.) Post: #7

Anna-senpai
L33t Member

Prestige: 11
Posts: 263
Joined: Jul 2016
Reputation: 55

> Bob White Wrote: (10-01-2016 07:38 PM)
> Proof or it did not happen

Have you seen Krabs On Security recently? im featured in his article for hitting him with 660gbps, and by ovh for hitting 1tbps

Onii-chan!

[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
L33t Member

Prestige: 11
Posts: 263
Joined: Jul 2016
Reputation: 55

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.

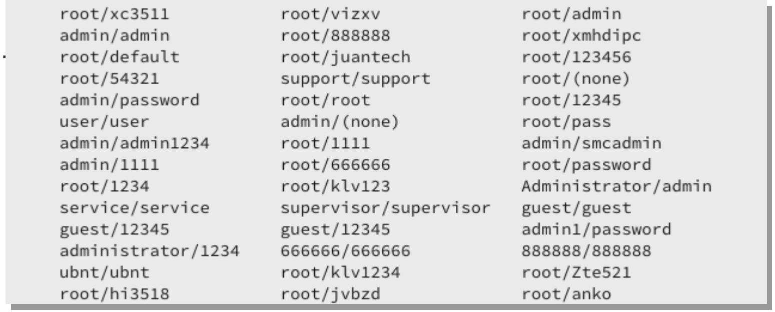
So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISPs been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

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

Mirai Botnet Overview

- **Bot** (written in C) targets IoT devices with BusyBox embedded Linux
- Compromised Devices establish **CnC** connection back, to join the Bot
- Existing infected devices also scan for new victims
- New Victims compromised using default username-password list
- **ScanListen** Process (written in GO) listens for bot reporting new victims



```
root/xc3511          root/vizxv              root/admin
admin/admin          root/888888             root/xmhdipc
root/default         root/juantech           root/123456
root/54321           support/support         root/(none)
admin/password       root/root               root/12345
user/user            admin/(none)            root/pass
admin/admin1234      root/1111               admin/smcadmin
admin/1111           root/666666             root/password
root/1234            root/klv123             Administrator/admin
service/service      supervisor/supervisor   guest/guest
guest/12345          guest/12345             admin1/password
administrator/1234   666666/666666           888888/888888
ubnt/ubnt            root/klv1234            root/Zte521
root/hi3518          root/jvbzd              root/anko
```

- **Loader** (wri new victim

Mirai Attack Armoury

- Multiple pre-loaded DDoS attack vectors to choose from:

```
#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 targeting DNS Server */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood with crude mitigation evasion */
#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 GET flood */
```

- Easy for derivatives to modify or include additional vectors

New Malware/Botnets Leveraging IoT

- **ELF_IMEIJ.A**[1] Targeting AVTech Cameras
  - 130,000 Vulnerable devices, of just one device type!
  - cgi-bin script pings random IPs searching for vulnerable devices
  - Uses reported CloudSetup.cgi command injection vulnerability
    - Tricks device into downloading and changing file's permissions to execute it locally

- **Tsunami** Botnet Variant "**Amnesia2**" Targeting TVT DVRs
  - Leverages remote code execution vulnerability, unpatched since March 2016
  - 227,000 Known Vulnerable Devices from same OEM manufacturer
  - Includes Malware Analysis Sandbox Evasion Techniques
  - Spreads by scanning for new devices to infect – similar to Mirai

[1] Originally Discovered by Trend Mirco Researchers in October 2016

[2] Recently Discovered by Palo Alto Networks 'Unit 42' Researchers

The Answer - Community Responsibility?

Carriers can do more to enable ‘clean pipe’ to their downstream subscribers – cleaning up attack traffic as well as ensuring that compromised devices on their access network are quickly identified and remediated

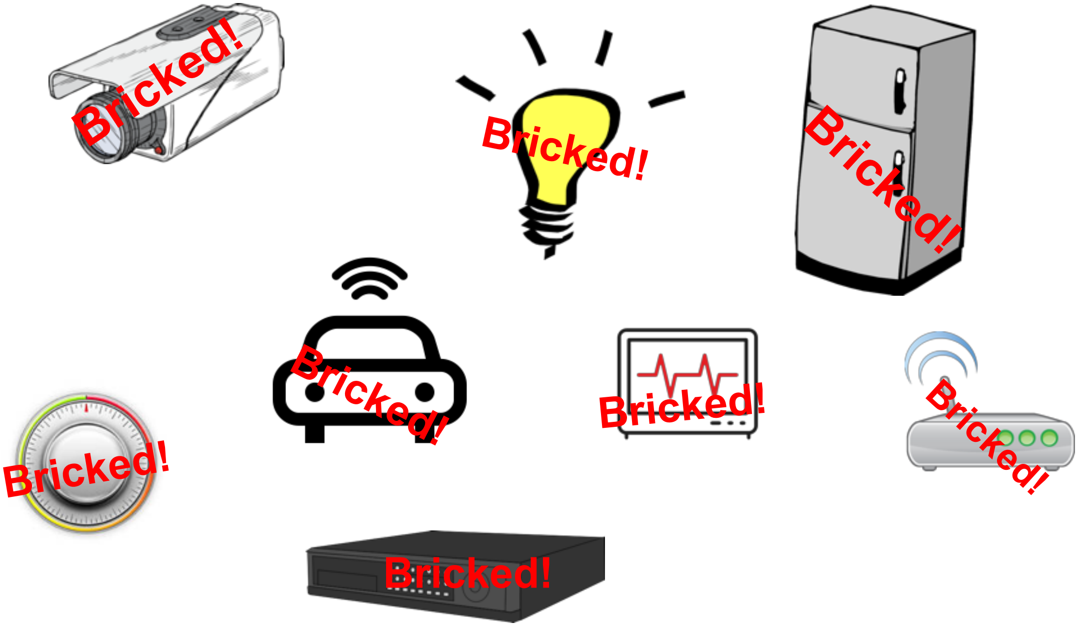
Device Manufacturers must put security measures in place. E.g. No device should connect to the Internet ‘out of the box’

May require government legislation forcing Carriers and Manufactures of IoT devices alike to work toward eliminating the problem

Can the security industry do more – for example the newly formed IoT Cybersecurity Alliance?

Probably *not* the Answer – BrickerBot!

- Vigilante Mirai-like Bot, disabling poorly secured IoT devices!



Questions?

Thank You!