

EPRIVACY Roma 2018  
in-sicurezza dei dati raccolti  
FabioCarletti aka Ryuw



# E-privacy Roma 2018

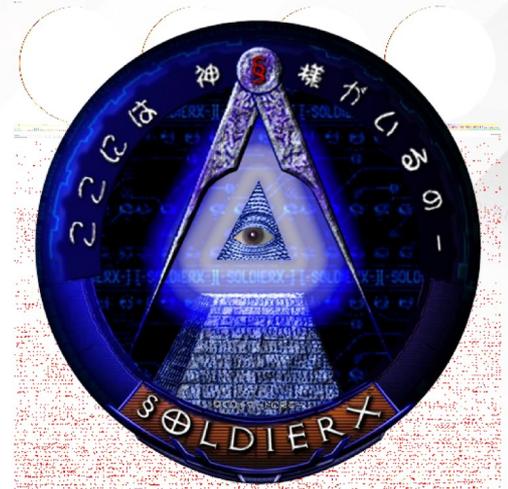
Whoami

Security/OpenSource evangelist ITC

Membro Soldierx

Work on Lejot OpenSource Technology

I like Unix ;-)





## E-privacy 2018 Roma IoT in-sicurezza

- In telecomunicazioni Internet delle cose (Internet degli oggetti o IoT, acronimo dell'inglese Internet of things) è un neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti.
- Applicazioni: domotica, robotica, avionica, industria automobilistica, telemetria, reti wireless di sensori, sorveglianza, smart metering, sistemi embedded e agricoltura,....



## E-privacy 2018 Roma IoT in-sicurezza

- Privacy-autonomia-controllo
- Tecnologia-forte influenza sulle nostre decisioni morali e agire dell'uomo e la sua privacy ed autonomia.
- Wired “ciò che stiamo per perdere è la nostra privacy”--→ non avremo più privacy dovremo guardare il concetto di privacy che verrà sconvolto sotto il nostro naso.



## E-privacy 2018 Roma IoT in-sicurezza

- Fenomeno domotica “Fai da te” - elettrodomestici/piccoli dispositivi di uso comune permettono di svolgere compiti “da remoto”.
- smartCam/smartTv/smartLight/smart...
- status simbol dal quale vantarsi
- dopo l’installazione si trascurano qualità supporto/assistenza del produttore.



# E-privacy 2018 Roma IoT in-sicurezza



## E-privacy 2018 Roma IoT in-sicurezza

- l'utente medio dopo l'installazione dimentica la loro esistenza.
- l'utente medio sottovaluta la in-sicurezza che può scaturire a causa di misconfigurazione di un dispositivo di rete IoT.
- L'utente medio non si preoccupa di aggiornare firmware dei sistemi.



# E-privacy 2018 Roma IoT in-sicurezza

-firmware/dispositivi abbandonati dal produttore.

-Tali dispositivi senza aggiornamenti espongono i dispositivi ad agenti malevoli l'ascianto l'utente ad attacchi mirati come webcam,..ecc



## E-privacy 2018 Roma IoT in-sicurezza

Confidenzialità (garanzia che solo le persone autorizzate possano modificare il sistema e i dati)

Integrità (garanzia che solo le persone autorizzate possano modificare i dati)

Disponibilità (garanzia che il sistema è in grado di fornire i servizi previsti)



## E-privacy 2018 Roma IoT in-sicurezza

Identificazione - risponde alla domanda chi sei?

Autenticazione - risponde alla domanda come mi accerto che sei te?

Il meccanismo della security IT si basa sulla risposta alla due domande: “chi sei?” E “cosa puoi fare?”



# E-privacy 2018 Roma IoT in-sicurezza

IoT=password default ---> botnet mirai.

Caso Mirai attacco dovuto errate  
configurazioni definite dall'utente  
utilizzatore.

- 93% degli attacchi rivelati bruteforce

-PreConfigure password vanno sostituite  
con password complicate



# E-privacy 2018 Roma IoT in-sicurezza

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	-
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	-
winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	-
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	-
RDP	3389	0.12%	Bruteforce	-
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	-



# E-privacy 2018 Roma IoT in-sicurezza

Shodan→ il motore di ricerca IoT

Shodan=servizio online che permette di trovare dispositivi IoT connessi in giro per il mondo come webcam,router,..ecc

-cercando vendor IoT possibile accedere a strade webcam interne di negozi e abitazioni.

-dispositivi lasciati liberamente raggiungibili senza password firmware obsoleti



# E-privacy 2018 Roma IoT in-sicurezza



SHODAN IoT  [Explore](#) [Developer Pricing](#) [Enterprise Access](#) [Contact Us](#)

[Exploits](#) [Maps](#)

---

**TOTAL RESULTS**

**8,723**

**TOP COUNTRIES**



Korea, Republic of	4,640
Taiwan	884
United States	785
China	329
Canada	264

**TOP SERVICES**

SNMP	3,351
8081	1,880
8083	1,764
HTTPS	463
HTTP	379

**TOP ORGANIZATIONS**

SK Telecom	2,366
Korea Telecom	1,642
Taiwan Academic Network (TANet) In...	291
Taiwan Academic Network	282
SoftLayer Technologies	231

**TOP OPERATING SYSTEMS**

Windows 6.1	7
Linux 3.x	3
QTS	1
Linux 2.6.x	1

---

**103.210.24.247**  
**Oocom Pty**  
Added on 2018-11-15 17:20:24 GMT  
 Australia, Cranbourne  
[Details](#)

FUJI XEROX DocuPrint M455 df; Net 81.31.ESS 201605230656, **IoT** 01.72.00

---

**223.62.48.226**  
**SK Telecom**  
Added on 2018-11-15 17:18:58 GMT  
 Korea, Republic of  
[Details](#)

HTTP/1.1 200 OK  
Content-Type: text/html  
ETag: "1036239157"  
Last-Modified: Fri, 01 Apr 2016 13:05:48 GMT  
Content-Length: 5703  
Date: Thu, 15 Nov 2018 17:13:27 GMT  
Server: lighttpd/1.4.20

```
<html>
<head>
<title>Login to SDT-CS3B1</title>
<meta http-equiv="content-type" content="text/html; ...
```

---

**ERROR: The request could not be satisfied**  
2800-9000:2009:c200:9:c26:1590:bd82  
Added on 2018-11-15 17:18:52 GMT  
 United States  
[Details](#)

HTTP/1.1 403 Forbidden  
Server: CloudFront  
Date: Thu, 15 Nov 2018 17:18:52 GMT  
Content-Type: text/html  
Content-Length: 556  
Connection: keep-alive  
X-Cache: Error from cloudfront  
Via: 1.1 9bf53fbf949b06bf7635b36bc0201861.cloudfront.net (CloudFront)  
X-Amz-Cf-Id: **iot-j\_1xxPk2\_luHW1vaYRFdc6h-C8...**

---

**77.85.193.44**  
77-85-193-44.jp.bto-net.bg  
**Vivacom**  
Added on 2018-11-15 17:18:58 GMT  
 Bulgaria  
[Details](#)



## Standout Industries In Sales Increases

LET'S TALK NEW JOBS

OTHER POTENTIALS

### TELECOMMUNICATIONS



### AUTOMOBILE



### FOOD PRODUCTS



### AIR TRANSPORTATION



### RETAIL



### PUBLISHING



-privacy18 Roma



# E-privacy 2018 Roma IoT in-sicurezza

					
<i>Cloud Services</i>	Nest Cloud/ Google Cloud	Azure IoT	AWS IoT	iCloud	ARTIK Cloud/ SmartThings
<i>Application Protocols</i>	Weave	AMQP	MQTT	HomeKit	MQTT
<i>Network Protocols</i>	WiFi/Thread	WiFi	WiFi	WiFi/BLE	WiFi/ZigBee/ BLE/Thread
<i>Operating Systems</i>	Linux/Android Things	Windows IoT	Linux/AWS Greengrass	iOS	Linux/ARTIK



## E-privacy 2018 Roma IoT in-sicurezza

-Mozilla, our mission is to “ensure the Internet is a global public resource, open and accessible to all.” The Internet of Things (IoT) is a new era of the Internet where everything around us can be connected. This presents many new opportunities and challenges. The Mozilla IoT community is dedicated to applying Mozilla's values to the Internet of Things and working towards a decentralized IoT with new standards around security, privacy and interoperability.





# E-privacy 2018 Roma [iot.mozilla.org](http://iot.mozilla.org)

Project Things is an experimental framework of software and services from Mozilla for connecting "things": [github.com/mozilla-iot](https://github.com/mozilla-iot)

-Things Gateway=An implementation of a Web of Things gateway.

-Things Cloud=A collection of IoT cloud services.

-Things Framework=A collection of re-useable software components for building Web Things.



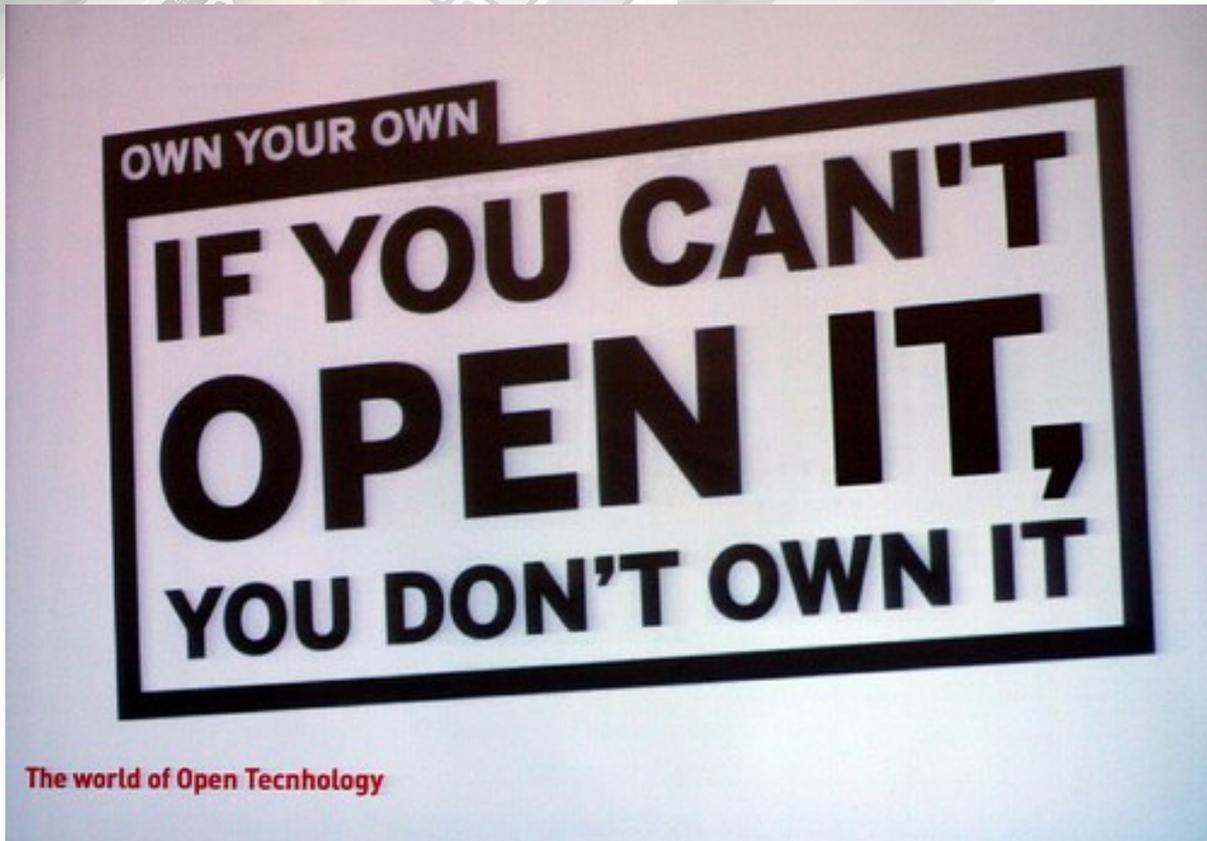
# E-privacy 2018 Roma IoT in-sicurezza

Problemi:

- produttori rilasciano patch di sicurezza?
- prodotti lowcost
- i venditori tendono al profitto e scapito della sicurezza
- mancanza di norme sulla sicurezza IoT



# e-privacy Roma IoT in-sicurezza



# e-privacy Roma IoT in-sicurezza

Open source is good for me. I will fully embrace it.  
Open source is good for me. I will fully embrace it.  
Open source is good for me. I will fully embrace it.  
Open source is good for me. I will fully embrace it.  
Open source is good for me. I will fully embrace it.  
Open source is good for me. I will fully embrace it.



Contatti

Skype:fabio.carletti.ryuw

Email:fabiocarlettiryuw@gmail.com

FB:facebook.com/fabioryuw

Links:

[www.facebook.com/sicurezzainformatica1/](https://www.facebook.com/sicurezzainformatica1/)

<https://iot.mozilla.org/>

[www.shodan.io](https://www.shodan.io)

***GRAZIE PER  
L'ATTENZIONE!!***

