



## ***OSINT e data leak su dispositivi IoT***

Leonida Reitano

Roma 17/12/2015

# Agenda

---

- ➔ • Presentazione relatore
- Osint introduzione
- Internet of Things
- I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- Bibliografia & sitografia

# Presentazione relatore

---

## Leonida Reitano

Dottore di ricerca in sociologia della comunicazione e McLuhan fellow dal febbraio 2003

Dal 2007 è Presidente dell'Associazione di Giornalismo Investigativo e svolge attività di ricerca e di didattica nell'ambito delle metodologie legate al giornalismo. Nel maggio 2012 ha frequentato uno dei migliori corsi internazionali di Open Source Intelligence: il corso di OSINT Methods and Training organizzato da Arno Reuser (Responsabile dell'unità di Osint dell'Intelligence Olandese) e Jane's International una delle società private di intelligence tra le più quotate a livello mondiale. E' autore di **Esplorare Internet. Manuale di investigazioni digitali e Open Source Intelligence**, Minerva, Bologna, 2014

# Agenda

---

- Presentazione relatore
- ➔ • Osint introduzione
- Internet of Things
- I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- Bibliografia & sitografia

- Osint introduzione

---

OSINT, è un abbreviazione delle parole inglesi Open Source INTelligence. Essa consiste nell'attività di raccolta di informazioni mediante la consultazione di fonti di pubblico accesso. Nell'ambito di operazioni di intelligence il termine "Open Source" si riferisce a fonti pubbliche, liberamente accessibili, in opposizione a fonti segrete o coperte.

# • Osint introduzione

---

## 1) General Information

- Information that is widely available to anyone – e.g. Websites
- Includes broadcast, posted and printed news

## 2) Commercial Data

- e.g. company reports and databases

## 3) Experts

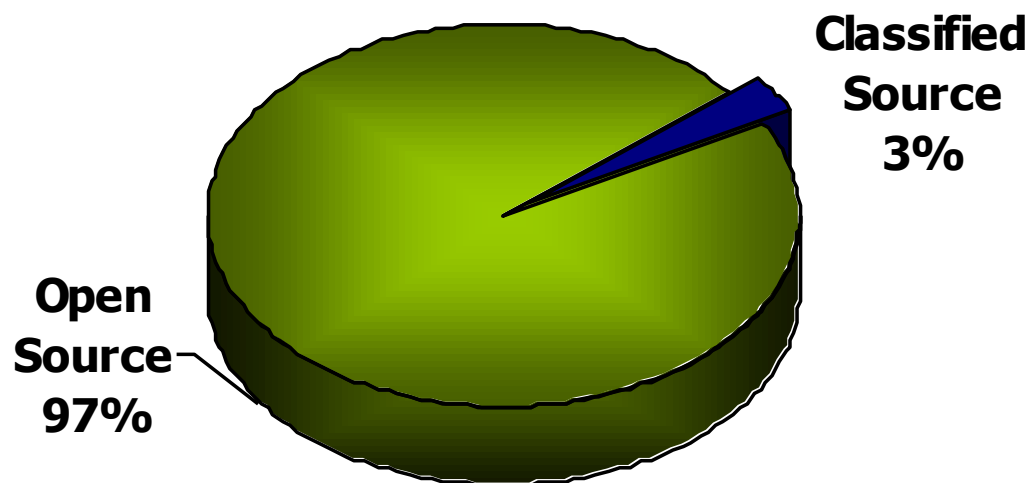
- Expertise of individual experts

## 4) “Grey” Literature

- “Grey” literature – e.g. reports produced by the private sector, government sources and academia that may be available on a limited basis only and not necessarily widely or freely distributed

- **Osint introduzione**

---



**Qualcuno ha stimato che nell'ambito delle stesse comunità d'intelligence di molti Paesi l'apporto OSINT si colloca tra il 35 % e il 97 %.**

## • Osint introduzione

---

- OSD (Open Source Data): dati grezzi, generici, generati da una fonte primaria (registrazioni, fotografie, immagini satellitari commerciali, corrispondenza personale resa pubblica);
  
- OSIF (Open Source of Information): informazione che, ancorché ancora generica, ha subito un processo editoriale di filtro e convalida (giornali, trasmissioni, libri, relazioni quotidiane);

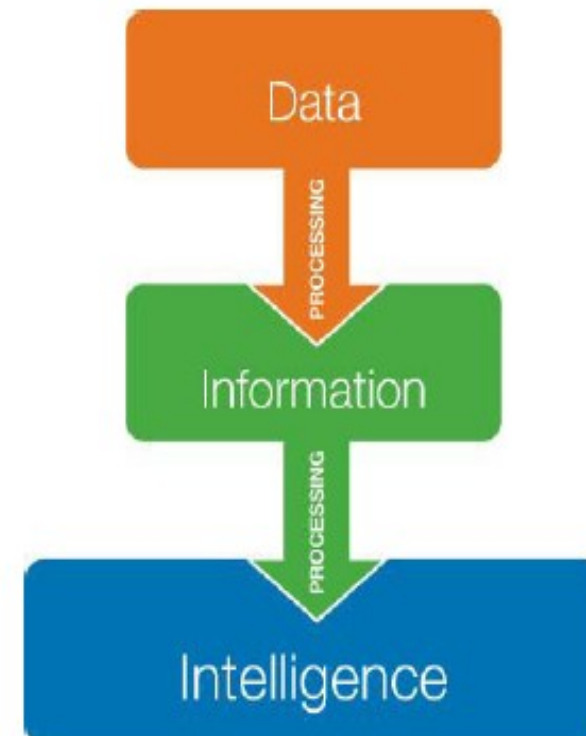
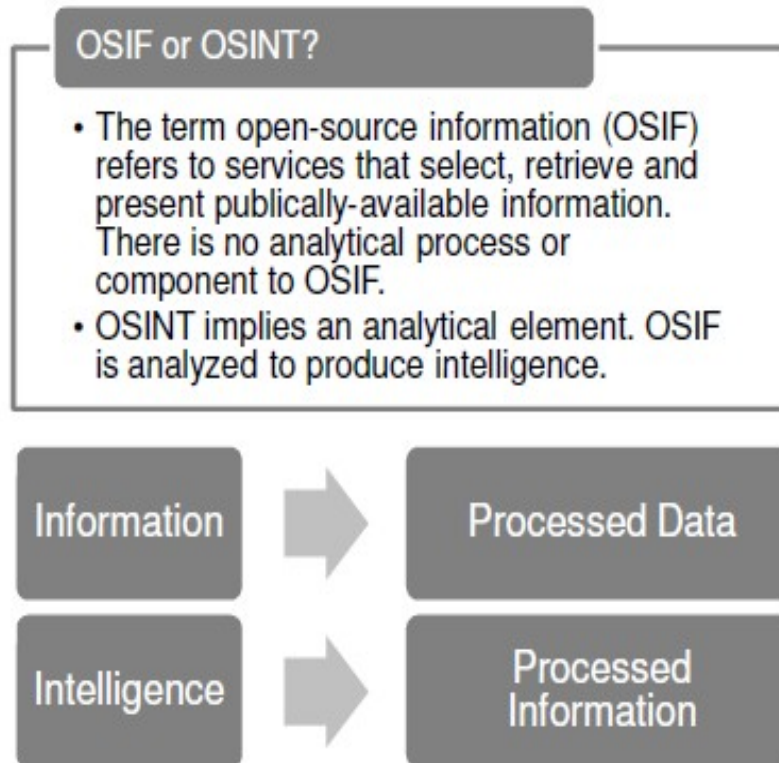


# • Osint introduzione

---

- OSINT (Open Source of Intelligence): informazioni appositamente cercate, selezionate, distillate e destinato a gruppo selezionato per affrontare una richiesta specifica;
- OSINT-V (Open Source of Intelligence Validated): informazioni convalidate ed ottenute attraverso la rielaborazione effettuata dall'analista, oppure attraverso il confronto con una fonte attendibile (di qualunque tipologia si tratti) che conferma quanto ottenuto.

# • Osint introduzione



# • Osint introduzione

---

**Nel mondo di Internet tutto parla se opportunamente interrogato.**

Email Title:	[REDACTED]
Email Date:	__Saturday, December 5, 2015, 09:07:22 AM (PST -08:00)
Your IP Address:	__199.58.81.144
Opened By Recipient:	__Saturday, December 5, 2015, 09:24:51 AM (PST -08:00) Your email has been opened <b>8</b> times
Recipient Location:	__Europe
Recipient IP Address:	__185.19.140.143
Recipient Application:	__Mozilla/5.0 (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12H143 [FBAN/MessengerForiOS;FBAV/50.0.0.15.72;FBBV/17975388;FBDV/iPhone5,4;FBMD/iPhone;FBSN/iPhone OS;FBSV/8.4;FBSS/2;FBCR/VodafoneIT;FBID/phone;FBLC/it_IT;FBOP/5]

# Agenda

---

- Presentazione relatore
- ➔ • Internet of Things
- I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- Bibliografia & sitografia

# Internet of Things

---

L'Internet delle cose (IoT) è la rete di oggetti fisici o di "cose" integrati con l'elettronica, software, sensori e network di rete, che consente a questi oggetti la raccolta e lo scambio di dati.

# Internet of Things

---

L'Internet delle cose permette agli oggetti di essere individuati e controllati a distanza attraverso l'infrastruttura di rete esistente, creando opportunità di integrazione più diretta tra il mondo fisico e i sistemi basati su computer, e con conseguente maggiore efficienza, accuratezza e vantaggio economico.

# Internet of Things

---

Ogni oggetto appartenente alla IoT è univocamente identificabile, ma è in grado di interoperare all'interno dell'infrastruttura Internet esistente.

Gli esperti stimano che il IoT sarà composto da circa 50 miliardi di oggetti entro il 2020.

# Internet of Things





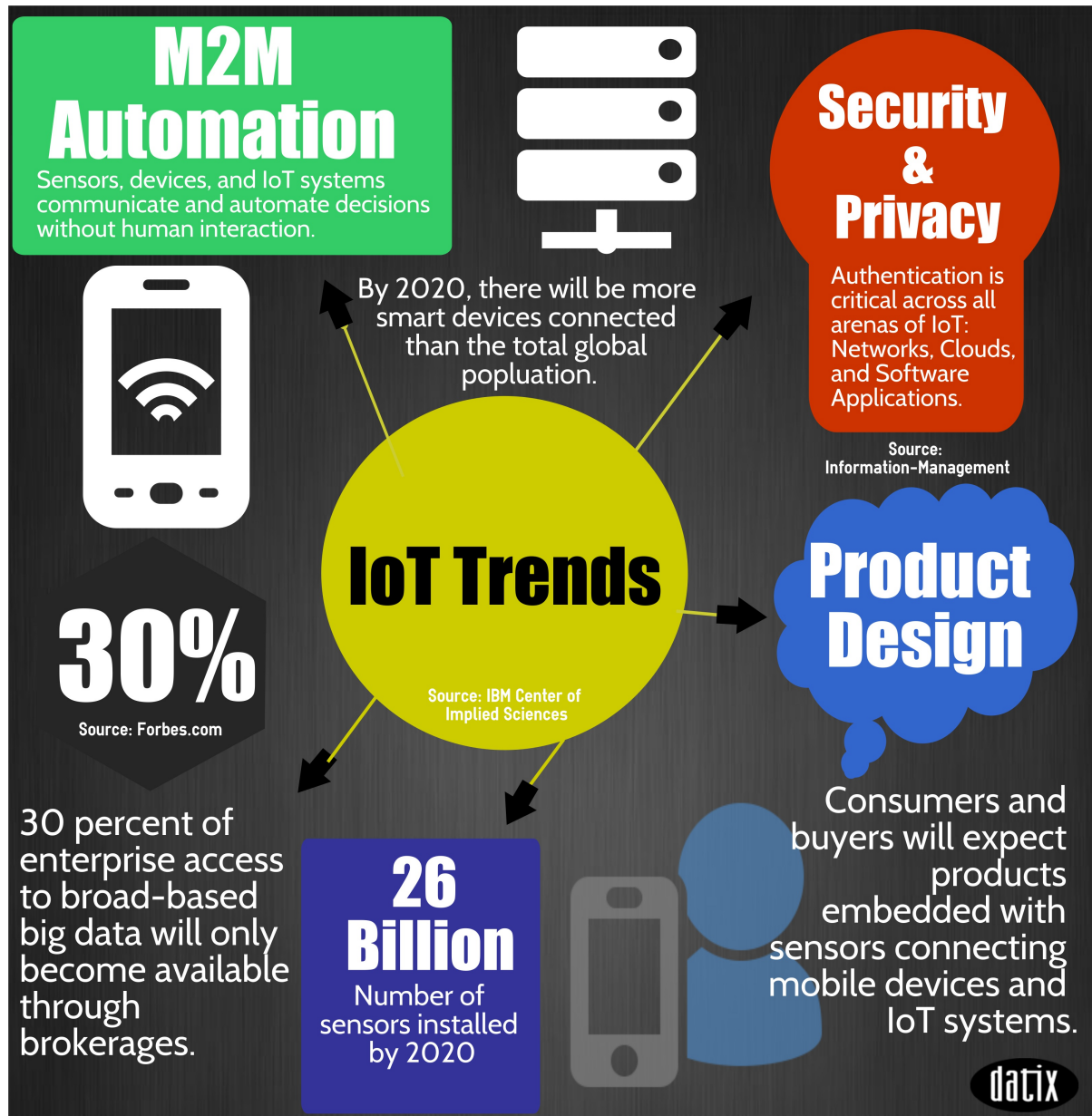
# Internet of Things - Trends

---

Secondo il rapporto FutureScape di IDC, "Worldwide Internet of Things 2016 Predictions, come i Millennials (i nati tra gli anni '80 e i 2000) si muoveranno in ruoli aziendali decisionali nei prossimi tre anni, spingeranno per implementazioni più rapide, in tempo reale e IoT cioè applicazioni con sensori collegati in rete.

**[\(IDC Link\)](#)**

# Internet of Things -Trends



# Internet of Things

## Building the Era of Integration

Our devices are becoming smarter to enhance productivity in this new age. We're seeing new capabilities, from foldable screens and lightweight, affordable options that automatically speak with connected objects.



We are moving away from a world of screens and devices to one of immersive experiences



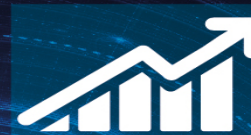
PAST

PRESENT

FUTURE

## The Age of the Internet of Things

Consisting of billions of connected smart devices, our connected world is growing at a breathtaking pace.



Predictions forecast market growth from \$1.9trillion in 2013 to \$7.1trillion by 2020\*

IoT will enrich everyday life, improve government efficiency, transform business and increase productivity.

\* Worldwide and Regional Internet of Things (IoT) 2014-2020 Forecast: A Virtuous Circle of Proven Value and Demand, May 2014. <http://www.idc.com/getdoc.jsp?containerId=248451>



## IT Predictions: The Era of Integration Intel's views on 2015

Smarter devices in 2015 will become easier to use, tailored to individual needs. We'll see the emergence of new form factors, capabilities and experiences, such as wearables, 3D imaging and a world of no wires.



Device and transaction security will change - with passwords being replaced with advanced biometrics.



### Immersed in a New World

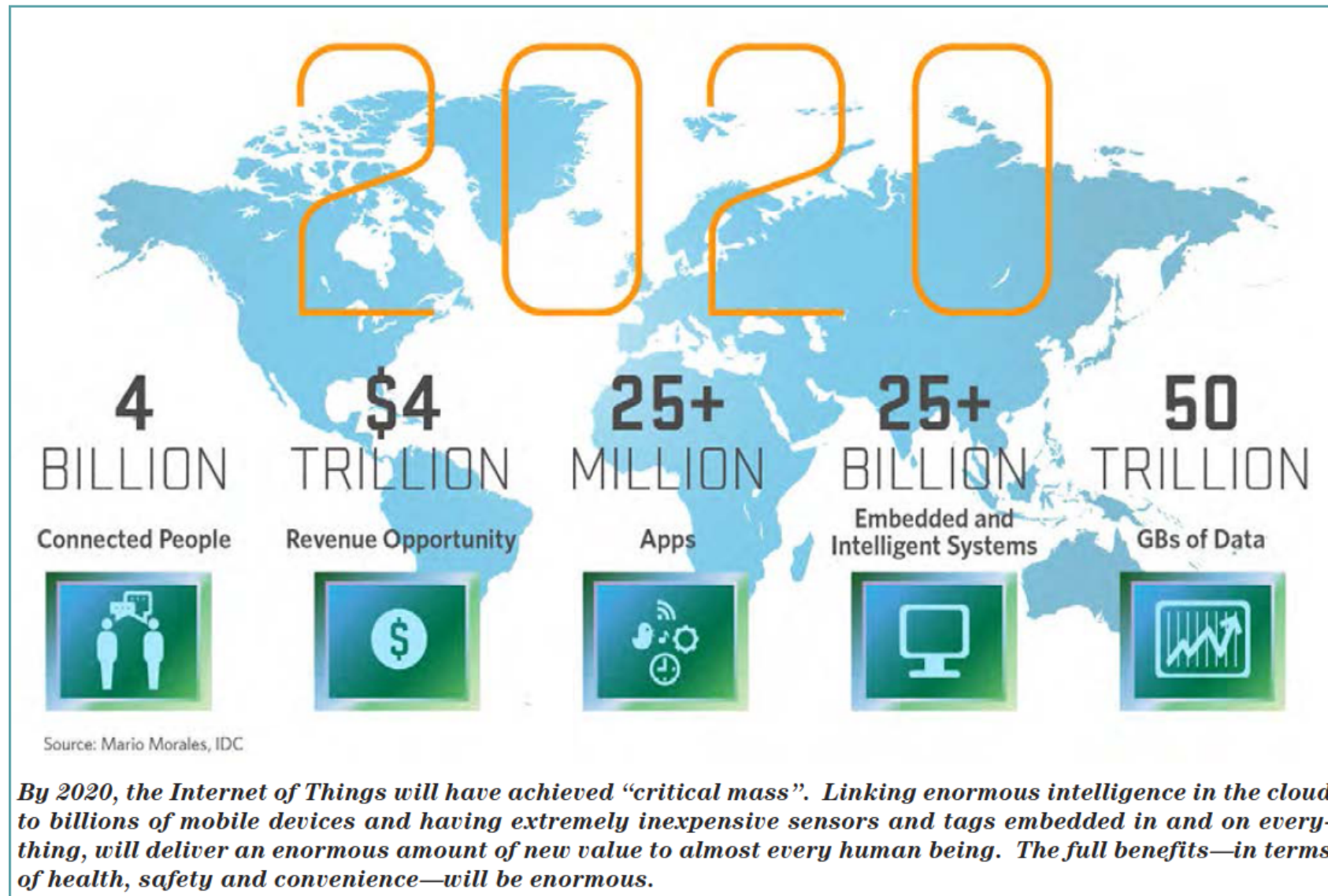
Technology holds the potential to entirely change the world we live in, from energizing developing countries through to enabling education for all.



By readying itself today, Asia will continue to be a hotbed of innovation in this new era of computing for years to come.


### Readying Ourselves for the Future

# Internet of Things



# Agenda

---

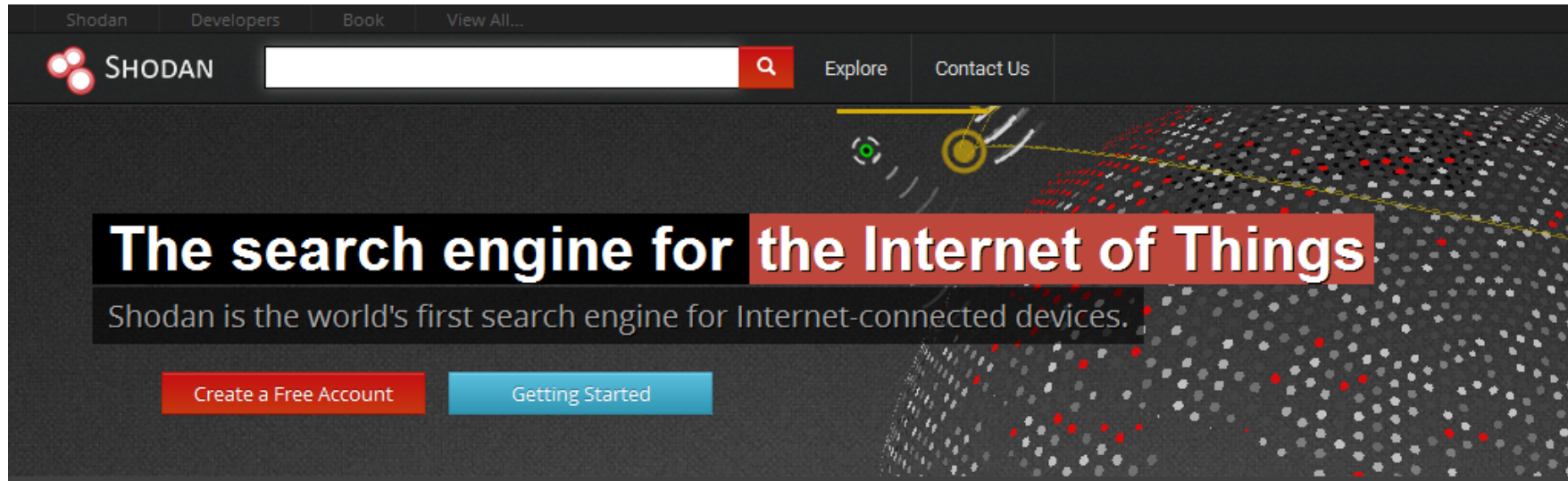
- Presentazione relatore
- Internet of Things
-  • I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- Bibliografia & sitografia

# Internet of Things

---

Con il crescere delle dimensioni e dell'importanza della IoT sono nati anche i dispositivi per scansionare la IoT e per individuare le vulnerabilità connesse.

# I motori di ricerca delle Internet of Things



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where



See the Big Picture

Websites are just one part of the Internet. The

# Internet of Things

---

**Shodan** è un motore di ricerca che consente all'utente di trovare specifici tipi di computer ( router, server , ecc ) collegati ad internet utilizzando una varietà di filtri .

È stato lanciato nel 2009 da programmatore John Matherly , che, nel 2003, ha concepito l'idea di cercare i dispositivi collegati a Internet .



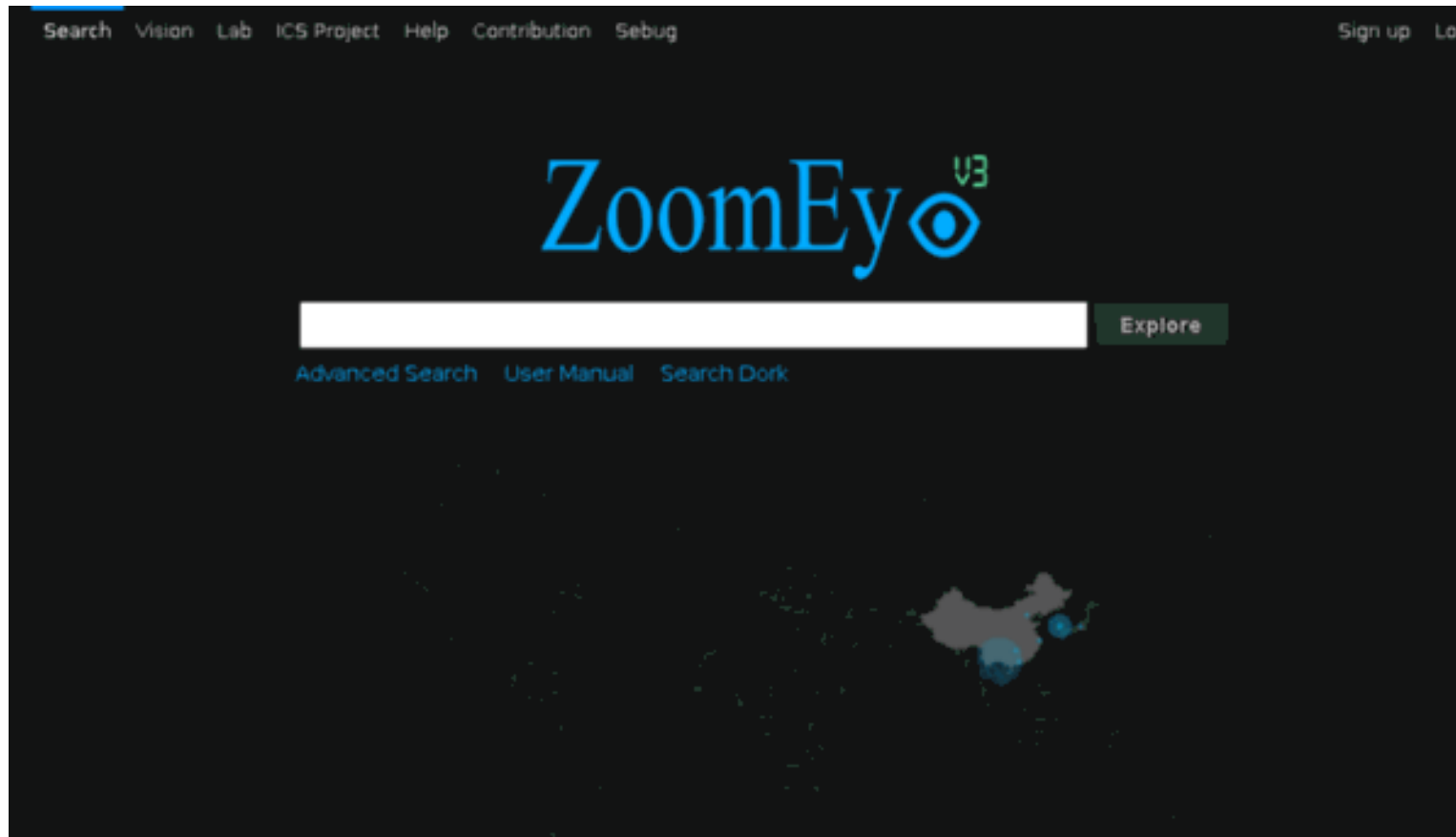
# I motori di ricerca delle Internet of Things

---

Il motore di ricerca Shodan è diventato una sorta di Google per l'Internet degli oggetti , un parco giochi per gli hacker e terroristi e uno strumento utile per le aziende che cercano di analizzare le proprie vulnerabilità informatiche.

# I motori di ricerca delle Internet of Things

---



# I motori di ricerca delle Internet of Things

---

**ZoomEye** è un motore di ricerca per il cyberspazio , prodotto dalla società cinese Knownsec, Inc nel 2013 con lo scopo di esplorare i dispositivi e siti web nel cyberspazio.

# I motori di ricerca delle Internet of Things

---

ABOUT SECURITY API



Search ▾

Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [\[more information\]](#)

# Internet of Things

---

**Censys** è un motore di ricerca per la IoT che è stato originariamente pubblicato nel mese di ottobre da ricercatori presso l'Università del Michigan, è attualmente supportato da Google.

# I motori di ricerca delle Internet of Things

---

Naturalmente non bisogna dimenticare che molte di questi motori di ricerca sono stati anticipati dalle attività via Google Hack cioè l'uso di specifiche query del motore di ricerca americano per trovare devices e vulnerabilità.

# I motori di ricerca delle Internet of Things

---

[Inurl: 'viewerframe?mode=motion'](#)

[intitle:"live view" intitle:axis](#)

[Intitle: "live view / - axis"](#)

[intitle:liveapplet](#)

[intitle:"netcam live image"](#)

[intitle:"snc-rz30 home"](#)

[intitle:"WJ-NT104 Main"](#)

[intitle:"EvoCam" inurl:"webcam.html"](#)

[intitle:"i-Catcher Console - Web Monitor"](#)

[intitle:"Live NetSnap Cam-Server feed"](#)

[allintitle:liveapplet](#)

# Agenda

---

- Presentazione relatore
- Internet of Things
- I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- Bibliografia & sitografia





# Rischi e vulnerabilità

---

L'attività di OSINT e fingerprinting sui device amplifica in maniera esponenziale la possibilità che si possano individuare difetti di impostazione, device senza protezioni o con vulnerabilità. Attraverso l'attività di ricerca online non ci si limita ad individuare gli elementi delle IoT, ma anche le vulnerabilità connesse e le tecniche con cui sfruttarle.

# Rischi e vulnerabilità

ZoomEy search results for "country:'italy' city:'rome' device:webcam". The search found about 3911 results in 0.919 seconds.

**Search Type:** Public Devices, Web Services

**Service:** http (3688), Unknown (163), ftp (39), telnet (18), rtsp (3)

**Country:** ITALY (3911), ROME (3911)

**App:** Netwave IP camera http config (1092), D-Link DCS-932L we... (646), Atech AVN801 netwo... (454), GM Streaming Serve... (260), @httpd (251), D-Link DCS-930L we... (167), Zmodo camera http in... (150), D-Link DCS-8020L w... (131), D-Link DCS-932LB1 ... (111), Hikvision IP camera h... (106)

**Result 1:** 217.133.65.197  
D-Link DCS-932L webcam http inte...  
webcam  
Italy Rome  
Nov. 28, 2015

**HTTP Headers:**  
HTTP/1.0 401 Authorization Required  
Server: alphasd  
Date: Fri Nov 27 18:16:59 2015  
Pragma: no-cache  
Cache-Control: no-cache  
Content-type: text/html  
WWW-Authenticate: Basic realm="DCS-932L"

**Result 2:** 217.133.133.150  
Netwave IP camera http config  
webcam  
Italy Rome  
Nov. 28, 2015

**HTTP Headers:**  
HTTP/1.1 200 OK  
Server: Netwave IP Camera  
Date: Fri, 27 Nov 2015 17:16:55 GMT  
Content-Type: text/html  
Content-Length: 372  
Cache-Control: private  
Connection: close

**HTML Snippet:**  
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

# Rischi e vulnerabilità

## TOP COUNTRIES



Spain	246,837
Taiwan, Province of China	10,515
United States	6,866
Barbados	2,679
Costa Rica	2,254

## TOP SERVICES

SSH	277,498
2222	79

## TOP ORGANIZATIONS

Telefonica de Espana	246,799
CHTD, Chunghwa Telecom Co., Ltd.	9,630
Cable & Wireless (Barbados) Limited	3,620
Dansk Net A/S	1,946
Cable & Wireless Dominica	1,196

## TOP OPERATING SYSTEMS

Linux 2.4-2.6	35
Linux 2.6.x	3

## TOP PRODUCTS

Dropbear sshd	277,577
---------------	---------

Showing results 1 - 10 of 277,577

### 81.39.79.95

95.Red-81-39-79.dynamicIP.rima-tde.net

**Telefonica de Espana**

Added on 2015-02-17 06:24:33 GMT

Spain

[Details](#)

SSH-2.0-dropbear\_0.46

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQgCKj10BLi11/oSbukFarKJZTXvBvw+AUGfie6fdE7psCNwC  
LM5bYnJgJQZMP/V0hJkxkA539e2mM4fW9U4ECAUwgvLF9AZGhcmn0kF0jIjMUDgCV8kFIS850uBU  
/ayyswdYp6bpx3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMdfZM9P

Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...

### 83.52.234.21

21.Red-83-52-234.dynamicIP.rima-tde.net

**Telefonica de Espana**

Added on 2015-02-17 05:12:13 GMT

Spain, Madrid

[Details](#)

SSH-2.0-dropbear\_0.46

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQgCKj10BLi11/oSbukFarKJZTXvBvw+AUGfie6fdE7psCNwC  
LM5bYnJgJQZMP/V0hJkxkA539e2mM4fW9U4ECAUwgvLF9AZGhcmn0kF0jIjMUDgCV8kFIS850uBU  
/ayyswdYp6bpx3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMdfZM9P

Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...

### 83.36.133.215

215.Red-83-36-133.dynamicIP.rima-tde.net

**Telefonica de Espana**

Added on 2015-02-17 04:24:39 GMT

Spain, Navalmodal De La Mata

[Details](#)

SSH-2.0-dropbear\_0.46

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQgCKj10BLi11/oSbukFarKJZTXvBvw+AUGfie6fdE7psCNwC  
LM5bYnJgJQZMP/V0hJkxkA539e2mM4fW9U4ECAUwgvLF9AZGhcmn0kF0jIjMUDgCV8kFIS850uBU  
/ayyswdYp6bpx3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMdfZM9P

Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...

### 88.9.146.203

203.Red-88-9-146.dynamicIP.rima-tde.net

**Telefonica de Espana**

Added on 2015-02-17 03:15:43 GMT

Spain

[Details](#)

SSH-2.0-dropbear\_0.46

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQgCKj10BLi11/oSbukFarKJZTXvBvw+AUGfie6fdE7psCNwC  
LM5bYnJgJQZMP/V0hJkxkA539e2mM4fW9U4ECAUwgvLF9AZGhcmn0kF0jIjMUDgCV8kFIS850uBU  
/ayyswdYp6bpx3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMdfZM9P

Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...

# Rischi e vulnerabilità

"google hack" webcam

Tutti Immagini Video Notizie Maps Altro ▾ Strumenti di ricerca

Circa 13.800 risultati (0,28 secondi)


**How to Hack a webcam via Google « Internet**  
[internet.wonderhowto.com/.../hack-webcam-via-g...](#) ▾ Traduci questa pagina  
02 mag 2008 - How to Hack any webcam easily using Google - How to Interact with your ... your website hacked - How to Do the Chuck Norris Google hack ...

**Google Camera Hack « Wonder How To**  
[tag.wonderhowto.com > ... > Google camera](#) ▾ Traduci questa pagina  
How to Hack someone's web cam or online security camera This tutorial will let ...  
Google hack This video tutorial is how to do the Chuck Norris Google hack.

**Hacking Security Cameras on Google - Internet & Networking ...**  
[www.techtalkz.com > ... > Internet & Networking](#) ▾ Traduci questa pagina  
10 feb 2012 - 1 post  
intitle:"EvoCam" inurl:"webcam.html" - intitle:"i-Catcher Console - Web Monitor" ... Tags  
- google hack, live cam, security cam, security flaws ...

**Webcam Hacking - The Dutch HackInfo**  
<https://www.hackinfo.nl/hacking/webcam-hacking> ▾ Traduci questa pagina  
... us on Twitter. You are here: Home - Hacking Webcam Hacking. Web Cam Hack ....  
intitle:"EvoCam" inurl:"webcam.html" Mostlv European security cameras

# Rischi e vulnerabilità

intitle:"EvoCam" inurl:webcam.html 


Tutti Immagini Video Notizie Maps Altro ▾ Strumenti di ricerca

Circa 72 risultati (0,18 secondi)

**An office - EvoCam**  
[129.15.81.9:8080/webcam.html](http://129.15.81.9:8080/webcam.html) ▾ Traduci questa pagina

**Intitle Evocam Inurl Webcam Html - Nightfall - Enjin**  
[nightfall.enjin.com/.../10413103-intitle-evocam-in...](http://nightfall.enjin.com/.../10413103-intitle-evocam-in...) ▾ Traduci questa pagina  
Intitle Evocam Inurl Webcam Html bf1ccc675e. Microst virtual miniport wifi for hp. Porno vf italie interdite torrent. Srs Wow Essentials Serial Key | tested 부산 커튼

**EvoCam Java Example Page**  
[gauss.gge.unb.ca/webcam.html](http://gauss.gge.unb.ca/webcam.html) ▾ Traduci questa pagina  
Powered by EvoCam.

**EvoCam 1**  
[64.203.245.208:8088/1/webcam.html](http://64.203.245.208:8088/1/webcam.html) ▾ Traduci questa pagina 

# Rischi e vulnerabilità

98.101.223.10:8080/webcam.html

📄 | 🔄 | 🔍 Cerca

Questo sito web non fornisce informazioni relative all'identità.



# Rischi e vulnerabilità



[Home](#)

[Search more](#)

[Browse](#)

[Statistics](#)

[Find IP](#)

[Add New](#)

Your Last Views : [D-LINK DCS-932L](#) |  
[Search more](#)



## D-LINK DCS-932L default configuration

### Step 1

Router default Username is **admin**

Router default ( initial ) Password is **##blank**

Router default IP is [192.168.1.1](#) ( **suggested** )

# Rischi e vulnerabilità

---

L'accoppiamento tra l'individuazione di una falla di sicurezza di uno specifico device e la possibilità di individuare facilmente tutti i device con quel tipo di bug rende il rischio informatico esponenziale e vastissimo.



# Rischi e vulnerabilità

---

Pierluigi Paganini nel suo blog SecurityAffairs (2014) riporta il caso di una vulnerabilità del router distribuito da Algerie Telecom:»

Algerie Telecom TP-LINK TD-W8951ND Routers are vulnerable, they contain a critical vulnerability exploitable to gain unauthorized access and reveal user's password.

«

# Rischi e vulnerabilità

---

Il problema principale in questi casi è rappresentato dall'impatto della vulnerabilità, dopo la prima indagine del ricercatore algerino Abdelli che ha individuato per primo il problema ha trovato migliaia di vulnerabili TP-LINK Router, usando SHODAN.

# Rischi e vulnerabilità

---

Utilizzando su Shodan la query RomPager zxxxxxpaese : dz ' ha individuato 200,000 Algerian TP-LINK Routers.

Abdelli ha stimato che circa il 95 % dei dispositivi trovati con SHODAN era a rischio.

# Rischi e vulnerabilità

---

Sempre nel 2014 i ricercatori di sicurezza di **Proofpoint** hanno scoperto un attacco informatico contro la Internet of Things ( IoT ), più di 100.000 frigoriferi , televisori intelligenti e altri elettrodomestici intelligenti domestici erano stati hackerati e usati per inviare 750.000 email di spam.

# Rischi e vulnerabilità

---

Gli esperti di Proofpoint, hanno anche spiegato come attacchi informatici con sede nel IoT sono molto difficili da ridurre, in quanto le reti dell'internet degli oggetti sono composti da centinaia di migliaia di dispositivi, e ad ogni nodo è possibile assegnare un piccolo compito da fare.

# Rischi e vulnerabilità

---

Se ogni nodo trasmette alcune decine di richieste a un bersaglio in un attacco DDoS, o inviare solo un paio di email di spam la loro azione passerà inosservata anche se l'effetto complessivo potrebbe essere drammatico

(

[http://investors.proofpoint.com/releasedetail.cfm?](http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799)

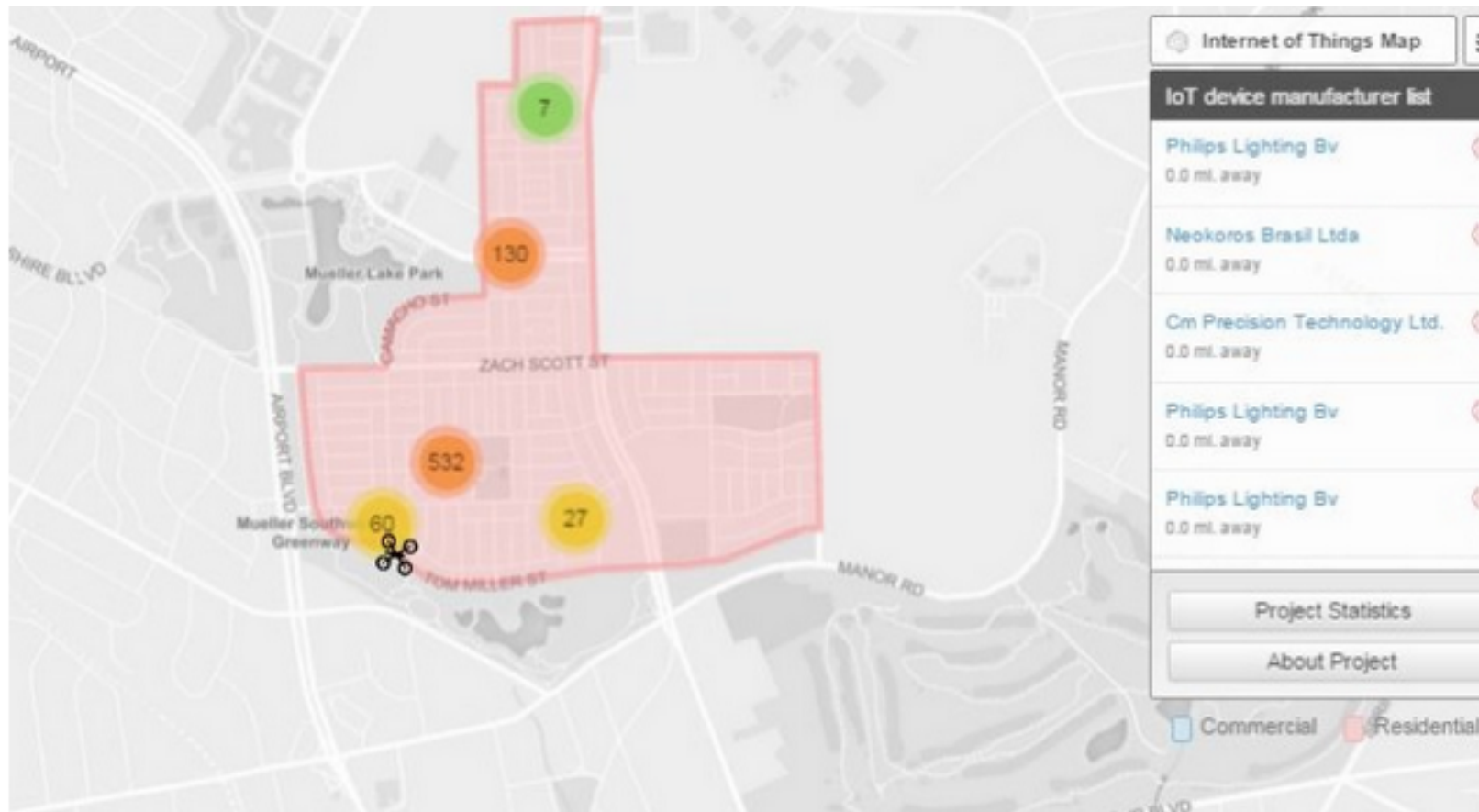
[ReleaseID=819799\)](http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799)

# Rischi e vulnerabilità

---

Insomma la partita è appena iniziata dobbiamo essere consapevoli del fatto che vivremo in un mondo in cui i droni possono essere usati per mappare zone specifiche in cui individuare le vulnerabilità delle strutture del territorio (una banca per esempio) o i frigoriferi potranno essere usati per aprire le nostre caselle di posta elettronica.

# Rischi e vulnerabilità



ZigBee-sniffing drone used to map online Internet of Things



# Rischi e vulnerabilità

---



Samsung smart fridge opens Gmail login to hack

---

# Agenda

---

- Presentazione relatore
- Internet of Things
- I motori di ricerca delle Internet of Things
- Rischi e vulnerabilità
- ➔ • Bibliografia & sitografia

# Bibliografia

---

Leonida Reitano, Esplorare Internet, Bologna, Minerva, 2014

# Sitografia

---

[http://www.cio.com/article/3013552/internet-of-things/millennials-will-accelerate-internet-of-things-action-idc-predicts.html#tk.NDR\\_nlt\\_idge\\_insider\\_newsletter\\_2015-12-10](http://www.cio.com/article/3013552/internet-of-things/millennials-will-accelerate-internet-of-things-action-idc-predicts.html#tk.NDR_nlt_idge_insider_newsletter_2015-12-10)

[https://it.wikipedia.org/wiki/Internet\\_delle\\_cose](https://it.wikipedia.org/wiki/Internet_delle_cose)

<http://securityaffairs.co>

<https://www.shodan.io/>

<https://www.zoomeye.org>

<https://www.censys.io>

<http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799>

<http://securityaffairs.co/wordpress/39558/hacking/samsung-smart-fridge-hack.html>

<http://securityaffairs.co/wordpress/39143/security/drone-internet-of-things.html>

[http://cispa.saarland/wp-content/uploads/2015/02/MongoDB\\_documentation.pdf](http://cispa.saarland/wp-content/uploads/2015/02/MongoDB_documentation.pdf)

# Contatti

---

- [agi@fastmail.fm](mailto:agi@fastmail.fm)
- [www.ricercheonline.org](http://www.ricercheonline.org)

*Grazie.*