ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

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

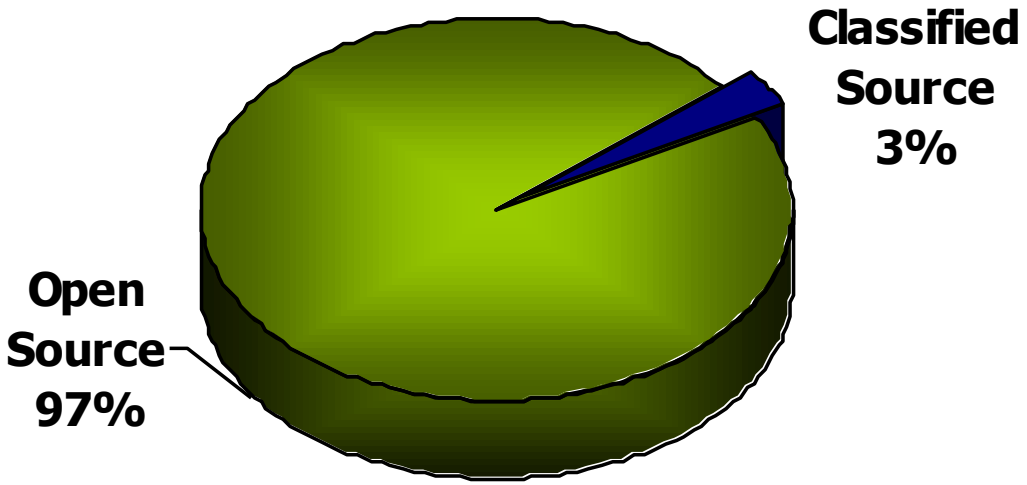
3) Experts

- 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);

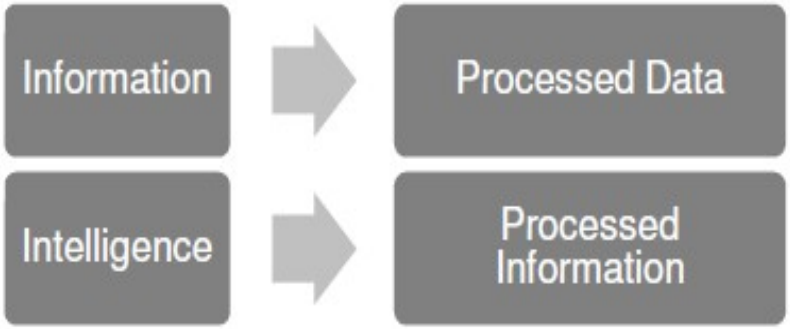
• Osint introduzione

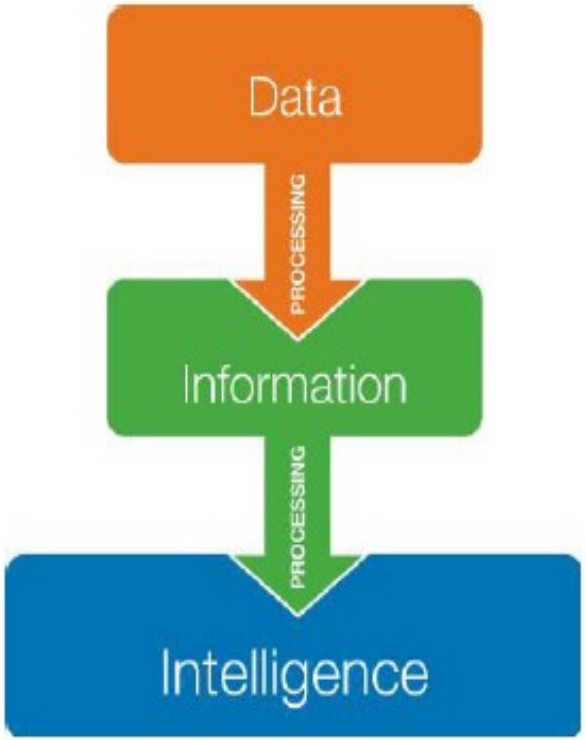
- OSINT (Open Source of Intelligence): informazioni appositamente cercate, selezionate, distillate e destinato a gruppo selezionato per affrontare una richiesta specifica;
- OSINT-V (Open Source of Intelligence Validated): informazioni convalidate ed ottenute attraverso la rielaborazione effettuata dall'analista,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

• Osint introduzione

OSIF or OSINT?

- The term open-source information (OSIF) refers to services that select, retrieve and present publically-available information. There is no analytical process or component to OSIF.
- OSINT implies an analytical element. OSIF is analyzed to produce intelligence.





• 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 **8** 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.

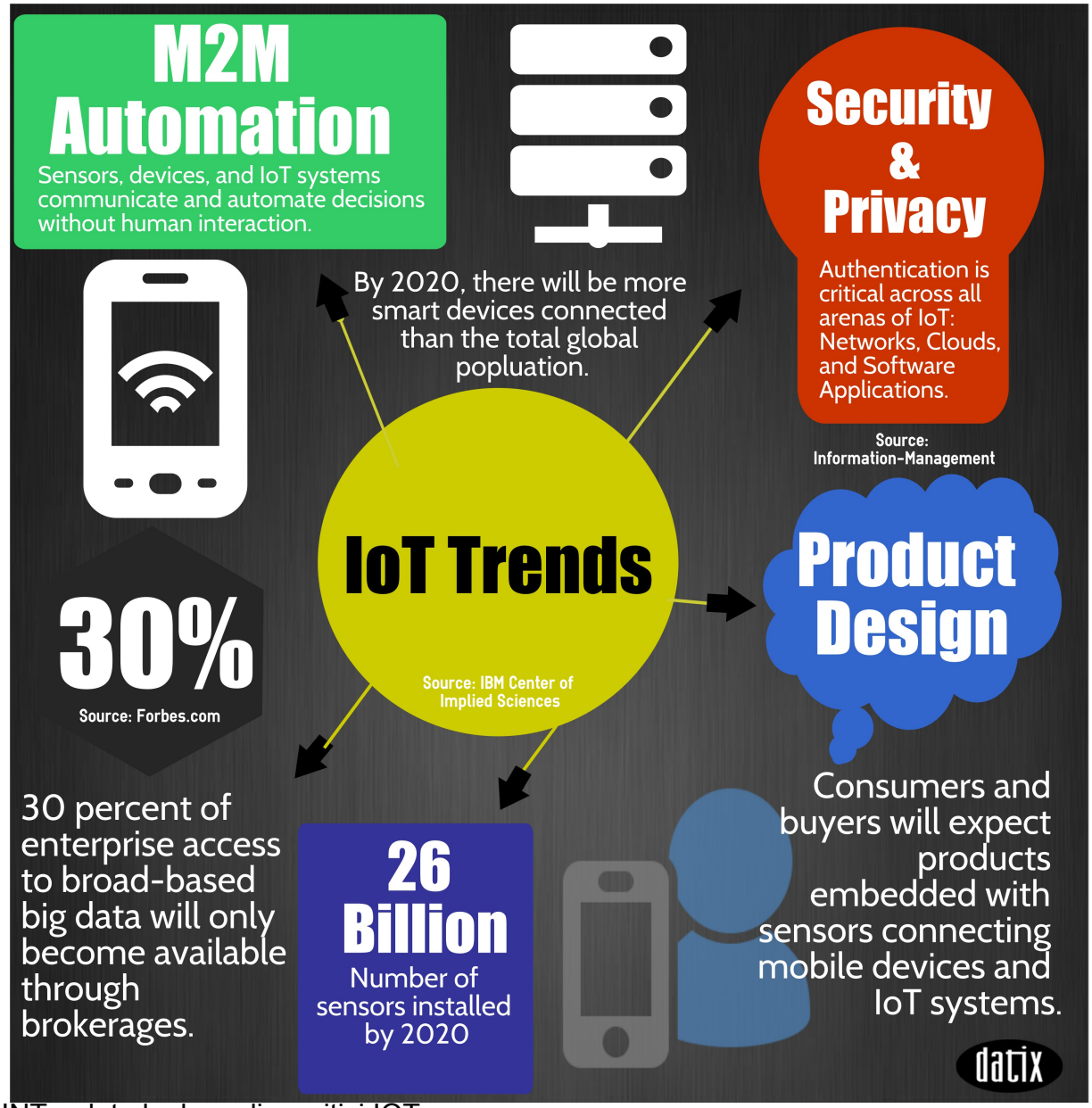
Gli esperti stimano che il IoT sarà composto da circa 50 miliardi di oggetti entro il 2020.

Internet of Things

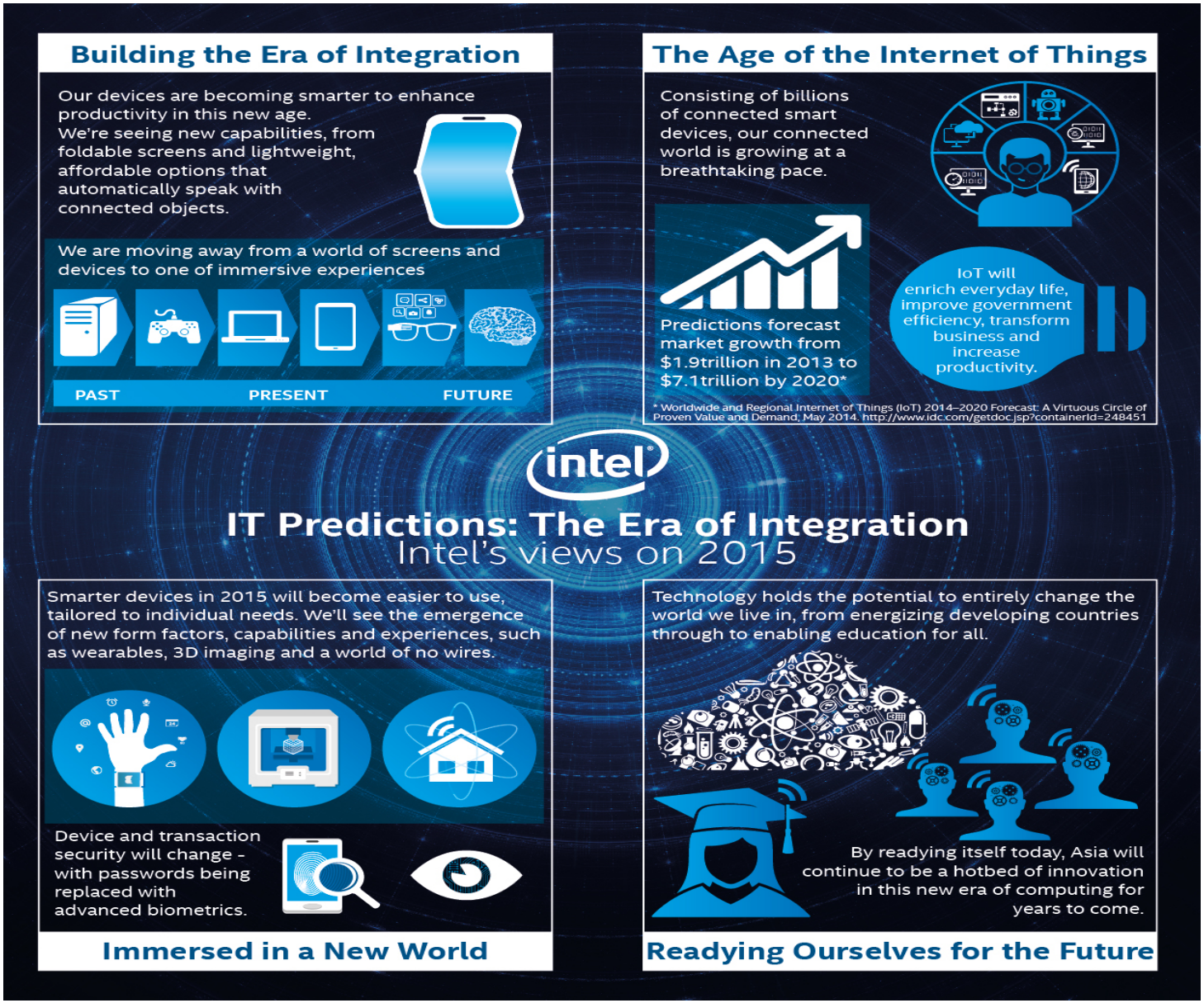
Internet of Things - Trends

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)

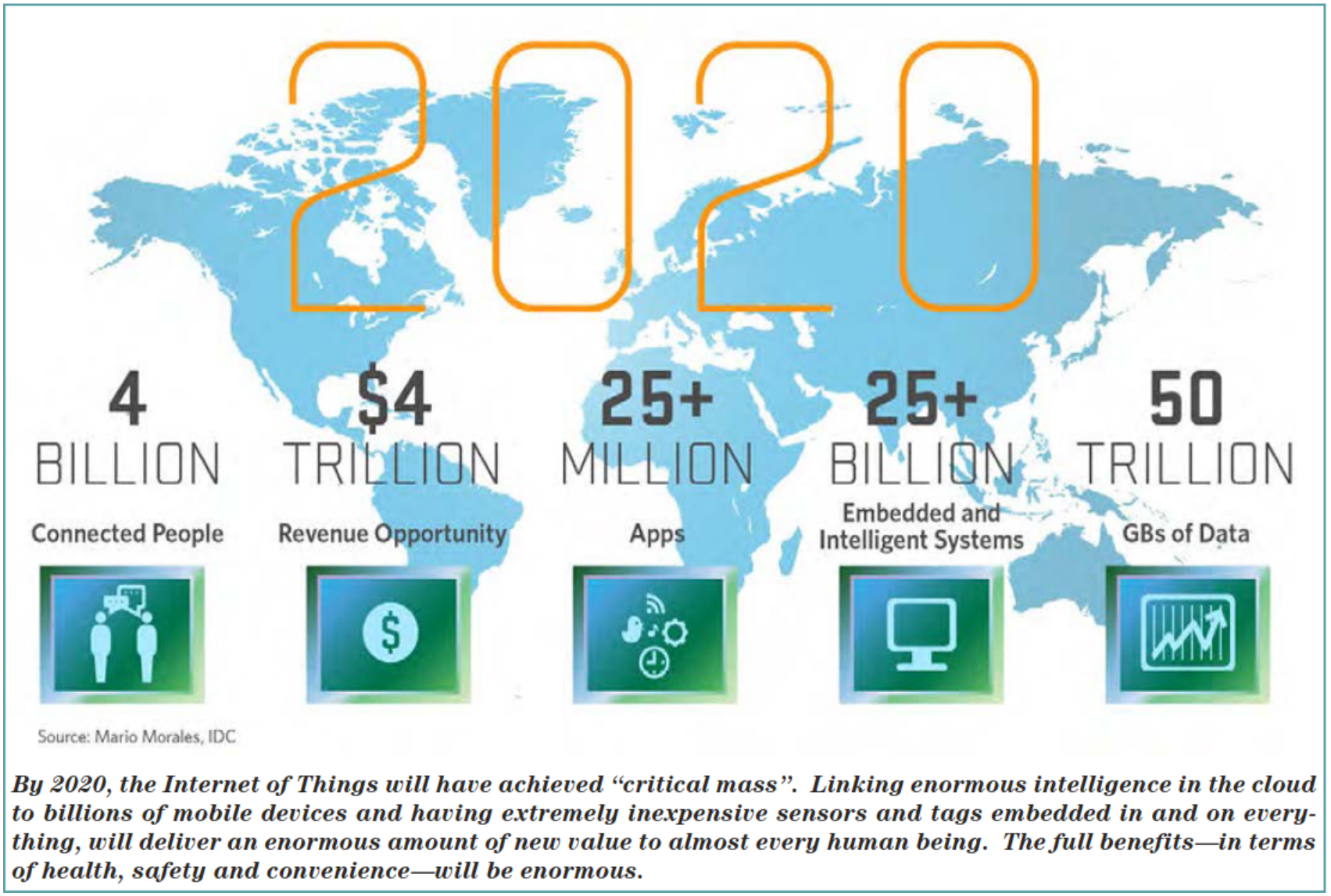
Internet of Things -Trends



Internet of Things



Internet of Things



By 2020, the Internet of Things will have achieved "critical mass". Linking enormous intelligence in the cloud to billions of mobile devices and having extremely inexpensive sensors and tags embedded in and on everything, will deliver an enormous amount of new value to almost every human being. The full benefits—in terms of health, safety and convenience—will be enormous.

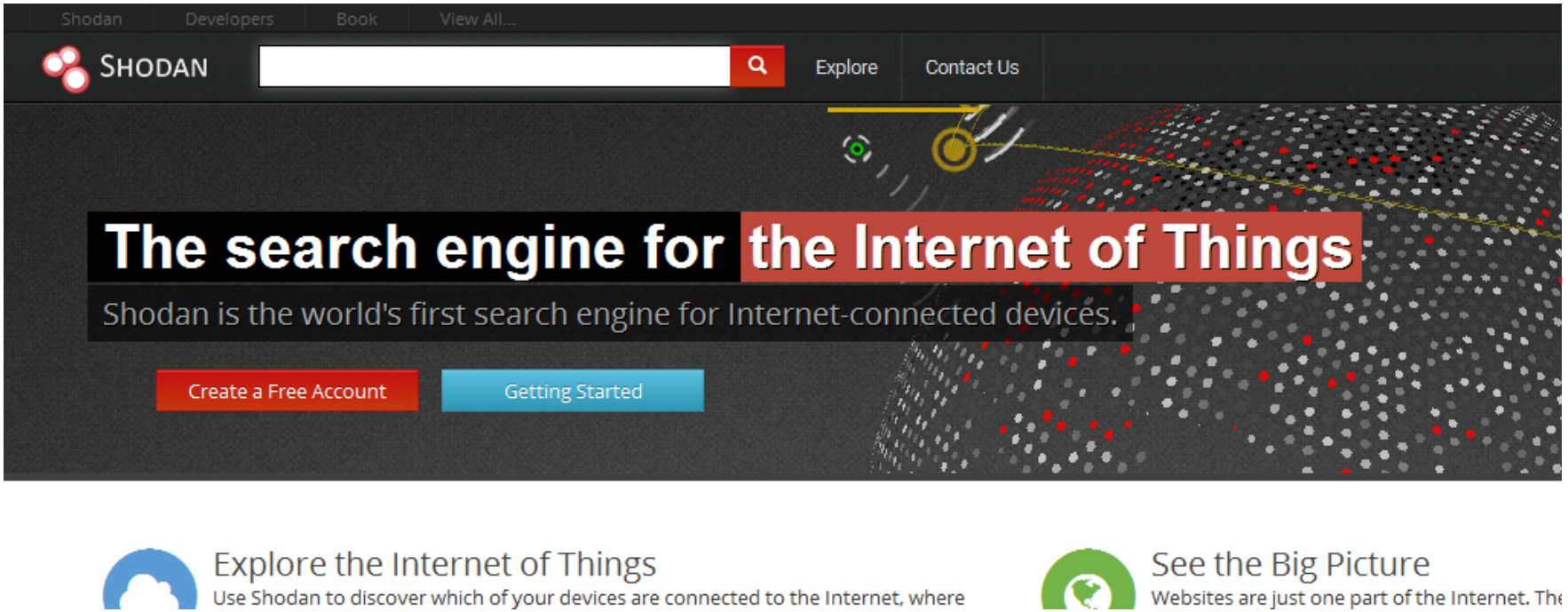
Agenda

- 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



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

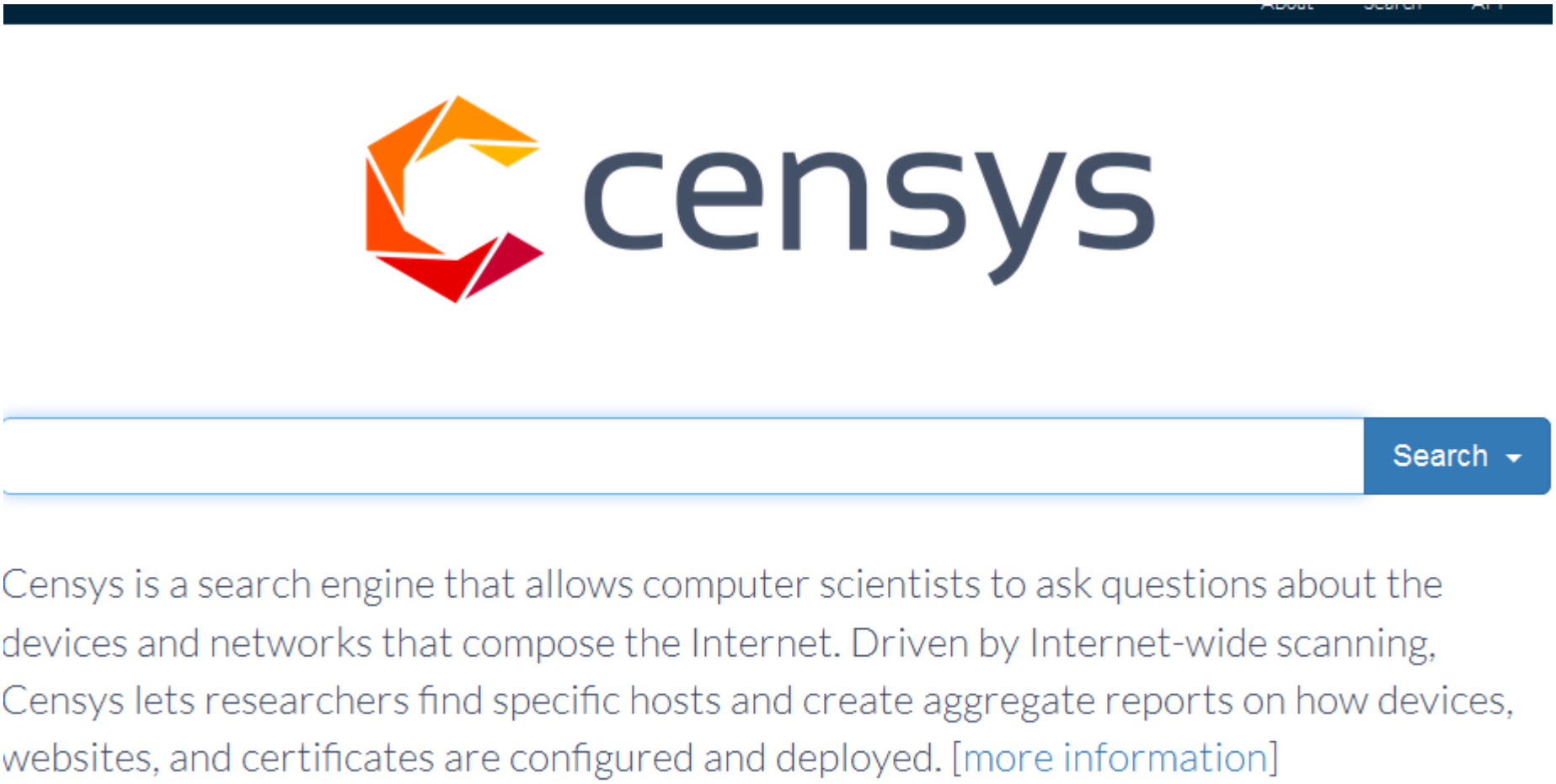
Il motore di ricerca Shodan è diventato una sorta di Google per l'Internet degli oggetti , un parco giochi per gli hacker e terroristi e uno strumento utile per le aziende che cercano di analizzare le proprie vulnerabilità informatiche.

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



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

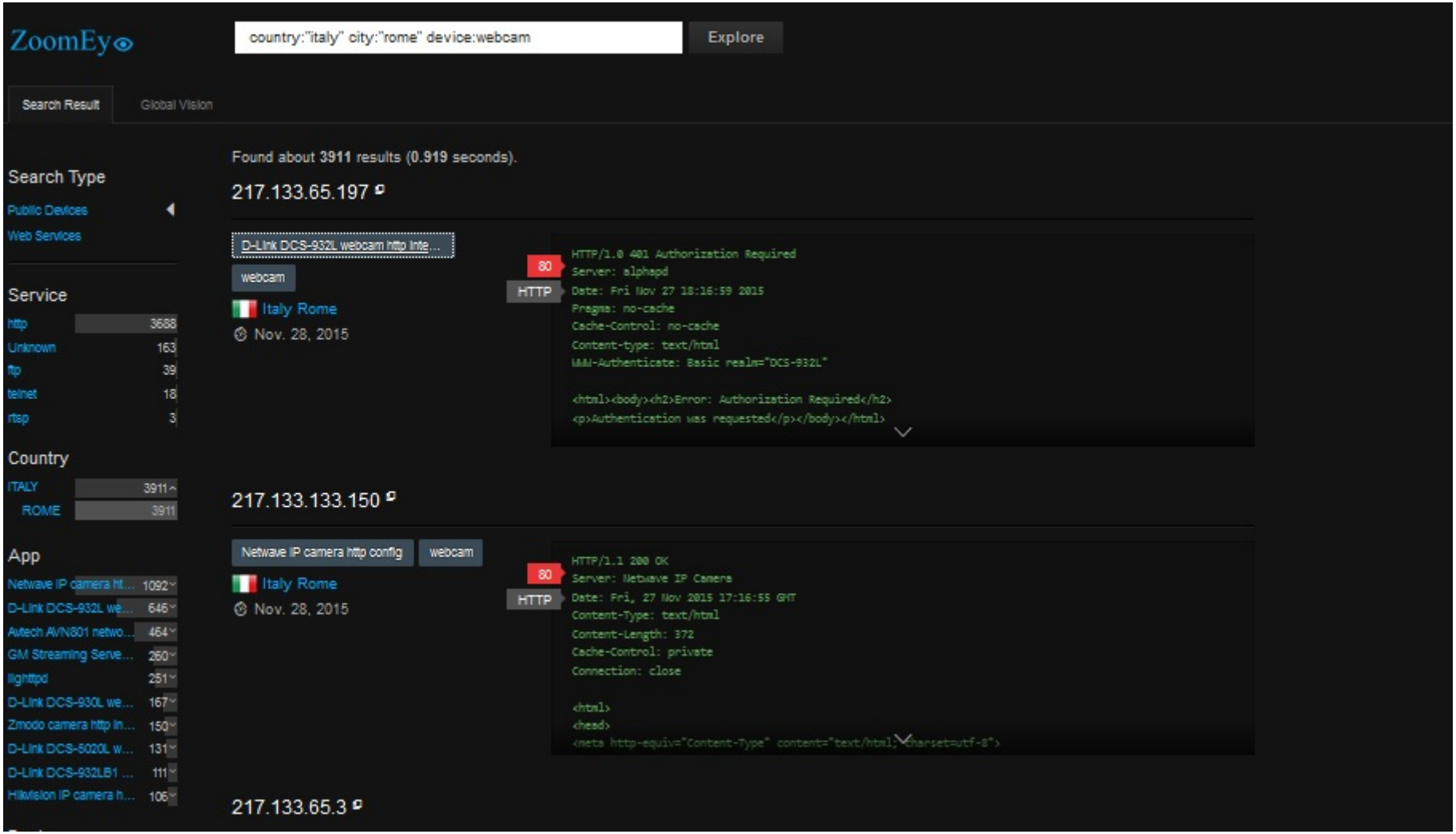
Agenda

- 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 qui sfruttarle.

Rischi e vulnerabilità



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: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCKj10BLi11/oSbukFArKJZTXvBvw+AUGfie6fdE7psCNwC
LM5bYnJgjQZMP/VOhJkxkA539e2mM4fW9U4ECAUwgvlF9AZGhcmn0kF0jIjMUDgCV8kFIS85OuBU
/ayyswdYp6bxp3zn0tGAh0Ty8ikf7CgWU5c+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: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCKj10BLi11/oSbukFArKJZTXvBvw+AUGfie6fdE7psCNwC
LM5bYnJgjQZMP/VOhJkxkA539e2mM4fW9U4ECAUwgvlF9AZGhcmn0kF0jIjMUDgCV8kFIS85OuBU
/ayyswdYp6bxp3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMDfZM9P
Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...
```

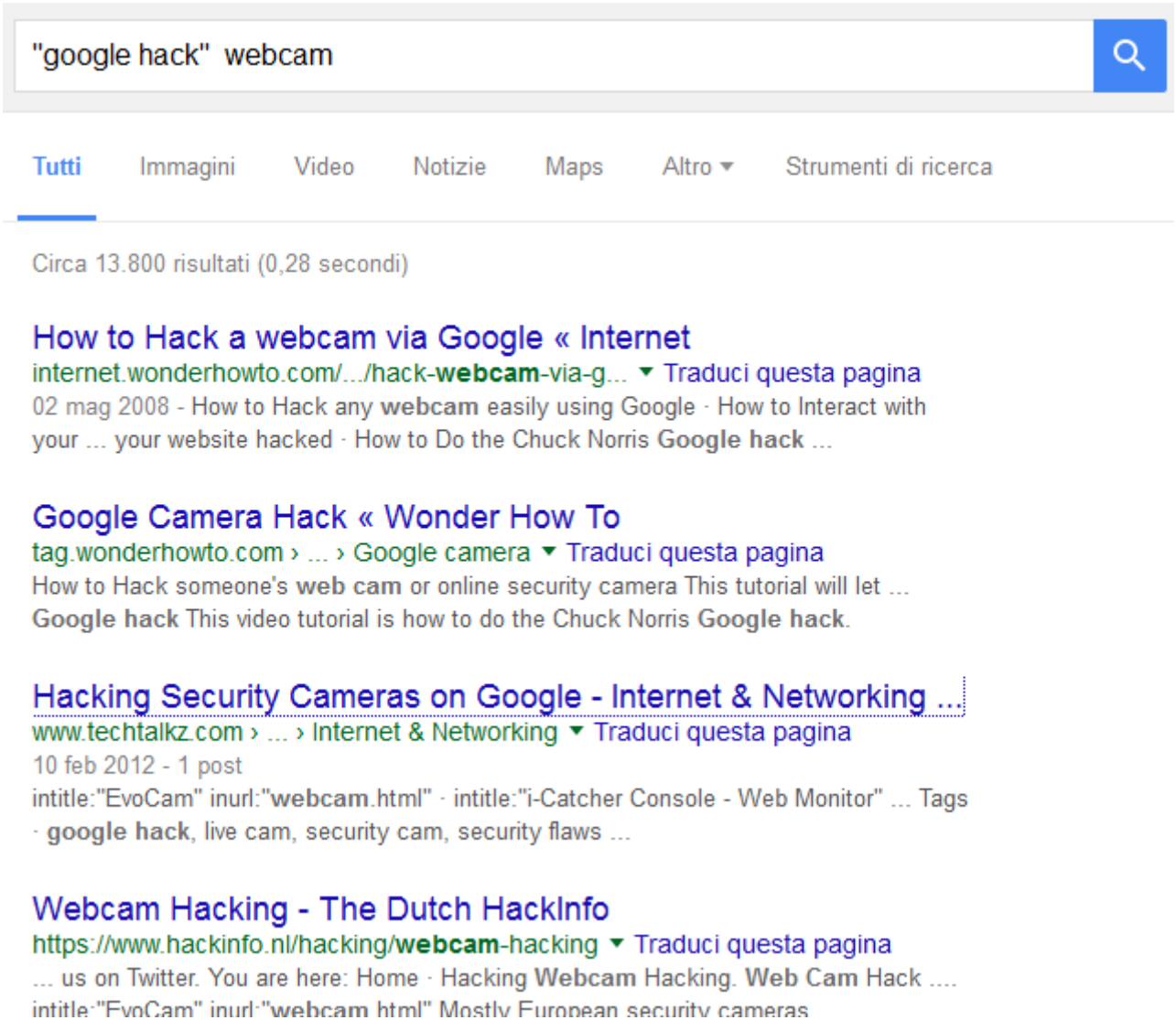
83.36.133.215
215.Red-83-36-133.dynamicIP.rima-tde.net
Telefonica de Espana
Added on 2015-02-17 04:24:39 GMT
Spain, Navalmoral De La Mata
Details

```
SSH-2.0-dropbear_0.46
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCKj10BLi11/oSbukFArKJZTXvBvw+AUGfie6fdE7psCNwC
LM5bYnJgjQZMP/VOhJkxkA539e2mM4fW9U4ECAUwgvlF9AZGhcmn0kF0jIjMUDgCV8kFIS85OuBU
/ayyswdYp6bxp3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMDfZM9P
Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...
```

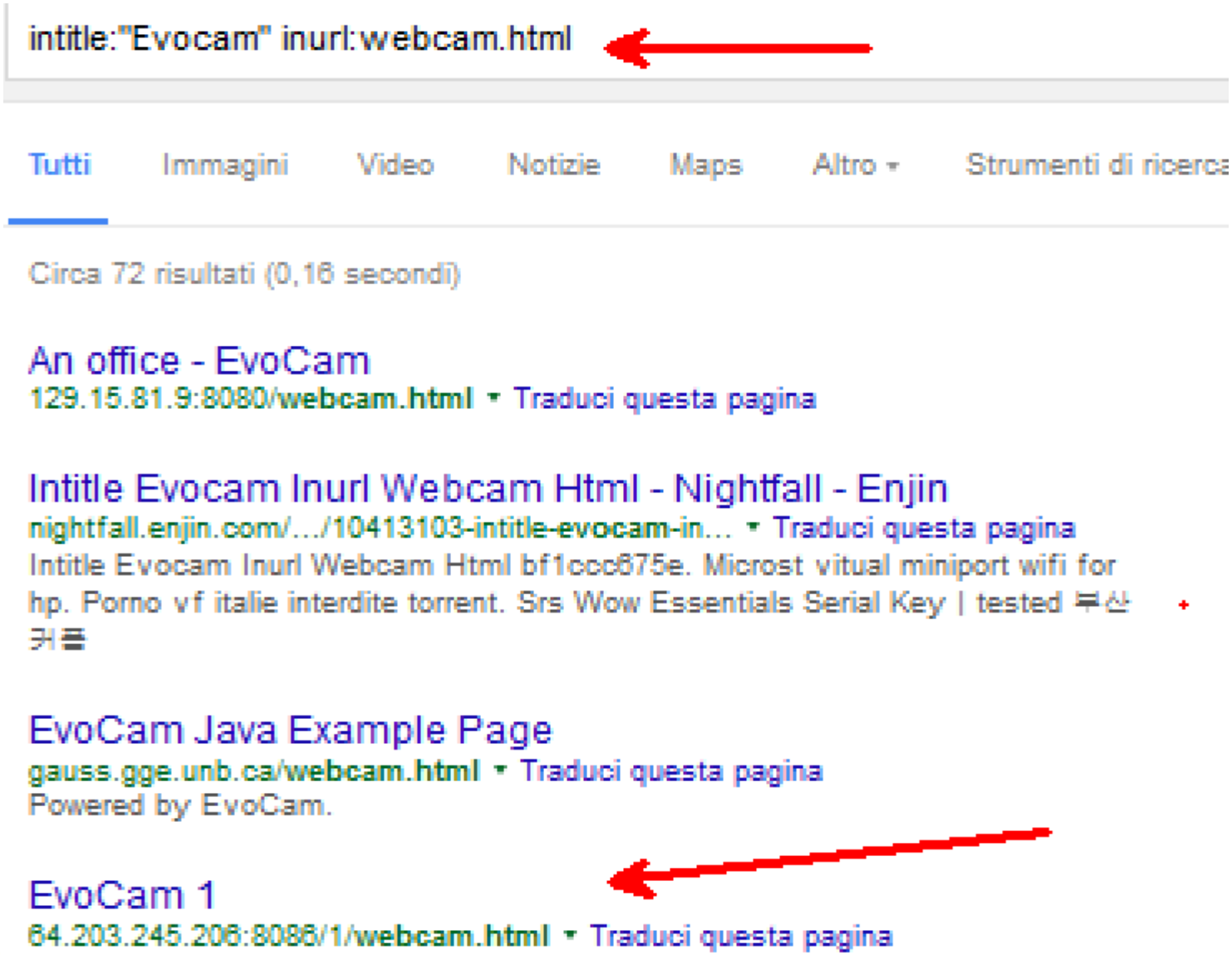
88.9.146.203
203.Red-88-9-146.dynamicIP.rima-tde.net
Telefonica de Espana
Added on 2015-02-17 03:15:43 GMT
Spain
Details

```
SSH-2.0-dropbear_0.46
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCKj10BLi11/oSbukFArKJZTXvBvw+AUGfie6fdE7psCNwC
LM5bYnJgjQZMP/VOhJkxkA539e2mM4fW9U4ECAUwgvlF9AZGhcmn0kF0jIjMUDgCV8kFIS85OuBU
/ayyswdYp6bxp3zn0tGAh0Ty8ikf7CgWU5c+PCbpygbBxMDfZM9P
Fingerprint: dc:14:de:8e:d7:c1:15:43:23:82:25...
```

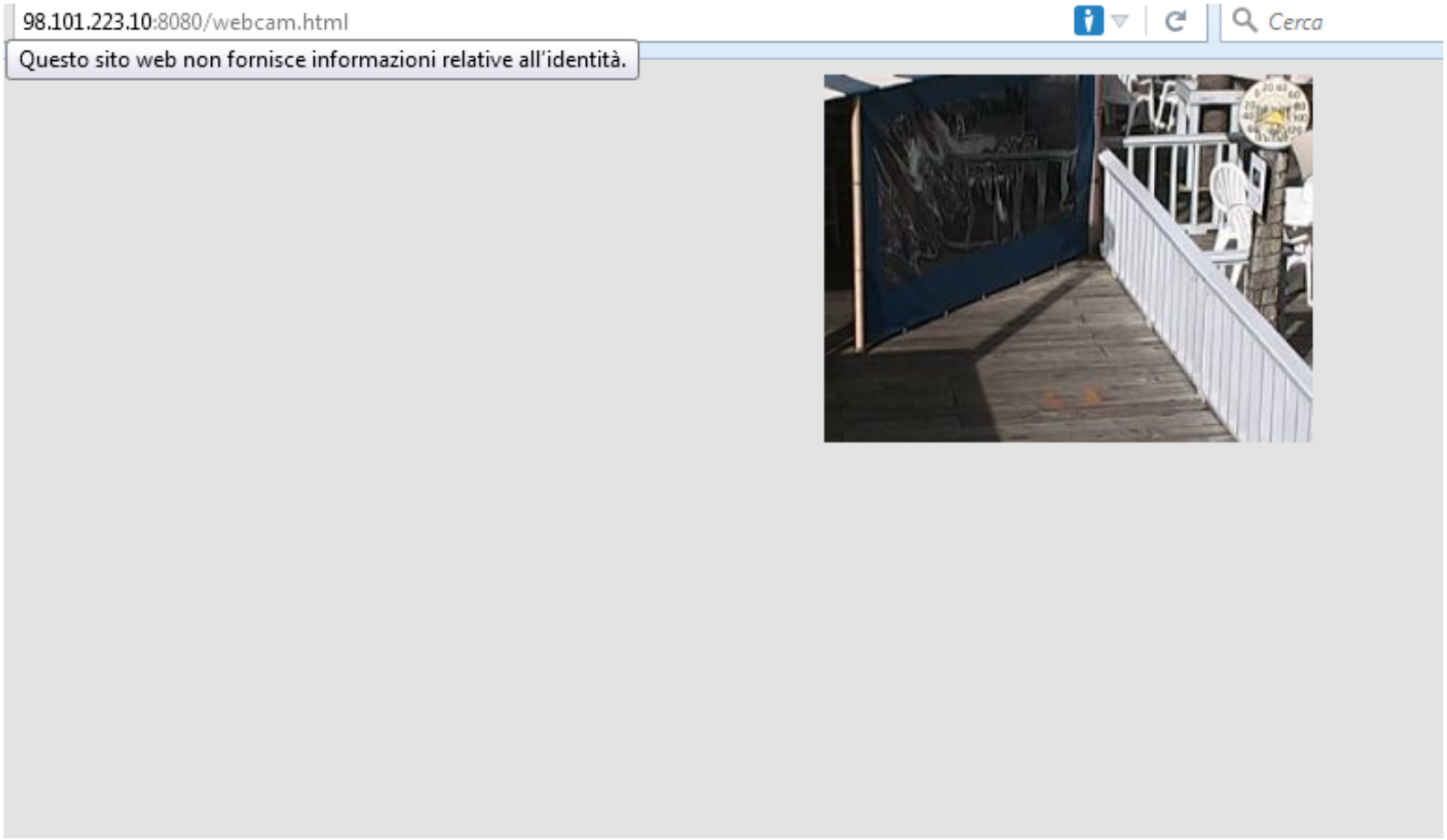
Rischi e vulnerabilità



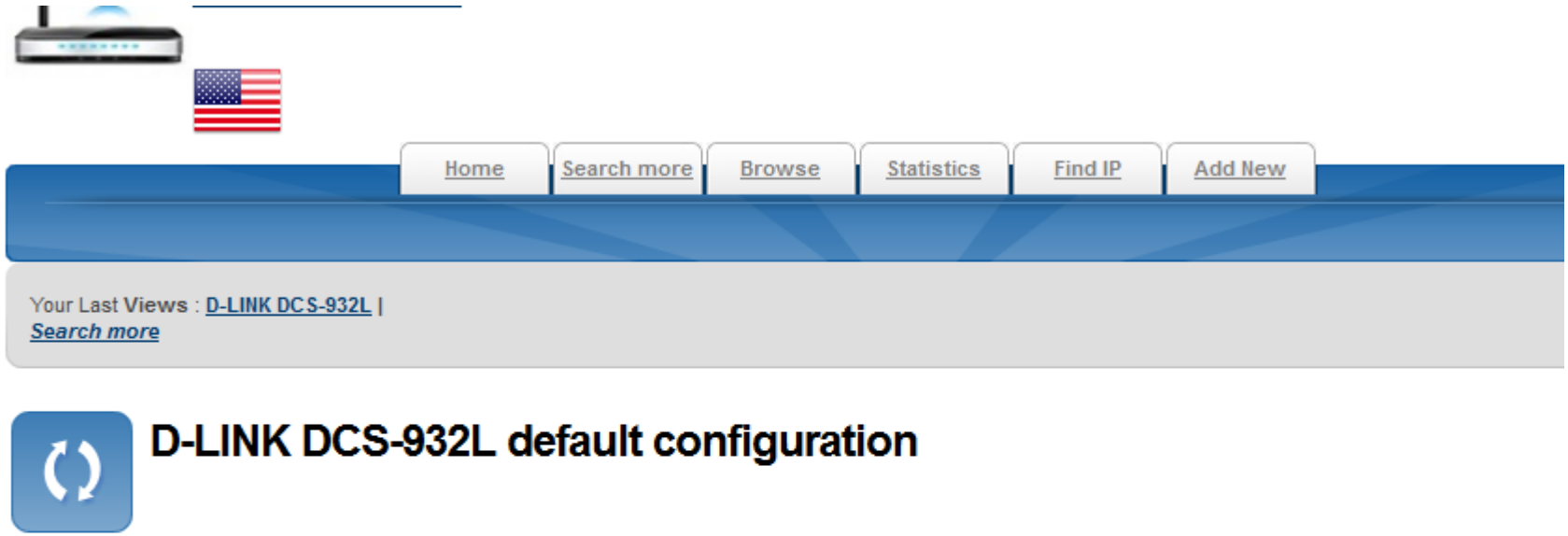
Rischi e vulnerabilità



Rischi e vulnerabilità



Rischi e vulnerabilità



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

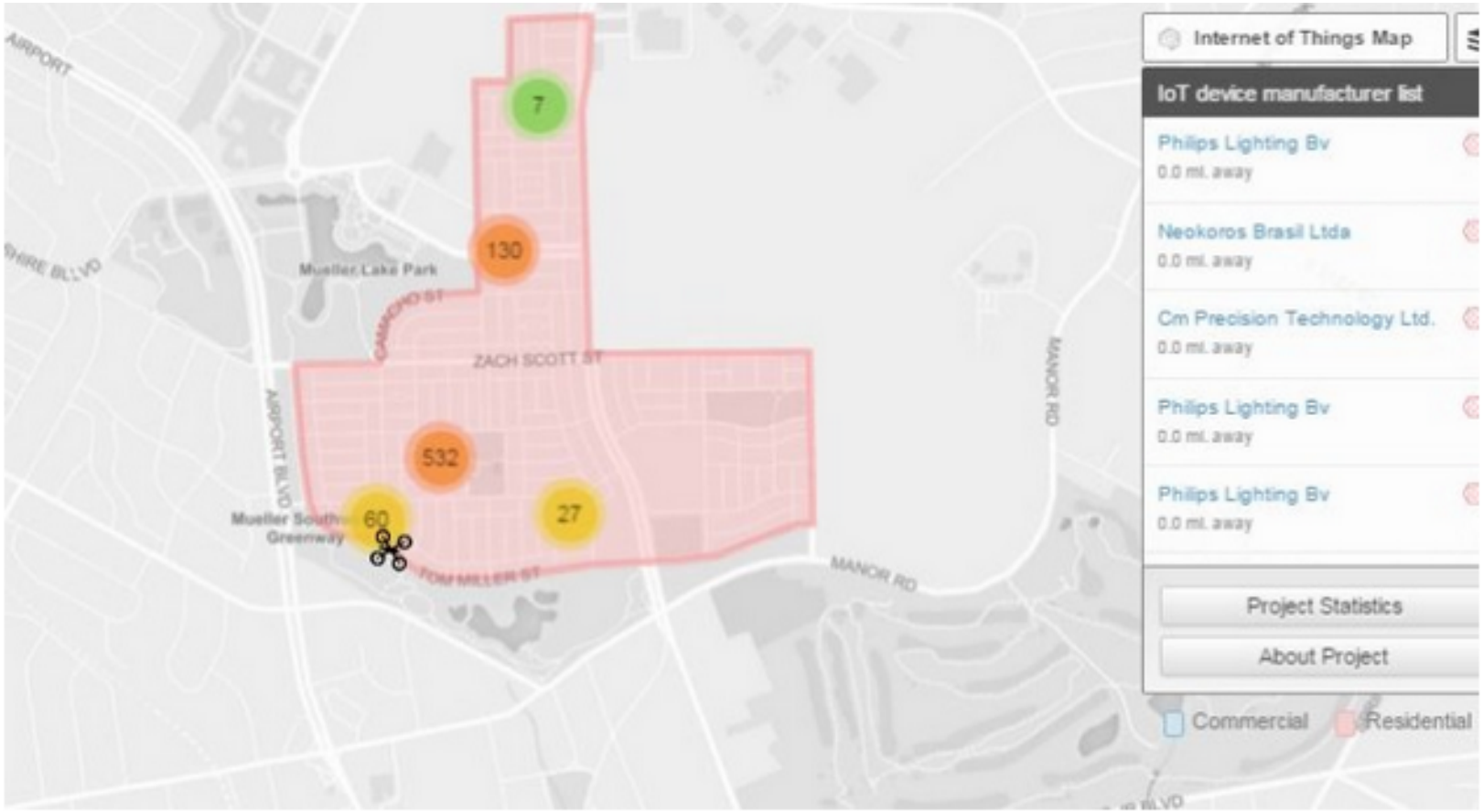
(

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

Rischi e vulnerabilità

Insomma la partita è appena iniziata dobbiamo essere consapevoli del fatto che vivremo in un mondo in cui i anche 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

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

Contatti

- agi@fastmail.fm
- www.ricercheonline.org

Grazie.