

# Mon frigo passe plus de temps sur Internet que moi

---

*LES TROUBLES DE L'INTERNET OF THINGS*

Guillaume Stephen



# About me:

---

- Bac S (Sciences de l'ingénieur)
- DUT réseaux et télécoms
- Actuellement en BSc Ethical Hacking

# Avertissement

---

Tout élément décrit par la suite est à un titre d'information et d'éducation.

Je n'incite ni ne valide l'utilisation du moindre des éléments suivants à un usage nocif.

La légalité des éléments varient selon le pays, l'usage, et l'époque, et la connaissance des lois est à la discrétion d'une personne tentant de l'utiliser.

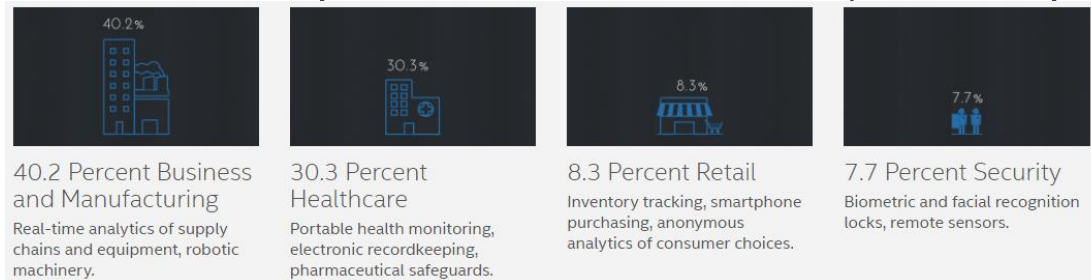
# Internet of Things: Définition

---

1974: Premiers distributeurs bancaires

Une toile « d'objets connectés » qui communiquent et interagissent entre eux.

Utilisation fréquente en milieu médical, domotique, industriel...



15 milliards d'objets en 2015...estimation de 200 d'ici à 2020!

Une des raisons de la nécessité de l'IPv6

# Internet of Things: Pourquoi?

---

- Uniformisation des objets du réseau
- Automatisation, surveillance des données
- Coolitude

# INVESTISSEZ!



# Les abus de l'loT

---

- Une course à la technologie qui n'est pas nécessaire
- Une démocratisation totale du système qui lui est néfaste
- Une approche plus marketing qu'informatique
- Des projets par financement participatifs quotidiens

# Lequel n'existe pas?

---

- Un pantalon qui envoie un sms si la fermeture éclair est baissée
- Une bouteille de vin connectée qui peut racheter du vin quand à court
- Des chaussettes qui mettent Netflix en pause si détection du sommeil du porteur
- Une multiprise commandée vocalement par Siri

# Solution:

---



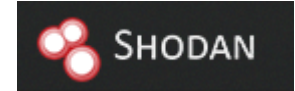
# Une multitude de données

---

- Moyens de paiement
- Sons, vidéos, images
- Données biologiques
  
- Contrôle à distance
- Surveillance des systèmes

# Shodan

---



- Moteur de recherche
- Recherche avant tout dans les bannières plutôt que contenu
- Indexe toutes les IP et scanne les ports
  
- Sert à identifier des failles
- Permet de rapidement visualiser l'étendue de l'IoT

# Shodan: Webcam Xp en France

webcamxp country:fr



Total results: 45

## webcamXP 5

APoitiers-652-1-374-176.w109-223.abo.wanadoo.fr

Orange

Added on 2016-06-29 14:58:51 GMT

France

Details

HTTP/1.1 200 OK

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 7618

Cache-control: no-cache, must revalidate

Date: Wed, 29 Jun 2016 14:58:49 GMT

Expires: Wed, 29 Jun 2016 14:58:49 GMT

Pragma: no-cache

Server: webcamXP 5

## webcamXP 5

ALille-651-1-246-53.w90-1.abo.wanadoo.fr

Orange

Added on 2016-06-29 11:01:04 GMT

France, Mons-en-barœul

Details

HTTP/1.1 200 OK

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 7413

Cache-control: no-cache, must revalidate

Date: Wed, 29 Jun 2016 11:01:00 GMT

Expires: Wed, 29 Jun 2016 11:01:00 GMT

Pragma: no-cache

Server: webcamXP 5

## webcamXP 5

cn106-1-ibx.proxad.net

Free SAS

Added on 2016-06-29 07:37:08 GMT

France, Contes

Details

HTTP/1.1 200 OK

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 2198

Cache-control: no-cache, must revalidate

Date: Wed, 29 Jun 2016 07:37:07 GMT

Expires: Wed, 29 Jun 2016 07:37:07 GMT

Pragma: no-cache

Server: webcamXP 5

# Shodan : Vizio SmartTV

ssl:"tv widgets" port:"8099" 

Total results: 741

  
 dhop.gwnt.ga.charter.com  
**Charter Communications**  
Added on 2018-06-20 18:24:35 GMT  
 United States, Thomaston  
[Details](#)

## SSL Certificate

Issued By:

| Common Name: TV Widgets

| Organization: Yahoo




Issued To:

| Common Name: TV Widgets

| Organization: Yahoo

## Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

  
 dhop.kmy.ne.charter.com  
**Charter Communications**  
Added on 2018-06-20 18:07:44 GMT  
 United States, Kearney  
[Details](#)

## SSL Certificate

Issued By:

| Common Name: TV Widgets

| Organization: Yahoo


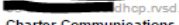

Issued To:

| Common Name: TV Widgets

| Organization: Yahoo

## Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

  
 dhop.rvsd.ca.charter.com  
**Charter Communications**  
Added on 2018-06-20 18:05:11 GMT  
 United States, Big Bear City  
[Details](#)

## SSL Certificate

Issued By:

| Common Name: TV Widgets

| Organization: Yahoo

Issued To:

| Common Name: TV Widgets

| Organization: Yahoo

## Supported SSL Versions


SSLv3, TLSv1, TLSv1.1, TLSv1.2

## TOP COUNTRIES




United States	683
Korea, Republic of	29
Canada	13
Mexico	6
Venezuela, Bolivarian Republic of	5

# Shodan : Icy Clever Thermostat

title:"ICY Clever Thermostat" 


Total results: 47

---

**ICY Clever Thermostat**  
[redacted]  
5ED4D5A8.cm-7-5d.dynamic.ziggo.nl  
Ziggo  
Added on 2016-06-29 18:17:38 GMT  
 Netherlands  
[Details](#)


HTTP/1.0 200 OK  
Server: uIP/1.0 http://www.sics.se/~adam/uip/  
Connection: close  
Content-Type: text/html

---

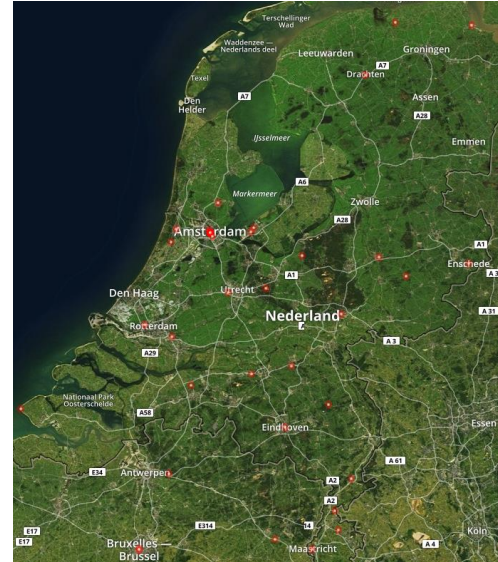
**ICY Clever Thermostat**  
[redacted]  
[redacted].dynamic.upc.nl  
UPC NL  
Added on 2016-06-29 11:28:44 GMT  
 Netherlands  
[Details](#)

HTTP/1.0 200 OK  
Server: uIP/1.0 http://www.sics.se/~adam/uip/  
Connection: close  
Content-Type: text/html

---

**ICY Clever Thermostat**  
[redacted]  
[redacted].ip.telfort.nl  
KPN  
Added on 2016-06-29 05:53:16 GMT  
 Netherlands, Amhem  
[Details](#)

HTTP/1.0 200 OK  
Server: uIP/1.0 http://www.sics.se/~adam/uip/  
Connection: close  
Content-Type: text/html



# Shodan

---

- Shodan pointe les failles, ne les déclenche pas
- Démontre la nécessité d'une protection de l'IoT
- Des cas dangereux avec utilisation néfaste de Shodan:

## **Large botnet of CCTV devices knock the snot out of jewellery website**

Welcome to the Internet of things, where security is lax or altogether nonexistent.

**rencontré un système de commande pour une centrale hydroélectrique en France. |**

## Proofpoint Uncovers Internet of Things (IoT) Cyberattack

MORE THAN 750,000 PHISHING AND SPAM EMAILS LAUNCHED FROM "THINGBOTS" INCLUDING TELEVISIONS, FRIDGE

# Mitigation:

---

- S'assurer de la sécurité d'un dispositif, comprendre qu'il s'agit d'un ordinateur
- Utiliser des firewall pour « taire » les bannières
- S'interroger sur la nécessité de la dimension IoT des dispositifs
- Avoir un système de patchs de sécurité
- Ne pas connecter au web si fonction voulue en « circuit fermé »

# Conclusion

---

