The Internet of (Ransomware) Things

Rayna Stamboliyska

vente-privee | @MaliciaRogue | @ventepriveeTech

De quoi parle-t-on?

Can Powerwall work without Internet?
Powerwall needs internet (wired Ethernet or your home Wi-Fi) or cellular service to communicate with the Tesla mobile app and receive software updates. A reliable connection is required to provide new product features over time. Powerwall can function if the connection is temporarily lost but should not be installed in a location without internet or cellular service.

¯_(ツ)_/¯

De quoi parle-t-on?

sfist

You Can Only Wash Google And Levi's New $350 'Connected' Jacket Ten Times

BY **EVE BATEY** IN **ARTS & ENTERTAINMENT** ON SEP 26, 2017 12:15 PM

Via @InternetOfShit

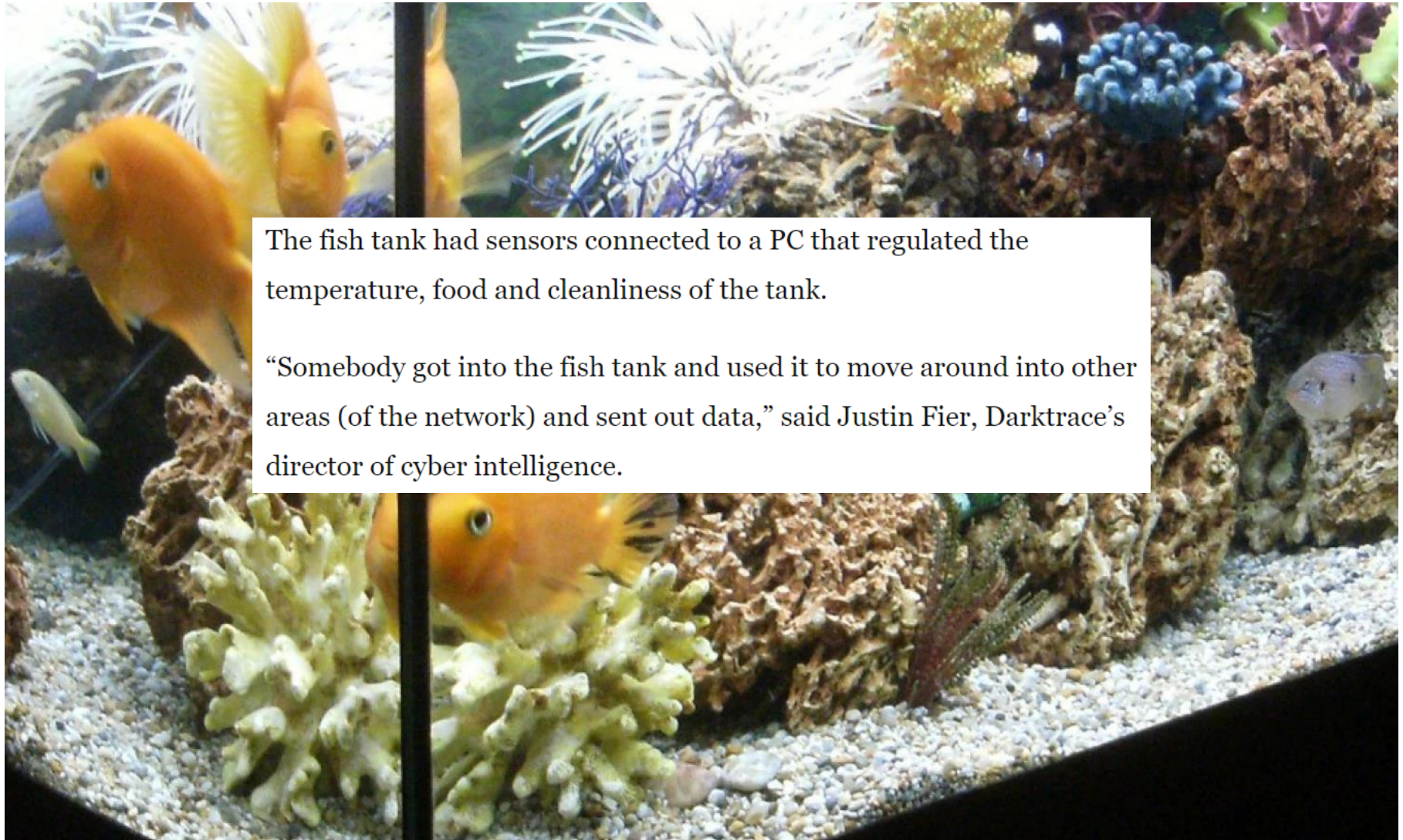
En parlant de DRM…

- Juicero == Epic fail
- Financement VC : 120 million USD ; 16 mois d'existence
- 700 USD au lancement, puis 400 USD
- Requiert des packs proprio pour faire du jus #oupas

IoT == Internet of Trash

- Mieux gérer les rondes des éboueurs
- Prédire le remplissage
- BlueCity repose sur du BLE seul + crowdsourcing
- OpenTrashCan parle et vous envoie des mails https://youtu.be/XlFvMDs3TFM
- bruno achète même les sacs poubelle

In IoT, 'S' stands for Security



The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank.

"Somebody got into the fish tank and used it to move around into other areas (of the network) and sent out data," said Justin Fier, Darktrace's director of cyber intelligence.

In IoT, ‘S’ stands for Security

- Hello Barby
- My Friend Cayla
- Ours en peluche
- Montres connectées

...

Sextoys connectés

- On ne rigole pas
- Oui, ça sert pour de vrai
- 56 sextoys avec au moins du Bluetooth (aussi WiFi/3G/4G)
- 46 applis Android
- 31 applis iOS
- Dorcel (in-cul-bateur)

rod_lee tipped 20 tokens

Notice:

Notice: MY LOVENSE LUSH VIBRATOR IS SET TO REACT TO YOUR TIPS. THERE ARE 5 LEVELS OF INTENSITY OR RANDOMLY CHOOSE A LEVEL FROM 1-5 :

Notice: ■ Level 1 - Tip (1-14) 3 seconds (Low vibrations)

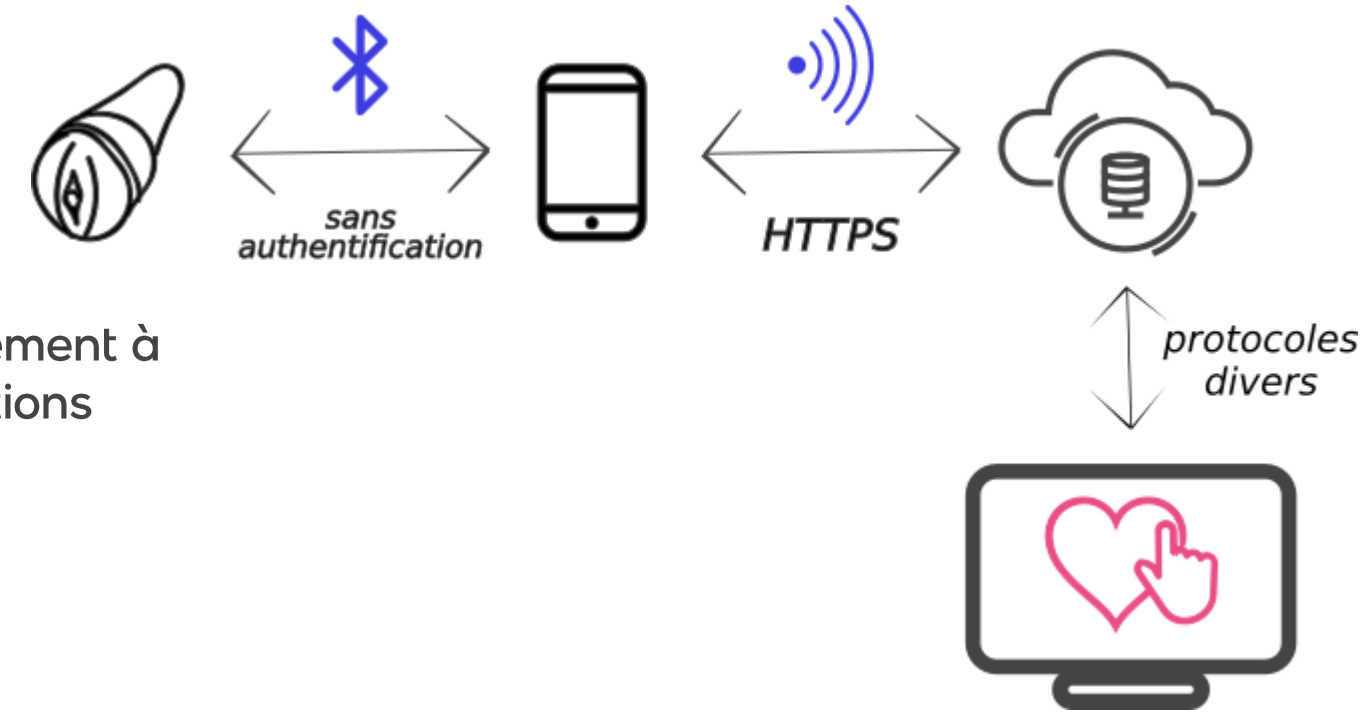
Notice: ■ Level 2 - Tip (15-99) 6 seconds (Medium vibrations)

Notice: ■ Level 3 - Tip (100-499) 10 seconds (Medium vibrations)

Notice: ■ Level 4 - Tip (500-999) 1 Minute (High vibrations)

Notice: ■ Level 5 - Tip (1000 - 1000+) 3 Minutes (High vibrations)

Sextoys connectés



BLE positions des parties mobiles pour mouvement à venir et de la vitesse de mouvement + interactions boutons ; appairage : 1234

Sextoys connectés Kiiroo

- Autorisations excessives
- Certif X.509 OK depuis 23/02/17
- Durée de conservation des données ?
- pubnub.com et hidashhi.com utilisent toujours du SSLv3 (=> /!\ POODLE)
- hidasshi.com en WordPress 3.9.2 (v4.8)

... mais Kiiroo a un programme de disclo

Sextoys connectés (inconnu)

- Autorisations excessives
- Certif X.509 OK depuis 23/02/17
- Durée de conservation des données ?
- pubnub.com et hidashhi.com utilisent toujours du SSLv3 (=> /!\ POODLE)
- hidasshi.com en WordPress 3.9.2 (v4.8)

... mais Kiiroo a un programme de disclo

Avec assez de lubrifiant…

- 6 pour ♀, 2 pour ♂ et 2 😁
- 3 applis mobiles (Java)
- Cert X.509 auto-signé (“F”), vuln. à OpenSSL Padding Oracle

```
public final class Config
{
// snip
  public static String CY_APP_KEY = "f20e6f99c74d4cbfaae0f2868f320201";
  public static String CY_HTTP;
  public static final String DATE = "date";
  public static final String DEVICE_ADDRESS = "device_address";
  public static final String DEVICE_NAME = "device_name";
  public static final String EMAIL = "email";
  public static final String FIRST_PAIRING = "first_pairing";
  public static String HTTP = "http://api.masqué.tld";
  public static final String HTTP_IP = "http://74.xxx.xxx.xxx";
```

PCAP or it didn't happen

En bref :

- Remonte en clair des données vers une machine Windows avec un FTP en clair sur le port 21
- le serveur web (IIS) est accessible en clair sur le port 80
- Umeng plutôt que GA ;
- Adware Android.Igexin (2015, *Low risk* pour Symantec)
- IMEI, IMSI, versions de l'OS, du noyau, autres applis installées + en cours d'exécution, etc.

```
n=rayna.st%40xxxxxx.com&sc=FC7996F1A4974AA30F92B400C4187D35&t=2&access_token=F6F66EB
078A0958A59C9E2CF09FCABF9&p=74F5CFB03AA9ECB3B40DC7FFBFB8D2C5&e=rayna.st%40xxxxxx.com
&

//

Set-Cookie: impron_userinfo=uid=5ed1a49c-38d4-43fa-b01d-4d34a936b327&token=;
expires=Thu, 10-May-2018 20:27:38 GMT; path=/
```


THE INTERNET OF RANSOMWARE
THINGS IS UPON US

Objets à visée médicale connectés

- IoMT = 25 milliards USD investissement
- Pompe de transfusion Medfusion 400 : réa + anesthésie + traitement

-> mdp en dur, buffer overflow, etc.

Réaction : *“The possibility of this exploit taking place in a clinical setting is highly unlikely, as it requires a complex and an unlikely series of conditions.”*

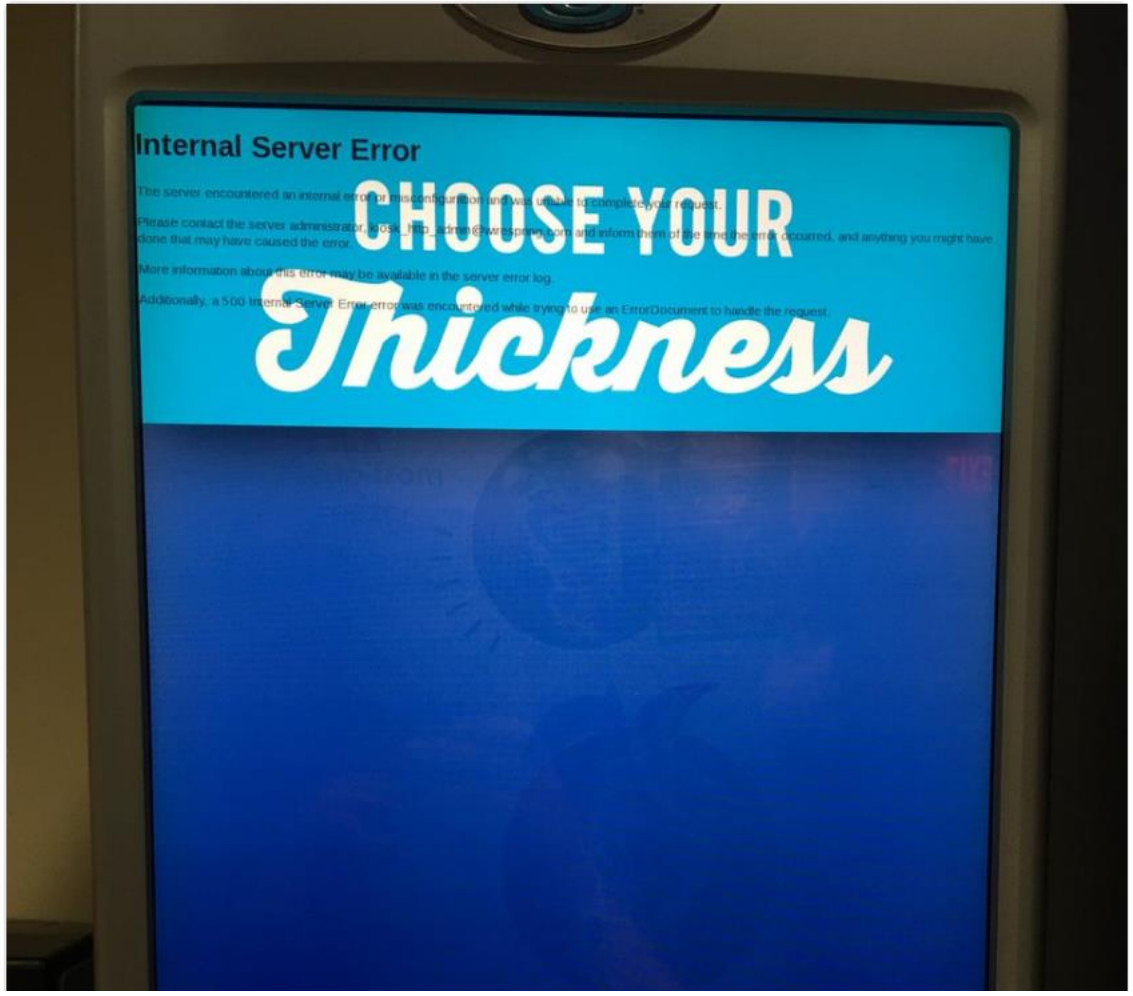
Repenser la « vie privée »

- GDPR renforce le rapport « producteur » - « gestionnaire »
- Quid de l'horizontalité introduite par les IoT ?
- Frigo, pacemaker,...
- Êtes-vous victime de viol/agression sexuelle ?
- Données à caractère personnel *vs.* données personnelles ;
- « Commodification » des données (Ashley Madison)
- Certains objets sont plus intimes que d'autres

=> Gradient d'intimité

.@internetofshit all I wanted was a milkshake

À l'origine en anglais



Merci !

Rayna Stamboliyska

vente-privee | @MaliciaRogue | @ventepriveeTech