



# MASTER 2 – TLS-SEC



Cybersécurité, cerner les menaces et se protéger

**Lundi 07 octobre 2019**



**Fabrice CRASNIER**

*Doctorant en intelligence artificielle*

Consultant expert senior - Responsable du pôle FORENSIC  
Laboratoire SCASSI-CYBER - Société SCASSI Conseil

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## *Cerner les menaces*



## Le phishing

**Le phishing est une technique frauduleuse** utilisée par les pirates informatiques pour récupérer des informations sensibles, personnelles et/ou confidentielles (coordonnées bancaires, vol d'identité...) appartenant à des internautes. Pour cela, ils reproduisent parfaitement le design d'un site commercial légitime, d'un fournisseur d'accès à Internet, d'une banque, etc.

### Campagne Hack Academy - WILLY (2015)



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le phishing

Cybersécurité : Bercy a testé les réactions de ses employés avec un faux courriel de "hameçonnage"



*Plus de 30.000 personnes ont cliqué sur les liens entre 10 heures et midi lundi matin.*

Dans cette vaste opération de "hameçonnage", **1 employé du ministère des Finances sur 5 a cliqué sur des liens frauduleux.**

**Plus de 20% des employés piégés**

Ils sont 145.000 collaborateurs et agents du ministère de l'Economie et des Finances à avoir reçu ce mail lundi matin. Les expéditeurs font référence à d'illustres noms de la littérature, comme Emma Bovary ou Jean-Baptiste Poquelin, ou encore Isabelle de Merteuil.

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les fraudes

### Les Faux ordres de virement Internationaux ou l'escroquerie au PDG (FOVI)

#### Fraude aux Faux Ordres de Virement #FOVI





# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les fraudes

**Les Faux ordres de virement Internationaux  
ou l'escroquerie au PDG (FOVI)**

**Les escrocs se renouvellent régulièrement.**

- L'escroquerie « *au faux président* »
- L'escroquerie « *au faux fournisseurs* »
- L'escroquerie « *au changement de Relevé d'Identité Bancaire* »
- L'escroquerie « *au virement SEPA, à l'informatique* »

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les fraudes



CYBERMALVEILLANCE.GOUV.FR  
Assistance et prévention du risque numérique

### L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

#cybermalveillance #TechSupportScam ,  
le #FBI confirme la recrudescence  
constatée par @cybervictimtes en France  
des arnaques au faux support technique :  
+86% de plaintes en 2017 pour un  
préjudice évalué à 15 M\$ aux US. Nos  
conseils pour éviter ce fléau 📌  
[ic3.gov/media/2018/180...](https://www.ic3.gov/media/2018/180...)

#cybermalveillance #TechSupportScam  
Recrudescence des arnaques au faux  
support technique également confirmée  
par #Microsoft qui constate une  
augmentation de + 24% des cas qui lui  
sont remontés dans 183 pays.

**SOURCE :** [https://www.cybermalveillance.gouv.fr/wp-content/uploads/2017/12/20171214\\_fiche\\_arnaque\\_support\\_technique.pdf](https://www.cybermalveillance.gouv.fr/wp-content/uploads/2017/12/20171214_fiche_arnaque_support_technique.pdf)

**SOURCE :** <https://www.cybermalveillance.gouv.fr/>

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

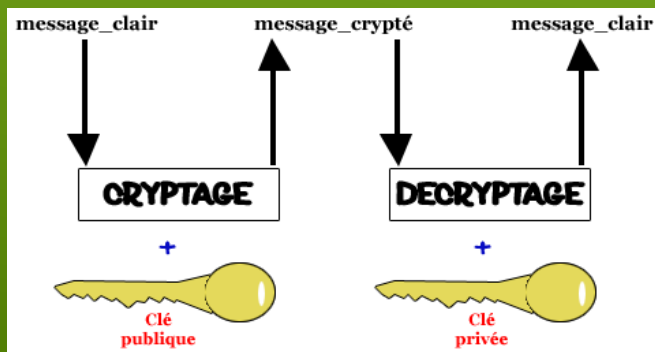
L'usage du chiffrement par les cybercriminels



**+ de 100** ransomwares différents

### Les outils utilisés

- Le chiffrement symétrique
- Le chiffrement asymétrique
- La signature numérique



## Les rançongiciels

**0143485322 : fax du Numéro masqué (1 page)**

MonFax [fax@monfax.com]

Envoyé : mar. 13/10/2015 11:45

À :



Message



fax-0143485322-000-20151006072552-1444109152.3022.doc (100 Ko)

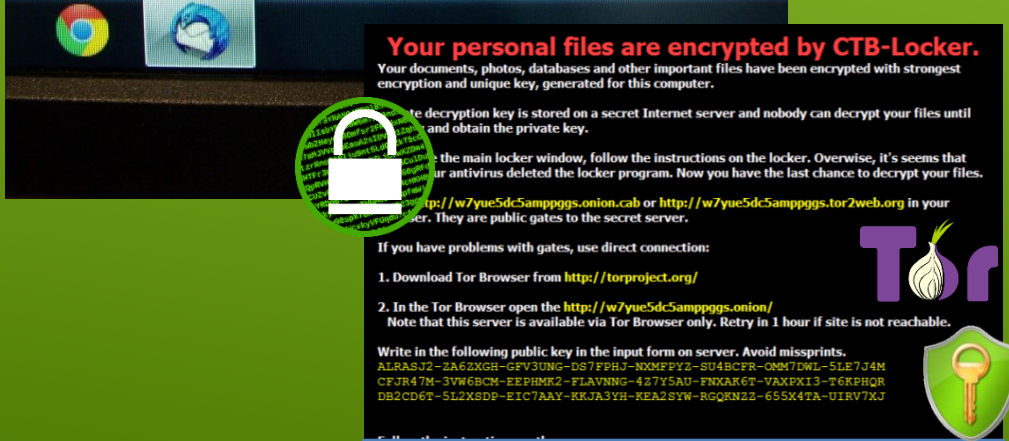
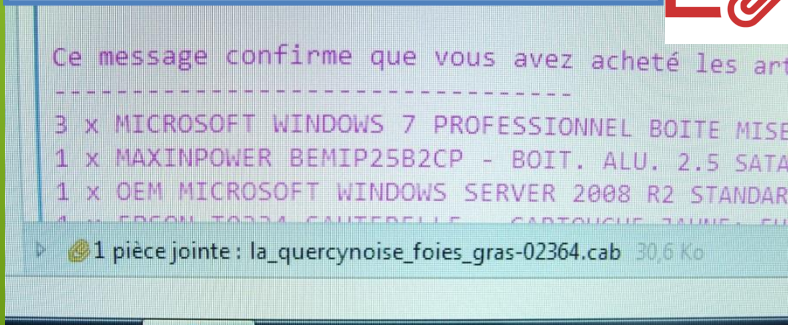
Vous avez reçu un fax en provenance du **Numéro masqué**.  
Le fax au format DOC est joint à ce mail.

## Les rançongiciels

Janvier 2013 – 2018++

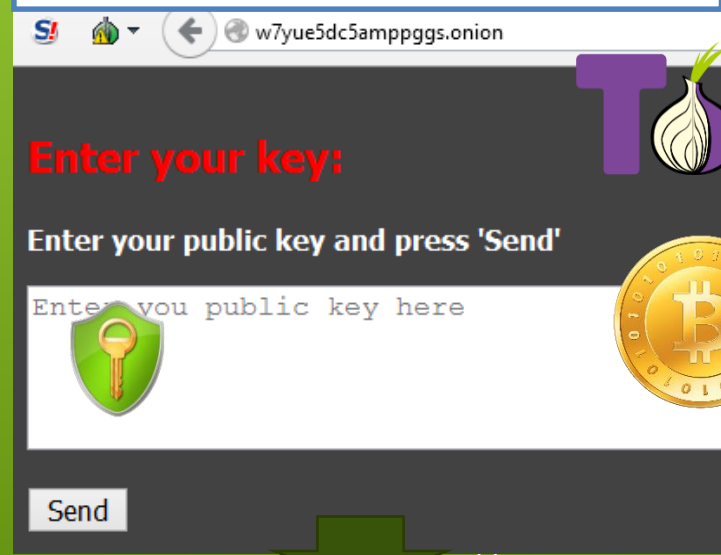
### La contamination

#### 1 - Courriel avec pièces jointes



#### 2 – demande de rançon

#### 3 – Mécanisme de paiement



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

*L'adaptabilité des cybercriminels aux usages*



Les évolutions de la fonction RH



Mon CV

9 chances sur 10 d'obtenir un clique



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

***L'adaptabilité des cybercriminels  
aux usages***

Répondre Répondre à tous Transférer

dim. 17/06/2018 17:55

A

Abonnées - PRO <jf.levenez@wanadoo.fr>

Modification sur votre adresse de contact

ston.gif

PDF

Open --Office (1).pdf



Politique de protection des données personnelles

Consulter vos données de contact afin d'éviter tout piratage, cliquez et reconnectez-vous en cliquant sur la pièce jointe.

Merci pour votre fidélité  
Bien cordialement,

L'e-mail est envoyé automatiquement. Nous vous remercions de ne pas y répondre : votre demande ne pourrait être traitée.

# RGPD

Le  
Règlement  
Général sur  
la  
Protection  
des  
Données

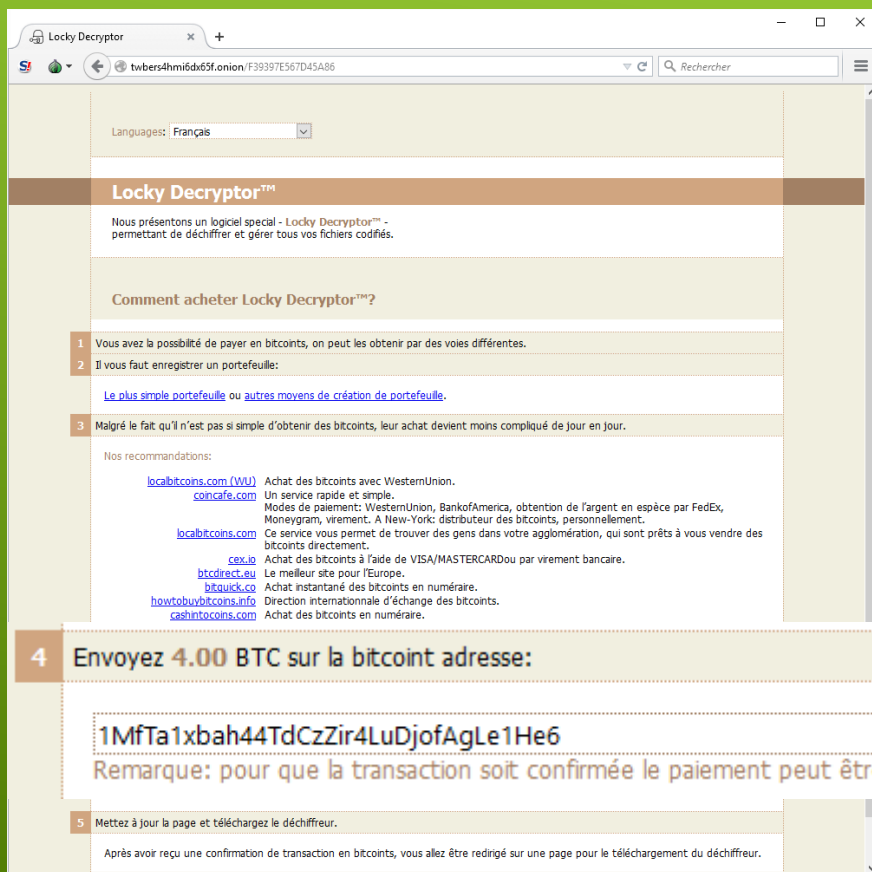
**25 mai  
2018**

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

### Les Ransomwares (Cryptolocker)

Janvier 2013 – 2017++



The screenshot shows the Locky Decryptor website interface. At the top, there's a browser window with the URL 'twbers4hmi6dx65f.onion/F39397E567D45A86'. Below the browser, the website has a language dropdown set to 'Français'. The main heading is 'Locky Decryptor™'. Below it, a paragraph states: 'Nous présentons un logiciel special - Locky Decryptor™ - permettant de déchiffrer et gérer tous vos fichiers codifiés.' A section titled 'Comment acheter Locky Decryptor™?' follows, with a numbered list of instructions. Step 4 is highlighted: 'Envoyez 4.00 BTC sur la bitcoin adresse: 1MfTa1xbah44TdCzZir4LuDjofAgLe1He6'. Below this, a note says: 'Remarque: pour que la transaction soit confirmée le paiement peut être...'. Step 5 is also visible: 'Mettez à jour la page et téléchargez le déchiffreur.' At the bottom, it says: 'Après avoir reçu une confirmation de transaction en bitcoins, vous allez être redirigé sur une page pour le téléchargement du déchiffreur.'



The screenshot shows the language selection menu of the Locky ransomware. The menu is titled 'Languages:' and has a dropdown arrow. The selected language is 'Français'. The list of languages includes: Français, Български, Català, Čeština, Dansk, Ελληνικά, English, Español, Français (highlighted), Hrvatski, Magyar, Italiano, 한국어, Nederlands, Norsk bokmål, Polski, Português, Slovenčina, Српски, Svenska, and Türkçe. Below the list, there are several small icons representing different languages or currencies.

## Les rançongiciels

**Wannacry**  
(12 mai 2017)

Janvier 2013 – 2017++

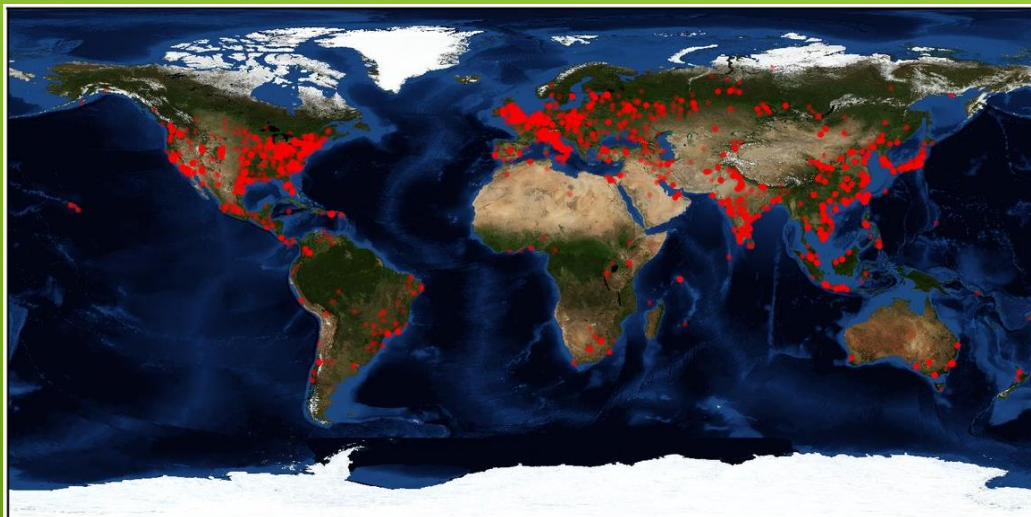
### L'attaque mondiale des PME

Les virus utilisés  
exploiteraient une  
faille dans les  
système Windows,  
divulguée dans des  
documents piratés  
de l'agence de  
sécurité américaine  
NSA.



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

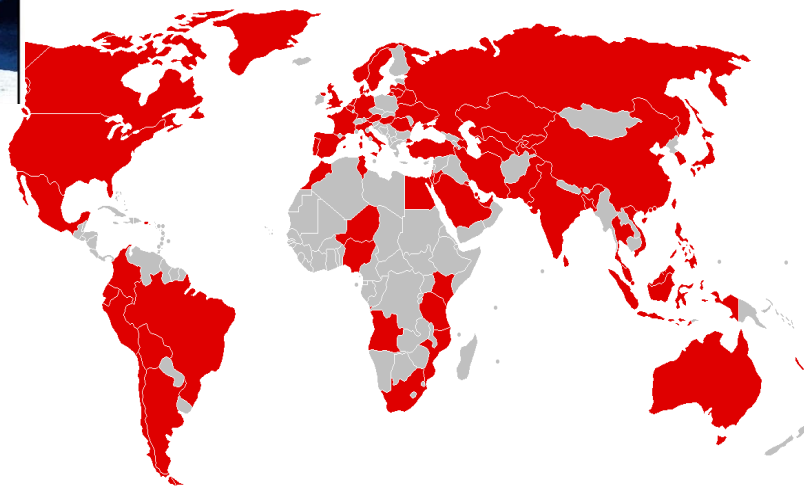


Wannacry, le 12 mai 2017

On évoque désormais  
« 300.000 victimes dans au  
moins 150 pays »

Wannacry, le 14 avril 2017

On évoque  
« 36.000 machines  
infectées »

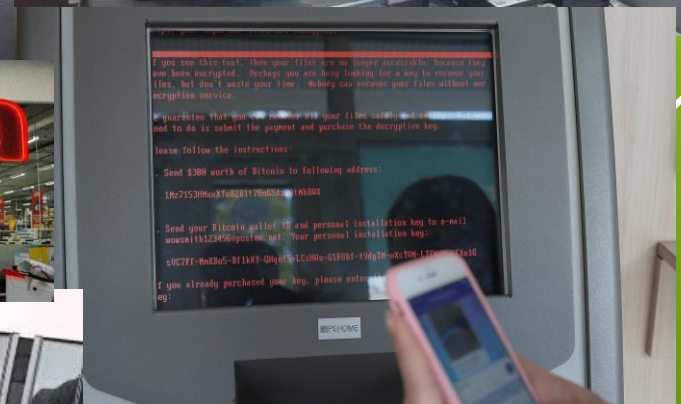


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

NotPetya  
(27 juin 2017)

Janvier 2013 – 2017++



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

### Fiabilité de la source d'information





# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les rançongiciels

Campagne Hack Academy - MARTIN (2015)



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les mécanismes de propagation

La clé USB est le support de transport de données le plus utilisé, mais ne fait-elle que transporter des données ?



Elles ressemblent à des  
clés USB  
mais il ne s'agit pas de  
clé USB



## Les mécanismes de propagation

La clé USB est le support de transport de données le plus utilisé, mais ne fait-elle que transporter des données ?



### USB Rubber Ducky



\$49.99



<https://ducktoolkit.com/>

<https://github.com/hak5darren/USB-Rubber-Ducky/wiki>

<https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads>

<https://shop.hak5.org/products/usb-rubber-ducky-deluxe>

## Les mécanismes de propagation

La clé USB est le support de transport de données le plus utilisé, mais ne fait-elle que transporter des données ?

### USB Lily GO



\$13.99



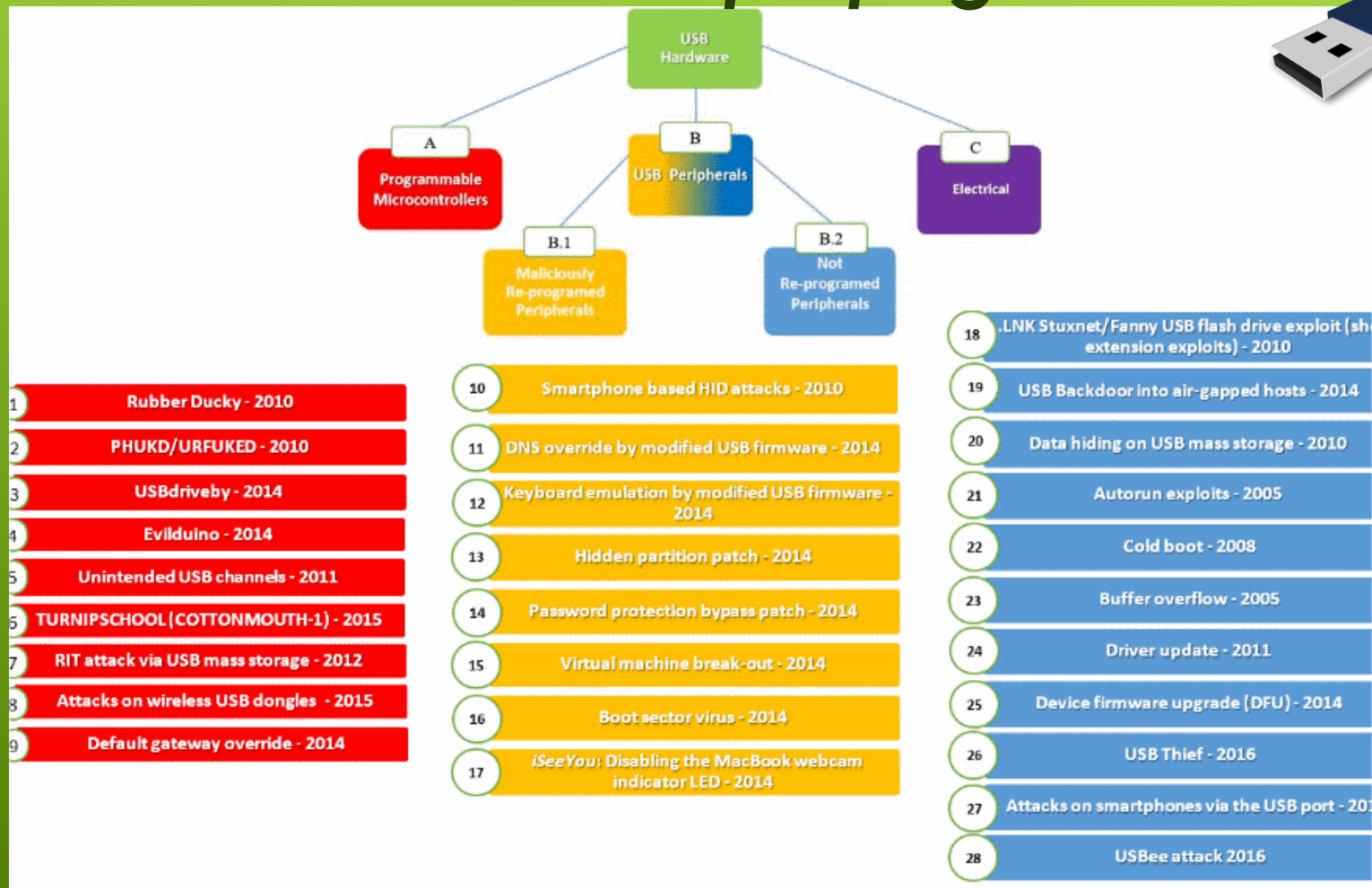
<https://hackingethani.com/physical-hacking-with-usb/>

<http://roothaxor.gitlab.io/ducky2arduino/>



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les mécanismes de propagation



Voici une liste de **29** différents types d'attaques USB

## Les mécanismes de propagation

La clé USB est le support de transport de données le plus utilisé, mais ne fait-elle que transporter des données ?



Teensy 3



Borne de  
rechargement



Goodies



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les mécanismes de propagation

### Satan Ransomware Service

Il est là pour  
vous aider et  
répandre la  
terreur



Thread Tools ▾
Search this Thread ▾
Rate Thread ▾
Display Modes ▾

Today, 16:06 #1

**Cold\_As\_Ice**  
Junior Member  
  
Join Date: Aug 2016  
Posts: 1  
Reputation: 0 [+/-]  
Balance: 0.00\$

Satan is a free to use ransomware kit, you only need to register on the site to start making your viruses. Satan only requires a user name and password to create an account, althrough, if you wish, you can set a public key for two-factor authentication. Satan has a initial fee of 30% over the victim's payment, however, this fee will get lower as you get more infections and payments. All of the user transactions are covered by the server, you'll always get what the victim paid, minus the fee of course.

When creating your malware you can specify the ransom value (in bitcoins), a multiplier for the ransom after X days have passed, the number of days after the multiplier takes place, a private note so you can keep track of your victims.

- Satan is free. You just have to register on the site.
- Satan is very easy to deploy, you can create your ransomware in less than a minute.
- Satan uses TOR and Bitcoin for anonymity.
- Satan's executable is only 170kb.

If english is not your first language or you speak a second language you can translate the ransom notes to help your victims understand better what is happening.  
In case you're looking for a way to spread the ransomware, there is a droppers page, where you can generate a crude code for a Microsoft Word macro and CHM file.  
If you have any problem with the ransomware, you can report it using the leftmost button on the malwares table. The middle blue button is used to update the malware to a newer version, if available, and the green one is used to edit your malware configuration.

**<http://satan6dll23napb5.onion>**

Disponible sur le darknet

## Les bons réflexes

La clé USB est le support de transport de données le plus utilisé, mais son apparence peut être contrefaite, il est alors nécessaire d'être vigilant.

1. J'évite de charger mon téléphone sur des bornes de recharge publiques.
2. Je fais attention aux cadeaux connectés (*goodies*)
3. Je pense à verrouiller (*Win + L*) ma session sur mon ordinateur lorsque je quitte mon poste de travail.
4. Je ne connecte pas une clé USB inconnue à mon ordinateur, je la remets à mon service informatique pour vérification.
5. Je ne connecte pas mon téléphone à un ordinateur même pour le recharger.





**L'e-réputation** est la réputation, l'opinion commune (informations, avis, échanges, commentaires, rumeurs...) sur le Web d'une entité (marque, personne morale (*entreprise*) ou personne physique (*particulier*), réelle (*représentée par un nom ou un pseudonyme*) ou imaginaire).



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## La eRéputation

« Mon Dieu, gardez-moi de mes amis.  
Quant à mes ennemis, je m'en charge ! »

Voltaire



## La eRéputation

### Atteinte à la réputation eRéputation

Une vidéo montre comment un simple stylo permet l'ouverture d'un cadenas pour vélos de la société Kryptonite.

La société n'a pas les ressources humaines suffisantes pour répondre aux bloggeurs et à la presse. La société n'a pas de blog.

L'affaire va prendre des proportions inquiétantes.



**Google :**  
**Cadenas U Kryptonite**  
**& stylo bille**

**15 minutes pour faire la vidéo,**  
**10 millions de dollars de perte pour la société en 10 jours.**

## L'usurpation d'identité

### Usurpation d'adresse mail



Envoyer un Mail Anonyme

La manière la plus simple pour envoyer un e-mail anonymement



Le « **Spoofing** » est un terme anglais utilisé traduit par **usurpation d'identité** électronique. Il s'agit de se faire passer pour quelqu'un d'autre et de commettre des délits via Internet

## L'usurpation d'identité

### Vinci victime d'une attaque de pirates informatiques en usurpation d'identité

Dans ce document, ils affirmaient que des irrégularités comptables sur quelque 3,5 milliards d'euros venaient d'être découvertes à la suite d'un audit interne chez ce major du BTP.



**Quelques minutes après l'envoi du communiqué trompeur, l'action a perdu plus de 18 %. Et, pendant environ trente minutes, la cotation du titre a été suspendue. Finalement, Vinci a perdu 3,76 %.**

**Les faits ce sont déroulés entre 16H05 et 17H35**

## Principe de sécurité de développement

Une faille dans le système de sécurité du magasin en ligne d'Apple a été détectée par les internautes. Selon eux, ce problème technique a provoqué la fuite des codes PIN de **72 millions d'utilisateurs**.



La faille permettait d'introduire d'une manière illimitée les chiffres du code PIN pour chaque **numéro de portable fonctionnant avec l'opérateur mobile T-Mobile**.

### Contournement de la sécurité avec la double authentification

Avec le code PIN attaché à un numéro fonctionnant avec l'opérateur T-Mobile, certains sites américains et européens permettent d'authentifier son identité et d'effectuer différentes opérations. Par exemple, activer des services payants ou bien bloquer le numéro du téléphone.

## Principe de sécurité de développement

### Goto fail :

### la vulnérabilité "très étonnante" d'Apple



```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer
signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;
    (...)

    hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
    hashOut.length = SSL_SHA1_DIGEST_LEN;
    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signature)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

    err = sslRawVerify(ctx,
                      ctx->peerPubKey,
                      dataToSign,          /* plaintext */
                      dataToSignLen,       /* plaintext length */
                      signature,
                      signatureLen);

    if(err) {
        sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
        goto fail;
    }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

*Tribune* : Apple est actuellement aux prises avec une faille **mettant directement en cause la sécurité des usagers** de ses produits. Dans cette tribune, trois experts en sécurité de Lexsi décortiquent les aspects techniques de la faille et formulent des recommandations pour les utilisateurs. (2014)



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Principe de sécurité de développement

### Un hack causé par une fuite d'information sur Google

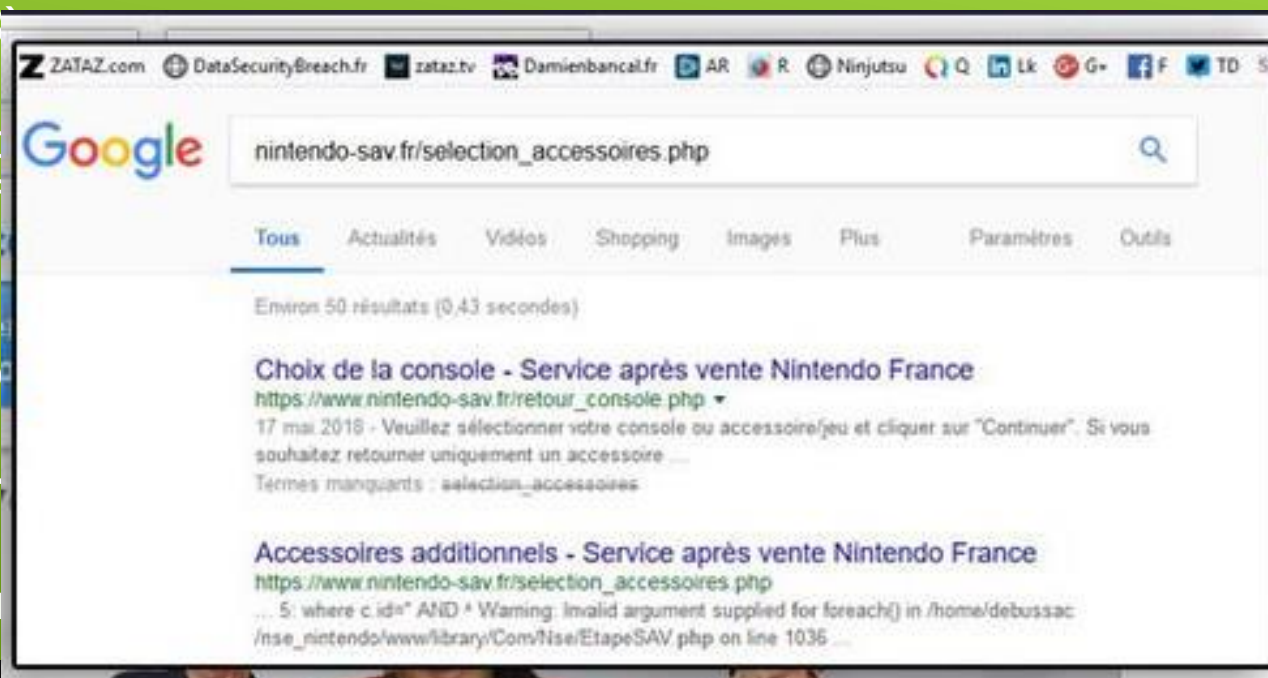
(24 mai 2018)

Le site web de Nintendo France a été victime d'une grave faille de sécurité. Il était possible de récupérer des informations sensibles.

Une telle faille a permis d'accéder aux mots de passe de milliers de clients. Toutes les informations personnelles, y compris leur identité, leur adresse, leur numéro de téléphone, ont été divulguées. Les utilisateurs ont encore le moyen de se protéger.

jeudi soir  
r Google,  
rnet.

d'accéder  
équent, à  
s que leur  
éparer ou



**SOURCE :** <https://www.clubic.com/pro/entreprises/nintendo/actualite-843750-nintendo-fuite-information-hack-site-sav-ferme-portes.html>



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Principe de sécurité de développement

Conséquence : Défaçage de site

Janvier 2015



Hacked By Mr  
Mrmounir

Je ne suis pas Char  
suis musul

Ce que fais ch

Ca s'appelle le

S

Un peut de respect pour les autres reeligions.

n Kingdom

قوا

suis musulman et fier de l'être.

é d'expression...

lectuel.

autres religions.





# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Principe de sécurité de développement

ShellCode utilisé en janvier 2015 par DAESH



Le fichier était encodé en 64 bits dans un fichier nommé pat.php

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Principe de sécurité de développement

Modus operandi en janvier 2015 par DAESH

### SQL Injection.

User-Id :

Password :

```
select * from Users where user_id= 'srinivas '  
and password = 'mypassword '
```

User-Id :

Password :

```
select * from Users where user_id= '' OR 1 = 1; /* '  
and password = '*/-- '
```

9lessons.blogspot.com

### Après une analyse informatique de la base de données

Confirmation d'une intrusion  
dans la base de données liée au  
site Web et découverte 9  
comptes administrateurs créés  
depuis septembre 2014 à janvier  
2015 avec un accès à  
l'ensemble des ressources de la  
BDD,

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le darknet

Le Web



Le Deep Web

Le Darkweb

D'après les estimations la société de cybersécurité Trend Micro, la sphère cybercriminelle française se compose de **40.000 escrocs qui réalisent un chiffre d'affaires compris entre 5 et 10 millions d'euros par mois.**

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le darknet

### L'économie souterraine de la cybercriminalité française

Prix de vente de produits illégaux sur le darknet français



@Statista\_FR

Source : Trend Micro

LA TRIBUNE statista



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le darknet

Home Your Account Your Purchases Forum

Categories

- Drugs (5625)
- Services (1337)
- Data (313)
- Weapons (252)
- Collectables (14)
- Metals/Stones (16)
- Other (374)
- Software (152)
- Movies (12)
- Tobacco (235)
- Counterfeits (336)
- Alcohol (14)
- eBooks (2313)
- Weight Loss (91)

Weapons > Firearms

A Walther P22 - Excellent condition Full Escrow

Price: 9.84107 BTC  
\$ 2,000.00 £ 1,245.72 € 1,455.60

Ship from: Direct Supplier  
Ship to: EU, N. America, S. America, Asia  
Stock: 1  
Created in: 2013-09-20 15:27 UTC  
Last update: 2013-10-05 08:25 UTC  
Listing feedback: 0/0/0

Quantity: 1 Buy

Arms Depot: Class III - Sub Machine Guns:

ASSAULT RIFLES IN STOCK

HK MPS 9MM  
Total Price: \$4995.00USD  
P.P.P. Price: \$5322.12USD  
Initial Price Difference of: \$3673.83USD (41%)

Christmas Special - ONLY \$7500!  
Get a fucking submachine gun for Christmas!

HK MPS WITH SUPPRESSOR  
Total Price: \$12995.00USD  
P.P.P. Price: \$10257.70USD  
Initial Price Difference of: \$7738.20USD (43%)

ACTION	SEMI/BURST/AUTO
CALIBER	9MM
BARREL	10-1/4"
CAPACITY	30+1

Silk Road anonymous market

messages 1 orders 0 account \$0.00

Search

Shop by Category

- Drugs: 4,093
  - Cannabis 999
  - Dissociatives 78
  - Ecstasy 314
  - Opioids 354
  - Other 153
  - Precursors 18
  - Prescription 803
  - Psychedelics 586
  - Stimulants 390
- Apparel 82
- Art 5
- Books 788
- Collectibles 15
- Computer equipment 42
- Custom Orders 27
- Digital goods 309
- Drug paraphernalia 153
- Electronics 35
- Erotica 296
- Fireworks 8
- Food 4
- Forgeries 55
- Hardware 7
- Herbs & Supplements 11
- Home & Garden 8
- Jewelry 87

5G Cocaine Pure Catal Flakes \$41.94

28.0G High Quality Crystal Meth \$188.72

SPECIAL OFFER \* BRAND SUBOXONE \$0.91

alprazolam [Xanax] 100 x 1mg \$11.31

Cocaine of high quality over 80% purity 25 gram \$190.12

"Ethphenidate" -2.5g- of the best racemic HCl salt \$6.16

Colombian Cocaine Lady's and Gentleman 10G \$67.32

0.5g #3 Brown Heroin - good quality! \$7.52

## How To Connect To A Darknet

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le darknet

### SOLUTIONS POUR LES PLUS EXPERTS

RAT : outil de prise  
de contrôle de la  
machine

300 \$

Stealer : programme  
de vol d'information

150 \$

Crypter : outil de  
chiffrement automatique  
des données de  
l'ordinateur

150 \$

Bot : programme  
de gestion de la  
machine

5000 \$

G DATA | SIMPLY SECURE | PARIS | 2015 |

### SERVICES POUR LES MOINS TECHNIQUES

Installation de programmes  
malveillants sur 1000  
machines

70 \$

DDoS : attaque de  
serveurs Internet  
à l'heure

100 \$

Camouflage clé en main  
du code pour éviter les  
Antivirus

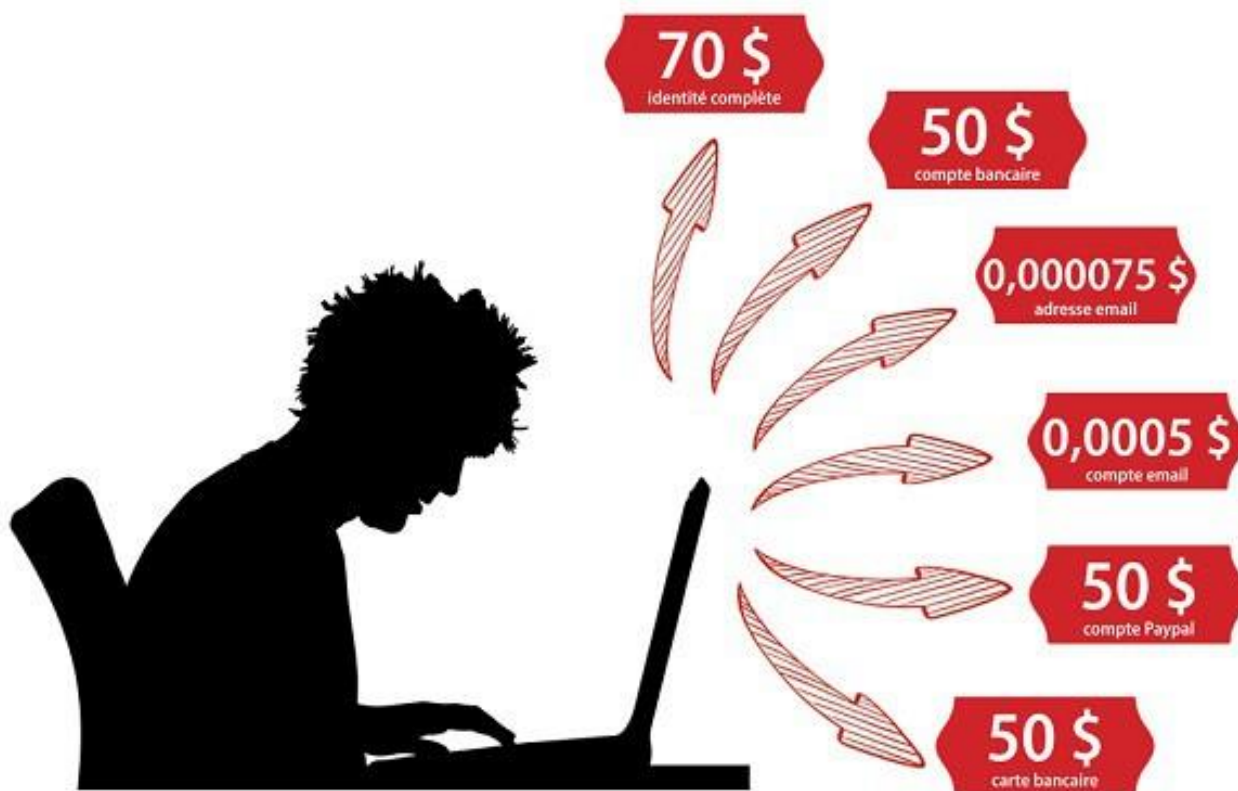
10 \$

G DATA | SIMPLY SECURE | PARIS | 2015 |

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Le darknet

### LE PRIX DE LA VIE PRIVÉE SUR LE BLACKMARKET



Source : GDATA Software

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Les cyber attaques dans le spatial sont elles envisageables ?



## Thousands of High-Risk Vulnerabilities Found in NOAA Satellite System

September 10, 2014 Swati Khandelwal

The informational systems that the National Oceanic and Atmospheric Administration (NOAA) run are loaded with several critical vulnerab...



## Satellite Communication (SATCOM) Devices Vulnerable to Hackers

April 18, 2014 Swati Khandelwal

The growing threat of cyber-attacks and network hacking has reached the satellite-space sector, posing a growing challenge to the satel...



## Russian Hackers Hijack Satellite To Steal Data from Thousands of Hacked Computers

September 10, 2015 Swati Khandelwal

A group of Russian hackers, most notably the Turla APT (Advanced Persistent Threat) is hijacking commercial satellites to hide command...

**Les satellites ont différents gradients de protection face aux cybermenaces**

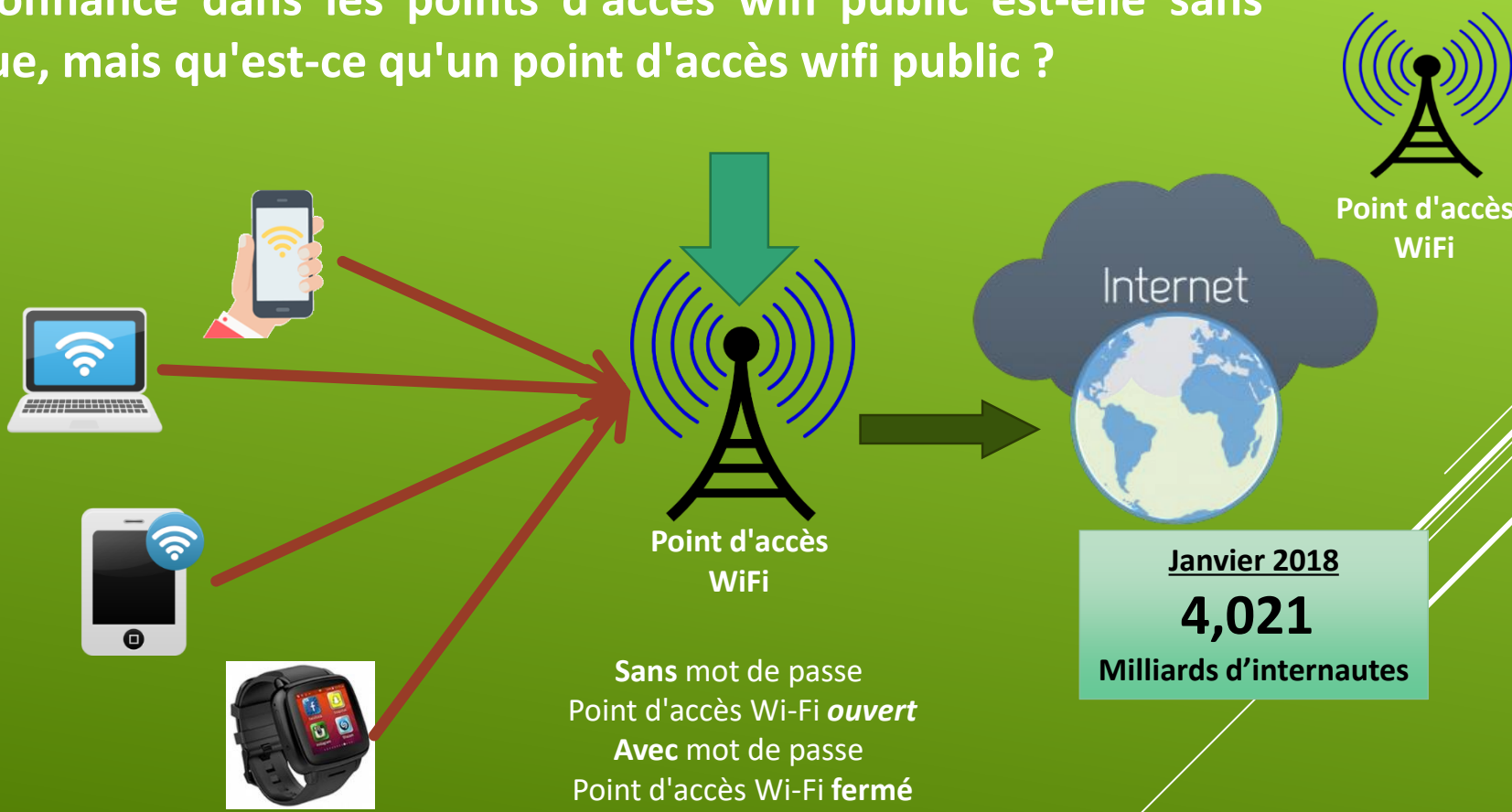
**Le satellite n'est plus réservé au gouvernement**

**Micro satellite de service Tracteur, drone**



## Les réseaux sans fil

La confiance dans les points d'accès wifi public est-elle sans risque, mais qu'est-ce qu'un point d'accès wifi public ?



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les réseaux sans fil



Point d'accès  
WiFi



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

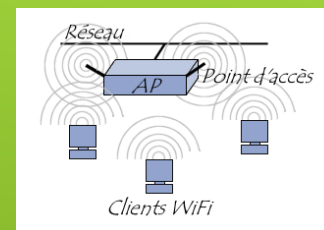
## Les réseaux sans fil



Point d'accès  
WiFi public fermé



Attaque de l'homme du milieu

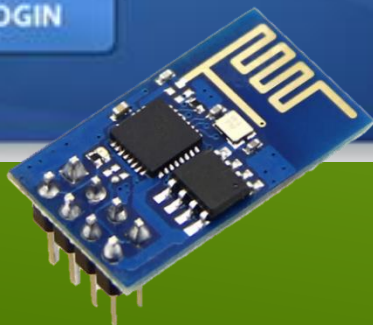


Scanner l'architecture  
du réseau



Scanner les ports  
des machines sur le réseau  
et découvrir les services.

# Le portail captif

[illegible]

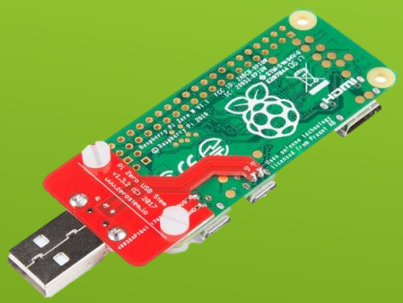
**Capture de données no : 12.**



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les réseaux sans fil

Capture des  
identifiants  
WiFi



<http://172.24.0.1:8000/#/hid>

```
C:\Users\>netsh wlan show profiles

Profils sur l'interface Wi-Fi 3 :

Profils de stratégies de groupe (lecture seule)
-----
<Aucun>

Profils utilisateurs
-----
Profil Tous les utilisateurs : TP-LINK_B15362
```

<https://github.com/mame82/P4wnP1>

```
C:\Users\>netsh wlan show profile name=TP-LINK_B15362 key=clear

Profil TP-LINK_B15362 sur l'interface Wi-Fi 3 :
-----

Appliqué : Profil Tous les utilisateurs

Informations sur le profil
-----
Version : 1
Type : Réseau local sans fil
Nom : TP-LINK_B15362
Options de contrôle :
  Mode de connexion : connexion manuelle
  Diffusion réseau : Connecter uniquement si ce réseau diffuse
  Commutation auto : ne pas basculer vers d'autres réseaux
  Randomisation MAC : Désactivée

Paramètres de connectivité
-----
Nombre de SSID : 1
Nom du SSID : "TP-LINK_B15362"
Type de réseau : Infrastructure
Type de radio : [ Tous les types de radio ]
Extension du fournisseur : absente

Paramètres de sécurité
-----
Authentification : WPA2 - Personnel
Chiffrement : CCMP
Authentification : WPA2 - Personnel
Chiffrement : GCMP
Clé de sécurité : Présent
Contenu de la clé : XXXXXXXXXX ← Password

Paramètres du coût
-----
Coût : sans restriction
Encombrement : Non
Limite de données presque atteinte : Non
Limite de données dépassée : Non
Itinérance : Non
Source de coût : Par défaut

C:\Users\bbword>
```

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les Smartphones

### La réalité des faits

**Plus de 300 applications  
malveillantes se cachent sur le  
Google Play Store (2017)**



**Malware Judy : le Google Play  
Store en danger, 36,5 millions  
d'appareils infectés (29/05/2017)**

27 août 2016



#### SOURCES :

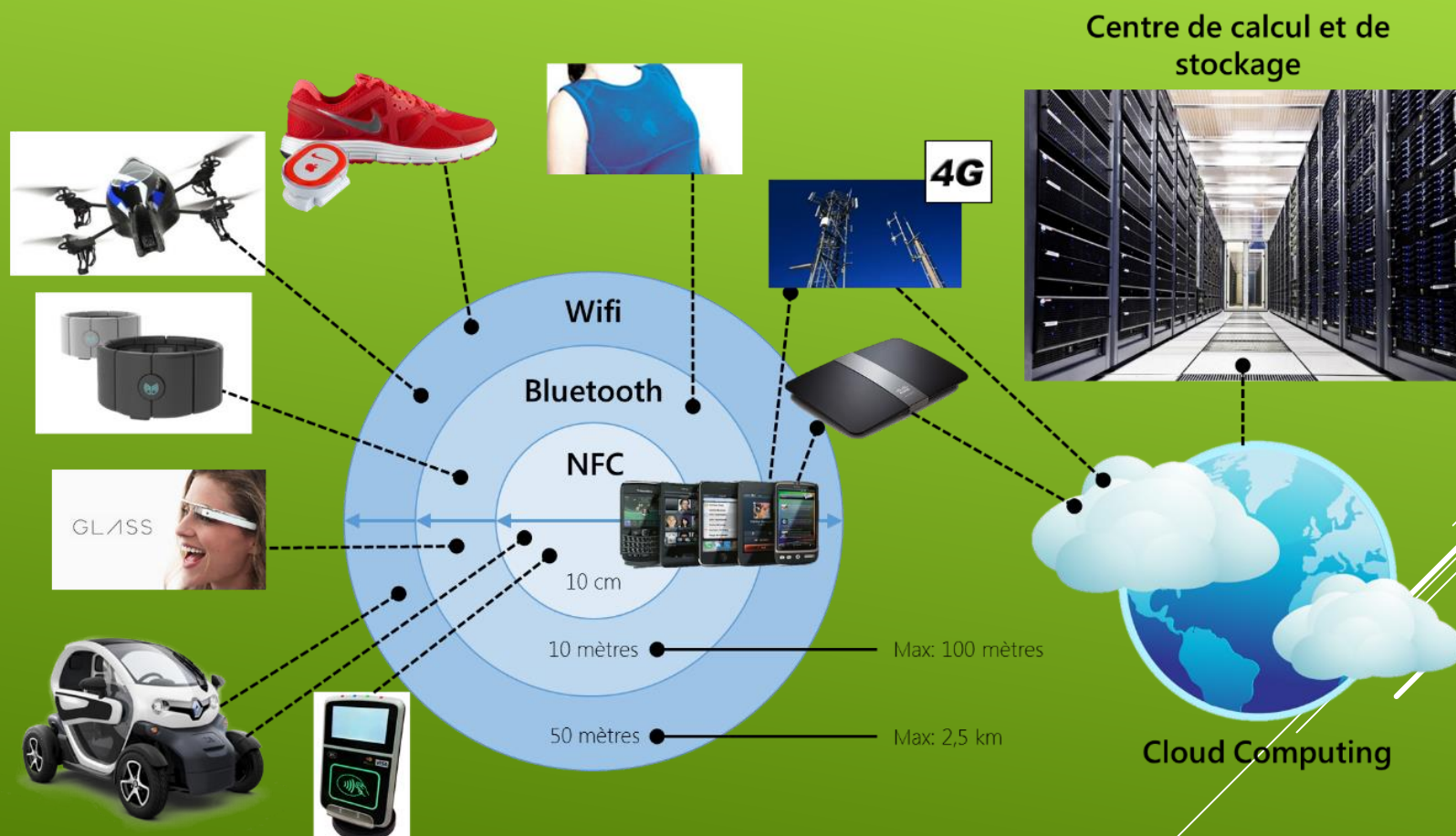
<http://www.phonandroid.com/play-store-300-malveillantes-dapplications-frauduleuses.html>

<http://www.phonandroid.com/malware-judy-google-play-store-en-danger-365-millions-appareils-infectes.html>

<https://www.undernews.fr/malwares-virus-antivirus/pegasus-le-malware-qui-a-mis-a-mal-apple.html>

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

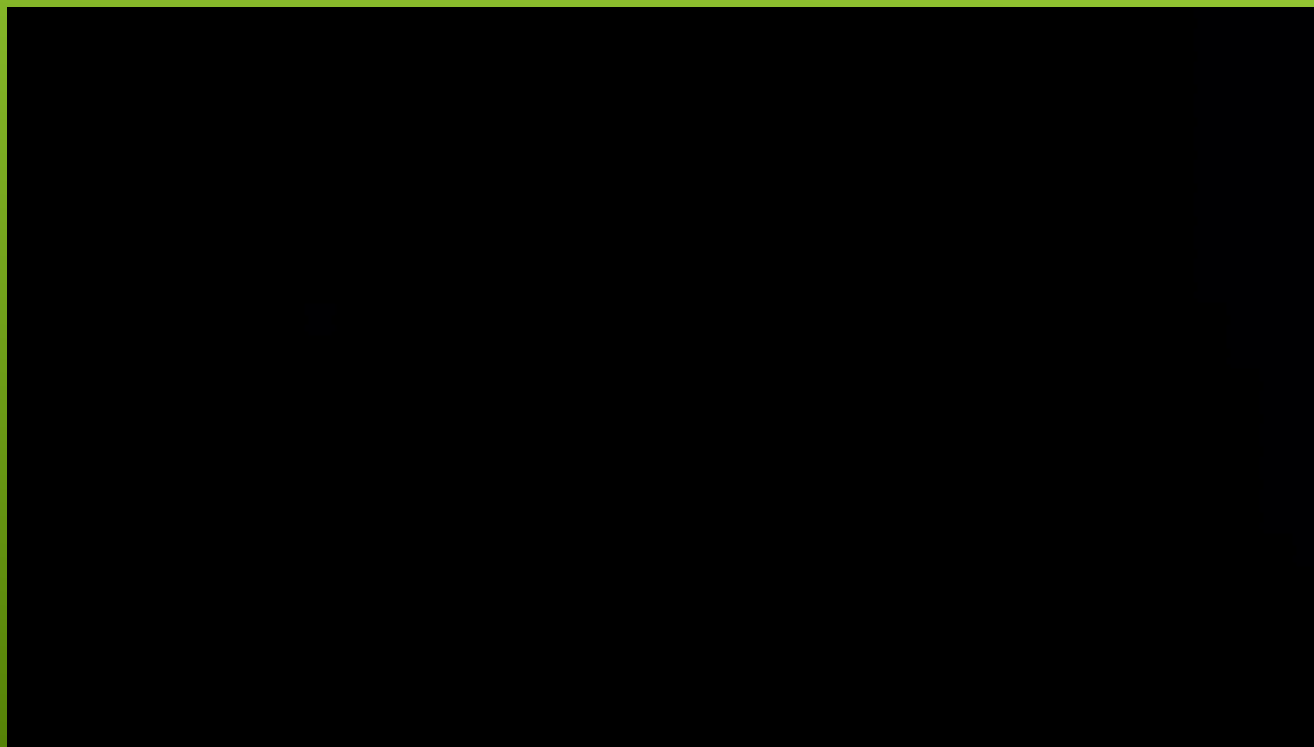




# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## *L'Internet des objets*

**Forum International de la Cybersécurité (FIC 2015)**



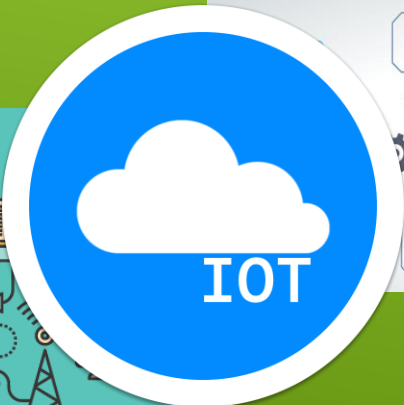


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

*Les cibles ?*

### SMART CITY

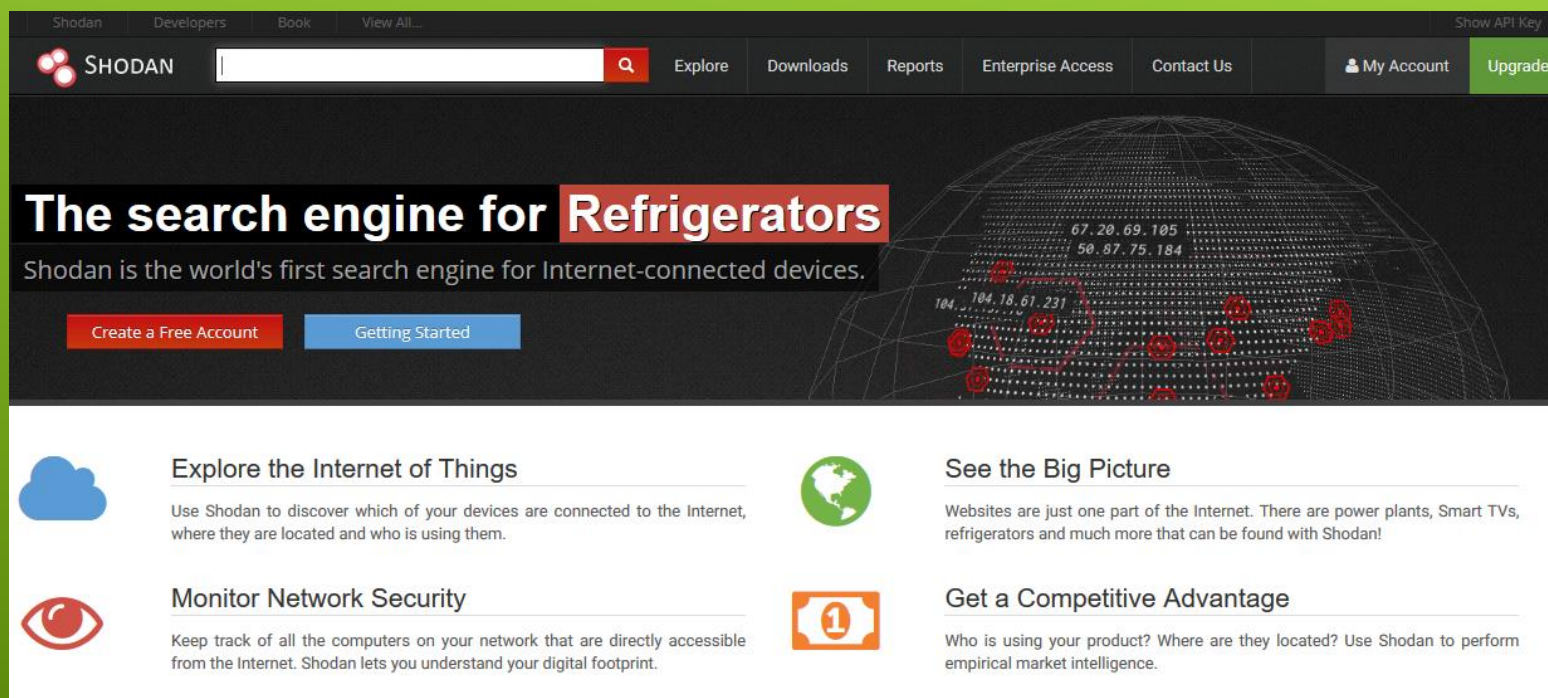


### L'USINE 4.0

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

Shodan répertorie à peu près tout ce qui est relié à Internet



The screenshot shows the Shodan website interface. At the top, there's a navigation bar with links: Shodan, Developers, Book, View All..., and a 'Show API Key' link on the right. Below this is a search bar with the Shodan logo and a search button. To the right of the search bar are links: Explore, Downloads, Reports, Enterprise Access, Contact Us, My Account, and an Upgrade button. The main content area features a large banner with the text 'The search engine for Refrigerators' and 'Shodan is the world's first search engine for Internet-connected devices.' Below the banner are two buttons: 'Create a Free Account' and 'Getting Started'. The background of the banner shows a globe with various IP addresses and red circular markers. Below the banner, there are four sections with icons and text:

- Explore the Internet of Things**: Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them. (Icon: Cloud)
- Monitor Network Security**: Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint. (Icon: Eye)
- See the Big Picture**: Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan! (Icon: Globe)
- Get a Competitive Advantage**: Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence. (Icon: Coin with '1')

Caméras Web, installations de traitement de l'eau, yachts, appareils médicaux, feux de circulation, éoliennes, lecteurs de plaques d'immatriculation, téléviseurs intelligents, réfrigérateurs.

## L'Internet des objets

Shodan répertorie à peu près tout ce  
qui est relié à Internet

### Démonstration MQTT

Caméras Web, installations de  
traitement de l'eau, yachts, appareils  
médicaux, feux de circulation,  
éoliennes, lecteurs de plaques  
d'immatriculation, téléviseurs  
intelligents, réfrigérateurs.



Faire de Shodan un outil défensif



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

Shodan répertorie à peu près tout ce  
qui est relié à Internet


Shodan Developers Book View All...

SHODAN mqtt country:"FR" city:"Toulouse" Explore Downloads Reports Developer Pricing Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS  
17

TOP COUNTRIES



France 17

TOP CITIES

Toulouse 17

TOP ORGANIZATIONS

Orange	8
Tetaneutral.net	3
SFR	3
Free SAS	2
Bouygues Telecom	1

TOP PRODUCTS

Mosquitto	12
MQTT	5

**90.5.184.225**  
AToulouse-054-1-281-225.v90-5.abo.wanadoo.fr  
Orange  
Added on 2018-07-10 18:18:51 GMT  
France, Toulouse  
Details

MQTT Connection Code: 0

Topics:  
\$SYS/broker/version  
\$SYS/broker/timestamp  
\$SYS/broker/uptime  
\$SYS/broker/clients/total  
\$SYS/broker/clients/inactive  
\$SYS/broker/clients/disconnected  
\$SYS/broker/clients/active  
\$SYS/broker/clients/connected  
\$SYS/broker/clients/expired  
\$SYS/broker/messages/stored  
\$SYS...

**92.95.150.124**  
124.150.95.92.rev.sfr.net  
SFR  
Added on 2018-07-09 21:17:51 GMT  
France, Toulouse  
Details

MQTT Connection Code: 0

Topics:  
\$SYS/broker/version  
\$SYS/broker/timestamp  
\$SYS/broker/uptime  
\$SYS/broker/clients/total  
\$SYS/broker/clients/maximum  
\$SYS/broker/clients/inactive  
\$SYS/broker/clients/disconnected  
\$SYS/broker/clients/active  
\$SYS/broker/clients/connected  
\$SYS/broker/clients/expired  
\$SYS...

1883 tcp mqtt

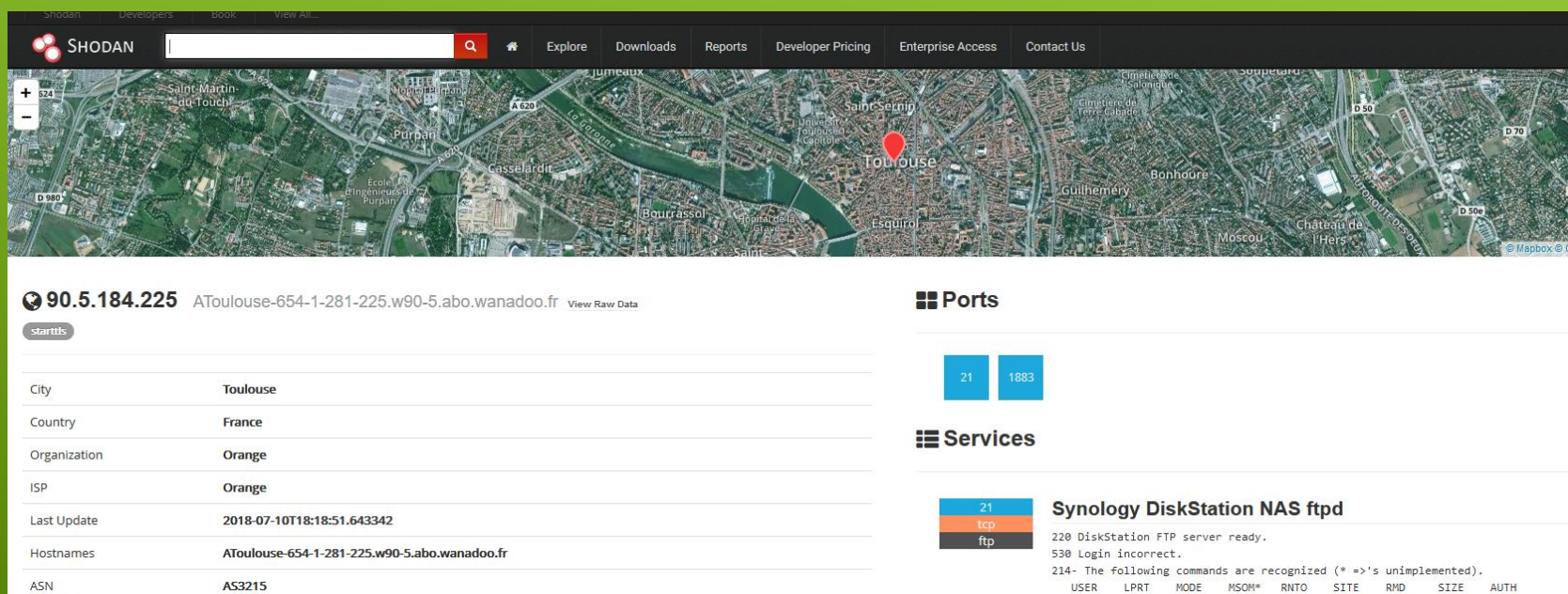
**Mosquitto** Version: 1.4.14

MQTT Connection Code: 0

Topics:  
\$SYS/broker/version  
\$SYS/broker/timestamp  
\$SYS/broker/uptime  
\$SYS/broker/clients/total  
\$SYS/broker/clients/inactive  
\$SYS/broker/clients/disconnected  
\$SYS/broker/clients/active  
\$SYS/broker/clients/connected  
\$SYS/broker/clients/expired  
\$SYS/broker/messages/stored  
\$SYS/broker/messages/received  
\$SYS/broker/messages/sent  
\$SYS/broker/subscriptions/count  
\$SYS/broker/retained messages/count  
\$SYS/broker/heap/current  
\$SYS/broker/heap/maximum  
\$SYS/broker/publish/messages/dropped  
\$SYS/broker/publish/messages/received  
\$SYS/broker/publish/messages/sent  
\$SYS/broker/publish/bytes/received  
\$SYS/broker/publish/bytes/sent  
\$SYS/broker/bytes/received  
\$SYS/broker/bytes/sent

## L'Internet des objets

Shodan répertorie à peu près tout ce qui est relié à Internet



The screenshot shows the Shodan search engine interface. At the top, there's a navigation bar with links like 'Shodan', 'Developers', 'Book', and 'View All...'. Below this is a search bar with the IP '90.5.184.225' entered. The main content area displays a satellite map of Toulouse, France, with a red pin indicating the location. Below the map, there's a table of metadata for the IP address.

Field	Value
City	Toulouse
Country	France
Organization	Orange
ISP	Orange
Last Update	2018-07-10T18:18:51.643342
Hostnames	AToulouse-654-1-281-225.w90-5.abo.wanadoo.fr
ASN	AS3215

On the right side of the interface, there's a 'Ports' section showing open ports 21 and 1883. Below that, a 'Services' section lists the detected services: Synology DiskStation NAS ftpd. The output of the 'nmap' scan is visible, showing the FTP service is running on port 21.

```

21
tcp
ftp

220 DiskStation FTP server ready.
530 Login incorrect.
214- The following commands are recognized (* =>'s unimplemented).
USER  LPRT  MODE  MSON*  RNTO  SITE  RMD  SIZE  AUTH
  
```

# Cybersécurité, cerner les menaces et se protéger


## L'Internet des objets

Shodan répertorie à peu près tout ce qui est relié à Internet

**TOTAL RESULTS**

**19**

**TOP COUNTRIES**



Korea, Republic of	6
Turkey	3
Japan	3
Singapore	2
Taiwan	1

**TOP SERVICES**

HTTP	7
27015	3
8081	2
SMTP	2
Automated Tank Gauge	1

**TOP ORGANIZATIONS**

GABIA	5
Netinternet Bilisim Teknolojileri AS	2
Gmo Cloud K.k.	2
DigitalOcean	2
Zipitel IT Solutions Pvt	1

**TOP OPERATING SYSTEMS**

QTS	1
-----	---

**TOP PRODUCTS**

nginx	2
Sendmail	2
Counter-Strike	2
Samba	1
Postfix smtpd	1

**153.122.132.244**

polestar-hk.com  
Gmo Cloud K.k.  
Added on 2018-07-10 12:18:58 GMT  
● Japan, Tokyo  
[Details](#)

554 polestar-hk.com ESMTP not accepting messages  
250-polestar-hk.com Hello 69.235.85.211 [69.235.85.211], pleased to meet you  
250 ENHANCEDSTATUSCODES

**128.199.226.122**

DigitalOcean  
Added on 2018-07-10 01:24:19 GMT  
■ Singapore, Singapore  
[Details](#)

HTTP/1.1 200 OK  
Server: nginx/1.4.6 (Ubuntu)  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
X-Powered-By: PHP/5.5.9-1ubuntu4.25  
Cache-Control: no-cache  
Date: Tue, 10 Jul 2018 01:24:01 GMT  
Set-Cookie: XSRF-TOKEN=eyJpdii61kRuvThBTXRPbkxIaElGwJR53kx...

**153.122.132.244**

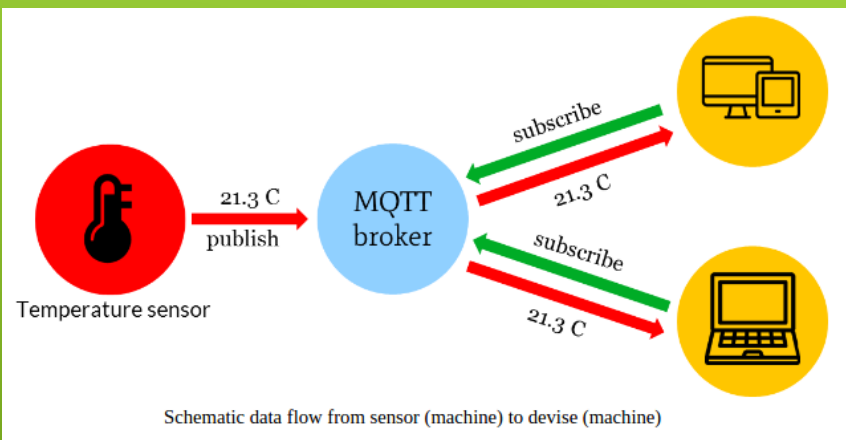
polestar-hk.com  
Gmo Cloud K.k.  
Added on 2018-07-08 23:48:37 GMT  
● Japan, Tokyo  
[Details](#)

220 polestar-hk.com ESMTP Sendmail 8.14.5/8.14.5; Mon, 9 Jul 2018 08:48:32 +0900  
250-polestar-hk.com Hello 90.235.172.42 [90.235.172.42], pleased to meet you  
250-ENHANCEDSTATUSCODES  
250-PIPELINING  
250-8BITMIME  
250-SIZE  
250-DSN  
250-ETRN  
250-AUTH PLAIN LOGIN  
250-DELIVERBY  
250 HELP

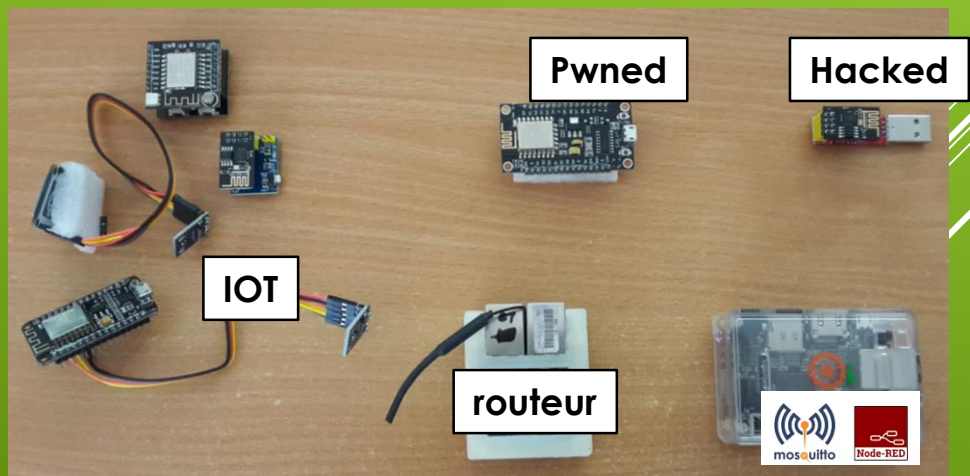
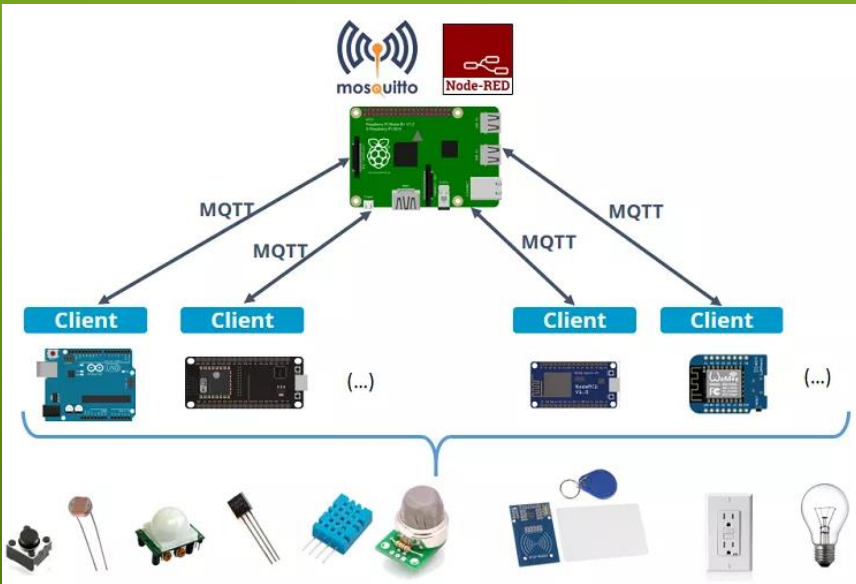
**POLESTAR Cloud**

121.78.87.218  
GABIA  
Added on 2018-07-08 07:35:36 GMT  
🇰🇷 Korea, Republic of  
Technologies: [swf](#) [Dw](#)  
[Details](#)

HTTP/1.1 200 OK  
Set-Cookie: JSESSIONID=EF5970FB2EC0F1967EABFF40DFECB61B; Path=/  
Content-Type: text/html; charset=UTF-8  
Content-Language: ja  
Content-Length: 7533  
Date: Sun, 08 Jul 2018 07:35:36 GMT  
Server: Polestar XEUS



**MQTT** (Message Queuing Telemetry Transport) est un protocole de **messaging publish-subscribe** basé sur le protocole TCP/IP. Il a été initialement développé par Andy Stanford-Clark (IBM) et Arlen Nipper (EuroTech).



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

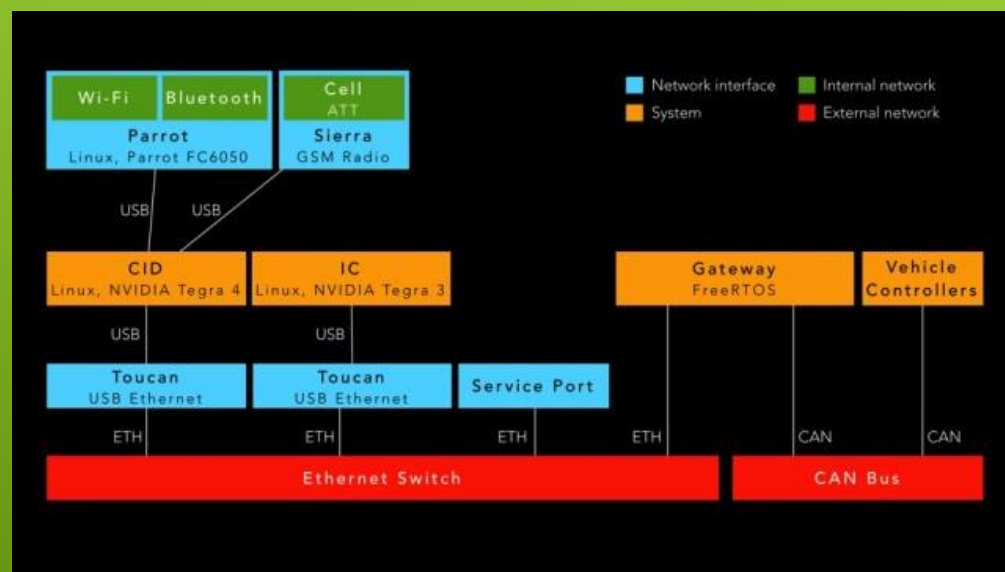
**Sécurité : des hackers testent le contrôle à distance d'une Jeep**  
(22 juillet 2015, 16:56)



Pour démontrer la faiblesse de la sécurité des voitures connectées, deux hackers ont démontré la prise de contrôle d'une Jeep à distance allant des essuie-glaces aux freins.

**DEF CON 23: comment des hackers ont piraté la Tesla Model S**

(08/08/2015 à 08h55 Mis à jour le 10/08/2015 à 10h44)



**A grande échelle cela donnerait quoi ?**

## L'Internet des objets

17/01/2014

Une société de sécurité informatique a mis à jour le premier réseau d'objets connectés à l'Internet, utilisé par des pirates informatiques pour diffuser des centaines de milliers de spams.



## L'Internet des objets

14/11/2016

Ransomware qui s'exécute sur un thermostat connecté ? Un scénario plausible qui a été démontré lors de la dernière conférence DEF CON par PenTest Partners.



## A-t-on réellement changé les choses ?

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

### telnet login

login: vstarcam2015  
passwd: 20150602

[Feb.17] Strange behaviour

### hexedit tveth

```
/root/home/mirai/bot/attack_udp.c
/root/home/mirai/bot/attack_tcp.c
.....
```



**Two way audio**

Choose Listen/Talk over smartphone APP, start to communicate with your families. Communicate at anytime anywhere.



PORT	STATE	SERVICE	VERSION
23/tcp	open	telnet	BusyBox telnetd
81/tcp	open	http	GoAhead WebServer

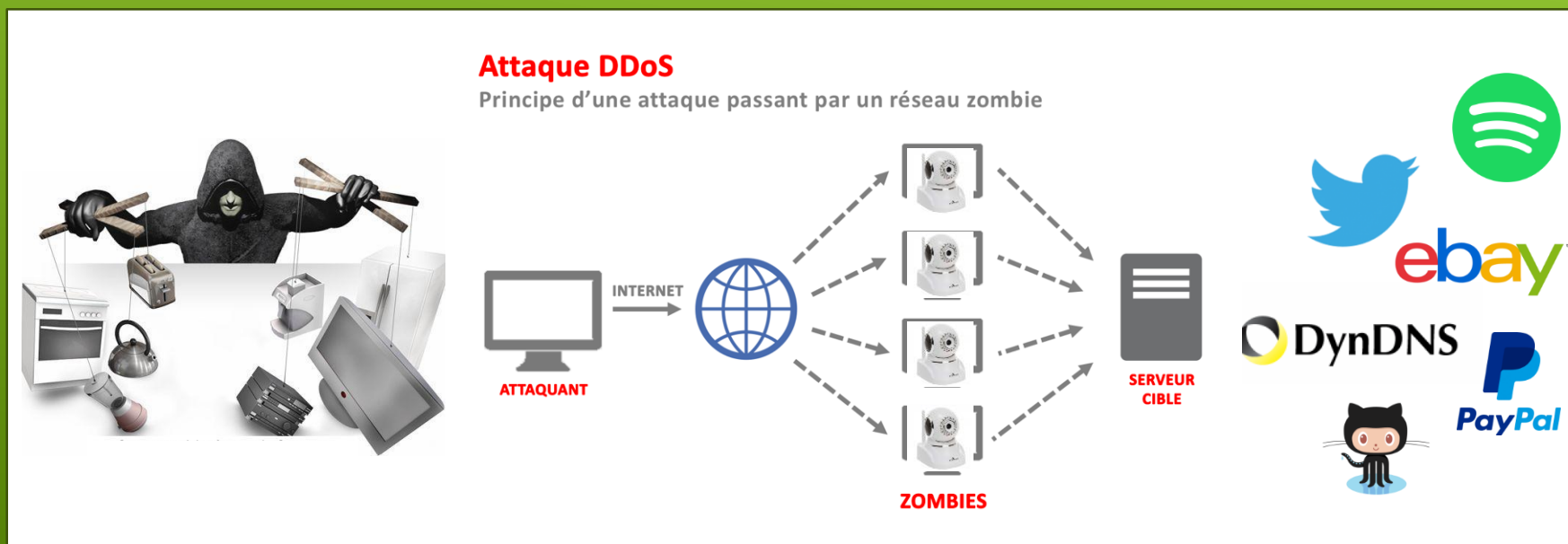
### Telnet login

Login : root  
Passwd : 123456

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets

**ATTAQUE DDOS, le 21 octobre 2016** qui a vu apparition d'un botnet au nom de « **Mirai** » composé d'objets connectés (145.000 caméras) visant le service Dyn Managed DNS qui utilisent ce service (différent de DynDNS), tels que **Twitter, Ebay, Netflix, GitHub, PayPal, Spotify.**

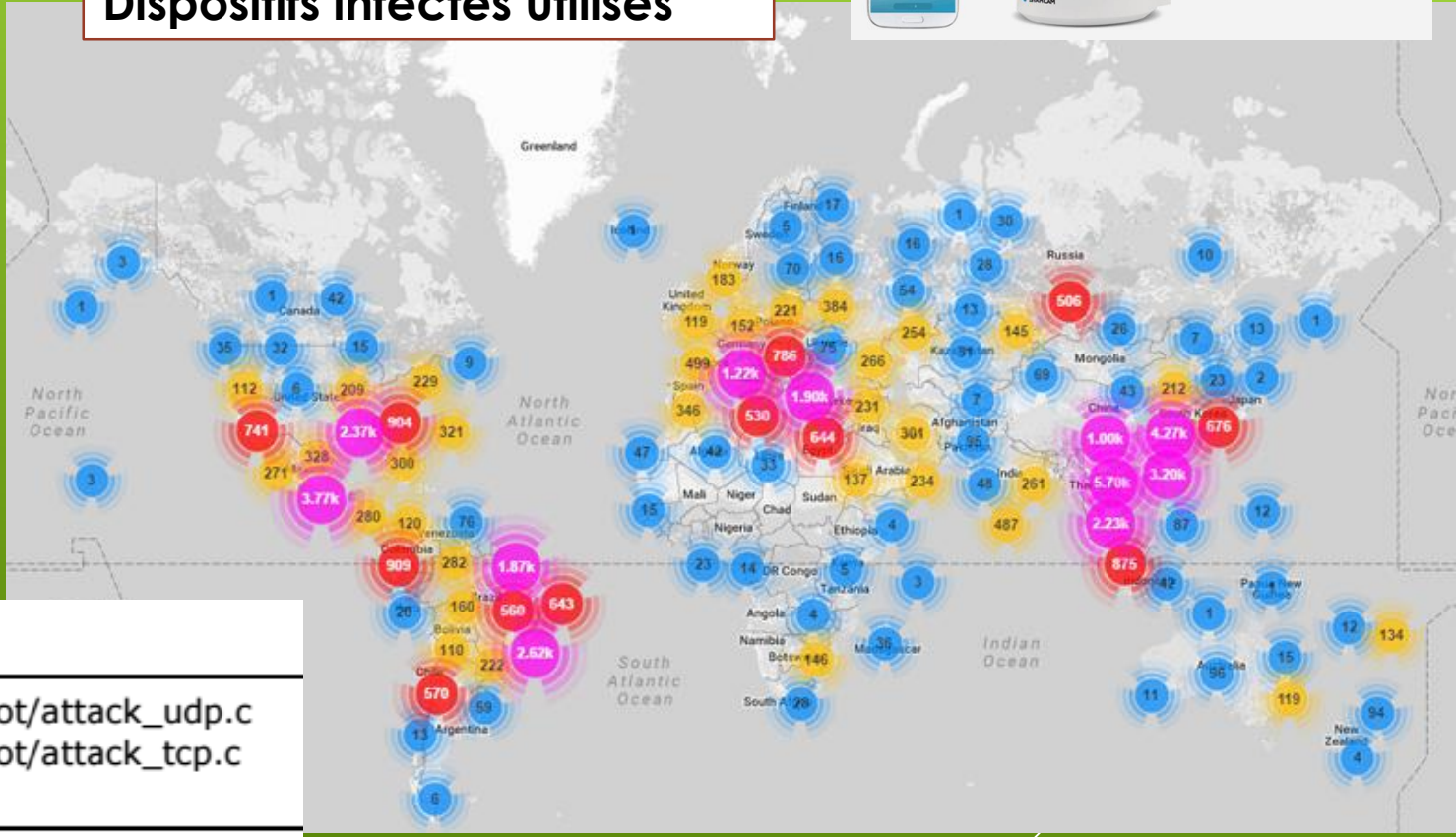


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'Internet des objets



### Dispositifs infectés utilisés



**1 Two way audio**  
Choose Listen/Talk over smartphone APP, start to communicate with your families. Communicate at anytime anywhere.

hexedit tveth

```
/root/home/mirai/bot/attack_udp.c  
/root/home/mirai/bot/attack_tcp.c  
*****
```

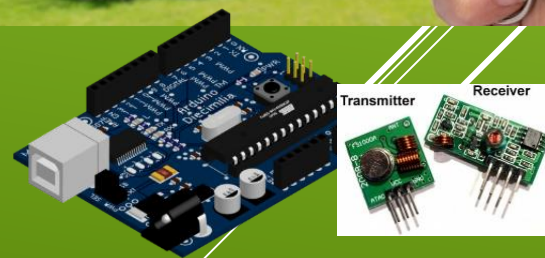
# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Attaque de protocole de transmission RF

### Le cambriolage à l'ancienne



### La transformation numérique du cambriolage



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

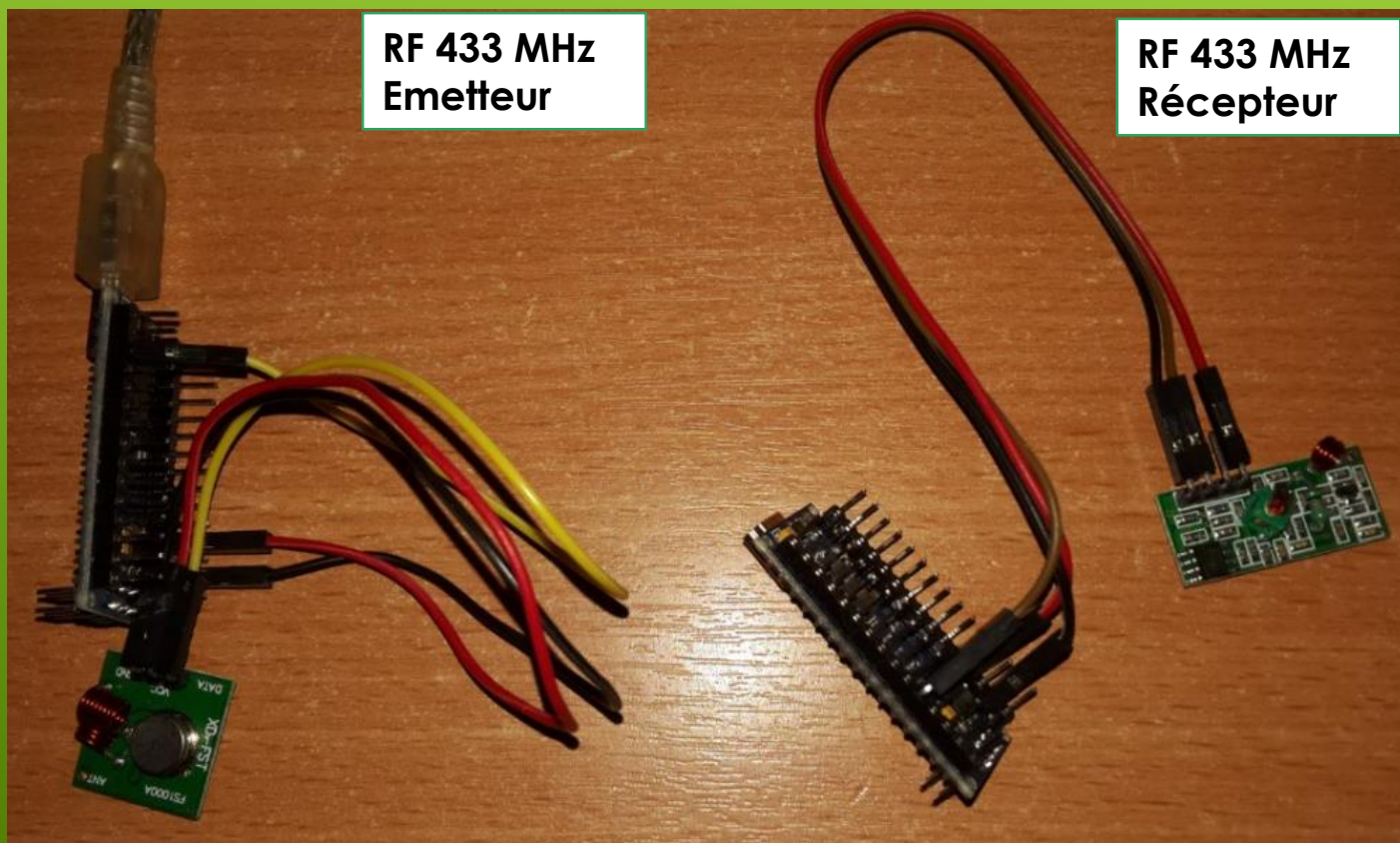
## Attaque de protocole de transmission RF

### La domotique



## Attaque de protocole de transmission RF

### La domotique

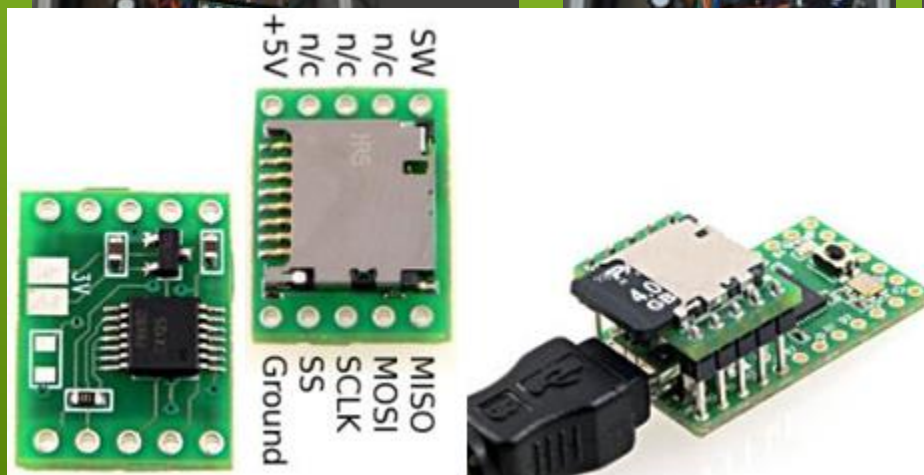


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Des cadeaux empoisonnés

Keylogger – une souris malicieuse

D.I.Y



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Des cadeaux empoisonnés

Keylogger – Un chargeur USB déguisé

D.I.Y

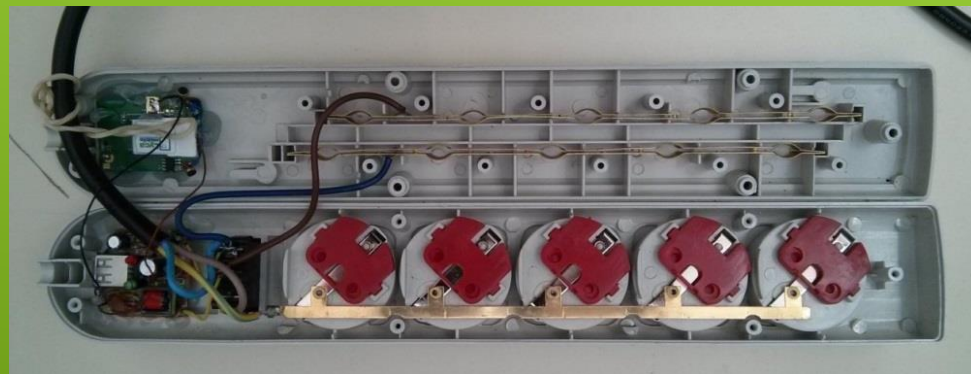
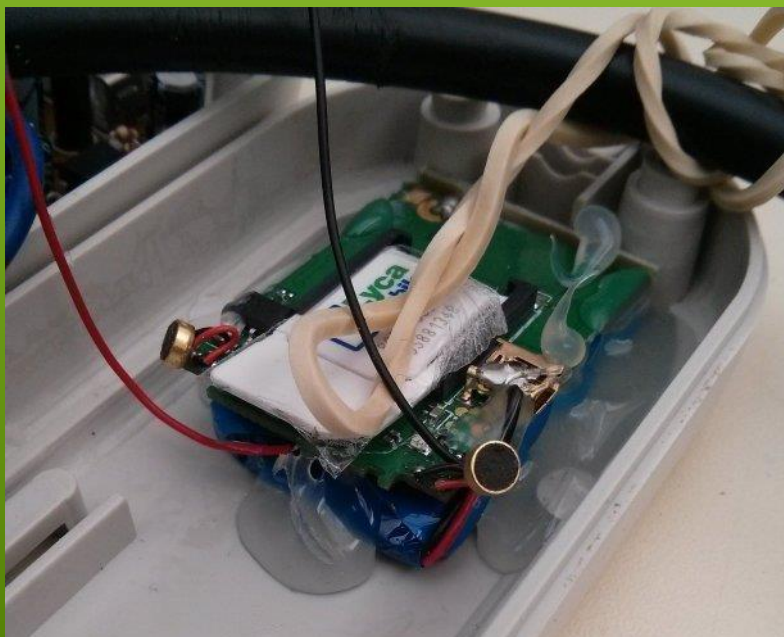


Image courtesy: <http://samy.pl/keysweeper>

## Des cadeaux empoisonnés

L'espionnage en vente libre

D.I.Y



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Des cadeaux empoisonnés

### USB Rubber Ducky



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Compromission d'un poste utilisateur

Teensy



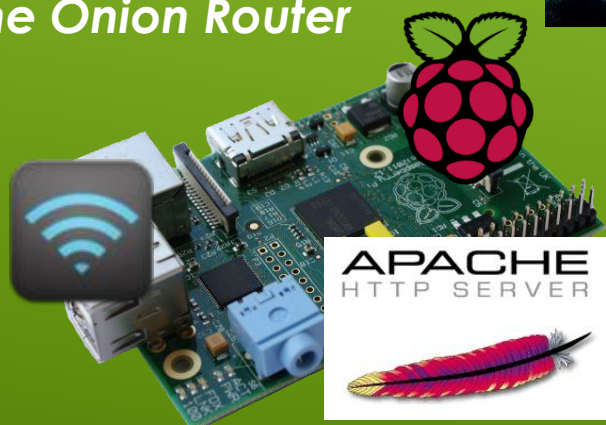


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Usage dérivé

### Escroquerie et anonymisation à l'aide d'un Raspberry Pi

Anonymisation  
des traces



Serveur anonyme  
d'outils  
Achats et ventes

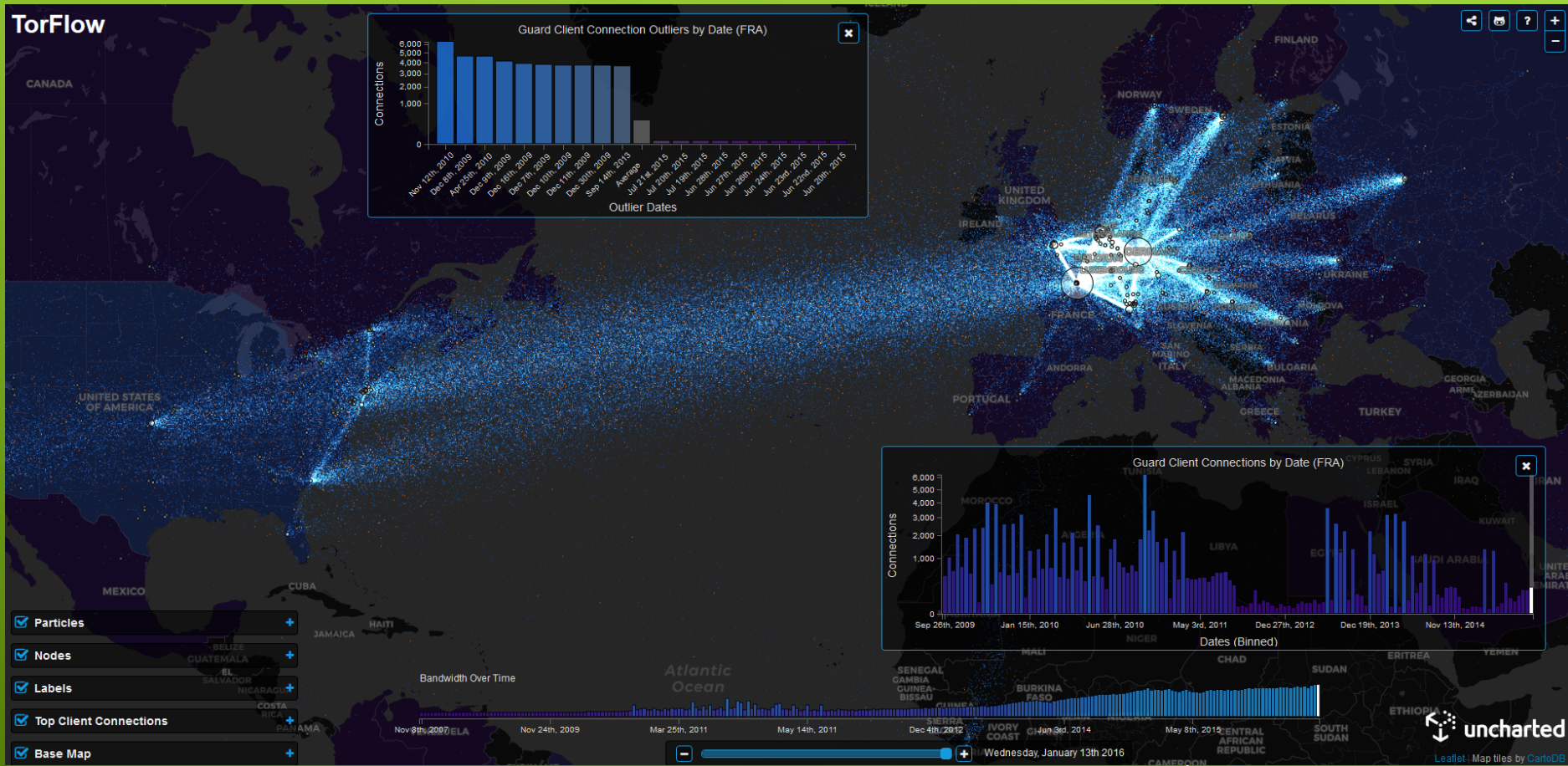




# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## TorFlow –

Visualisez en temps réel le trafic du réseau TOR

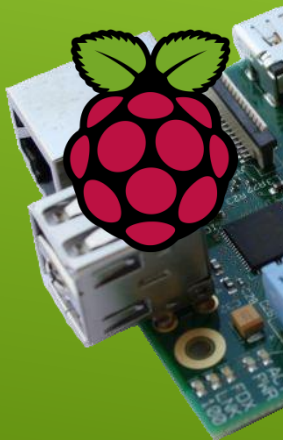


SOURCE : <https://torflow.uncharted.software/#/2016-1-13?C=fr,FRA&ML=-28.652343749999996,40.91351257612758,4>  
<https://metrics.torproject.org/>

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Usage dérivé

L'anonymat à l'aide d'un Raspberry Pi



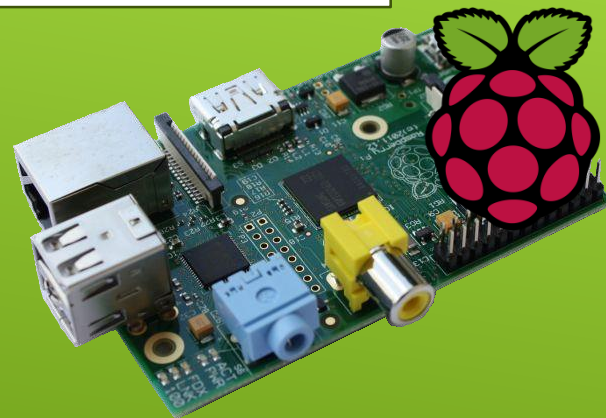
on Router

fi avec  
léatoire  
esse IP

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Usage dérivé

### Piratage à l'aide d'un Raspberry Pi



Mai 2016

### Attaque SQLMap

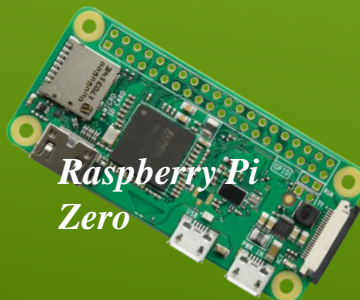
- 2 Sociétés
- 2 Associations
- 1 Comité d'entreprise
- 2 Collectivités territoriales



### Espionnage

Juillet 2016

Découverte dans une armoire de brassage d'un équipement de surveillance de réseau



## Un oubli de conception

Une serrure connectée à 160€ déverrouillée en... 4 secondes !



## Et l'intelligence artificielle ?

**Oups ! Une enceinte Echo d'Amazon enregistre une conversation privée et la diffuse**

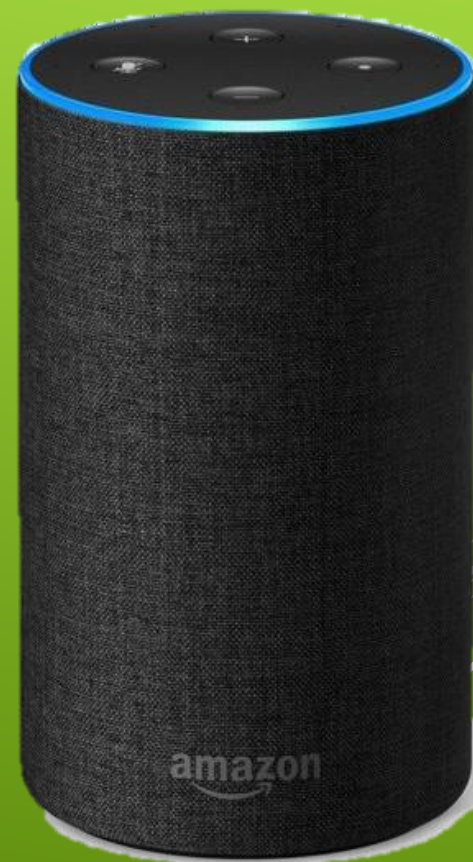
Aux États-Unis, une enceinte connectée Echo d'Amazon a accidentellement enregistré la conversation privée d'un couple à son domicile puis l'a envoyée à l'une de leurs connaissances.



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

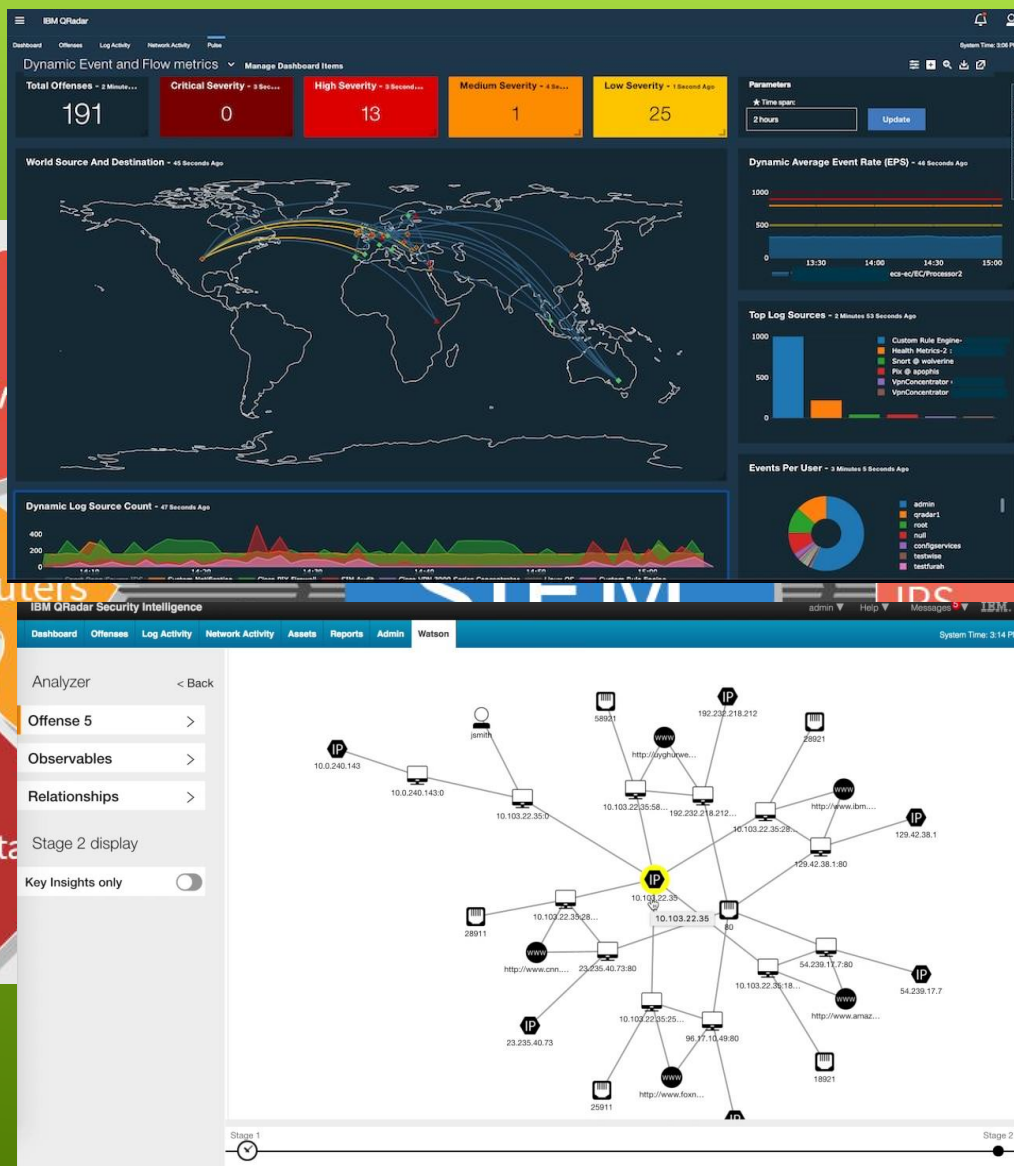
## Et l'intelligence artificielle ?

**Le géant du commerce électronique a fini par livrer des explications officielles sur ce qui s'est passé.** Apparemment, l'assistant Alexa de l'enceinte Echo s'est activé en croyant avoir entendu le mot clé comportant son nom dans la conversation qu'avait le couple. Puis, le logiciel aurait interprété la commande « Envoyer un message » de ce qu'il entendait des échanges verbaux et donc enclenché l'enregistrement audio. Continuant sur cette improbable lancée, Alexa a ensuite demandé « À qui ? » elle devait envoyer le message avant d'entendre ce qu'elle a pris pour un nom figurant dans la liste des contacts enregistrés. Alexa a alors demandé confirmation du nom du contact et aurait entendu un « c'est bien ça ».



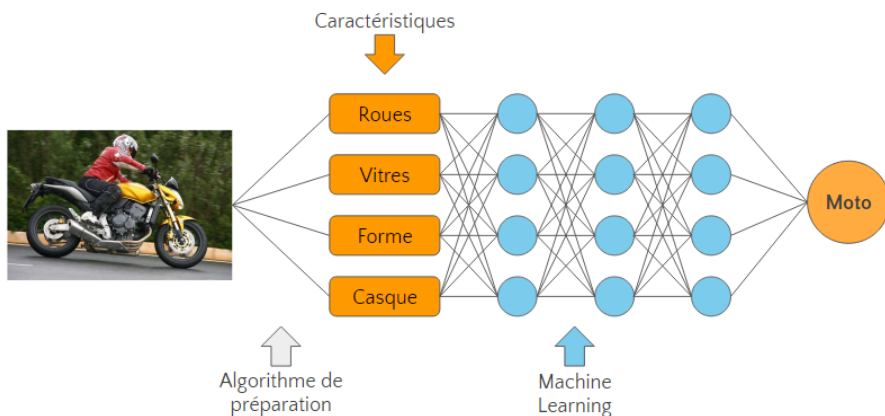
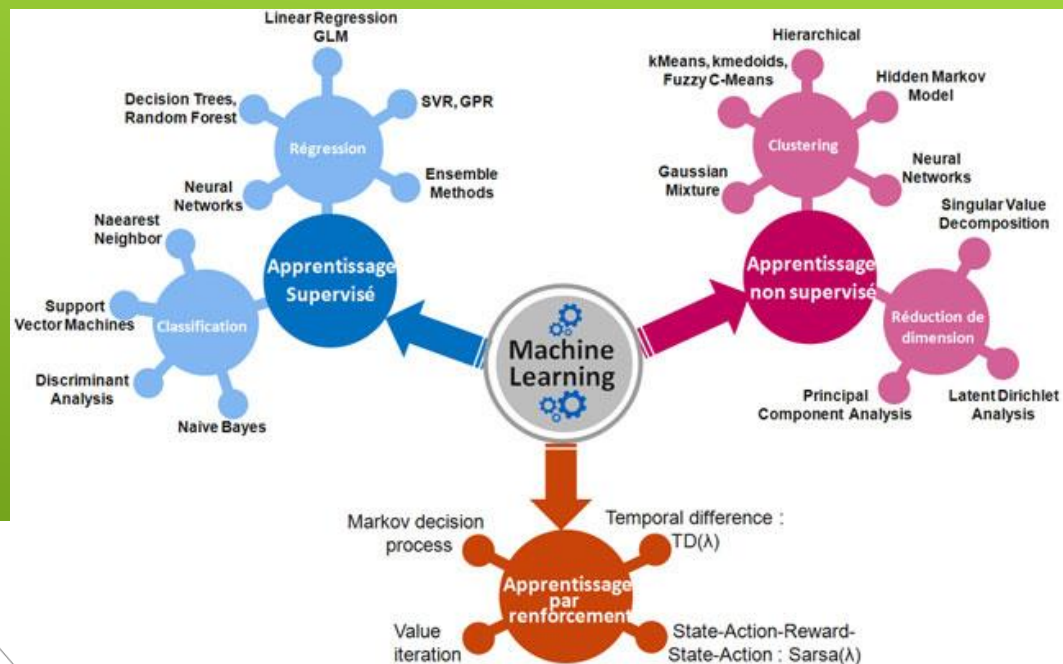
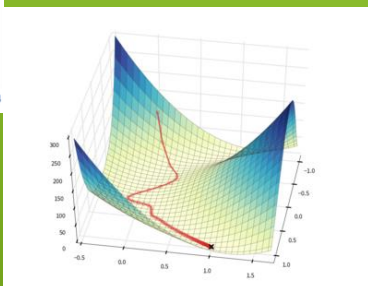
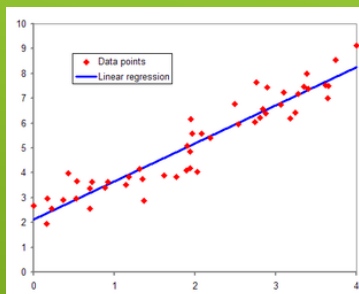


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire



## Intelligence Artificielle et Univers Judiciaire

### La cybercriminalité et machine learning

Weka



La cybersécurité doit mettre en place des services adaptatifs pour résister aux attaques

La cybercriminalité peut se doter d'outils de machine learning pour améliorer leur attaque



Protégé

Profilage

furtivité

Polymorphisme



TensorFlow

將軍

Shogun

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

### La cybercriminalité et machine learning

La cybersécurité doit mettre en place des services adaptatifs pour résister aux attaques

La cybercriminalité peut se doter d'outils de machine learning pour améliorer leur attaque



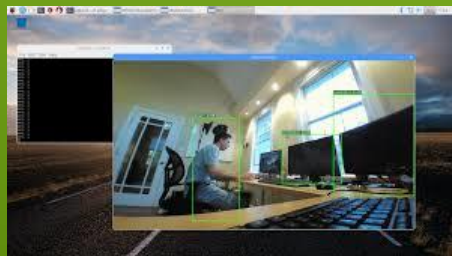
Orange Pi AI Stick 2801 :  
Une clé pour booster les  
IA à 67€



Profilage

furtivité

Polymorphisme



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

### Le jeu de la vie

Survie si  
2 ou 3 voisines

Naissance  
si 3 voisines

	1	
	✓	
2		3

1	2	
3	☠	
4		5

		1
	★	2
3		

### Automate cellulaires

	★			★		
					☠	
		★	★	★		



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

Le jeu de la vie

Planeur

Canon à planeurs

Emgerence

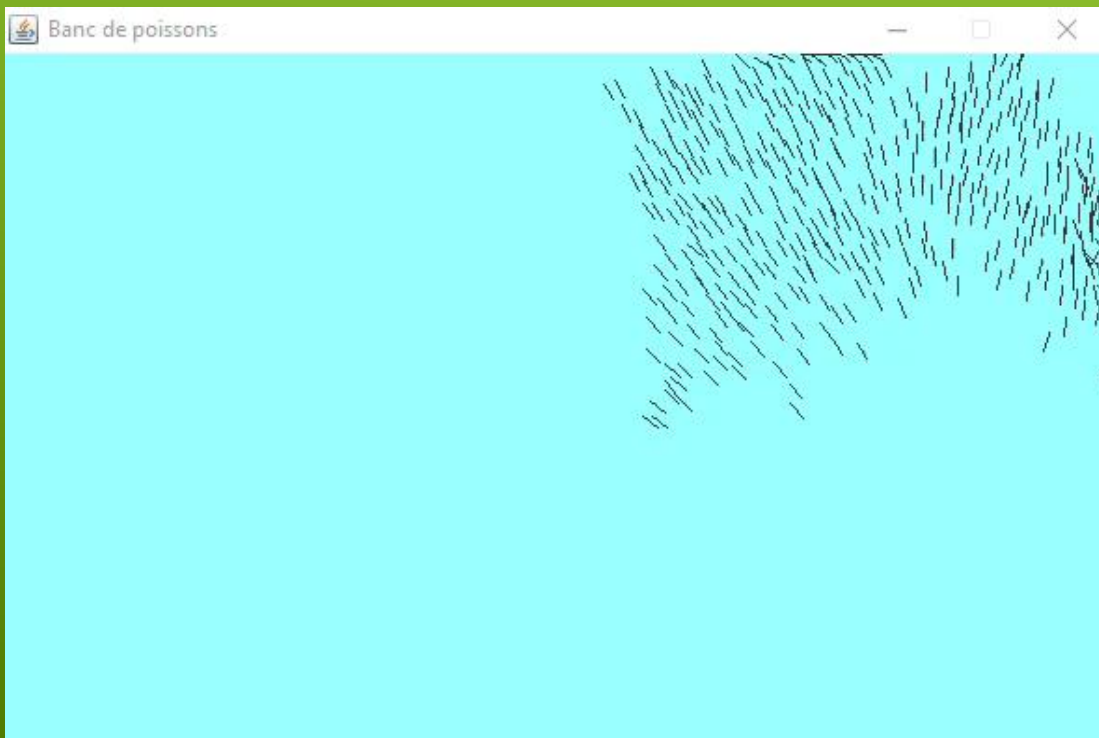


# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

L'explicabilité de la décision d'une IA ?

### Les systèmes multi-agents coopératifs



Institut de Recherche  
en Informatique de Toulouse  
CNRS - INP - UT3 - UT1 - UT2J



#### 4 règles comportementales

- ☐ Éviter les murs
- ☐ Éviter les zones obstacles
- ☐ S'éloigner des poissons proches
- ☐ S'aligner sur la trajectoire d'un poisson proche

## Emergence

### Banc de poissons



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

### L'explicabilité de la décision d'une IA ?

Des scientifiques alertent: les algorithmes sont devenus si complexes que certaines machines prennent des décisions que **l'humain ne parvient plus à expliquer**.

### Dans ces conditions comment rendre un jugement ?

*L'enquête de personnalité dans le cadre d'une enquête criminelle revient à découvrir les décisions prises par un individu qui l'ont conduit à commettre un crime.*

**L'enquête de traçabilité des décisions** dans le cadre d'une responsabilité d'une intelligence artificielle ne pourrait-elle pas permettre d'acquérir un niveau de compréhension suffisant pour juger ?





# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Intelligence Artificielle et Univers Judiciaire

### L'aide à la décision judiciaire

Calcul  
de la  
probabilité  
de récidive



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

En cas d'accident qui est responsable : Le conducteur, le propriétaire de la voiture ou le constructeur ?



## Niveaux d'automatisation de la conduite

Niveau 0 Uniquement conducteur	Niveau 1 Assistance	Niveau 2 Automatisation partielle	Niveau 3 Automatisation élevée	Niveau 4 Automatisation complète	Niveau 5 Sans conducteur
Le conducteur se charge constamment du guidage longitudinal <b>et</b> latéral du véhicule.	Le conducteur se charge constamment du guidage longitudinal <b>ou</b> latéral du véhicule.	Le conducteur <b>doit constamment</b> surveiller le système du véhicule.	Le conducteur ne <b>doit plus constamment</b> surveiller le système du véhicule.	Pas de conducteur nécessaire dans certains cas de figure.	Aucun conducteur nécessaire <b>du début à la fin</b> de la conduite.
Conducteur					Automatisation
Aucune intervention d'un système du véhicule.	Le système reprend la fonction non assurée par le conducteur.	Le système se charge du guidage longitudinal <b>et</b> latéral du véhicule dans des cas de figure spécifiques*.	Le système se charge du guidage longitudinal <b>et</b> latéral du véhicule dans des cas de figure spécifiques*. Il reconnaît ses limites et demande suffisamment tôt au conducteur de reprendre le contrôle du véhicule.	Le système est en mesure de gérer toutes les situations de manière automatique, <b>dans certains cas de figure</b> .	Le système prend en charge l'intégralité de la conduite pour tous les types de routes, limitations de vitesse et conditions liées à l'environnement.

■ Conducteur ■ Niveau d'automatisation de la fonction

\* Un cas de figure comprend les éléments suivants: types de routes, limitations de vitesse et/ou conditions liées à l'environnement.

Source: Verband der Automobilindustrie (VDA), Berlin, 2016, illustration du bpa

**SOURCE :** [https://fr.slideshare.net/PSA\\_Peugeot\\_Citroen/la-voiture-autonome-de-psa-peugeot-citron](https://fr.slideshare.net/PSA_Peugeot_Citroen/la-voiture-autonome-de-psa-peugeot-citron)



## Se protéger



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Services institutionnels

- Agence nationale de la sécurité des systèmes d'information (**ANSSI**)
- Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (**DIRECCTE**)
- Direction générale de la Sécurité intérieure (**DGSI**)
- **Gendarmerie Nationale** (Enquêteurs en cybercriminalité)
- Direction du Renseignement et de la Sécurité de la Défense (**DRSD**)
- **Réserve Citoyenne Cyberdéfense (RCC)**



## Les bons réflexes face à une cyberattaque

### L'utilisateur

- Ne pas paniquer
- Suivre les directives d'urgence mise en place par la D.S.I.
- Isoler sa machine du réseau
- Enlever les disques USB et autres supports connectés
- Prévenir la DSI dans les plus bref délais



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les bons réflexes face à une cyberattaque

### La DSI

- Vérifier la menace
- Faire appliquer les mesures d'urgence sur le S.I
- Mettre en place une cellule de crise si besoin
- Appliquer le plan gestion de crise informatique si besoin

#### Préparer

Identifier les risques et élaborer les objectifs à atteindre en termes de sécurité

Plan

Do

#### Réaliser

Mise en place des mesures de sécurité

#### Réagir

Analyser et améliorer la sécurité

Act

Check

#### Vérifier

Surveiller et vérifier l'efficacité de la sécurité en place

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Les bons réflexes face à une cyberattaque

**Vers qui dois-je me tourner pour rapporter à la justice un incident délictuel survenu au sein de mon SI ?**

Contacter un service de police ou de gendarmerie pour faire intervenir un **spécialiste en cybercriminalité** aux fins de constatations immédiates.

procéder soi-même aux constatations ;  
ou  
✓ faire appel à un huissier ;  
ou  
✓ faire appel à un expert ou une société spécialisée dans la réponse à incident.

**Quelles mesures conservatoires prendre au sein du SI ; à qui confier ces missions ?**

**Confiner** : mettre en quarantaine les postes informatiques  
**Isoler** : couper tous les accès réseaux pour stopper l'incident ;  
**Sauvegarder** : les journaux d'activités  
**Collecter les renseignements internes** : auprès des 1ère personnes  
**Collecter les renseignements externes** : auprès des prestataires  
**Communiquer**

**Constitution d'un dossier d'incident**

**Le processus de gestion d'un incident ne peut s'improviser.**

**Dépôt de plainte ?**

## *L'information pratique*

- [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) (**plateforme PHAROS**)
- [www.ssi.gouv.fr](http://www.ssi.gouv.fr) (**site de ANSSI**)
- [www.cnil.fr](http://www.cnil.fr) (**Commission information et liberté**) **Droit sur les données personnelles (RGPD)**
- [www.gendarmerie.interieur.gouv.fr](http://www.gendarmerie.interieur.gouv.fr)
- [www.service-public.fr/particuliers/vosdroits/](http://www.service-public.fr/particuliers/vosdroits/)
- [www.pre-plainte-en-ligne.gouv.fr/](http://www.pre-plainte-en-ligne.gouv.fr/)
- <https://www.cybermalveillance.gouv.fr/>



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'information pratique



MINISTÈRE DE L'INTÉRIEUR

Pré-plainte en ligne

MINISTÈRE DE L'INTÉRIEUR



PREFECTURE DE POLICE



POLICE NATIONALE



Gendarmerie NATIONALE

Bienvenue sur le site de la pré-plainte en ligne

Adresse IP détectée : 78.245.84.214



Ce service vous permet d'effectuer une **déclaration pour des faits d'atteinte aux biens (vols, dégradations, escroqueries...)** dont vous êtes victime et **pour lesquels vous ne connaissez pas l'identité de l'auteur**. Cette démarche vise essentiellement à vous faire gagner du temps lors de votre présentation à l'unité ou service choisi.

Pour qu'elle soit enregistrée comme une plainte, vous devrez signer cette déclaration dans une unité de gendarmerie ou un service de police que vous allez choisir.

Dans les autres cas, présentez-vous directement dans une unité de gendarmerie ou un service de police.

**Dans tous les cas d'urgence, appelez immédiatement par téléphone le 17 ou le 112.**

**In case of emergency, please dial 17 or 112.**

**En cualquier caso de situación de urgencia, llame inmediatamente por teléfono el 17 o 112.**




Veillez à préserver les traces et indices qui pourront être exploités par les enquêteurs.


Vous avez pris connaissance des conditions d'utilisation de ce service, voulez-vous continuer ?

Continuer

Les renseignements demandés sont exclusivement destinés au traitement informatisé de la déclaration. Seuls les agents dûment habilités des unités de gendarmerie ou des services de police peuvent avoir accès à ces données dans le seul but d'organiser un rendez-vous avec la victime ou son représentant légal pour la signature de la plainte.

Conformément à la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, vous disposez d'un droit d'accès et de rectification aux informations. Vous pouvez exercer ce droit auprès de l'unité de gendarmerie ou du service de police où vous irez signer votre plainte.

Conditions d'utilisation Informations légales



CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention du risque numérique




Menu

## A propos de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est un programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. Vous êtes un particulier, une entreprise ou une collectivité territoriale et vous pensez être victime d'un acte de cybermalveillance ?

La plateforme en ligne du dispositif est là pour vous accompagner :

- établissement d'un diagnostic précis de votre situation ;
- mise en relation avec les spécialistes et organismes compétents proches de chez vous ;
- mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques.

*Le dispositif national d'assistance aux victimes d'actes de cybermalveillance Cybermalveillance.gouv.fr est animé par le groupement d'intérêt public (GIP) Action contre la cybermalveillance (ACYMA) et porté par une démarche interministérielle.*

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## L'information pratique

### Sensibiliser et former à la sécurité informatique



<https://www.secnumacademie.gouv.fr/>  
[https://www.youtube.com/watch?v=\\_UR5HJ-FCLg](https://www.youtube.com/watch?v=_UR5HJ-FCLg)



<https://www.phosforea.com/>  
<https://www.youtube.com/watch?v=xEpPcHvTa9U>

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

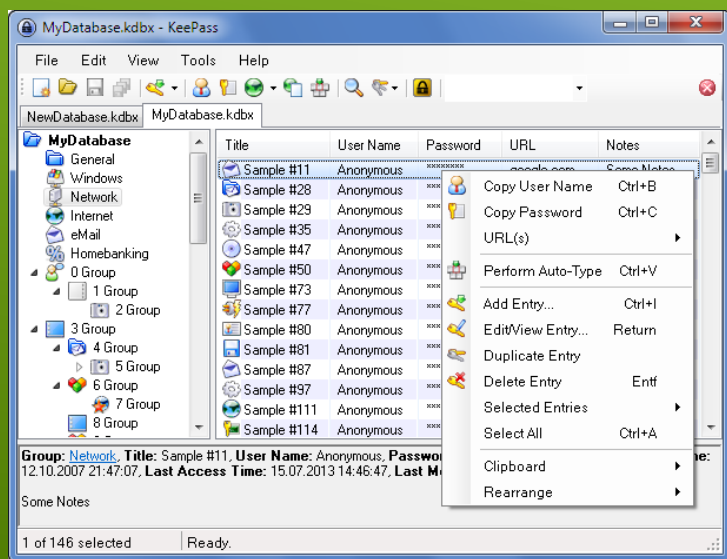
## Quelques logiciels pour les utilisateurs



### KEEPASS retenir et crypter ses mots de passe

**Keepass** est disponible sur de nombreux environnements : Windows, Windows Phone 7, Android, BlackBerry, iPhone, Linux et OS X...

<https://keepass.info/>



Rapport de  
certification ANSSI-  
CSPN-2010/07

[https://www.ssi.gouv.fr/uploads/IMG/cspn/anssi-cspn\\_2010-07fr.pdf](https://www.ssi.gouv.fr/uploads/IMG/cspn/anssi-cspn_2010-07fr.pdf)

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Quelques logiciels pour les utilisateurs



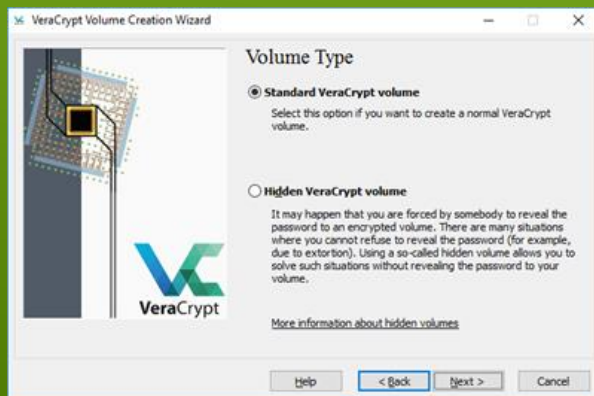
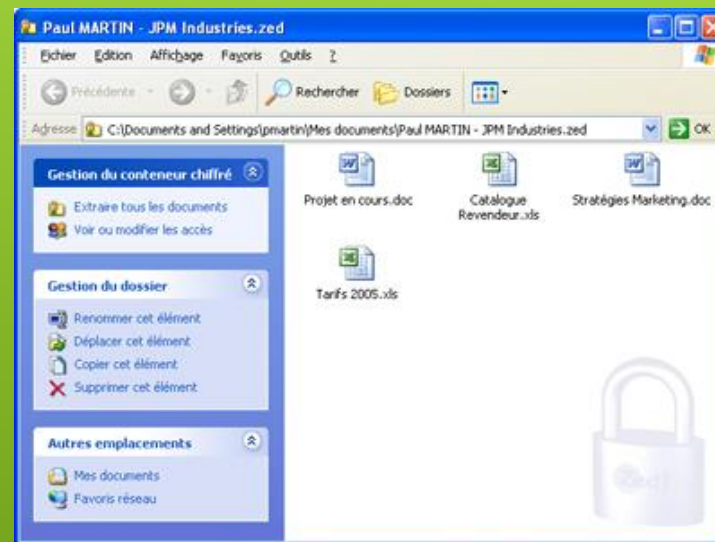
<https://www.primx.eu/zed.aspx>

### Produits qualifiés

Catégorie :  
Protection du  
poste de travail



<https://www.ssi.gouv.fr/entreprise/qualification/zed/>



**VeraCrypt**, un descendant  
audité et évolué de TrueCrypt

Pour les clouds on utilisera des outils tels  
que BoxCryptor ou Cryptomator qui  
sont prévus à cet effet.

# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

## Quelques logiciels pour les utilisateurs

EVIKEY NFC



<http://evikey.com/>



EVITAG NFC

<http://www.evitag-nfc.com/>

EVICARD NFC



<https://www.fulltoken.com/category/evicard-nfc/>



# CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Merci de votre attention

**Fabrice CRASNIER**

*Consultant expert senior*

*Responsable du pôle FORENSIC*

*Laboratoire SCASSI-CYBER*

Tel : 06.24.49.39.20

Courriel : [fabrice.crasnier@scassi.com](mailto:fabrice.crasnier@scassi.com)



**Société SCASSI**

Bâtiment AGORA 1

209 Rue Jean Bart

31670 Labège, France

tél : +33 (0)5 61 17 08 54

fax : +33 (0)5 61 54 50 02

courriel : [contact@scassi.com](mailto:contact@scassi.com)



**Doctorant en intelligence artificielle**

*Ecole doctorale MITT Mathématiques Informatique*

*Télécommunications de Toulouse.*

*Laboratoire IRIT - Equipe SMAC*

*Systèmes Multi-Agents Coopératifs*

Avenue de l'étudiant, 31400 Toulouse

Tel : 06.24.49.39.20

Courriel : [fabrice.crasnier@irit.fr](mailto:fabrice.crasnier@irit.fr)



neCampus

