

L'IoT peut-il être
utilisé comme
vecteur d'attaque ?

*Cybersécurité, Cyberdéfense et Cybercriminalité,
Comment peut-on faire face ?*



Fabrice CRASNIER

Maître de conférences associé
Consultant expert senior en Cybersécurité
d'expert de justice auprès de la Cour d'Appel de TOULOUSE

SÉCURITÉ DES SYSTÈMES D'INFORMATION

2

Fabrice CRASNIER

Maître de conférences associé à Toulouse,
Directeur de la recherche et du développement à Andorre

- Après un cursus d'Ingénieur en conception et développement informatique, je me suis dirigé vers la recherche sur l'informatique embraqué puis sur l'apprentissage automatique supervisé. Je termine à cet effet un doctorat en intelligence artificielle distribué à l'école doctoral de Toulouse.
- Durant 27 ans au service des unités de recherches de la Gendarmerie Nationale, dont 17 années consacrées au suivi de la cyberdélinquance, j'ai mis en place les équipes d'investigations en cybercriminalité de la section des recherches et de la section d'appui judiciaire de Toulouse.
- Durant 3 ans en tant que Consultant Expert Senior, j'ai pu également mettre en place le laboratoire SCASSI-CYBER où j'ai exercé au poste de responsable des activités de réponse sur incidents de sécurité et des expertises légales (FORENSIC).
- Je suis actuellement **enseignant-chercheur à l'université Paul Sabatier à TOULOUSE** en tant que maître de conférences associé où j'enseigne divers matière du la cybersécurité allant de l'audit de maturité au recours devant les tribunaux pour les activités de cybercriminalité.

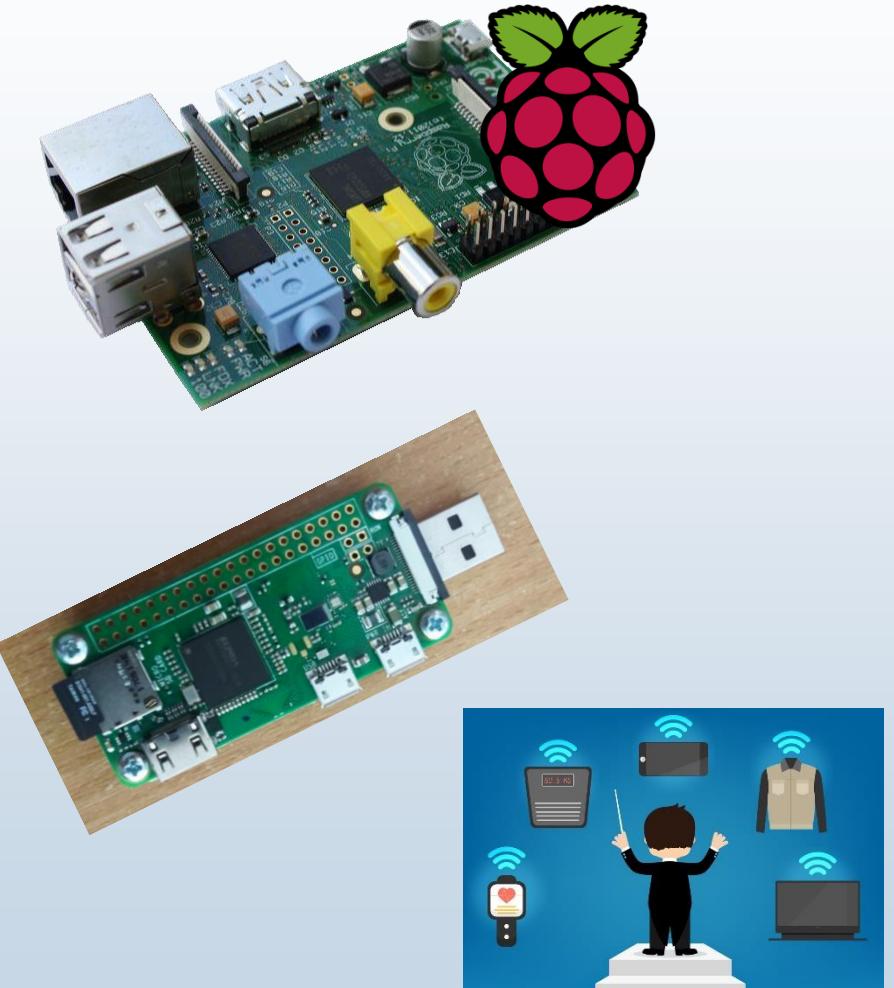
Expert en Cybersécurité



SÉCURITÉ DES SYSTÈMES D'INFORMATION

3

L'internet des objets était peut-il être utilisé comme vecteur d'attaque ?



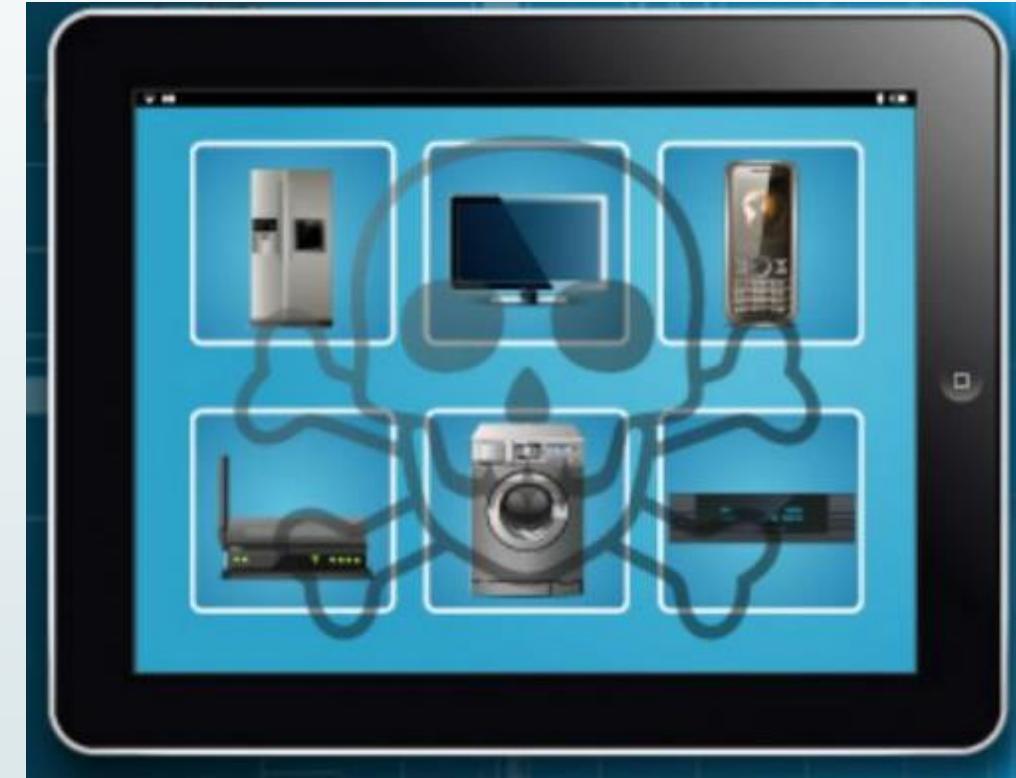


IoT un vecteur de cyberattaque ?

Quand un frigo envoie du spam

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.



<https://www.tomshardware.fr/internet-des-objets-quand-un-frigo-envoie-du-spam/>



IoT un vecteur de cyberattaque ?

Les ransomwares s'attaquent maintenant aux thermostats connectés

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.



<https://www.tomsguide.fr/les-ransomwares-sattaquent-maintenant-aux-thermostats-connectes/>



IoT un vecteur de cyberattaque ?

[Feb.17] Strange behaviour

telnet login

login: vstarcam2015
passwd:

hexedit tveth

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

<https://github.com/lestertang/mirai-botnet-source-code>

<https://github.com/jgamblin/Mirai-Source-Code>

<https://github.com/ruCyberPoison/-Mirai-Iot-BotNet>

<https://github.com/Kulukami/Build-a-Mirai-botnet>



1 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
443/tcp	closed	https	OpenSSL/1.0.2



Telnet login

Login : root
Passwd :



7

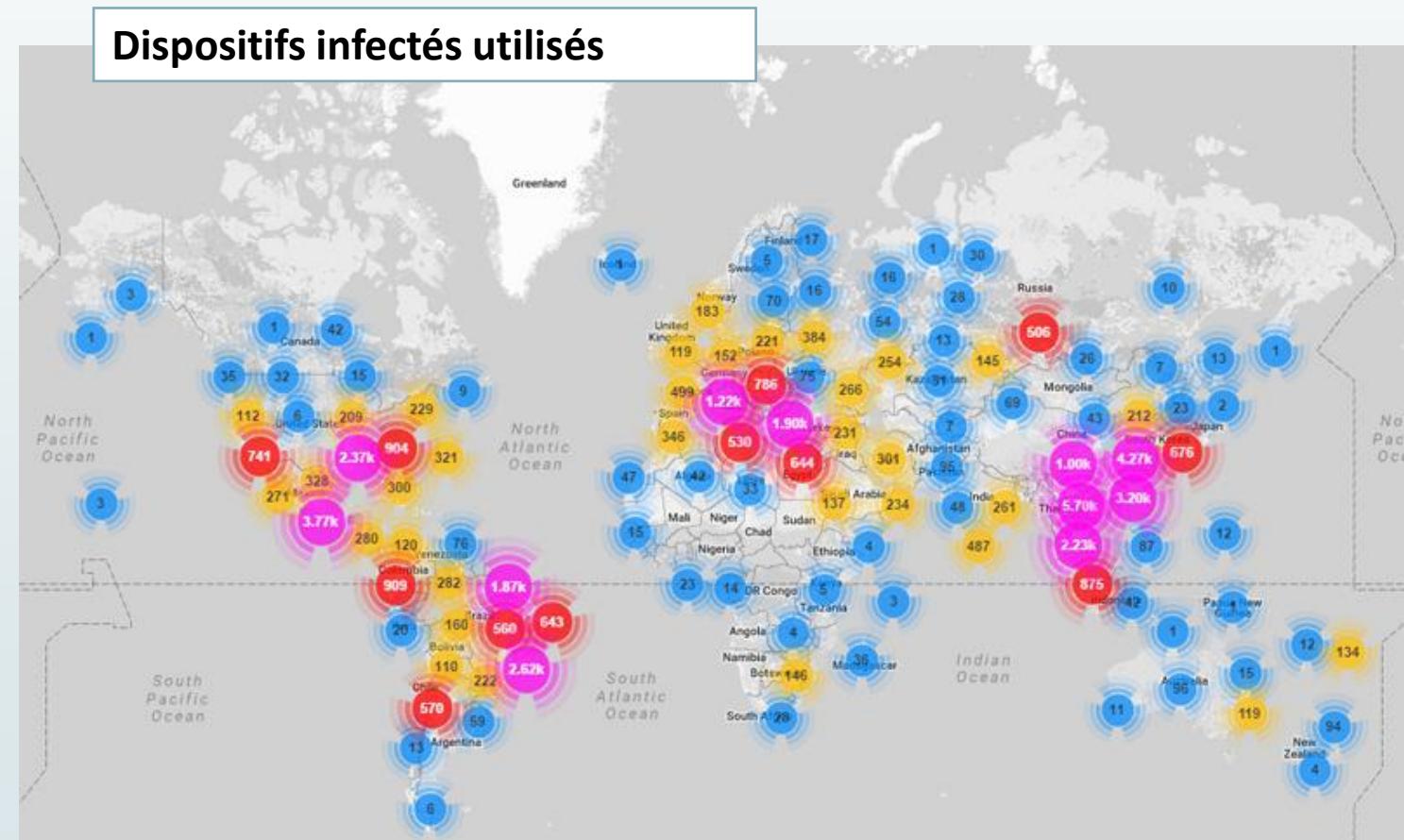
IoT un vecteur de cyberattaque ?

1. Attaques par déni de service distribué (DDoS)



hexedit tveth

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

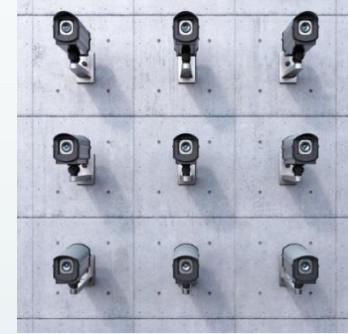
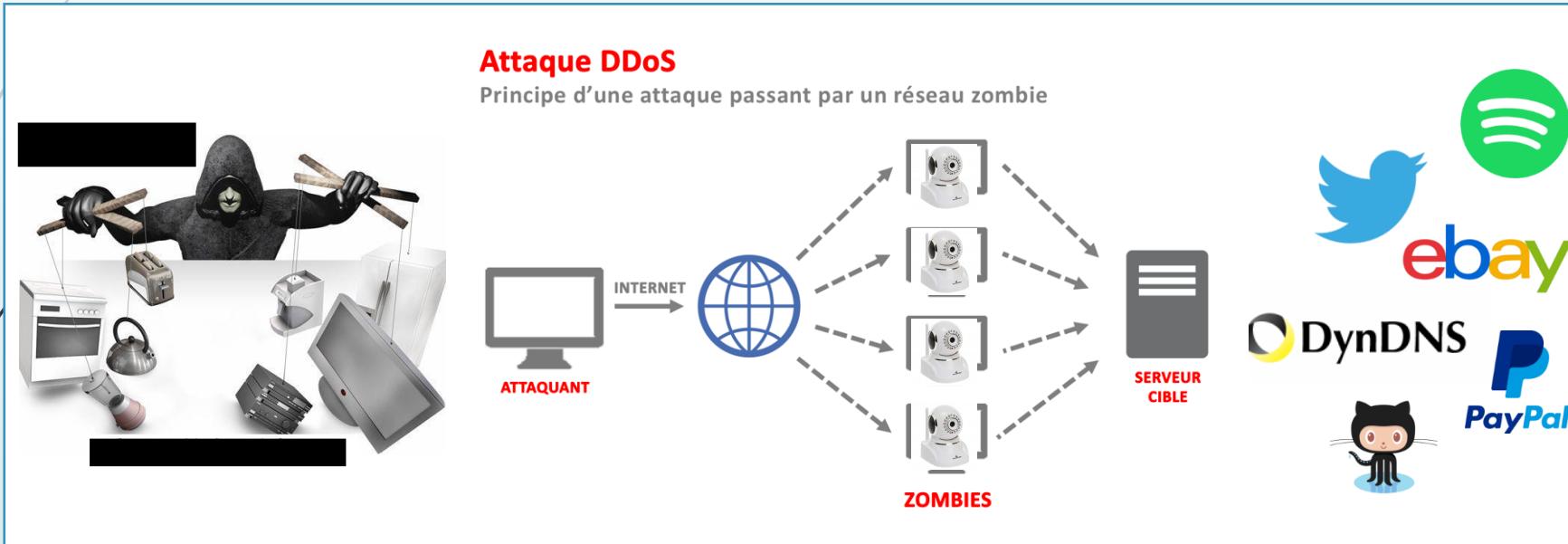




IoT un vecteur de cyberattaque ?

Dyn submergé par un botnet de 100 000 objets connectés

(27 octobre 2016, 12:29)



Internet : pourquoi le Liberia a-t-il été attaqué par le malware Mirai ?

(06 nov 2016 Mise à jour 07.11.2016 à 14:56)

la preuve du concept





Présentation

Etude des outils

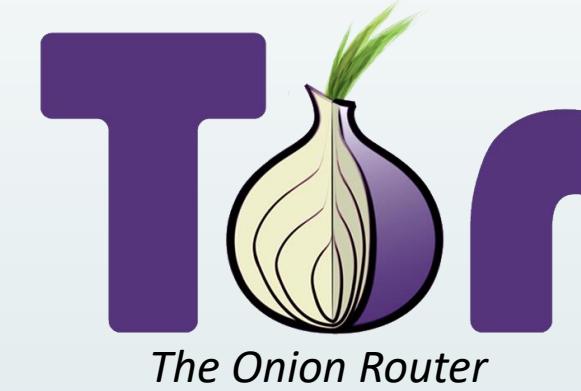
Ateliers

9

IoT un vecteur de cyberattaque ?

L'anonymat à l'aide d'un Raspberry Pi

D.I.Y



Routeur Wifi avec
allocation aléatoire d'une
adresse IP

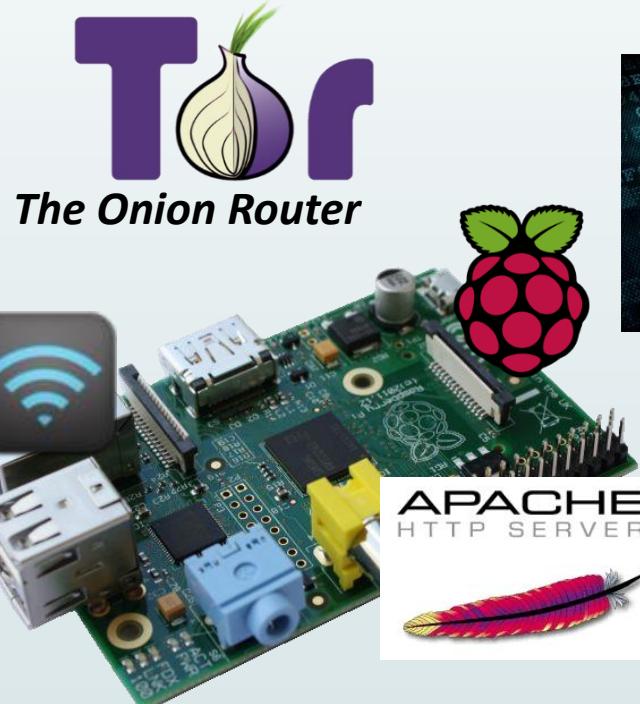


IoT un vecteur de cyberattaque ?

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

D.I.Y

Anonymisation
des traces



Serveur anonyme d'outils
d'achats et de ventes

The image displays two screenshots of darknet markets. The top screenshot shows the Silk Road website with categories like Drugs, Cannab, Ecstasy, Cocaine, Other, etc., and a search bar for 'browsing drugs'. The bottom screenshot shows the AlphaBay Market website with various listings for items such as CC AUTOSHOP, DRUGS & CHEMICALS, COUNTERFEIT ITEMS, DIGITAL PRODUCTS, JEWELS & GOLD, WEAPONS, CARDED ITEMS, SERVICES, and OTHER LISTINGS. Both sites feature a sidebar with account information and a footer with payment method icons.



Présentation

Etude des outils

Ateliers

11

IoT un vecteur de cyberattaque ?



Juillet 2016

Espionnage

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

Piratage à l'aide d'un Raspberry Pi

D.I.Y

Mai 2016

Attaque SQLMap

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

P4wnP1





Présentation

Etude des outils

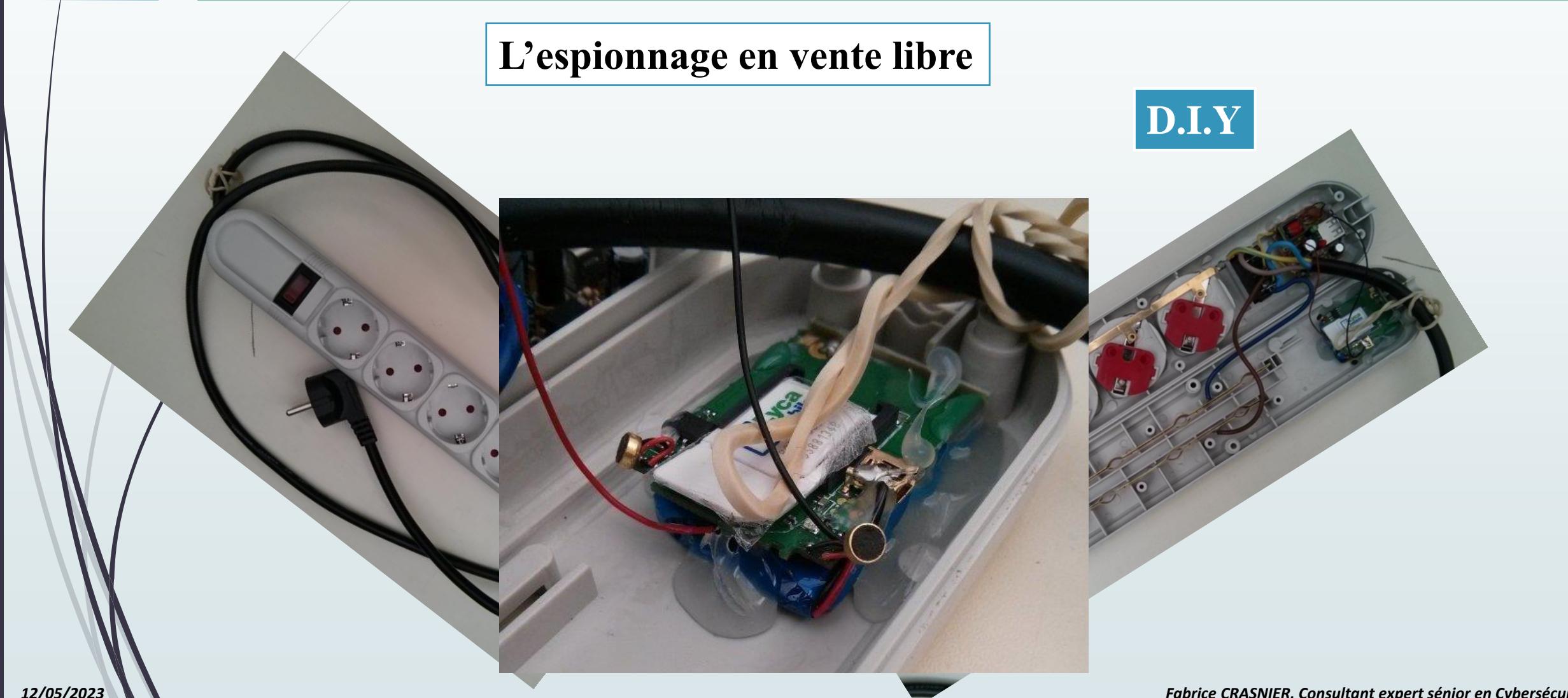
Ateliers

12

IoT un vecteur de cyberattaque ?

L'espionnage en vente libre

D.I.Y

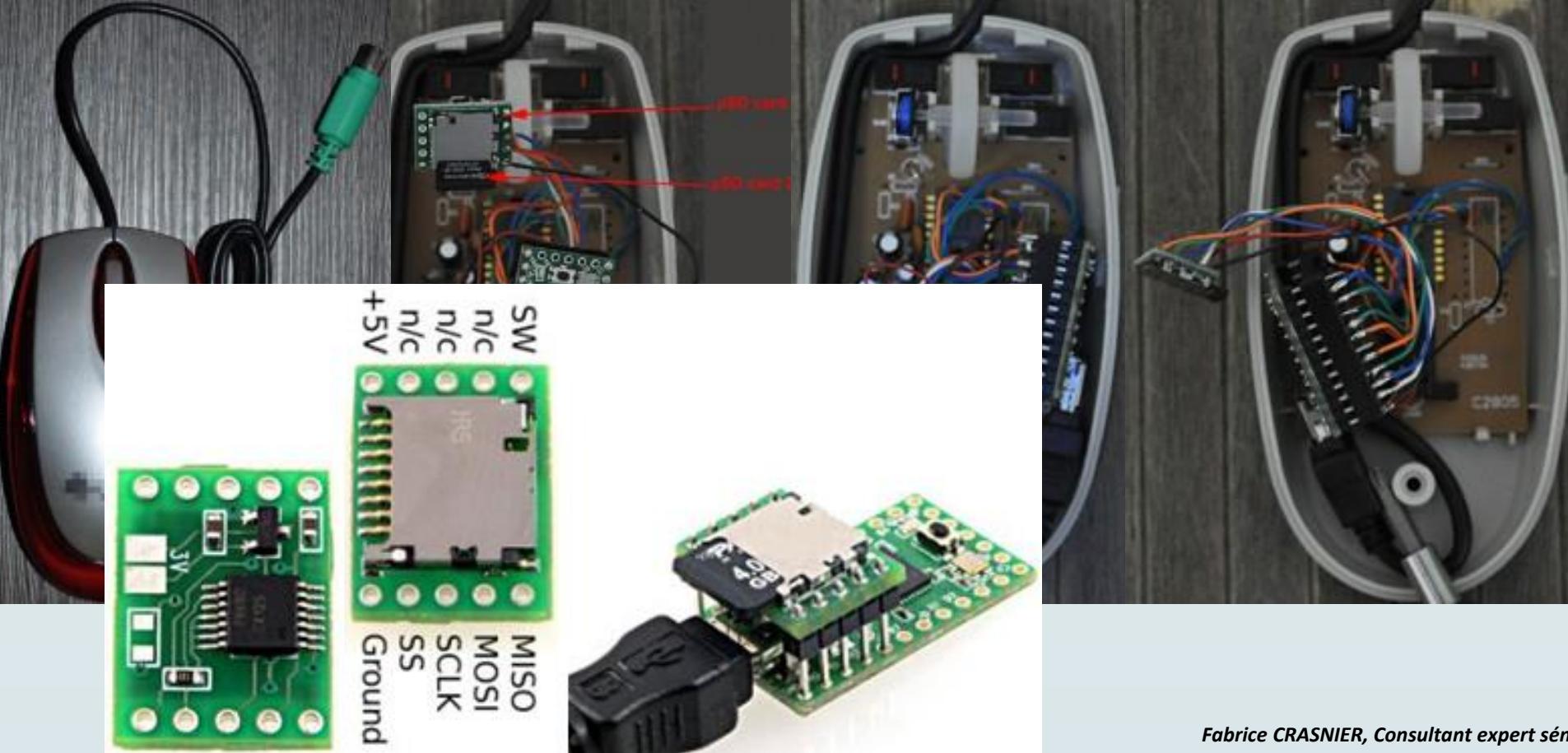




IoT un vecteur de cyberattaque ?

Keyloggueur – une souris malicieuse

D.I.Y





IoT un vecteur de cyberattaque ?

Keyloggueur – Un chargeur USB déguisé

D.I.Y

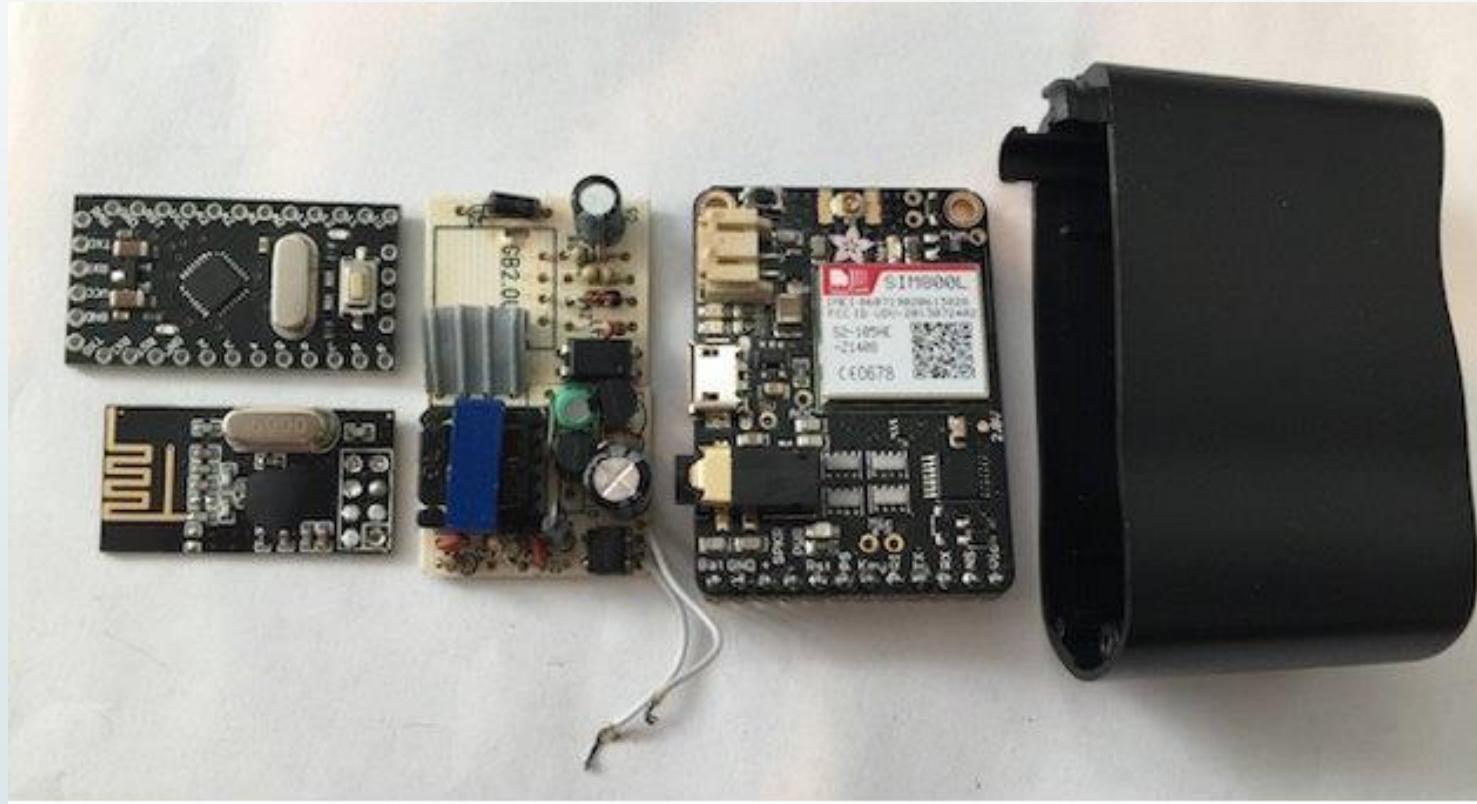


Image courtesy: <http://samy.pl/keysweeper>



IoT un vecteur de cyberattaque ?

Les pièces détachées importées

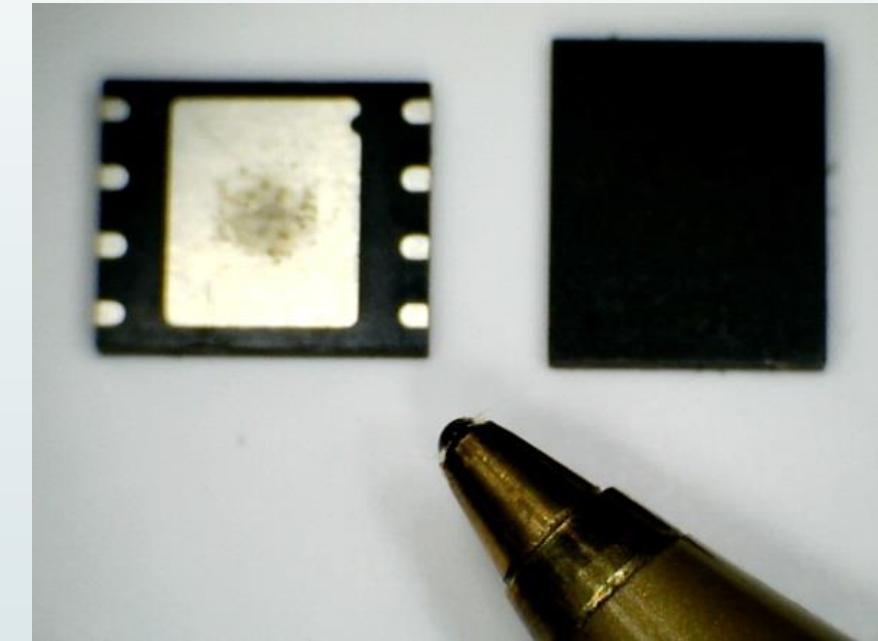




IoT un vecteur de cyberattaque ?

Carte SIM 4G pour le M2M

D.I.Y





IoT un vecteur de cyberattaque ?

Les technologies sans contact

D.I.Y





SÉCURITÉ DES SYSTÈMES D'INFORMATION

18

L'internet des objets était peut-il être utilisé comme vecteur d'attaque ?





Présentation

Etude des outils

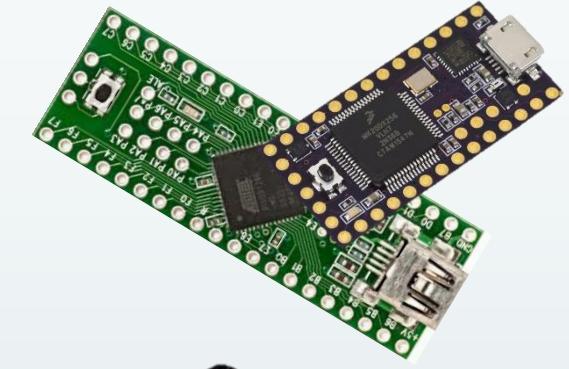
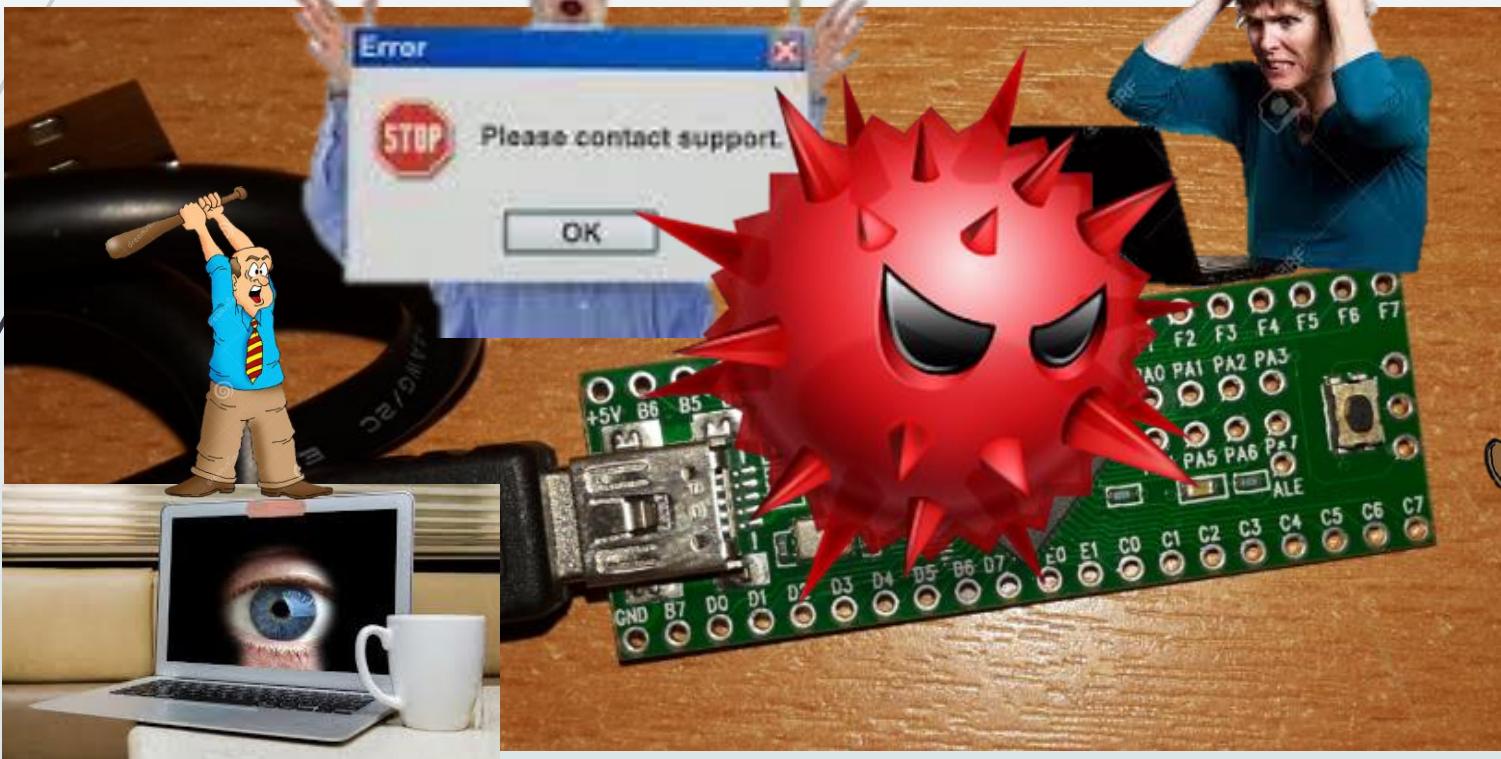
Ateliers

19

IoT un vecteur de cyberattaque ?

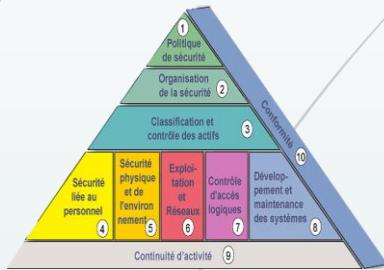
Compromission d'un poste utilisateur

Teensy





IoT un vecteur de cyberattaque ?

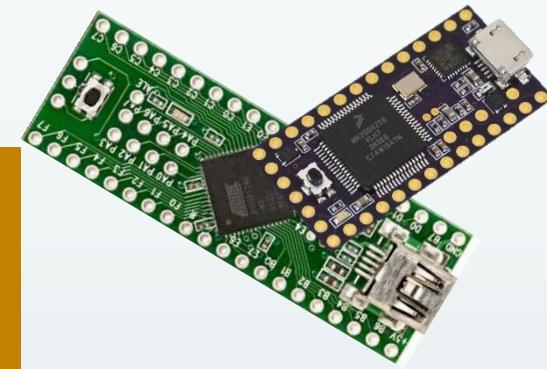


ISO/CEI
27002

-
- 1 • Identifier les actifs
 - 2 • Identifier les personnes responsables
 - 3 • Identifier les vulnérabilités
 - 4 • Identifier les menaces
 - 5 • Identifier les impacts
 - 6 • Evaluer la vraisemblance
 - 7 • Estimer les niveaux de risque

Le système d'exploitation doit se mettre en veille après 5 min d'inactivité pour assurer la sécurité physique du poste de travail.

Compromission d'une règle SSI





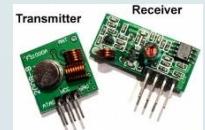
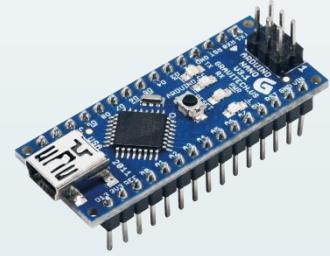
IoT un vecteur de cyberattaque ?

Attaque de protocole de transmission RF

Le cambriolage à l'ancienne



La transformation numérique du cambriolage





IoT un vecteur de cyberattaque ?

Attaque de protocole de transmission non sécurisé sans trace

Matériels utilisés



Domotique DIO, prise connectée, lumière connectée, volet roulant connecté, détecteur de fumée connecté, etc.



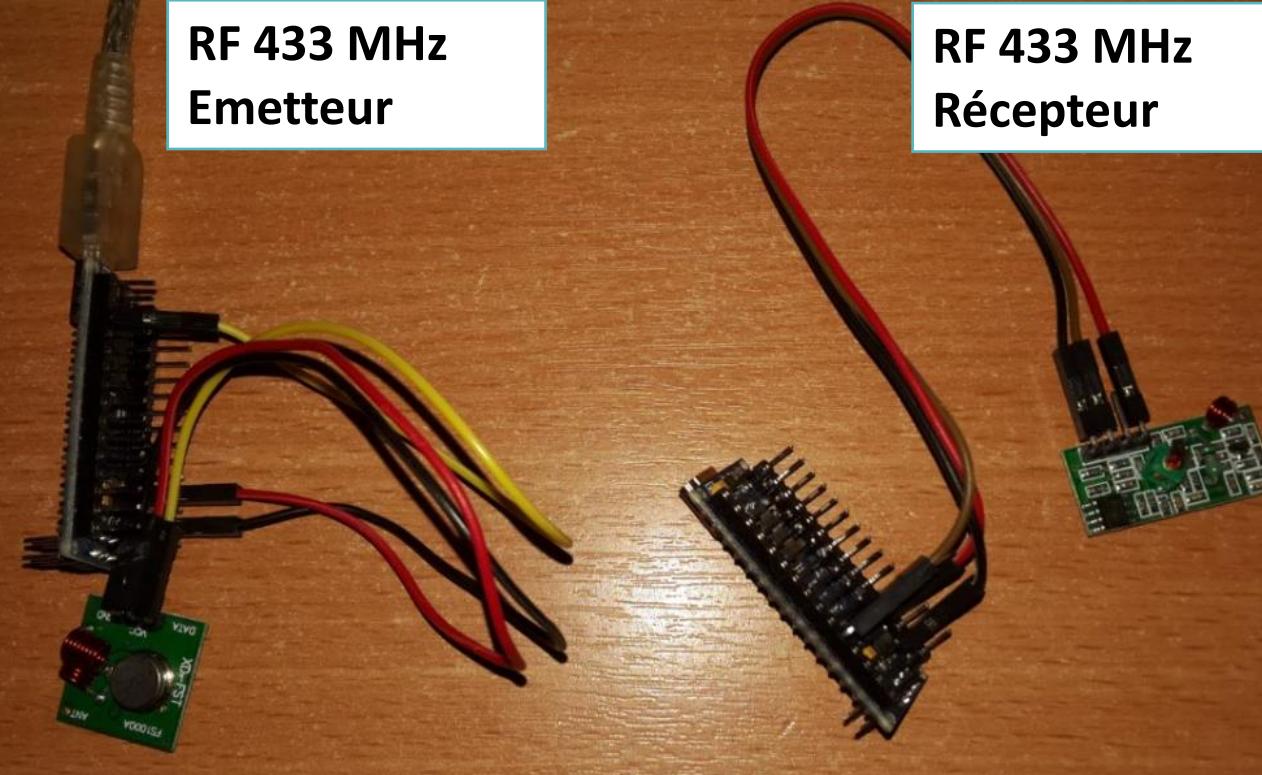
Arduino nano pour l'attaque



IoT un vecteur de cyberattaque ?

Attaque de protocole de transmission non sécurisé sans trace

Matériels utilisés pour l'attaque



```
Termite 3.4 (par CompuPhase)
COM10 115200 bps, 8N1, sans contrôle de flux  Réglages  Effacer  Infos  Fermer
Addr 26060414 unit 0 on, period: 270us.
Addr 26060414 unit 0 off, period: 270us.
Addr 26060414 unit 0 on, period: 270us.
Addr 26060414 unit 0 off, period: 270us.
Addr 26060414 unit 0 on, period: 270us.
Addr 26060414 unit 1 on, period: 270us.
Addr 26060414 unit 2 on, period: 270us.
Addr 26060414 unit 2 on, period: 270us.
Addr 26060414 unit 1 off, period: 318us.
Addr 26060414 unit 2 off, period: 270us.
Addr 26060414 unit 1 off, period: 269us.
Addr 26060414 group off, period: 269us.
```

Ecoute les trames émises en RF433

```
Termite 3.4 (par CompuPhase)
COM10 115200 bps, 8N1, sans contrôle de flux  Réglages  Effacer  Infos  Fermer
Menu (A) - cmd valeur courante / (N) - Nouvelle cmd
N
Veuillez saisir le code pour la telecommande
Changement de telecommande :
Changement de telecommande INT : 0
26060414
Changement de telecommande : 26060414
Changement de telecommande INT : 26060414
F
Changement de telecommande : 26060414
Changement de telecommande INT : 26060414
Veuillez saisir un etat :
A
Allumer la lampe !
Veuillez saisir un etat :
E
Eteindre la lampe !
Veuillez saisir un etat :
```

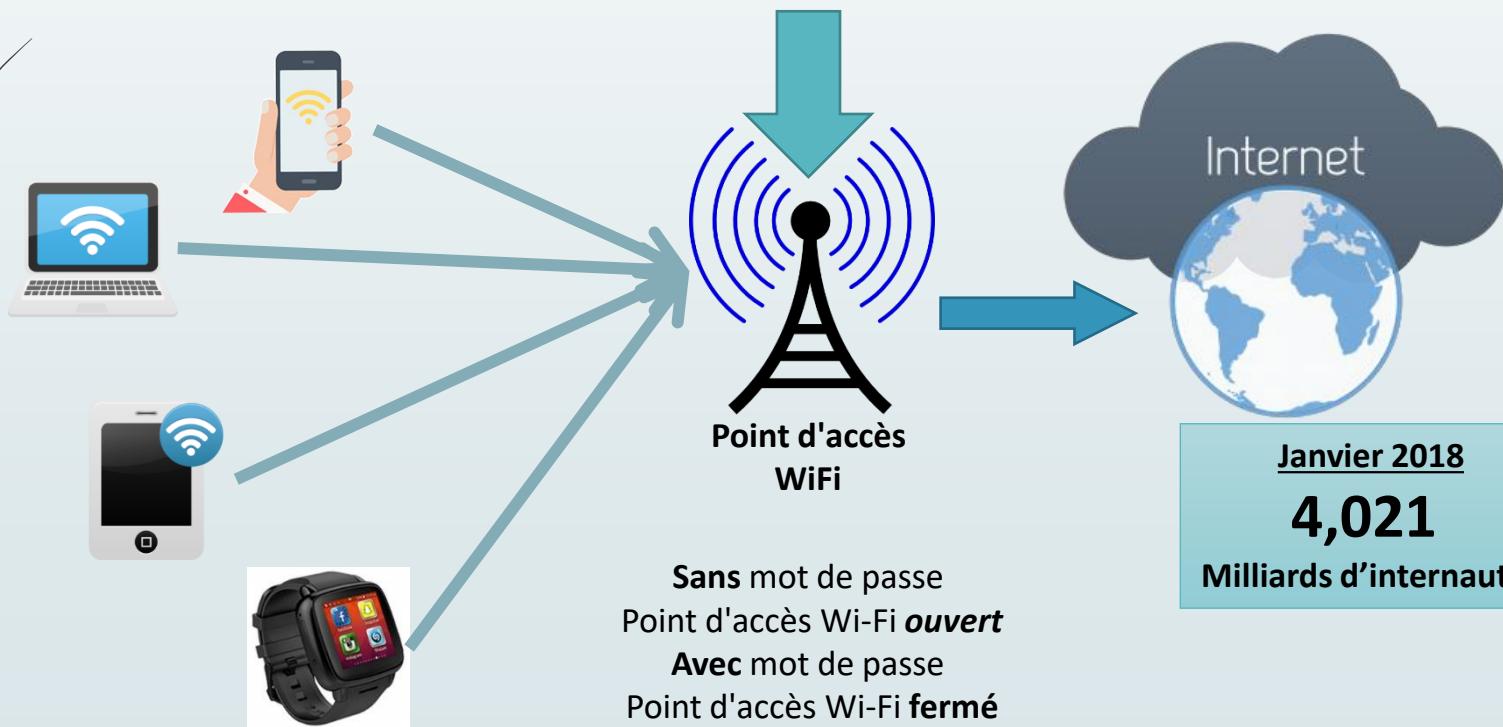
Emet les commandes en RF433



IoT un vecteur de cyberattaque ?

Attaque sur protocole de transmission Wifi

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





IoT un vecteur de cyberattaque ?

Attaque sur protocole de transmission Wifi



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

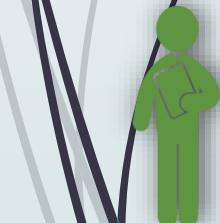




IoT un vecteur de cyberattaque ?



Point d'accès WiFi public ouvert



Attaque de l'homme du milieu

Attaque sur protocole de transmission Wifi

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

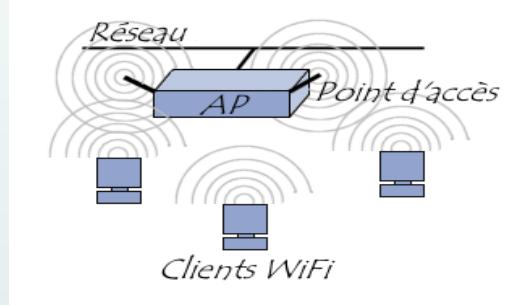


Point d'accès WiFi public fermé

WiFiScan



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





IoT un vecteur de cyberattaque ?



Point d'accès WiFi public ouvert



MIM_WIFI

Attaque sur protocole de transmission Wifi

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



Le portail captif



Duplicateur de portail captif

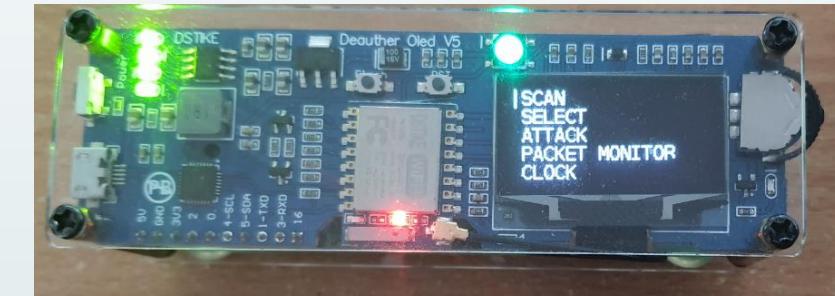
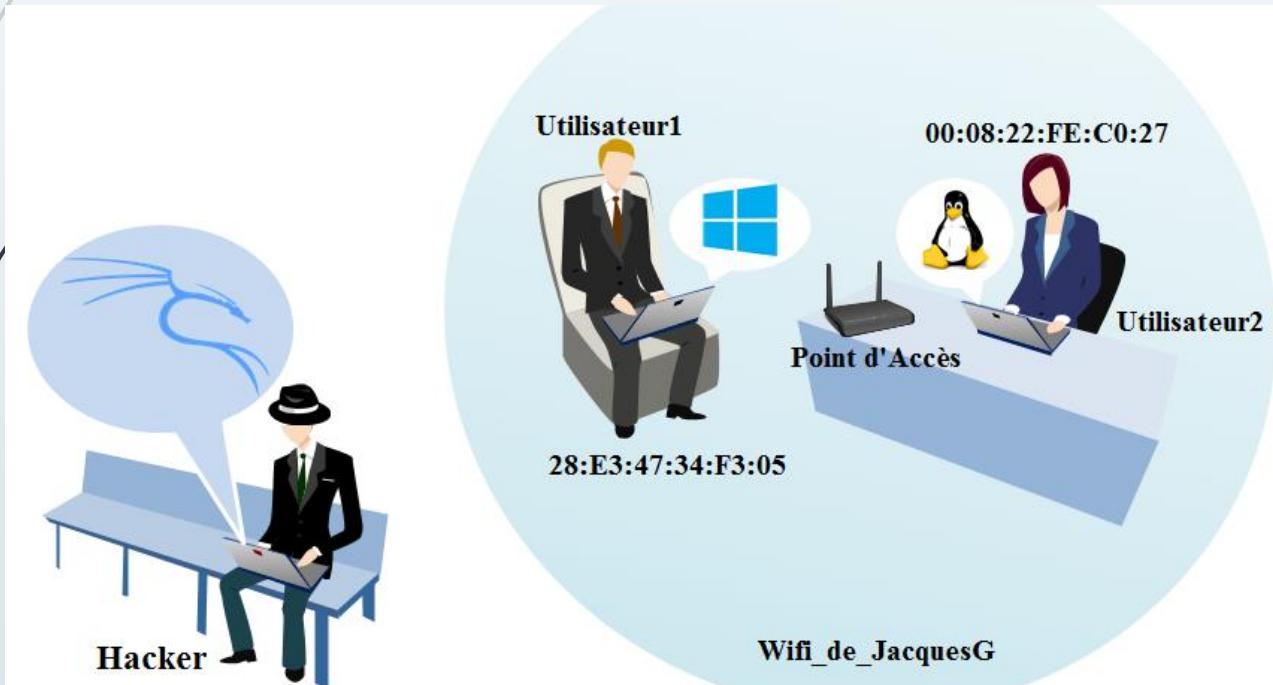




IoT un vecteur de cyberattaque ?

Attaque par désauthentification Wifi

Un NodeMCU WiFi Deauther, vous permet de déconnecter des appareils d'un réseau WiFi.



DSTIKE WiFi Deauther
OLED V6 ESP8266
NodeMCU WiFi
Deauther





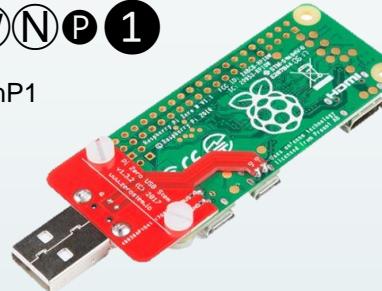
IoT un vecteur de cyberattaque ?

Commandes
via WiFi



Password : MaMe82-P4wnP1

<http://172.24.0.1:8000>



Attaques distantes

- Réseau via IP (Point d'accès Wifi)
- Connexion USB
- Connexion Bluetooth

IoT multi-usage pour générer des attaques distantes

P4wnP1 A.L.O.A.

USB SETTINGS WIFI SETTINGS BLUETOOTH NETWORK SETTINGS TRIGGER ACTIONS HIDSCRIPT EVENT LOG GENERIC

HIDScript editor

RUN STORE LOAD & REPLACE LOAD & PREPEND

```
1 layout('FR');           // US keyboard layout
2 typingSpeed(100,150)    // Wait 100ms between key strokes
3
4 // Starting notepad
5 press("WIN R");         // Windows key + R, to open run dialog
6 delay(500);              // wait 500ms for the dialog to open
7 type("notepad.exe\n");   // type 'notepad.exe' to the run dialog
8 delay(500);              // wait 2 seconds for notepad to open
9
10 // Type the message
11 type("Pentest Cyberfablab Expertises et Formations\n");
12 delay(1000);
13 type("Merci pour votre invitation en Andorre\n");
14 delay(1000);
15 type("Fabrice CRASNIER - Freemindtronic\n");
16
17 // close notepad after LED change
18 delay(2000);
19 //waitLED(ANY);          // wait for a single LED change
20 press("ALT F4");        // ALT+F4 shortcut to close notepad
21
22 //as we changed content, there will be a confirmation dialog
23 delay(1500);             // wait for the confirmation dialog
24 press("RIGHT");          // move focus to next button (don't use arrow keys)
25 delay(1500);              // wait for the confirmation dialog
26 press("SPACEBAR");       // confirm dialog with space
```

Running jobs (0 running jobs)

Succeeded (3 successful jobs)

- Job 29 State SUCCEEDED
- Job 30 State SUCCEEDED
- Job 31 State SUCCEEDED

Failed (0 failed jobs)

v0.1.0-alpha2 by MaMe82



IoT un vecteur de cyberattaque ?

Les mécanismes de propagation d'attaque

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





IoT un vecteur de cyberattaque ?

Les mécanismes de propagation d'attaque

USB Rubber Ducky



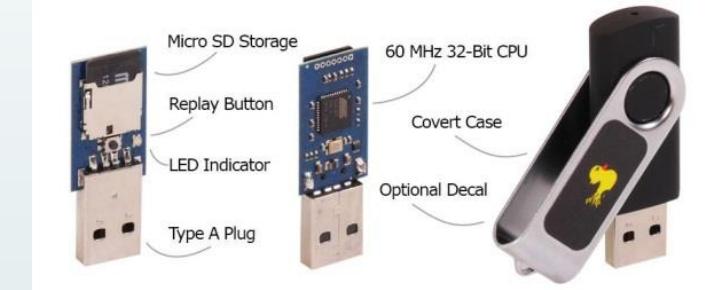
\$49.99

<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>





IoT un vecteur de cyberattaque ?

Les mécanismes de propagation d'attaque

USB Lily GO



\$13.99

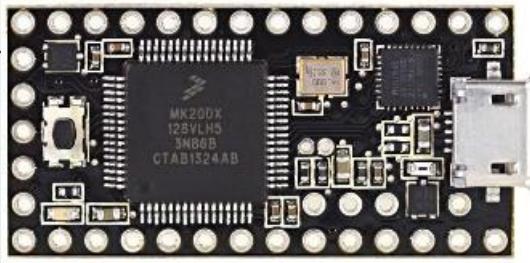
lilyGO_msg<https://hackinglethani.com/physical-hacking-with-usb/><http://roothaxor.gitlab.io/ducky2arduino/>



IoT un vecteur de cyberattaque ?

Les mécanismes de propagation d'attaque

Teensy 3



Borne de rechargeement



Goodies



IoT un vecteur de cyberattaque ?

Les mécanismes de propagation d'attaque

Comment récupérer les mots de passe des points d'accès wifi d'une entreprise ?



USB Lily GO

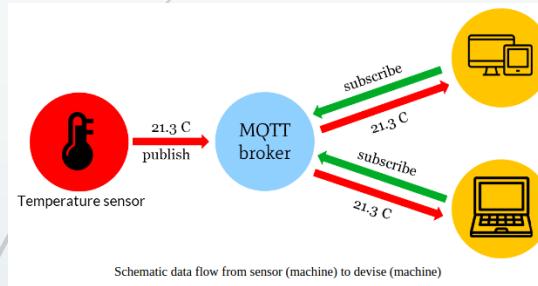
```
C:\Users\[REDACTED]>netsh wlan show profiles  
Profils sur l'interface Wi-Fi 3 :  
  
Profils de stratégies de groupe (lecture seule)  
-----  
    <Aucun>  
  
Profils utilisateurs  
-----  
    Profil Tous les utilisateurs      : TP-LINK_B15362
```

```
C:\Users\[REDACTED]>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    : [REDACTED] ← 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>
```

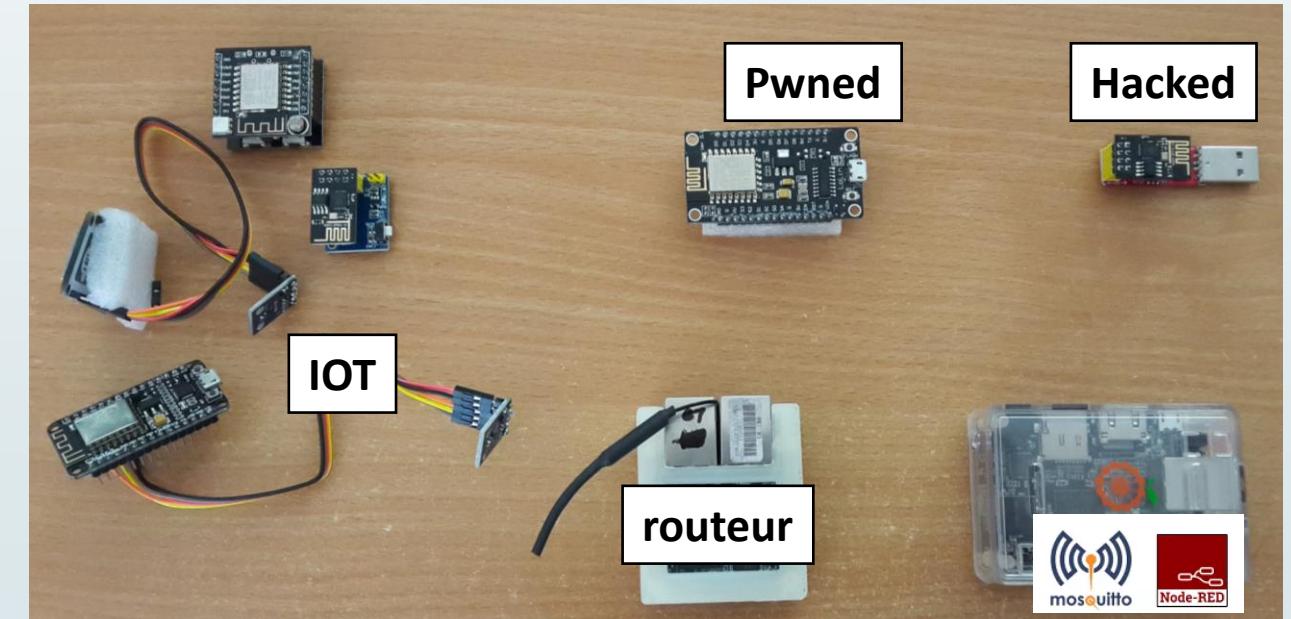
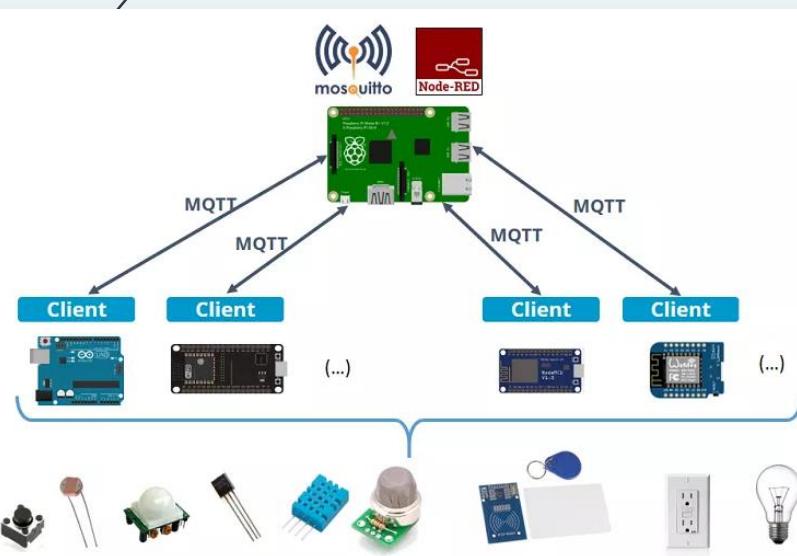


IoT un vecteur de cyberattaque ?

Multi-purpose IoT to generate remote attacks



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



Université Paul Sabatier

Faculté des sciences et de l'ingénierie

Merci de votre attention
A votre disposition pour un approfondissement

Maître de conférences associé

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

Courriel : fabrice.crasnier@irit.fr



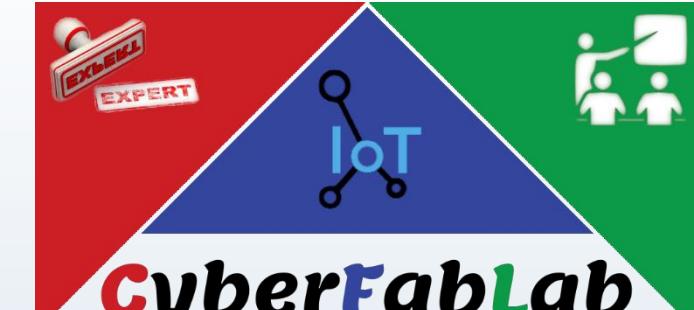
Domaines de compétences

- Formations en cybersécurité
- Réponse sur incident de sécurité
- Gestion de crise, conseil juridique
- Construction d'un dossier de plainte
- Expertises pénales et civiles



Tel : 06.24.49.39.20

Courriel : fabrice.crasnier@cyberfablab.fr



Expert en Cybersécurité

