Alien - Virus

Éric BERTHOMIER
berthomiereric70@gmail.com

4 janvier 2026

Version 1.1 - Version Stagiaire

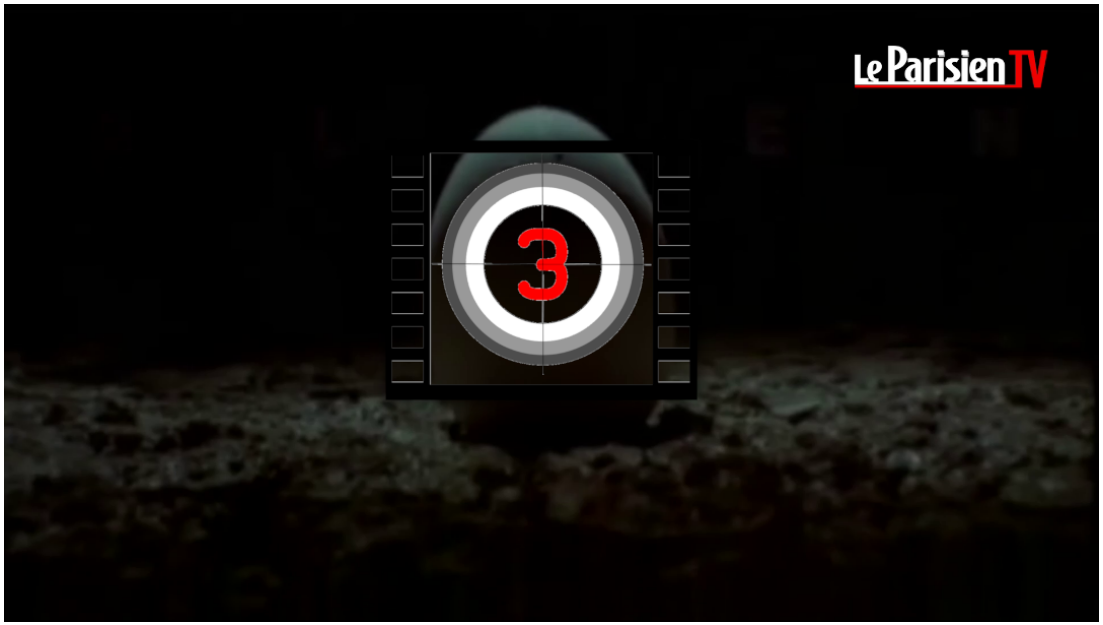
Difficile. . .

Difficile de comprendre les informaticiens et le fonctionnement des malwares.

Difficile. . .

Difficile de comprendre les informaticiens et le fonctionnement des malwares.
Aussi, nous allons tenter un parallèle entre un malware et notre ami Alien.

Vidéo



L'œuf

De l'œuf à la créature

1

L'ŒUF

Il est laissé en attente dans un **lieu clos.**

L'œuf

Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

L'œuf

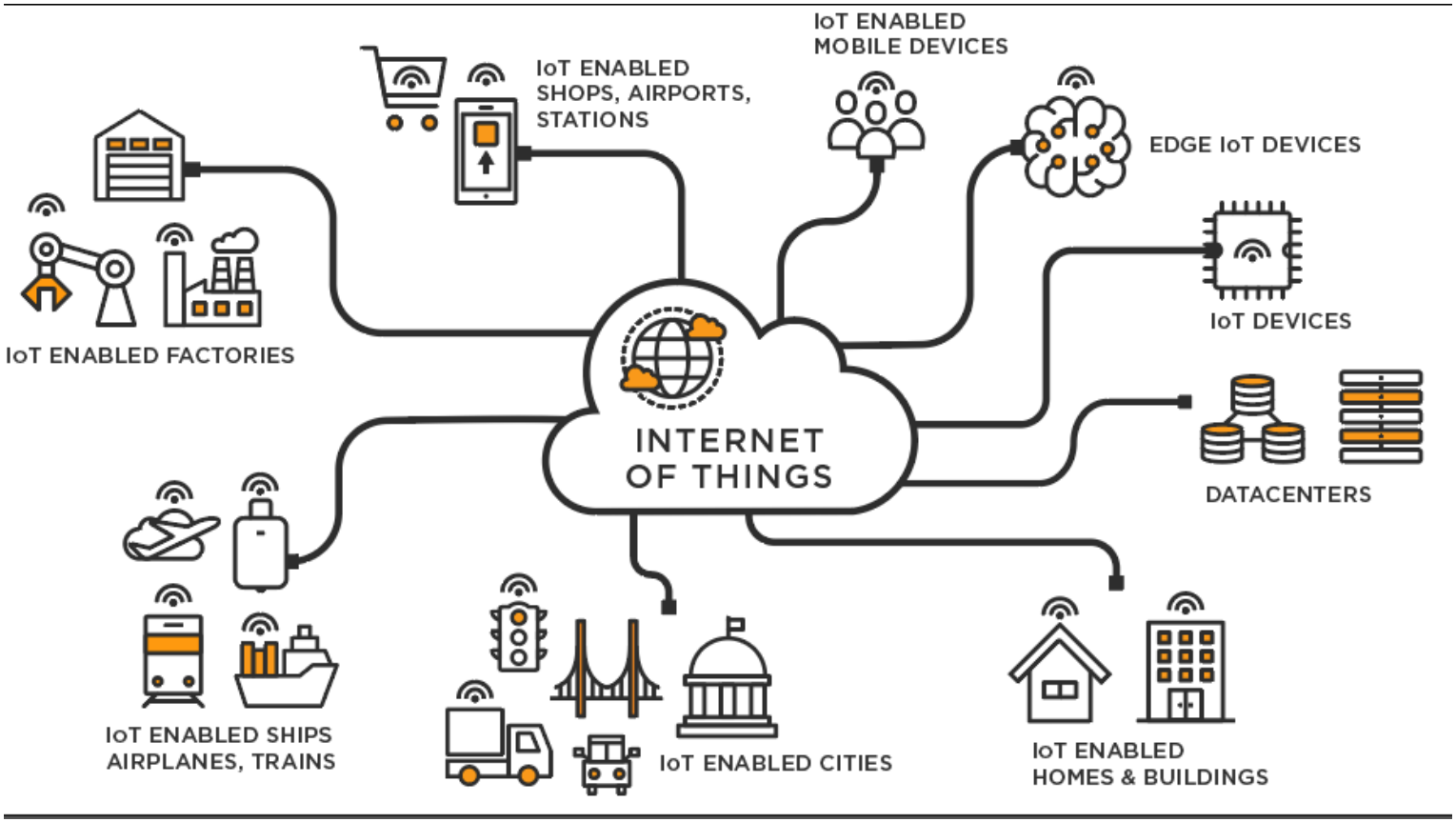
Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

Ce dernier peut donc dormir au sein de votre ordinateur / smartphone / tablette / montre connectée. . . tant qu'un antivirus n'a connaissance de sa malveillance.

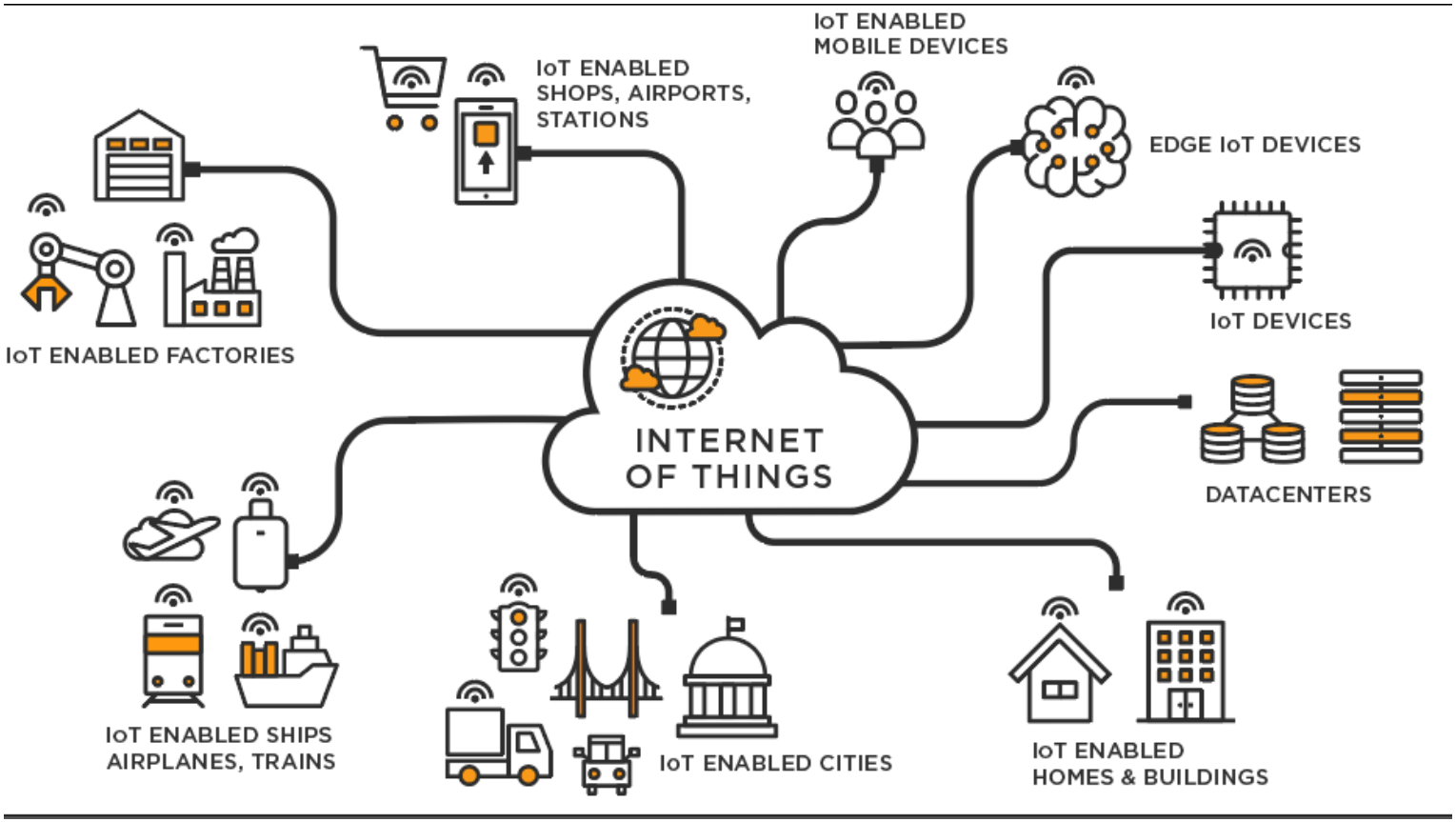
Interlude

On nomme Internet of Things (IOT), tout objet connecté à Internet.

Interlude

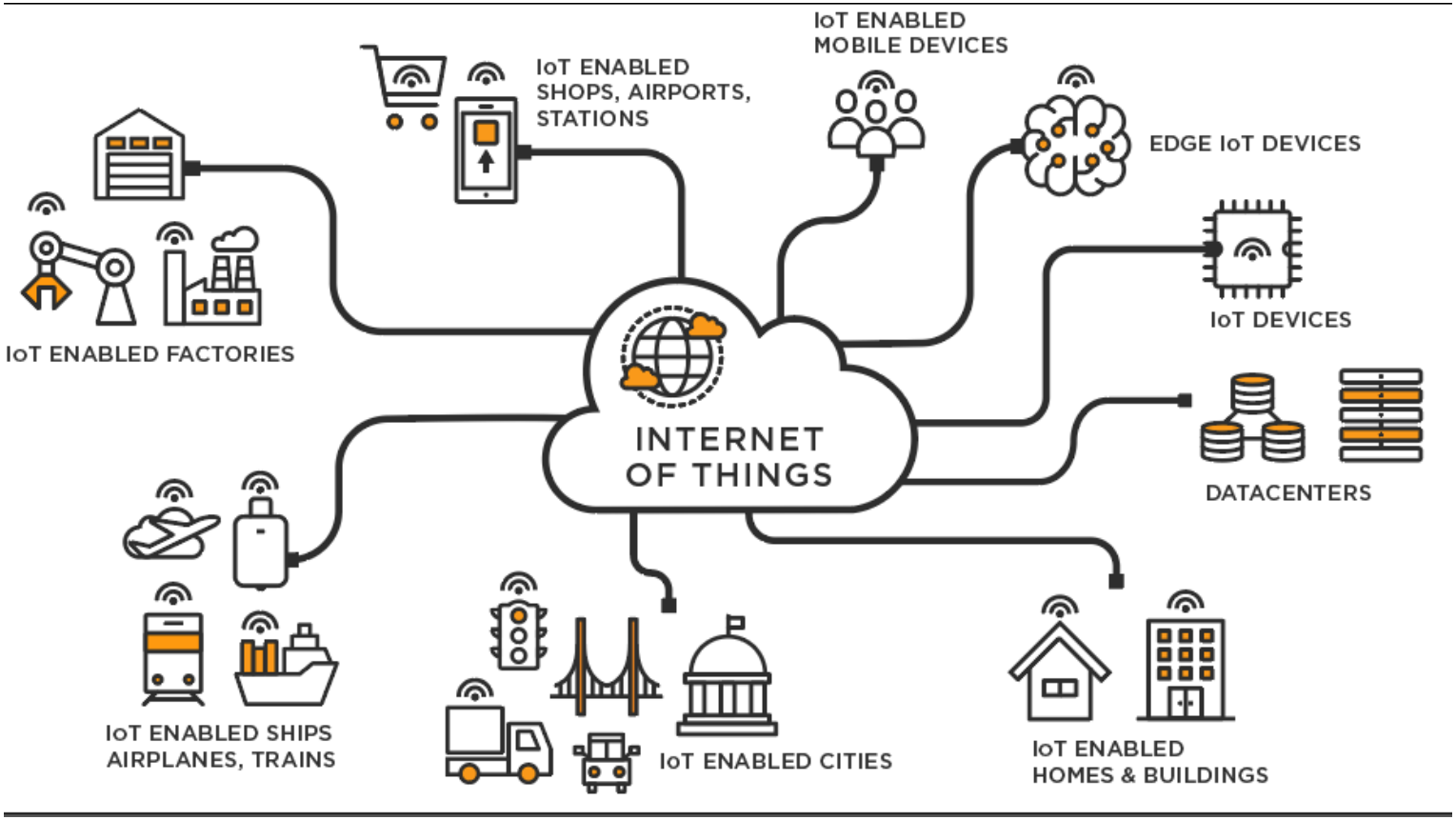

IoT ENABLED
MOBILE DEVICES
IoT ENABLED
SHOPS, AIRPORTS,
STATIONS
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET
OF THINGS
DATACENTERS
IoT ENABLED SHIPS
AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED
HOMES & BUILDINGS

Interlude



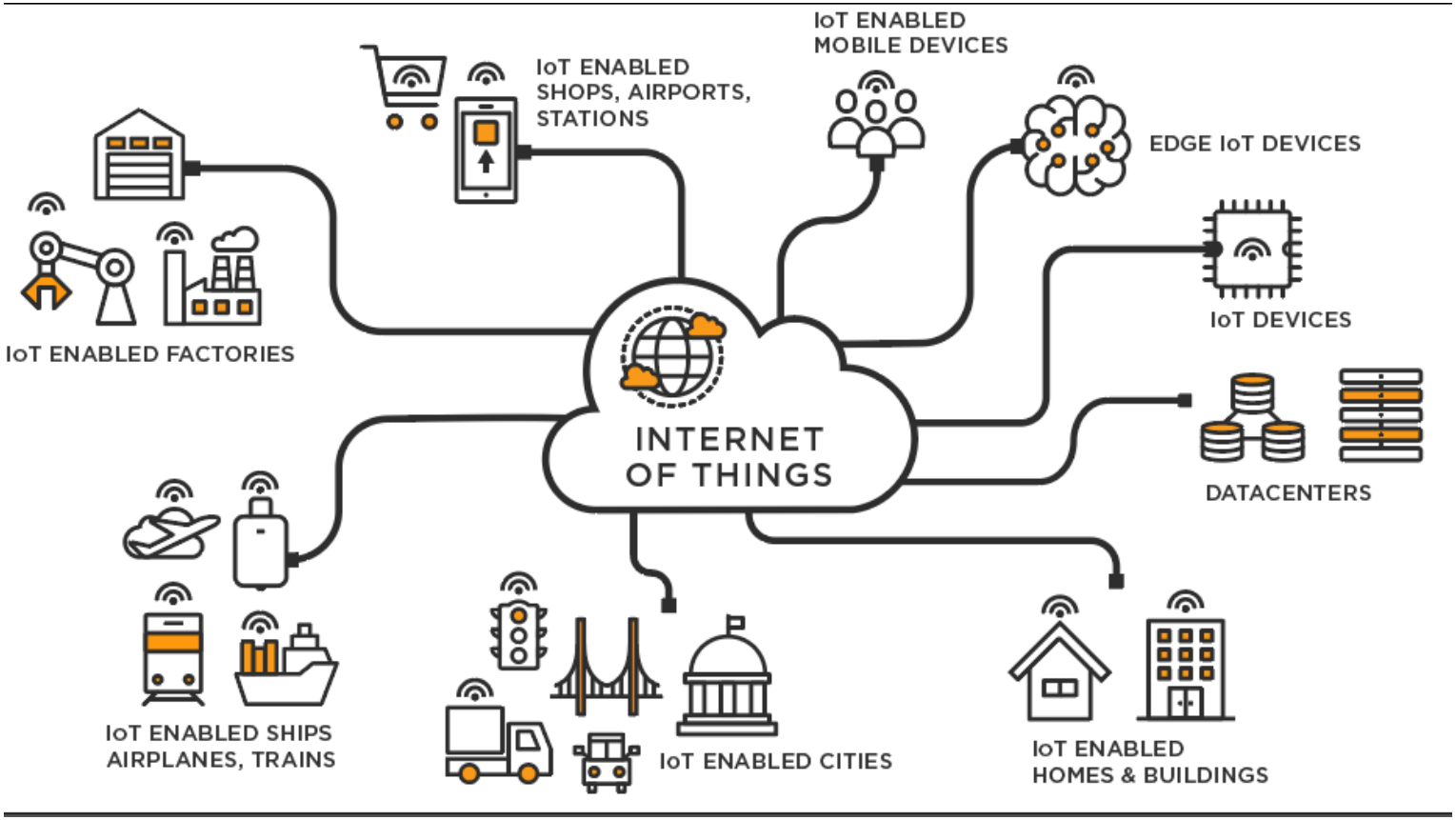
En général, un malware doit se lier à un IOT pour **véritablement** exister.

Interlude



Il existe cependant des malwares qui se propagent par les périphériques de stockage.

Interlude



En résumé, nous pourrions dire qu'un malware a besoin d'un hôte informatique pour exister.

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée
- Présence d'un élément déclencheur

L'éclosion

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée
- Présence d'un élément déclencheur
- . . .

L'implantation

Où s'implante le malware ?

L'implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)

L'implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)

L'implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)

L'implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)

L'implantation

Où s'implante le malware ?

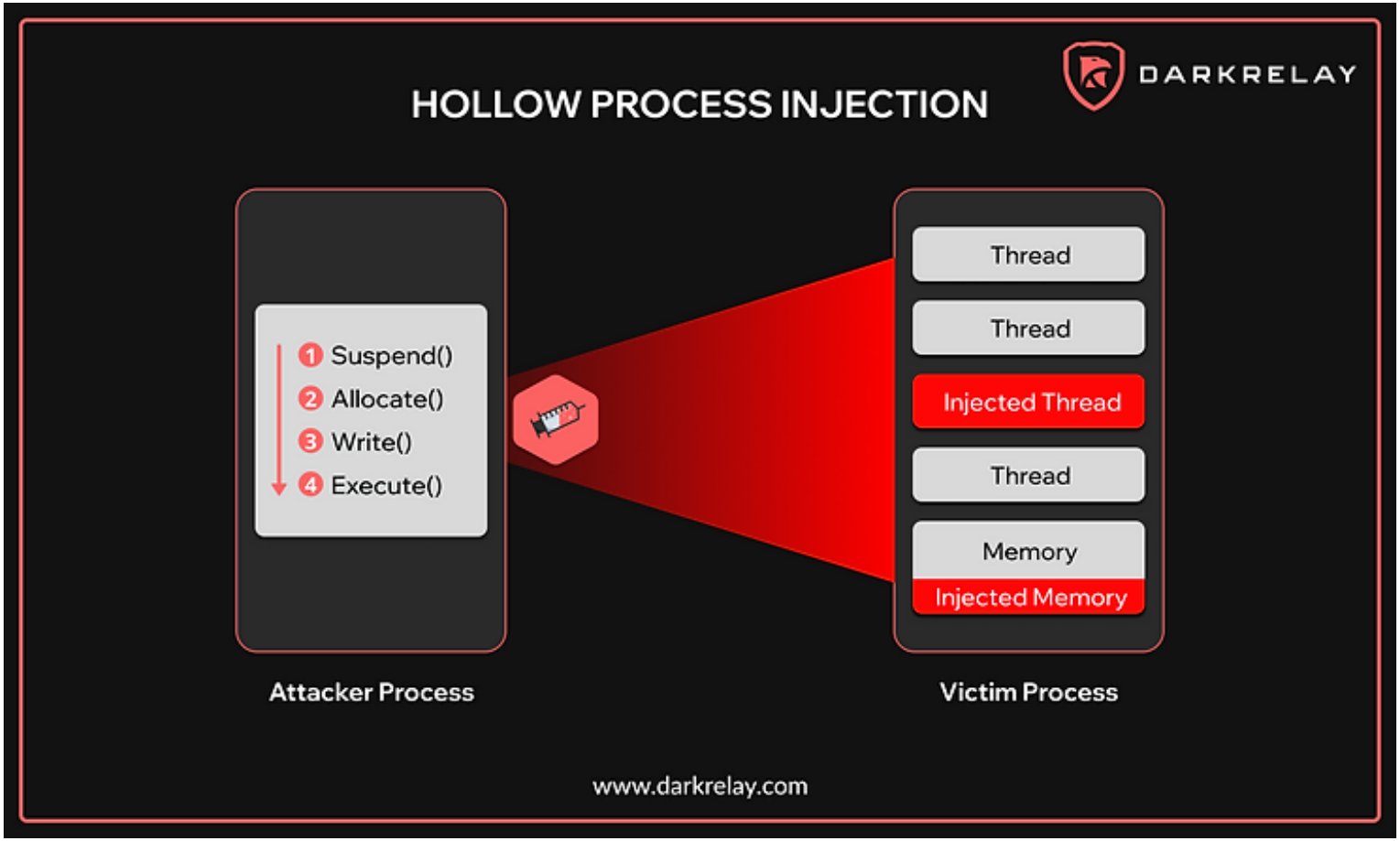
- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)
- À l'exécution d'un programme qui ne semblait pas être un malware

L'implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)
- À l'exécution d'un programme qui ne semblait pas être un malware
- ...

Exemple de Cobalt Strike



La gestation

La gestation

La gestation d'un malware est plus ou moins courte, cette phase peut-être réduite à 0 ou durer plusieurs mois, on parle alors de Command And Control (C&C).

La gestation

Dans l'optique d'échapper à la surveillance des différents systèmes anti-malware, le virus va dialoguer au travers du réseau et se mettre à jour en changeant ainsi sa signature et s'adaptant.

La gestation

Durant ce temps de gestation, le malware a la possibilité de communiquer des informations sur son environnement ou *"simplement"* miner pour le compte de son propriétaire.

La libération

La libération

Après un temps indéterminé (plusieurs années parfois), les chercheurs en cybersécurité trouvent le malware et le signale donc aux éditeurs.

La libération

Cependant, l'hôte n'en a pas pour le moins été infecté et même si l'antivirus indique avoir nettoyé le malware il est possible, voir probable que des éléments aient été corrompus.

La libération

Le système fonctionne donc correctement durant un certain temps mais peut-être avec la maladie.

La naissance

La naissance

Si le malware n'a pas été détecté, celui-ci peut-être programmé pour effectuer une attaque latérale.

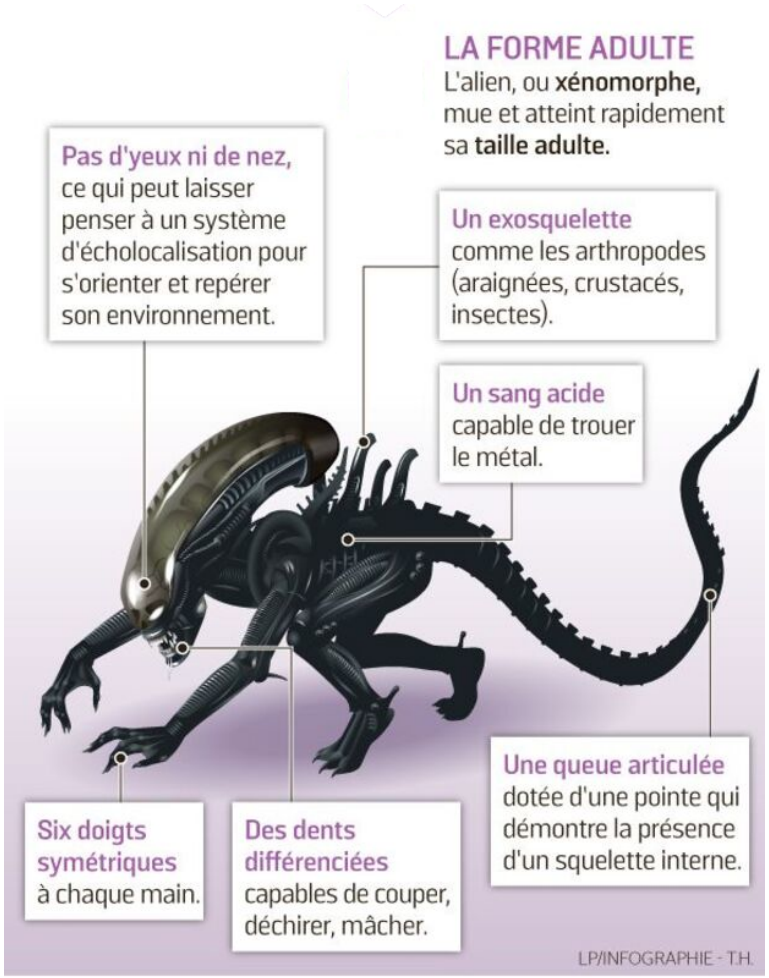
La naissance

Il va donc à son tour infecter les IOTs qui lui sont proches.

La naissance

Et chaque IOT fera alors de même tant que l'infection ne sera pas stoppée.

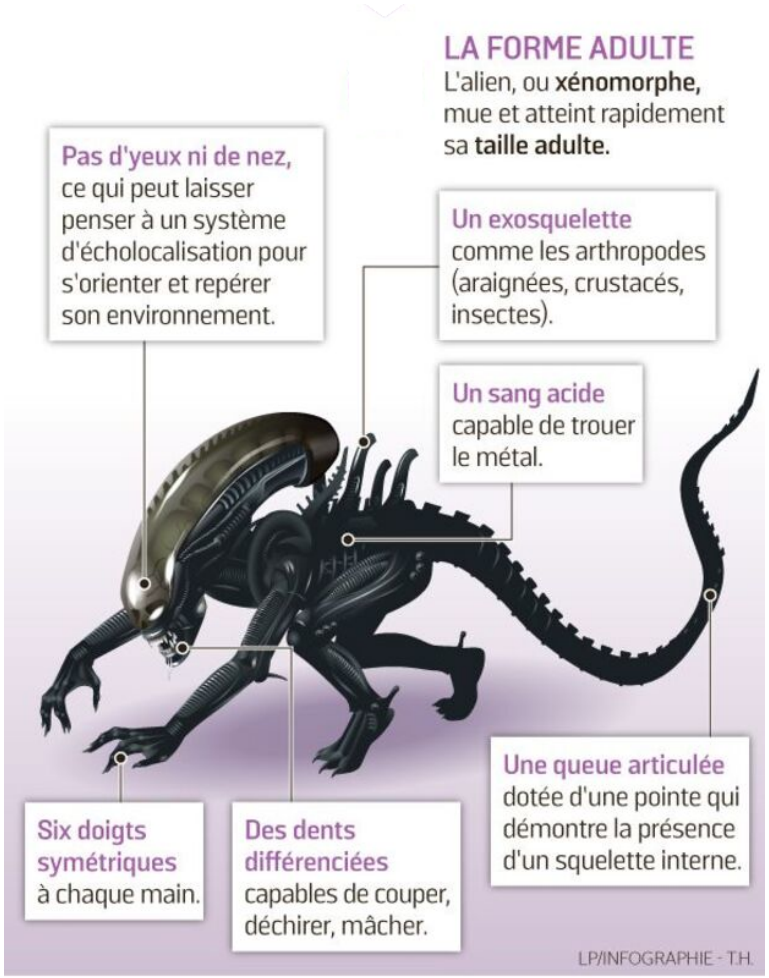
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret

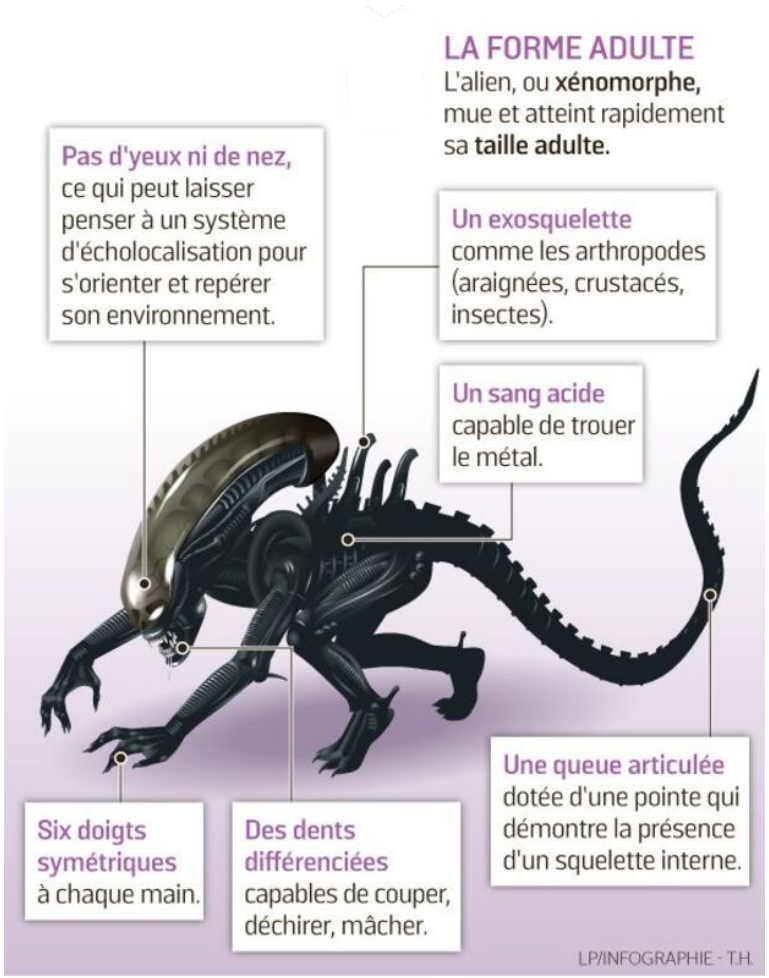
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué

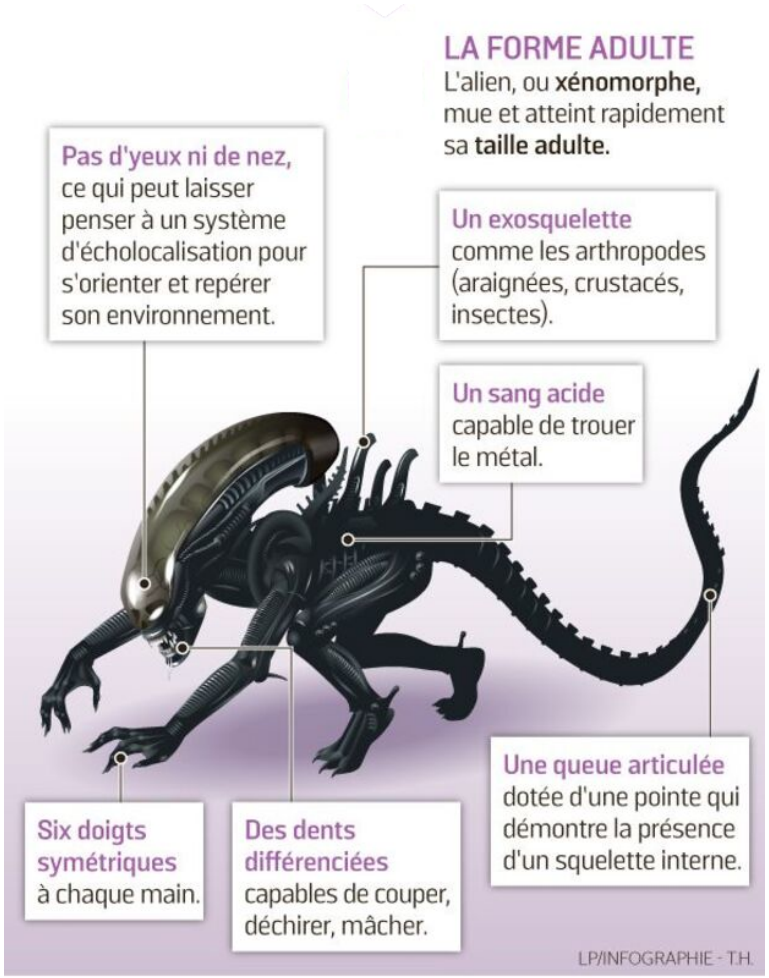
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace

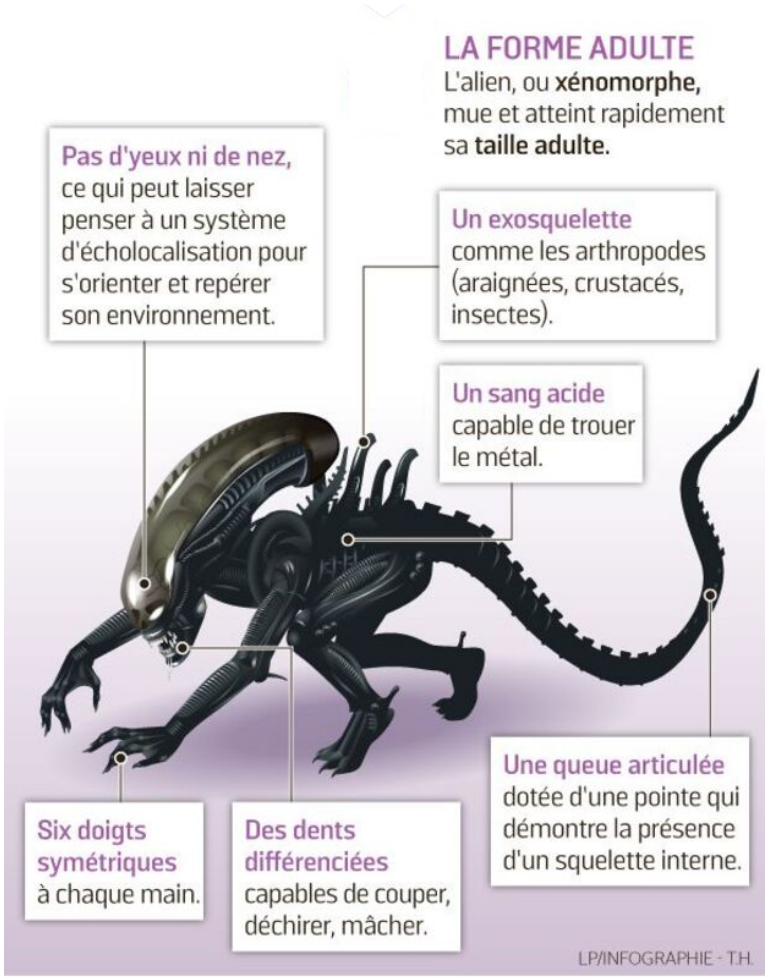
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent

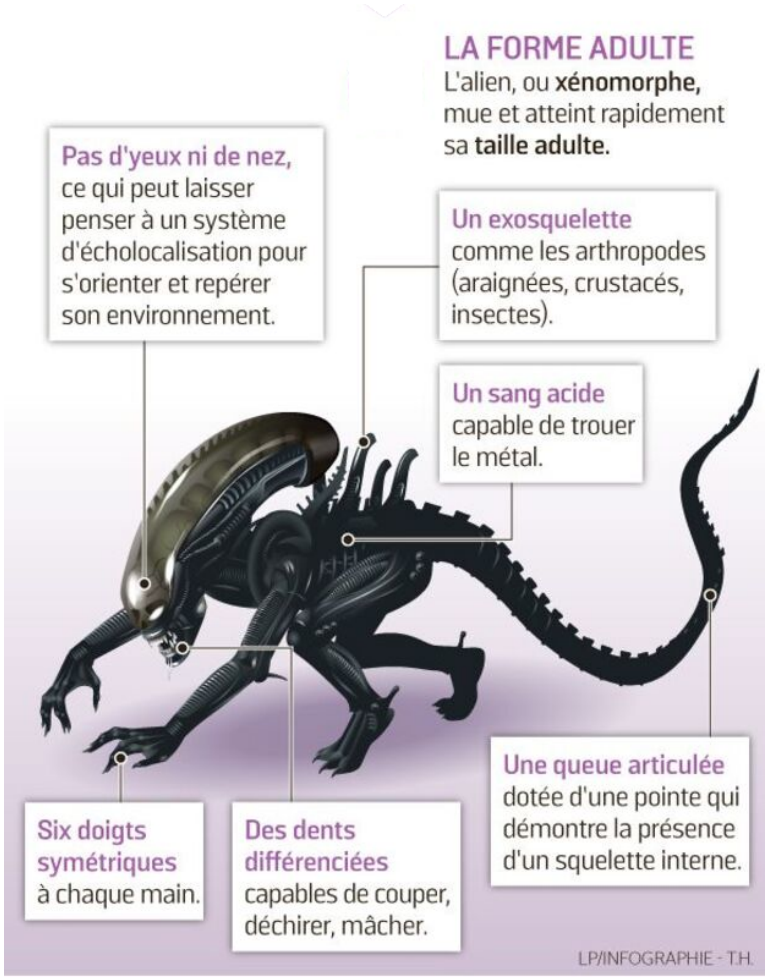
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe

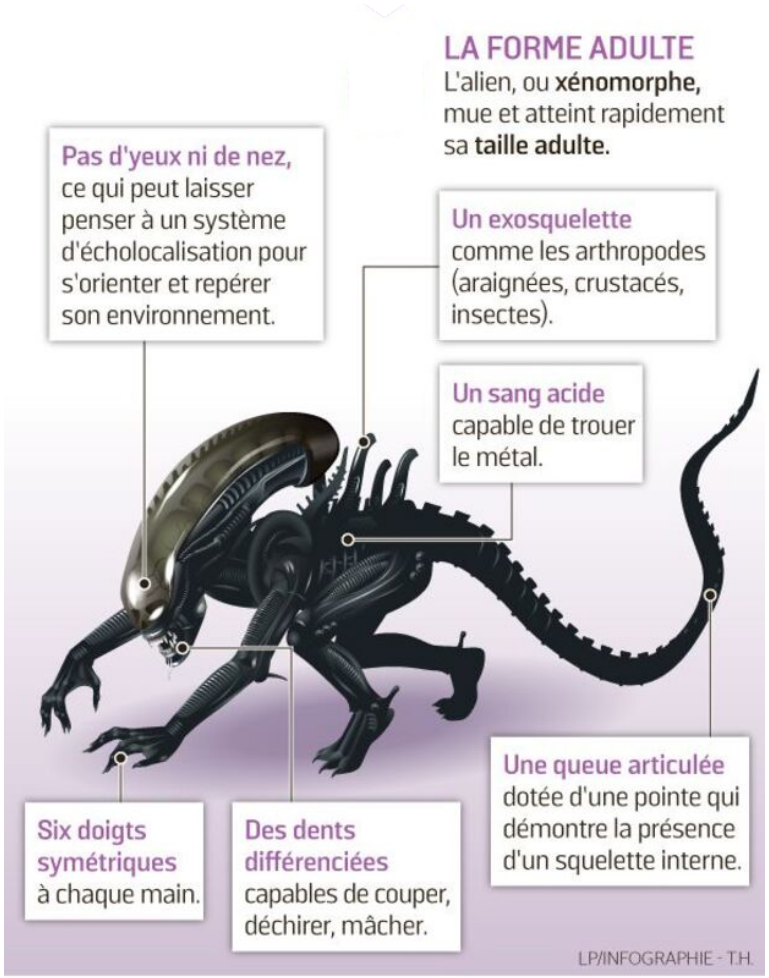
Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe
- Malin

Caractéristiques d'un malware



Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe
- Malin
- ...

Adoptez-moi. . .

Je suis *"cute"* et gratuit . . .

Comme un téléchargement gratuit. . .

Mais je me sers au passage. . .