Se protéger !

Éric BERTHOMIER
eric.berthomier@free.fr

24 novembre 2023

Version 1.9 - Version Stagiaire

Introduction

- Chacun d'entre nous se voit dans sa vie professionnelle ou personnelle confier des projets qui ont pour support l'informatique.

Introduction

- Chacun d'entre nous se voit dans sa vie professionnelle ou personnelle confier des projets qui ont pour support l'informatique.
- Mais l'informatique comme le papier n'est pas exonérée de contraintes liées à son utilisation.

Introduction

- Chacun d'entre nous se voit dans sa vie professionnelle ou personnelle confier des projets qui ont pour support l'informatique.
- Mais l'informatique comme le papier n'est pas exonérée de contraintes liées à son utilisation.
- Le but de cette séquence est de vous permettre de ne pas oublier qu'un accident n'arrive pas qu'aux autres . . .

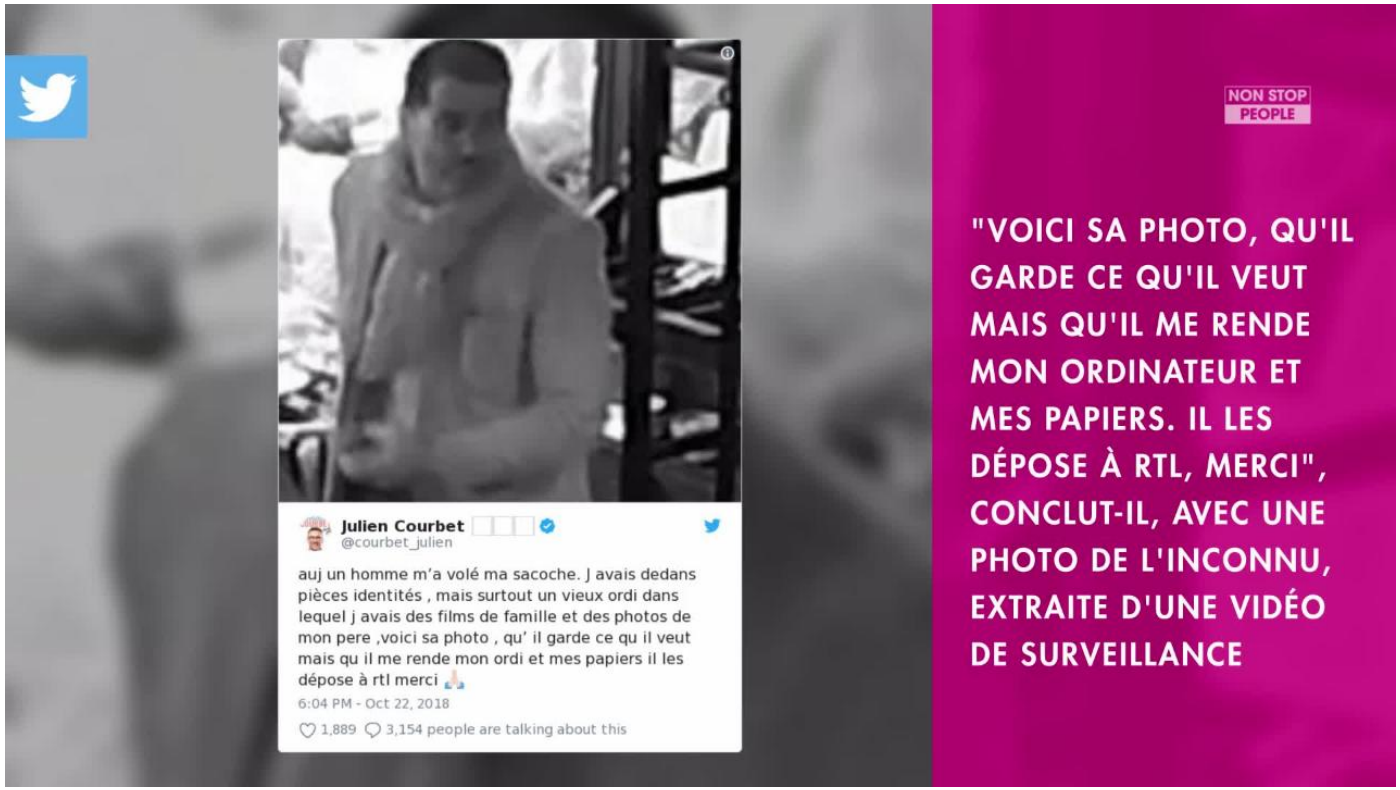
Introduction

- Chacun d'entre nous se voit dans sa vie professionnelle ou personnelle confier des projets qui ont pour support l'informatique.
- Mais l'informatique comme le papier n'est pas exonérée de contraintes liées à son utilisation.
- Le but de cette séquence est de vous permettre de ne pas oublier qu'un accident n'arrive pas qu'aux autres . . .
- Et que la ceinture de sécurité ce n'est pas uniquement pour la voiture...

À vous de jouer : Identifier les menaces

Par groupe ou en individuel, identifier les menaces qui pèsent sur votre travail personnel (votre travail, pas celui de l'entreprise)

Vol


Julien Courbet
@courbet_julien
auj un homme m'a volé ma sacoche. J avais dedans pièces identités , mais surtout un vieux ordi dans lequel j avais des films de famille et des photos de mon pere ,voici sa photo , qu' il garde ce qu il veut mais qu il me rende mon ordi et mes papiers il les dépose à rtl merci
6:04 PM - Oct 22, 2018
1,889 3,154 people are talking about this
NON STOP PEOPLE
"VOICI SA PHOTO, QU'IL GARDE CE QU'IL VEUT MAIS QU'IL ME RENDE MON ORDINATEUR ET MES PAPIERS. IL LES DÉPOSE À RTL, MERCI", CONCLUT-IL, AVEC UNE PHOTO DE L'INCONNU, EXTRAITE D'UNE VIDÉO DE SURVEILLANCE

Perte

Cette clé USB retrouvée dans des déjections de léopards de mer contenait . . .

Perte

Cette clé USB retrouvée dans des déjections de léopards de mer contenait . . .

des photos de lions de mer

Perte

30/10/2017 - Une clé USB contenant des documents confidentiels sur la sécurité de l'aéroport d'Heathrow, à l'ouest de Londres, a été retrouvée par un passant, en pleine rue.

Panne

Défaillance matérielle, système . . .

Virus

Confiance ultime dans votre anti-virus ?

Intrusion

Confiance ultime dans tous les logiciels téléchargés ?

Autre . . .

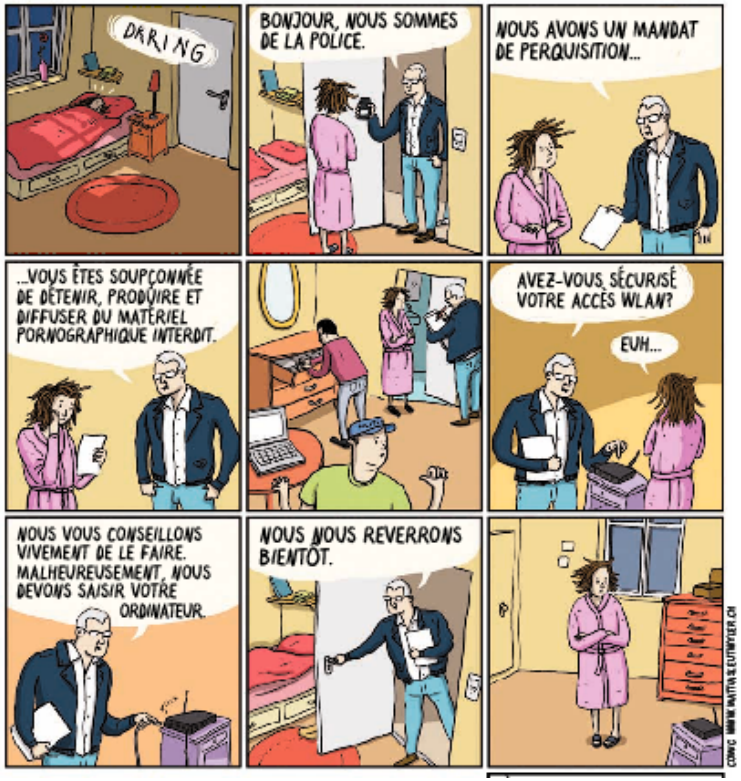
C'est le coup de foudre !!!!

Responsable

Fin de vie

https://insideevs.com/news/419525/tesla-data-leak-personal-info-ebay/

Responsable de sa box



Responsable des données de l'entreprise

La gouvernance de la donnée est un ensemble de processus qui assurent que ces données sont formellement gérées à travers l'entreprise.

Responsable des données de l'entreprise

La gouvernance de la donnée est un ensemble de processus qui assurent que ces données sont formellement gérées à travers l'entreprise.

Elle garantit la fiabilité des informations utilisées pour les processus métier critiques, la prise de décision et la comptabilité.

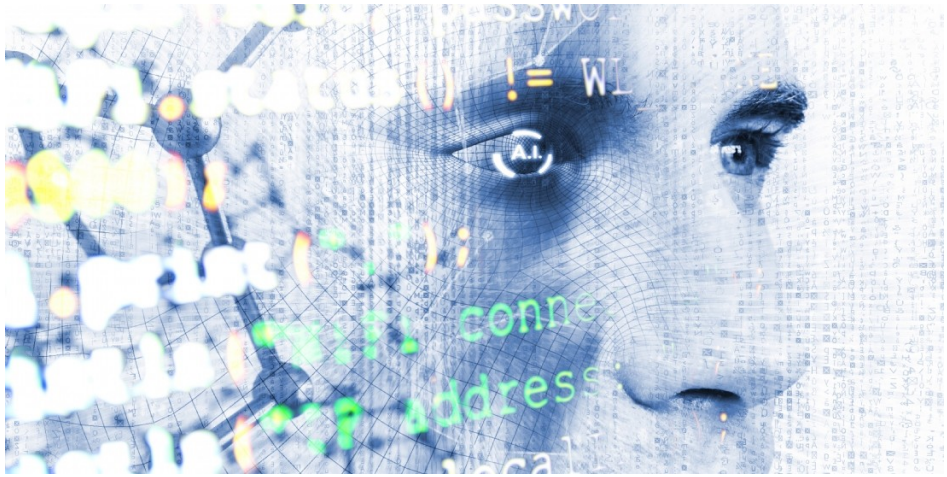
Cloud


DATA VIRUS
MALICIOUS SOFTWARE
THEFT
VIRUS
CYBERWARFARE
HACKING
THE
CLOUD
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
SYSTEM PENETRATION
CYBERSTALKING

Courriels

À vous de jouer : Contrer les menaces

Par groupe ou en individuel, prendre quelques-unes des menaces décrites et indiquer des solutions . . .



On prêtera bien-sûr fort attention au rapport protection / coût

Outils pour l'hygiène informatique

Nombreuses sont les personnes qui donnent des conseils mais rares sont celles qui les reçoivent avec reconnaissance, et encore plus rares celles qui les suivent.

Hagakure : Le Livre secret des samouraïs de Jocho Yamamoto

Introduction à la cryptologie

Vidéo "Comment ça marche la cryptographie"

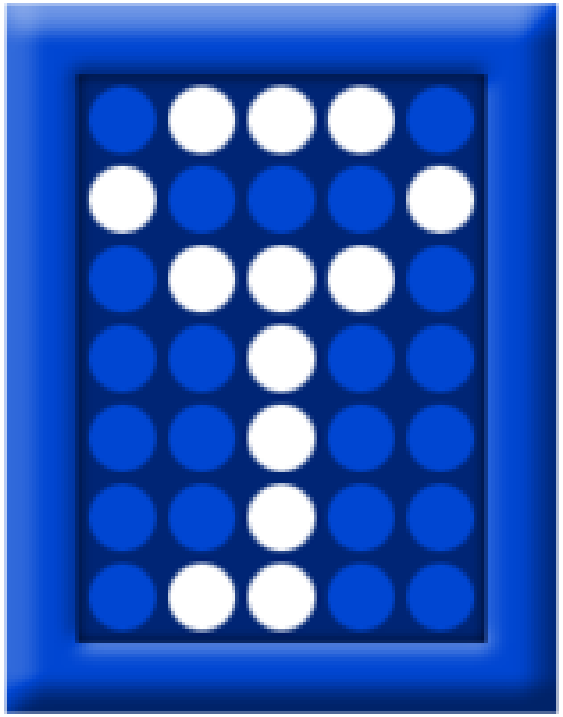
Câble anti-vol

Bitlocker

Documentation officielle BitLocker

Tutoriel - Malekal : BitLocker : chiffrer son disque dur sur Windows 10 Pro

TrueCrypt



https://truecrypt.fr/

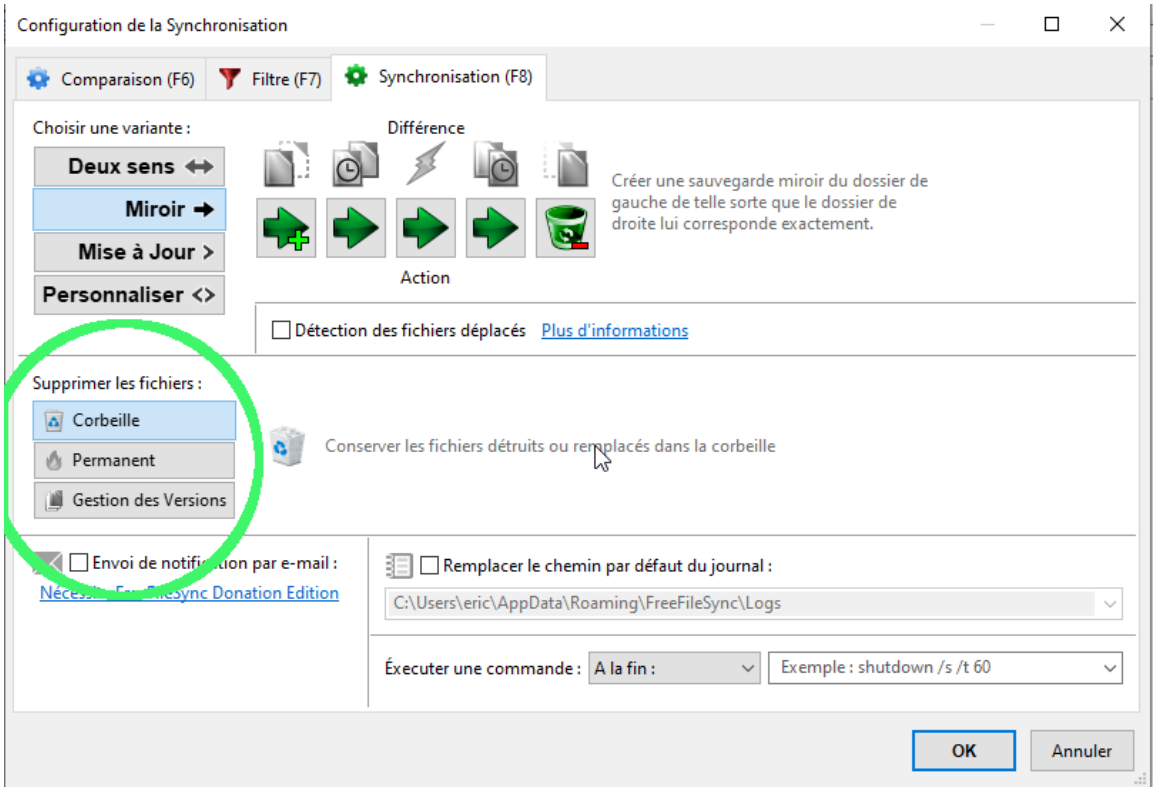
FreeFileSync

`https://freefilesync.org/`

Tutoriel - Malekal : FreeFileSync

FreeFileSync - Attention à la Poubelle !

Par défaut la synchronisation, envoie les fichiers supprimés à la corbeille ce qui peut vite devenir problématique. . .



FreeFileSync - Comparer / Sauvegarder

Une sauvegarde FreeFileSync s'effectue en 2 étapes :

1 - Comparaison des fichiers

Cette comparaison est paramétrable. . .

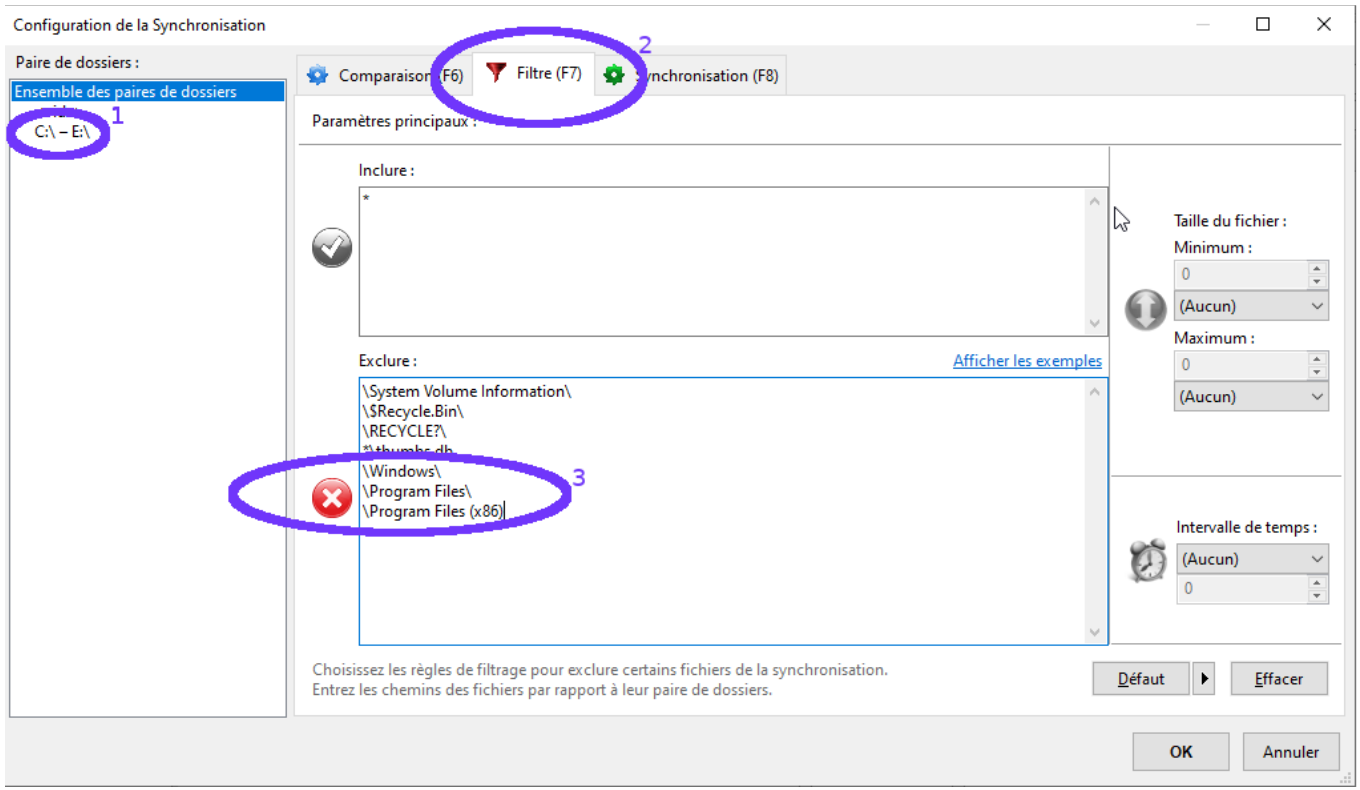
FreeFileSync - Comparer / Sauvegarder

Une sauvegarde FreeFileSync s'effectue en 2 étapes :

2 - Sauvegarde des fichiers

FreeFileSync - Sauvegarde tout (ce qu'il faut)

Vous avez peur d'oublier des éléments de votre travail et ne savez pas quoi sauvegarder, voici un moyen de tout sauvegarder sauf Windows et les programmes.



Clonezilla

`https://clonezilla.org/`

Tutoriel - Malekal : Clonezilla : créer et restaurer une image système

EICAR

eicar.org : European Institute for Computer Anti-Virus Research

amtso.org : Anti-Malware Testing Standards Organization

Limitation de l'antivirus

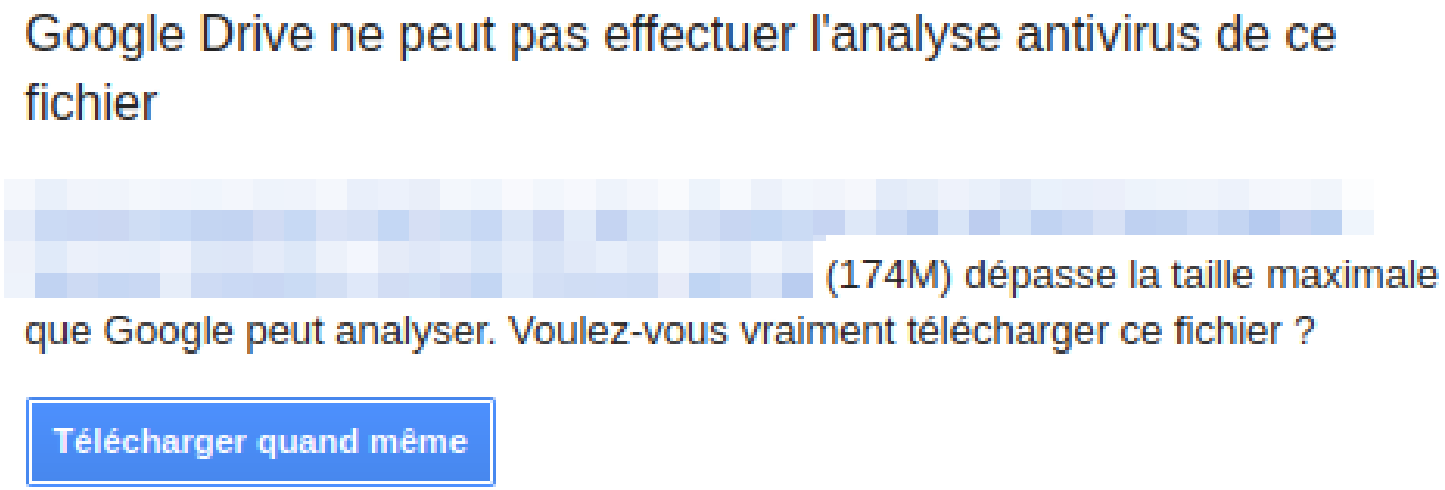
Vérifiez le fonctionnement de votre anti-virus en téléchargeant les différents éléments de cette page (eicar*.zip)) :

`https://exercices.ericberthomier.fr/eicar/`

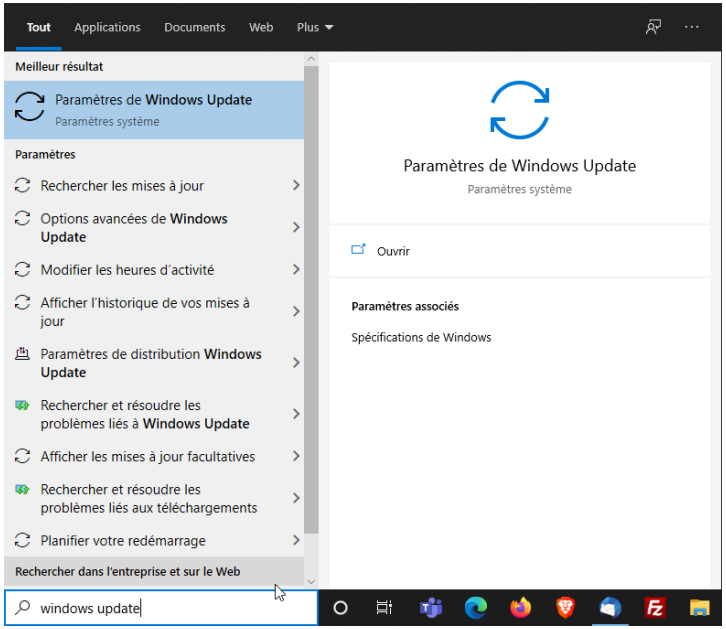
Limitation de l'antivirus

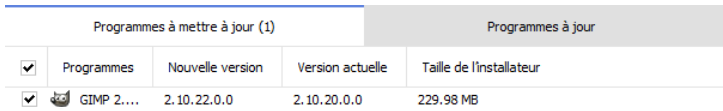
Vérifiez le fonctionnement de votre anti-virus en téléchargeant les différents éléments de cette page (eicar*.zip)) :

`https://exercices.ericberthomier.fr/eicar/`



Mise à jour du système et des logiciels



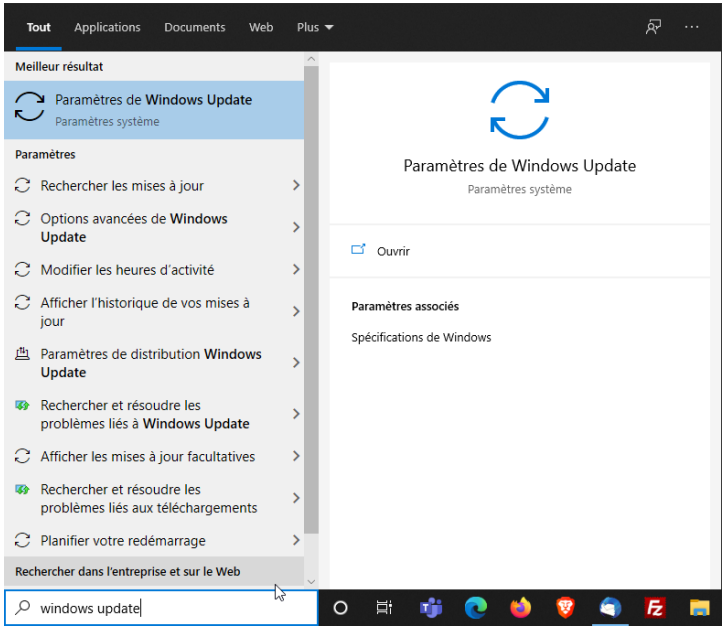


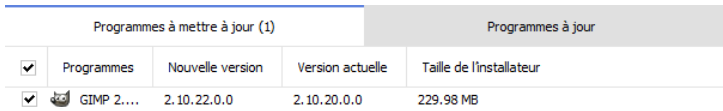
Système : Windows Update

Logiciels

Il est impératif de mettre à jour les logiciels

Mise à jour du système et des logiciels



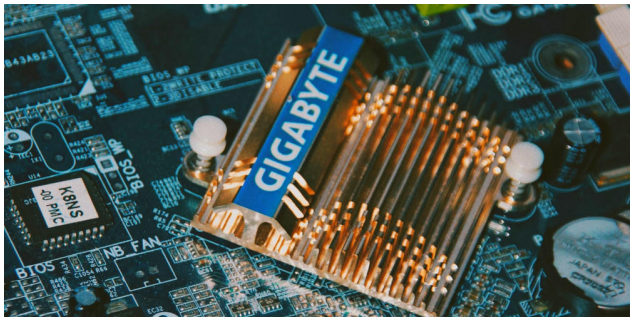


Système : Windows Update

Logiciels

Il est impératif de mettre à jour les logiciels
notamment ceux qui communiquent.
Messagerie / Navigateur / Assistance à distance . . .

Un driver pour stopper les antivirus !

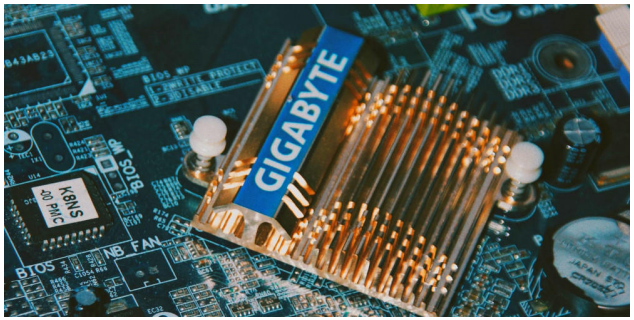


Les pirates :

1. Se connectent sur un réseau

Source : ZDNet

Un driver pour stopper les antivirus !

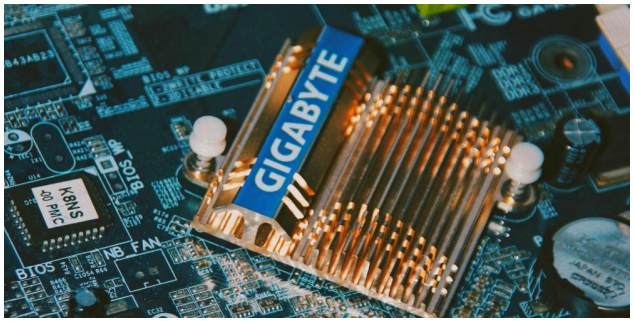


Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)

Source : ZDNet

Un driver pour stopper les antivirus !



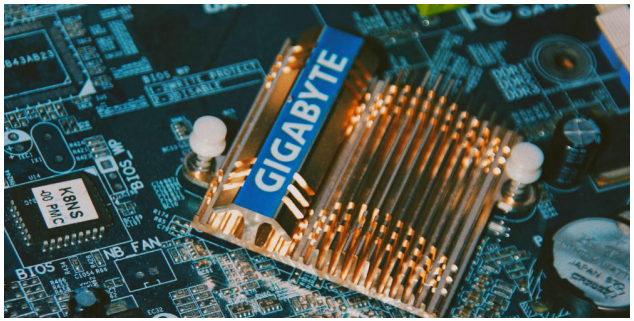
3. Utilisent une faille de sécurité de ce pilote **légitime** pour accéder au noyau

Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)

Source : ZDNet

Un driver pour stopper les antivirus !

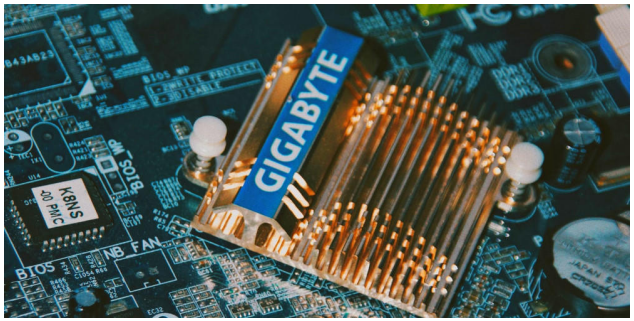


Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)
3. Utilisent une faille de sécurité de ce pilote **légitime** pour accéder au noyau
4. Utilisent l'accès au noyau pour désactiver la vérification des signatures des pilotes.

Source : ZDNet

Un driver pour stopper les antivirus !

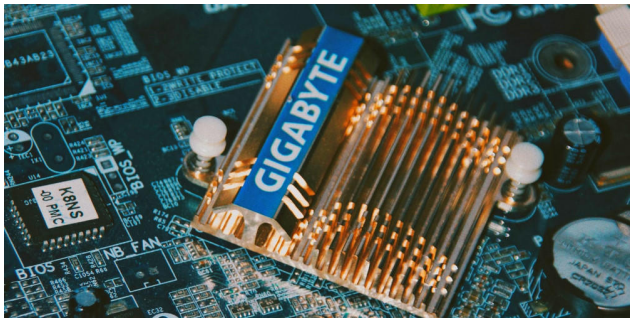


Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)
3. Utilisent une faille de sécurité de ce pilote **légitime** pour accéder au noyau
4. Utilisent l'accès au noyau pour désactiver la vérification des signatures des pilotes.
5. Installent un pilote de noyau malveillant

Source : ZDNet

Un driver pour stopper les antivirus !

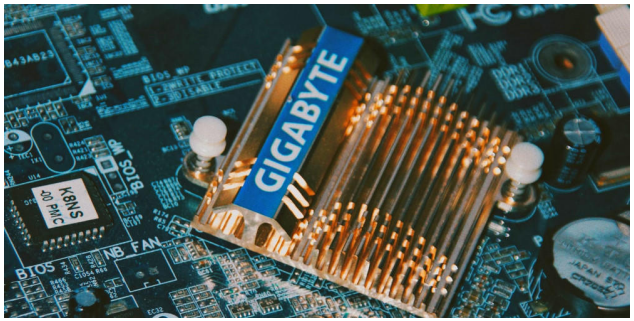


Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)
3. Utilisent une faille de sécurité de ce pilote **légitime** pour accéder au noyau
4. Utilisent l'accès au noyau pour désactiver la vérification des signatures des pilotes.
5. Installent un pilote de noyau malveillant
6. Désactivent l'antivirus

Source : ZDNet

Un driver pour stopper les antivirus !



Les pirates :

1. Se connectent sur un réseau
2. Installent le pilote légitime de Gigabyte (`gdrv.sys`)
3. Utilisent une faille de sécurité de ce pilote **légitime** pour accéder au noyau
4. Utilisent l'accès au noyau pour désactiver la vérification des signatures des pilotes.
5. Installent un pilote de noyau malveillant
6. Désactivent l'antivirus
7. Exécutent le ransomware RobbinHood.

Source : ZDNet

18 Octobre 2022 - Microsoft, mauvais élève !

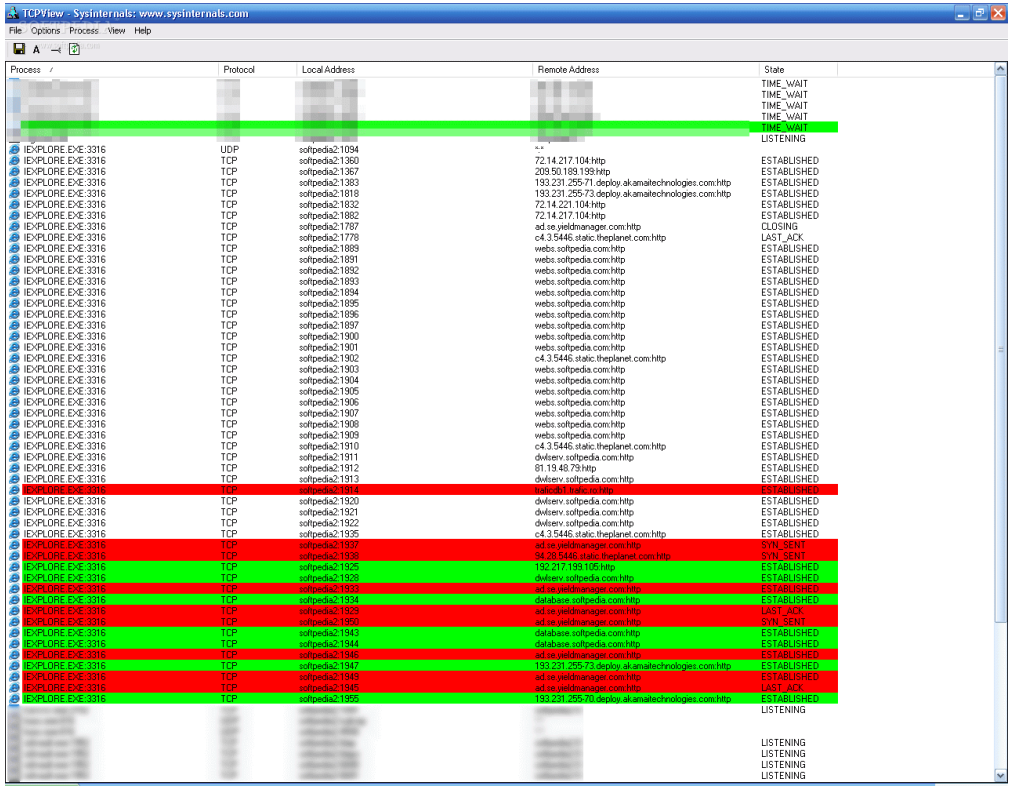
Pour déjouer la technique d'infection *" bring your own vulnerable driver "* (BYOVD), Microsoft expliquait depuis 2 ans avoir mis en place dans son système de mises à jour une liste noire des pilotes dangereux permettant de bloquer toute installation d'un de ces pilotes.
En effet, la technique BYOVD consiste à installer un pilote connu pour contenir une faille de sécurité puis de l'exploiter. Problème, comme l'a découvert Ars Technica, cette liste n'était pas mise à jour correctement, laissant les systèmes d'exploitation de Microsoft faillibles à ce genre d'attaques.
Microsoft a publié un outil permettant de mettre à jour la liste des pilotes dangereux de ces trois dernières années mais, comme l'expliquent nos confrères,

18 Octobre 2022 - Microsoft, mauvais élève !

Pour déjouer la technique d'infection " *bring your own vulnerable driver* " (BYOVD), Microsoft expliquait depuis 2 ans avoir mis en place dans son système de mises à jour une liste noire des pilotes dangereux permettant de bloquer toute installation d'un de ces pilotes.
En effet, la technique BYOVD consiste à installer un pilote connu pour contenir une faille de sécurité puis de l'exploiter. Problème, comme l'a découvert Ars Technica, cette liste n'était pas mise à jour correctement, laissant les systèmes d'exploitation de Microsoft faillibles à ce genre d'attaques.
Microsoft a publié un outil permettant de mettre à jour la liste des pilotes dangereux de ces trois dernières années mais, comme l'expliquent nos confrères, **c'est une mise à jour exceptionnelle et il nest pas certain que Microsoft puisse la faire régulièrement.**

Source : NextImpact

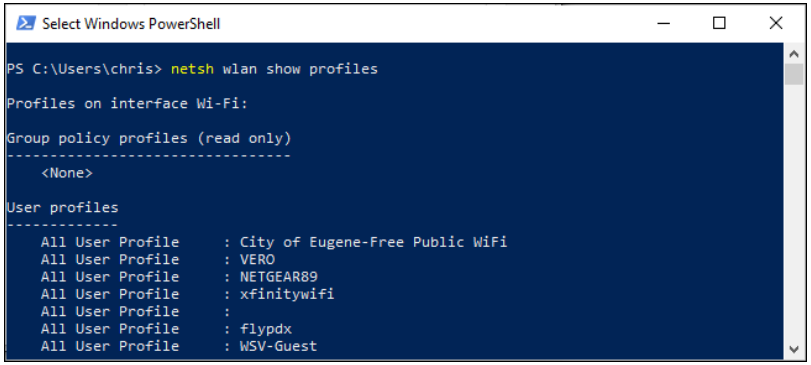
TcpView



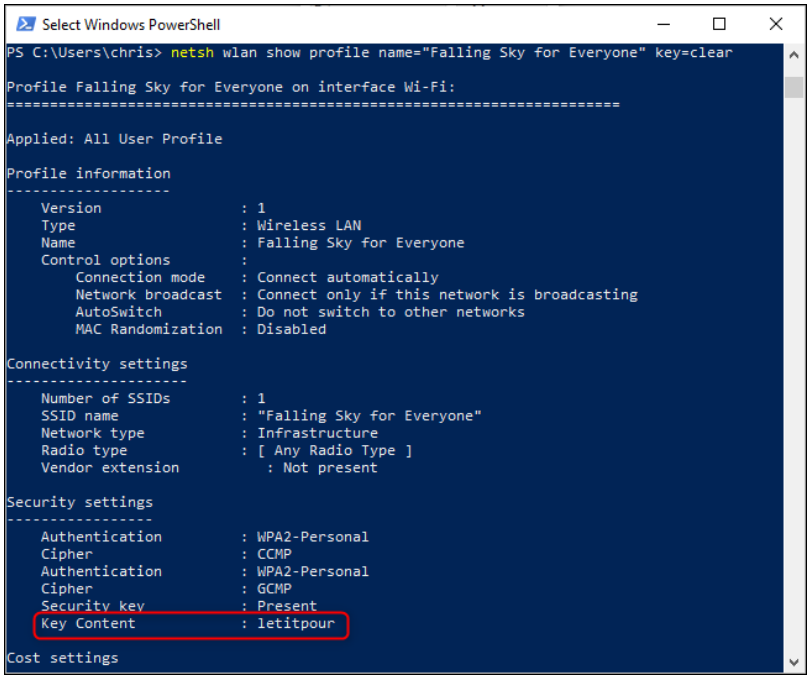
Sysinternals Suite(Module de formation spécifique)

Mes clés Wifi

+ X, et choisir "PowerShell".



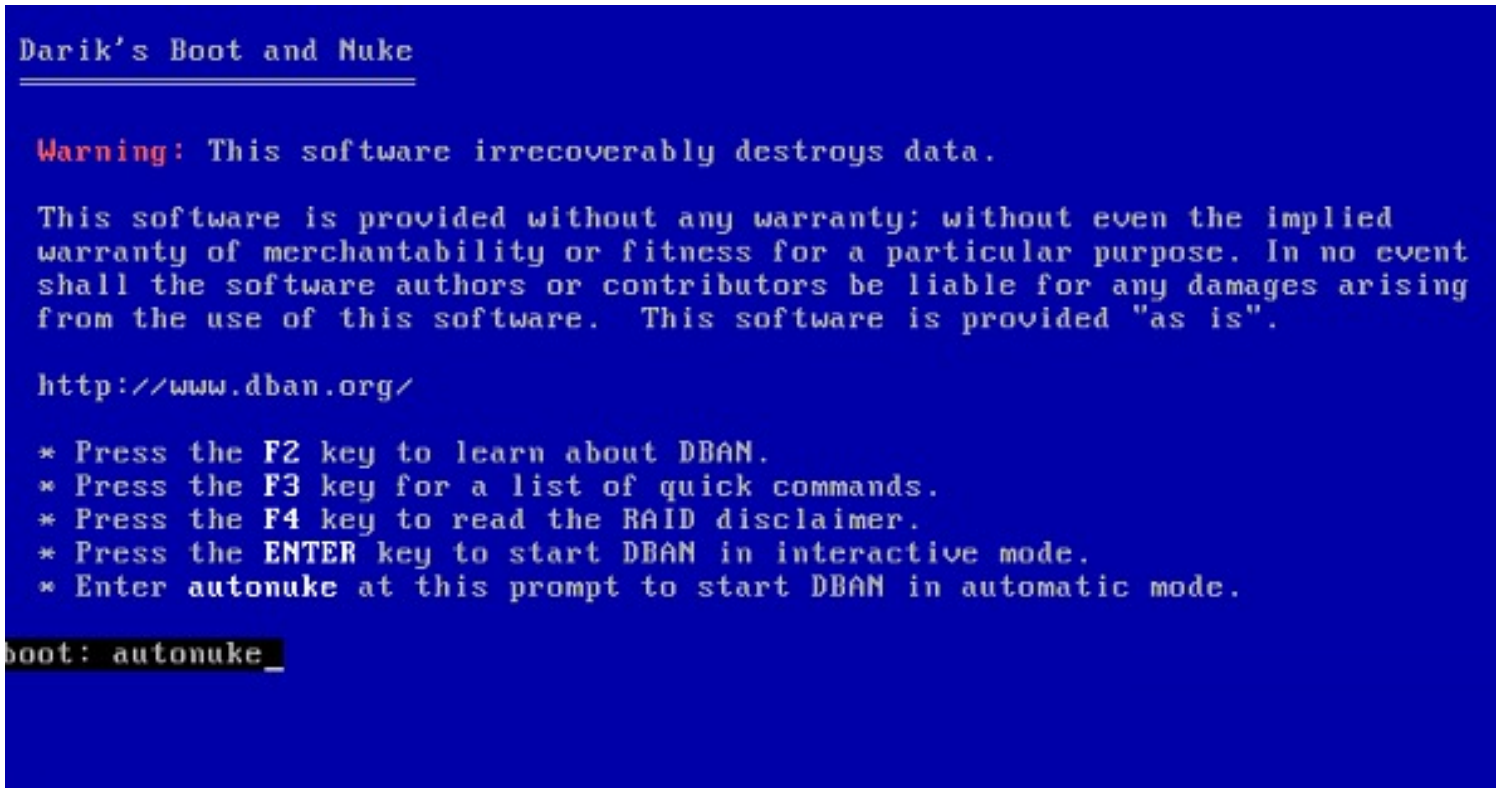
netsh wlan show profiles



netsh wlan show profile name="NETWORK" key=clear

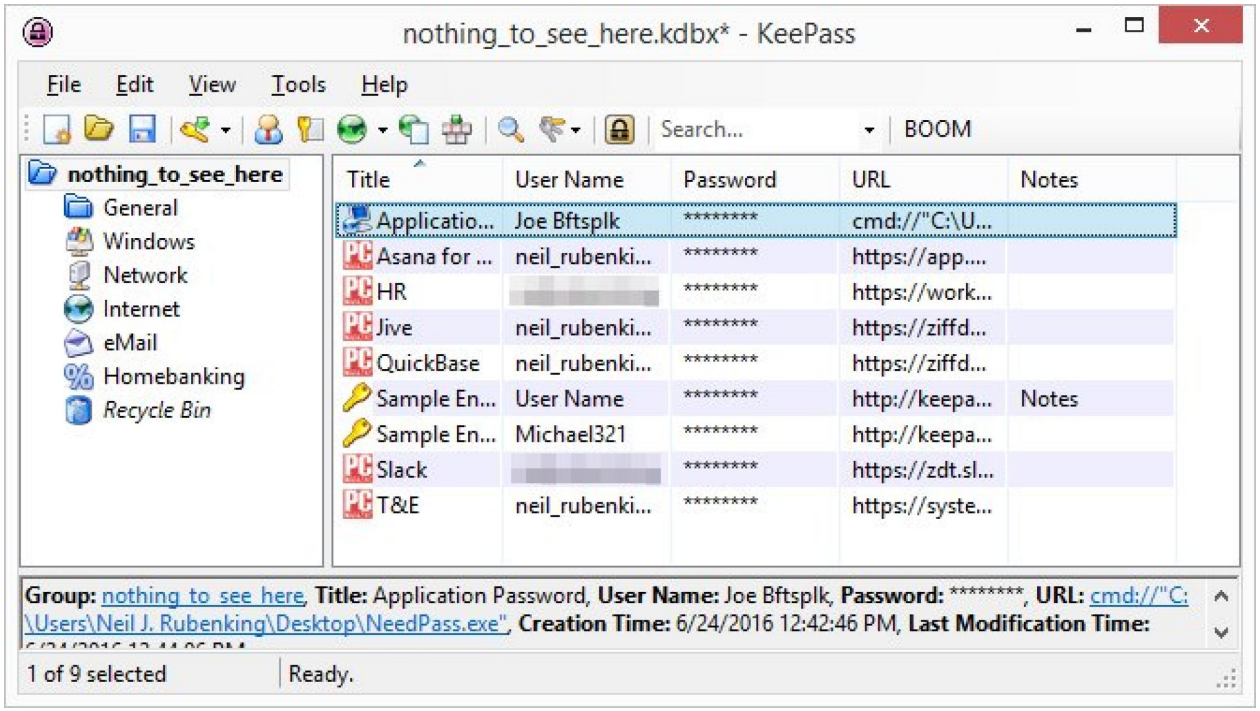
Onduleur

DBan



https://dban.org/

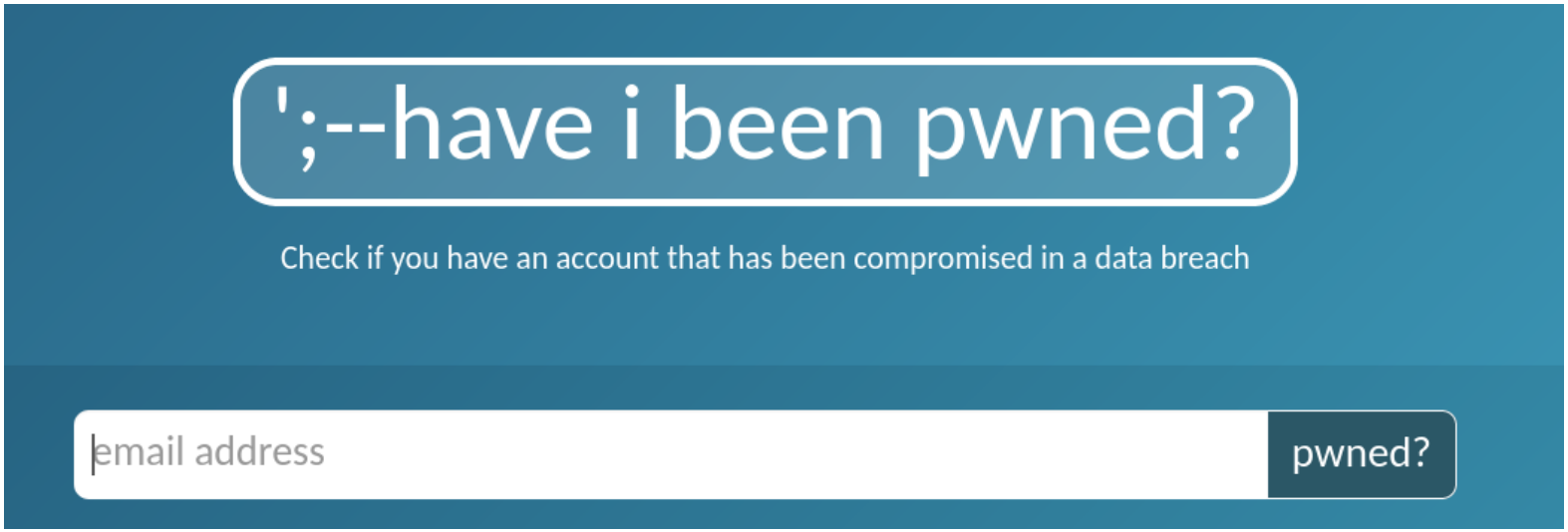
KeePass



`https://keepass.info/`

Tutoriel - Malekal : KeePass : utiliser le gestionnaire de mot de passe gratuit

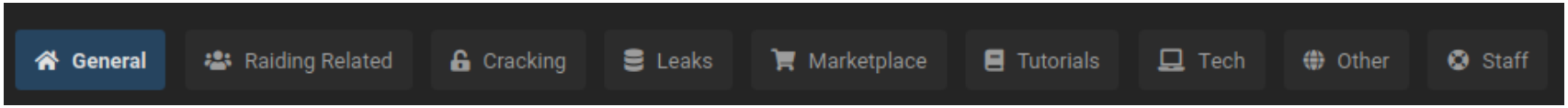
Ai-je été compromis ?



https://haveibeenpwned.com/

Je souhaite acheter ...

Raid Forums



GpgForWin

`https://www.gpg4win.org/`(Module de formation spécifique)

Conclusion


CONCLUSION
"Odin" par Jarry et Seure-Le Bihan © éditions Soleil

Hygiène informatique

À l'image de la ceinture, une bonne hygiène de sécurité informatique peut vous protéger de presque tout . . .

RGPD : Législation des bonnes pratiques

Être conforme au **25 mai 2018**

Amendes jusqu'à **4% du CA** annuel global ou 20M€

Garantir **la sécurité de toutes les données** collectées, traitées et stockées

Garantir aux personnes physiques l'**accès**, la **modification**, la **restitution** et l'**effacement** de leurs données

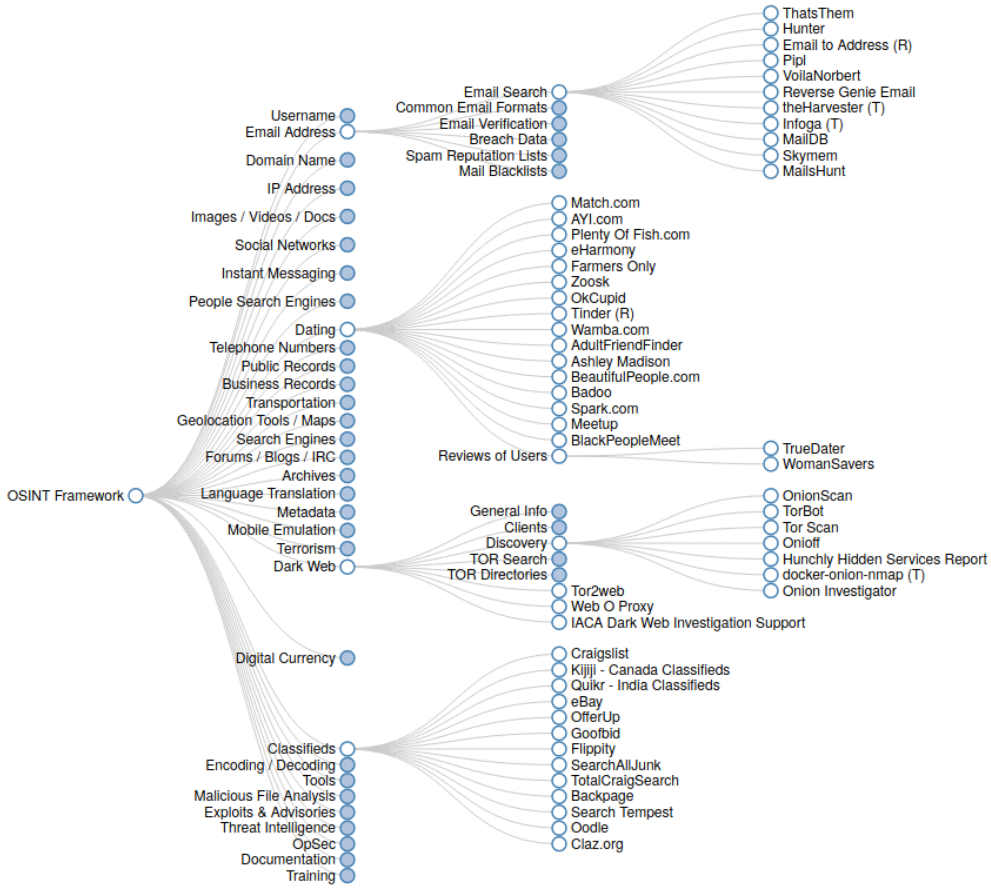
Notifier la **CNIL**, **sous 72h** en cas de risque réel d'atteinte à la protection de la vie privée

Recueillir et prouver le **consentement** éclairé des individus

Documenter les **mesures** et les **procédures** de protection

Sécuriser les données contre les risques de perte, de vol ou de divulgation

OSINT : S'auditer c'est mieux !



https://osintframework.com/

Amnésie informatique . . .

https://www.nirsoft.net/
https://www.nirsoft.net/utils/computer_turned_on_times.html
https://www.nirsoft.net/utils/computer_activity_view.html

Protéger son identité : Tails (Clé USB Bootable)

Qui l'utilise ?

Des activistes
utilisent Tails afin de cacher leurs identités, contourner la censure et communiquer en sécurité.

Des journalistes et leurs sources
utilisent Tails pour rendre publique des informations sensibles et accéder à internet depuis des endroits peu sûrs.

Des survivant-e-s de violences domestiques
utilisent Tails pour échapper à la surveillance à la maison.

Vous
à partir du moment où vous avez besoin de plus d'intimité dans ce monde numérique.

`https://tails.boum.org`