

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 . . .



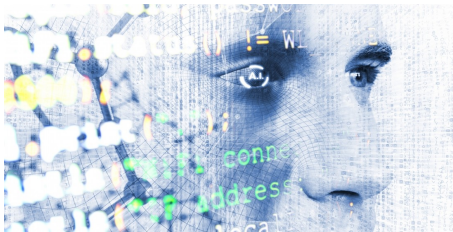
Introduction

- 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



RÉCUPÉRATION d'ordinateurs

Éliminez l'encombrement occasionné par vos vieux ordinateurs et récupérez de l'espace dans vos locaux.

- ▶ Entreprise
- ▶ Commerce
- ▶ Institution

Nous **revalorisons**, **reconditionnons** ou **récupérons** vos vieux ordinateurs et autres équipements électroniques de bureau.

Nous offrons un **service de cueillette**.

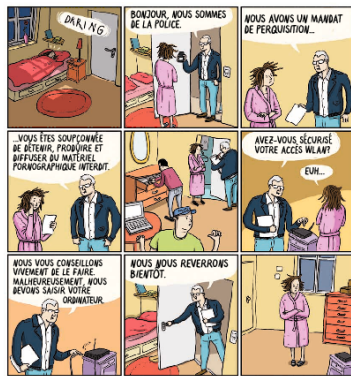
Contactez-nous pour une **estimation sans frais**!



<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



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

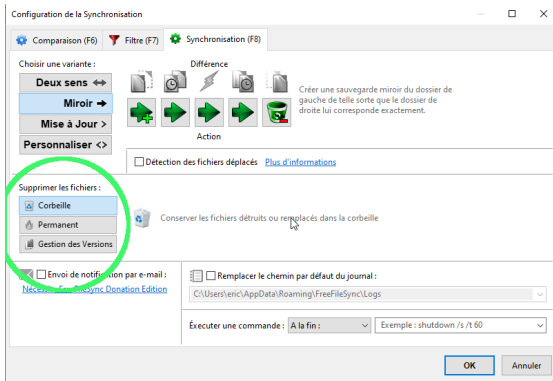


<https://freefilesync.org/>
Tutoriel - Malekal : FreeFileSync



FreeFileSync - Attention à la Poubelle !

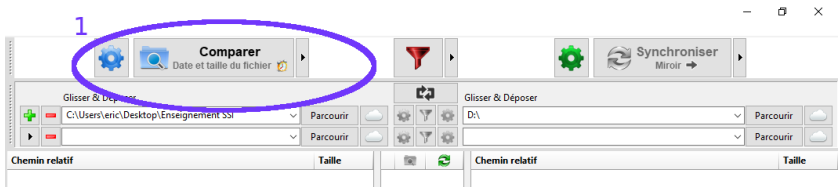
Par défaut la synchronisation, envoie les fichiers supprimés à la corbeille ce qui peut vite devenir problématique. . .



FreeFileSync - Comparer / Sauvegarder

Une sauvegarde FreeFileSync s'effectue en 2 étapes :

1 - Comparaison des fichiers



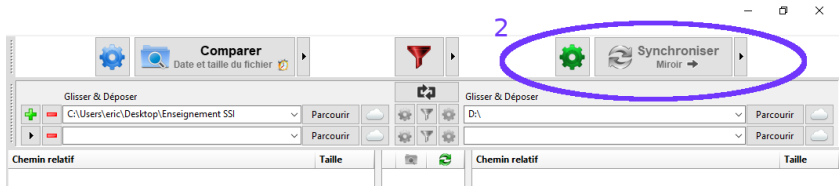
Cette comparaison est paramétrable. . .



FreeFileSync - Comparer / Sauvegarder

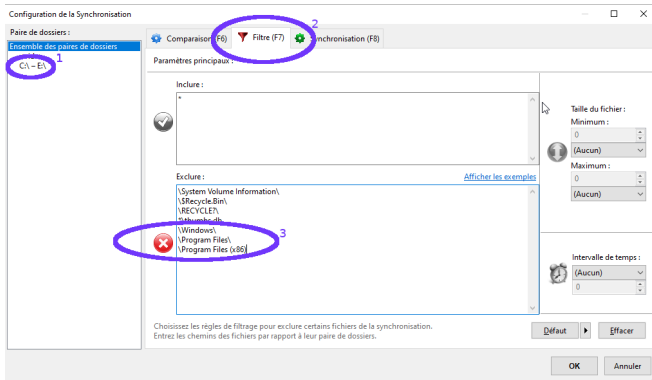
Une sauvegarde FreeFileSync s'effectue en 2 étapes :

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/`

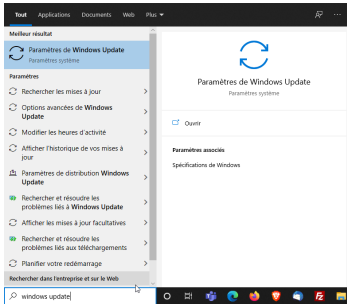
Google Drive ne peut pas effectuer l'analyse antivirus de ce fichier

(174M) dépasse la taille maximale que Google peut analyser. Voulez-vous vraiment télécharger ce fichier ?

Télécharger quand même



Mise à jour du système et des logiciels



Système : Windows Update

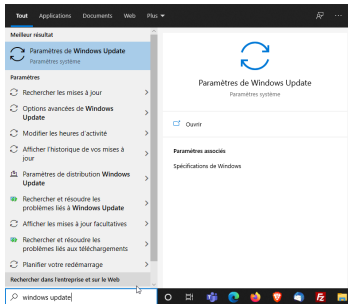
Programmes à mettre à jour (1)			Programmes à jour	
Programmes	Nouvelle version	Version actuelle	Taille de l'installateur	
☒ GIMP 2....	2.10.22.0.0	2.10.20.0.0	229.98 MB	

Logiciels

Il est impératif de mettre à jour les logiciels



Mise à jour du système et des logiciels



Programmes à mettre à jour (1)			Programmes à jour	
	Programmes	Nouvelle version	Version actuelle	Taille de l'installateur
☒	GIMP 2....	2.10.22.0.0	2.10.20.0.0	229.98 MB

Système : Windows Update

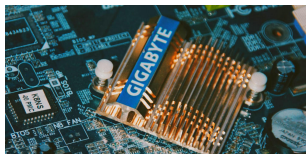
Logiciels

Il est impératif de mettre à jour les logiciels
notamment ceux qui communiquent.

Messagerie / Navigateur / Assistance à distance ...



Un driver pour stopper les antivirus !



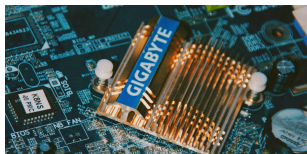
Les pirates :

- 1 Se connectent sur un réseau

Source : ZDNet



Un driver pour stopper les antivirus !



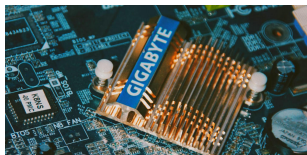
Les pirates :

- 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

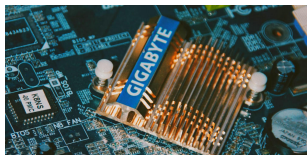
Les pirates :

- 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 :

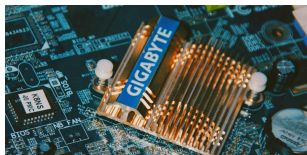
- 1 Se connectent sur un réseau
- 2 Installent le pilote légitime de Gigabyte (gdrv.sys)

- 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 :

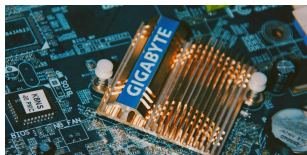
- 1 Se connectent sur un réseau
- 2 Installent le pilote légitime de Gigabyte (gdrv.sys)

- 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 :

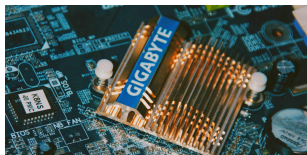
- 1 Se connectent sur un réseau
- 2 Installent le pilote légitime de Gigabyte (gdrv.sys)

- 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 n'est pas certain que Microsoft puisse la faire régulièrement.**

Source : NextImpact



TcpView

[illegible]

Sysinternals Suite (Module de formation spécifique)



Mes clés Wifi

 + X, et choisir "PowerShell".

```
Select Windows PowerShell

PS C:\Users\chris> netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
-----
<None>

User profiles
-----
All User Profile : City of Eugene-Free Public WiFi
All User Profile : VERO
All User Profile : NETGEAR89
All User Profile : xfinitywifi
All User Profile : 
All User Profile : flypdx
All User Profile : WSV-Guest
```

netsh wlan show profiles

```
Select Windows PowerShell

PS C:\Users\chris> netsh wlan show profile name="Falling Sky for Everyone" key=clear

Profile falling Sky for Everyone on interface Wi-Fi:
-----

Applied: All User Profile

Profile information
-----
Version                : 1
Type                   : Wireless LAN
Name                   : Falling Sky for Everyone
Control options        : 
Connection mode        : Connect automatically
Network broadcast      : Connect only if this network is broadcasting
AutoSwitch             : Do not switch to other networks
MAC Randomization      : Disabled

Connectivity settings
-----
Number of SSIDs        : 1
SSID name              : "Falling Sky for Everyone"
Network type           : Infrastructure
Radio type             : [ Any Radio Type ]
Vendor extension        : Not present

Security settings
-----
Authentication         : WPA2-Personal
Cipher                 : CCMP
Authentication         : WPA2-Personal
Cipher                 : CCMP
Security key           : Present
Key Content             : letitpour

Cost settings
```

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



Onduleur



DBan

Darik's Boot and Nuke

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

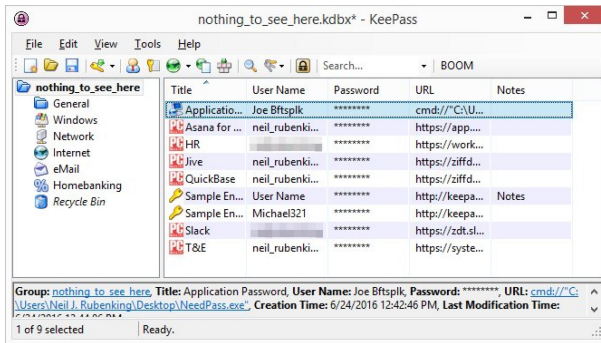
- * Press the **F2** key to learn about DBAN.
- * Press the **F3** key for a list of quick commands.
- * Press the **F4** key to read the RAID disclaimer.
- * Press the **ENTER** key to start DBAN in interactive mode.
- * Enter **autonuke** at this prompt to start DBAN in automatic mode.

boot: autonuke_

<https://dban.org/>



KeePass



<https://keepass.info/>
Tutoriel - Malekal : KeePass : utiliser le gestionnaire de mot de
passe gratuit



Ai-je été compromis ?

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

<https://haveibeenpwned.com/>



Je souhaite acheter ...

Pages (2): 1 2 Next »

pompompurin



000000000000000000000000
000000000000000000000000

Posts 194
Threads 12
Joined Oct 2020
Reputation **628**

January 16, 2021 at 07:01 PM #1

Website(s):
<https://bdv.fr/>
<https://www.bourse-des-vols.com/>
<https://monde-du-voyage.com/>

Date of leak:
Dumped by me on 1/11/2021 (January 11th, 2021)

Information:
"Réservez un vol pas cher avec Bourse des Vols. Des milliers de destinations en France, en Europe et dans le monde entier, toutes compagnies aériennes!"
Google Translated: "Book a cheap flight with Flight Exchange. Thousands of destinations in France, Europe and around the world, all airlines!" - <https://www.bourse-des-vols.com/>

Amount of users:
1,460,703 (Counted by unique emails)
Command used :

```
fg -aon -no-filename -e "[A-Za-z0-9][A-Za-z0-9_+]*@[A-Za-z0-9][A-Za-z0-9-]*\.[A-Za-z]{2,6}" | sort -ufbl | wc -l
```

Raid Forums

General Raiding Related Cracking Leaks Marketplace Tutorials Tech Other Staff



GpgForWin



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



Conclusion



Hygiène informatique



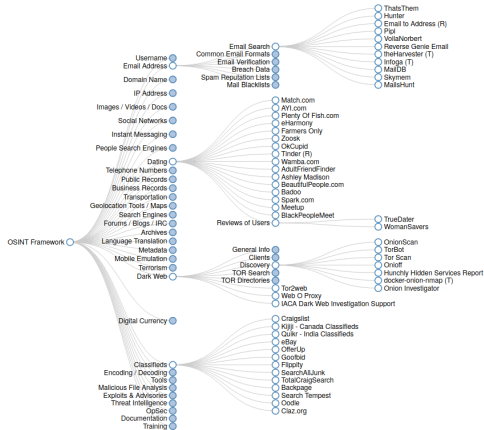
À l'image de la ceinture, une bonne hygiène de sécurité informatique peut vous protéger de presque tout ...



RGPD : Législation des bonnes pratiques



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>

