

Introduction à la cybersécurité et à la protection des données



- Hervé Suaudeau
Laboratoire SPPIN – CNRS UMR 8003
herve.suaudeau@u-paris.fr



Toutes les illustrations de cette présentation ont
été générées par intelligence artificielle
(moteur PaperCut du logiciel libre Stable Diffusion).
Merci à Michael Graupner (CNRS UMR 8003) pour le prêt de son serveur de
calcul.

stability.ai



Attribution - Attribution - Partage dans les Mêmes Conditions 4.0 International
([CC BY-SA 4.0 DEED](https://creativecommons.org/licenses/by-sa/4.0/))



Contexte



Actualités



La loi

Menaces



Qui sont les attaquants ?



Outils en vente libre



Types d'attaques

Bonnes pratiques



TP



DarkWeb

Actualité



L'IUT en chiffres

3000

Etudiants

1100

Apprentis et
stagiaires de
formation
continue

170

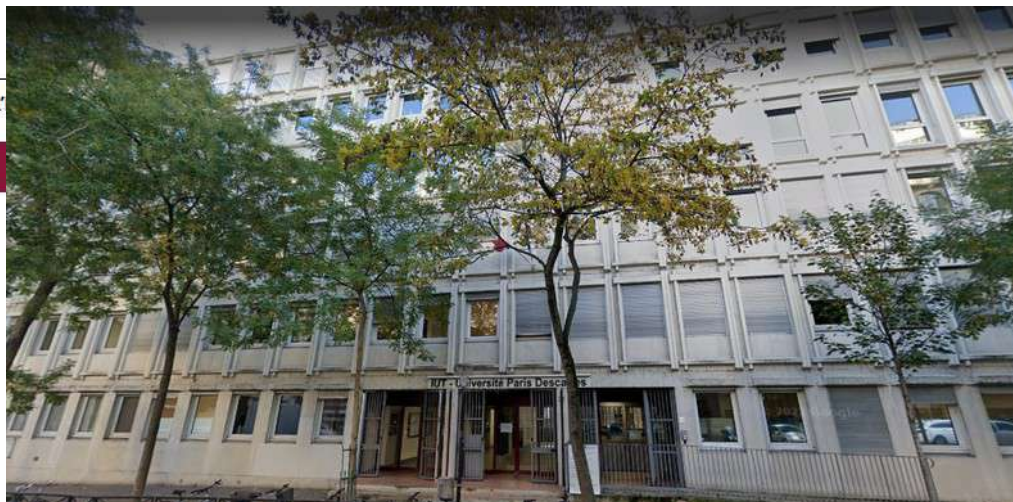
Enseignants
chercheurs

750

Intervenants
professionnels

84

Personnels
administratifs et
techniques



L'IUT en chiffres

3000

Etudiants

1100

Apprentis et
stagiaires de
formation
continue

17

Enseignants
chercheurs



La Cybersécurité est devenue un élément stratégique pour l'entreprise. De plus en plus conscientes des enjeux, les entreprises investissent davantage dans la sécurité de leurs systèmes d'information. Plus qu'une simple fonction support, l'intégration de ces problématiques devient un atout différenciant sur le marché, notamment pour les grandes entreprises. Tous les acteurs économiques et les administrations publiques sont aujourd'hui concernés par la Cybersécurité.

Diplôme ouvert uniquement en formation continue.

L'IUT en chiffre

3000

Etudiants

1100

Apprentis et
stagiaires de
formation
continue

17

Enseignants
chercheurs



Diplôme d'Université Cybersécurité

La Cybersécurité est devenue un élément stratégique pour l'entreprise. De plus en plus conscientes des enjeux, les entreprises investissent davantage dans la sécurité de leurs systèmes d'information. Plus qu'une simple fonction support, l'intégration de ces problématiques devient un atout différenciant sur le marché, notamment pour les grandes entreprises. Tous les acteurs économiques et les administrations publiques sont aujourd'hui concernés par la Cybersécurité.

Diplôme ouvert uniquement en formation continue.



Le Parisien



S'ABONNER

Reportage Paris

«On ressort les craies» : l'IUT Paris - Rives de Seine victime d'une cyberattaque

Situé dans le XVIe, l'IUT a été victime d'une attaque informatique ce week-end, constatée lundi et depuis circonscrite. Une enquête est en cours pour déterminer l'ampleur des dégâts. En attendant, tous les ordinateurs ont été débranchés.



Abonnements 01 83 97 46 50



HOME | ENSEIGNEMENT / RECHERCHE | ENSEIGNEMENT SUPÉRIEUR | DÉPÊCHE N°685092

Université Paris Cité : l'IUT de Paris Rives de Seine perd toutes les données de ses serveurs après une cyberattaque

L'IUT de Paris Rives de Seine – composante de l'université Paris Cité – a été victime d'une attaque par rançongiciel, le 5 décembre 2022. Les données des serveurs de l'institut sont "irré récupérables", indique à



Le Parisien



S'ABONNER

Reportage Paris

«On ressort les craies» : l'IUT Paris - Rives de Seine victime d'une cyberattaque

Situé dans le XVIe, l'IUT a été victime d'une attaque informatique ce week-end, constatée lundi et depuis circonscrite. Une enquête est en cours pour déterminer l'ampleur des dégâts. En attendant, tous les ordinateurs ont été débranchés.



Déroulé technique :

- Lundi 5/12/22:
 - Tous les serveurs de l'IUT sont chiffrés avec une demande de rançon de Vice Society.
 - Tous les accès numériques sont coupés, et l'IUT est isolée du reste du monde.
 - Une vérification sur tout le périmètre UPC est réalisée (latéralisation de la menace)
- Rétrospective:
 - Samedi 3/12/22: un accès à haut privilège réalise des actions anormales sur l'hyperviseur;
 - Samedi 3/12/22: exfiltration de données
 - Dimanche 4/12/22: chiffrement de tout le SI central.
- Conclusion:
 - Perte de toutes les données;
 - Par vol d'un compte à haut privilèges ayant accès à l'hypervision et aux couches basses ;
 - Pas de sauvegardes disponibles (chiffrées car sur le réseau de production)

Source : M. Thuairé – RSSI UPCité



Nouvelle université Française dans le collimateur de pirates

Posted On 19 Déc 2022 By : Damien Bancal Comment: 0 Tag: fuite de données, Université Paris Cité, vice society

L'Université Paris Cité visée par une cyberattaque début décembre. Les pirates informatiques cachés derrière cette infiltration diffusent 160 000 documents exfiltrés.

Rapports de stages, des évaluations, des bilans personnels, des devis, des CV, des cours, des pièces d'identité, ainsi que Shakira et Mariah Carey ! Voilà des exemples de fichiers diffusés par le groupe de pirates informatiques **Vice Society**. Des hackers malveillants spécialisés dans l'exfiltration de documents et demandes de rançons pour ne pas les diffuser.

Plus de 160 000 fichiers que Vice Society a mis en pâture sur le darkweb, mais que le **Service Veille ZATAZ** a déjà pu repérer sur deux espaces web !



Index of		
../		
A SUIVI DEBITEUR/	22-Apr-2022 19:51	-
ANNUL 07 03 2022/	22-Apr-2022 19:32	-
ANNULATION 2019/	22-Apr-2022 19:51	-
ANNULATION 2020/	22-Apr-2022 19:51	-
ANNULATION 2021/	22-Apr-2022 19:51	-
ASSISTANTE SOCIALE/	22-Apr-2022 19:34	-
A RAR FIDES COURRIER/	22-Apr-2022 19:32	-
A TARIFS JOURNALIERS PARTICULIERS ETC/	22-Apr-2022 19:50	-
BIBLIOTHEQUE/	22-Apr-2022 19:15	-
BUREAU DES ENTREES/	22-Apr-2022 19:32	-
DIRECTION GENERALE/	22-Apr-2022 19:34	-
PARAMETRAGE/	22-Apr-2022 19:51	-
PIA PIE/	22-Apr-2022 19:34	-
PROJET NOE/	22-Apr-2022 19:50	-
RAR +	22-Apr-2022 19:51	-
REGLES DE FACTURATION/	22-Apr-2022 19:15	-
REJET 2019/	22-Apr-2022 19:50	-
REJET 2020/	22-Apr-2022 19:32	-
REJET 2021/	22-Apr-2022 19:32	-
REJET 2022/	22-Apr-2022 19:32	-
REJET	22-Apr-2022 19:50	-
SERVICES FINANCIERS/	22-Apr-2022 19:12	-
mail/	22-Apr-2022 19:48	-

With Love!

**RAN
SOM
WARE**

Vice Society

FOR JOURNALISTS

FOR VICTIMS

OUR BLOG

V-society.official@onionmail.org, ViceSociety@onionmail.org

University Institute of Technology of Paris

<http://www.iutparis-seine.u-paris.fr/>

Home

The University Institute of Technology (IUT) of Paris - Rives de Seine welcomes 3,000 students each year from a wide variety of backgrounds, ranging from recent high school graduates, holders of a higher education diploma and students engaged in continuing education. All our students share a common goal founded on professionalization, academic innovation and educational quality.



[View documents >>](#)

A@valuation bilan perso PPP.doc	16-Dec-2022
A@valuation bilan prA@-pro PPP.doc	17-Dec-2022
A@valuation colloque.doc	16-Dec-2022
A@valuation de mA@moire.doc	16-Dec-2022
A@valuation de stage p5.pdf	16-Dec-2022
A@valuation des politiques publiques 3.pdf	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	16-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire et soutenance universitair..>	17-Dec-2022
A@valuation mA@moire.doc	16-Dec-2022
A@valuation promo 7.doc	16-Dec-2022
A@valuation promo 8.doc	16-Dec-2022
A@valuation rapport PPP.doc	16-Dec-2022
A@valuation rapport de stage.doc	17-Dec-2022

Après la cyberattaque contre l'université Paris-Saclay, une rentrée « système D »

Le vaisseau amiral de la recherche scientifique française, touché par une attaque au rançongiciel le 11 août, n'a pas encore rétabli les outils courants de communication et de gestion des étudiants. De nombreuses données pourraient ne pas être récupérées.

Par David Larousserie, Damien Leloup et Soazig Le Nevé

Publié le 31 août 2024 à 08h37 · 🕒 Lecture 5 min.



The screenshot shows the Université Paris-Saclay website with a navigation bar containing links: RENTRÉE 2024, INFORMATIONS UTILES, FAQ PIRATAGE, ACTUALITÉS, UNIVERSITÉ, and AGENDA. The main heading is 'FAQ piratage'. Below it are links for 'Informations générales', 'Informations pour les étudiants', 'Informations pour les personnels', and 'recherche'. A note states: 'Dernière mise à jour de la page : 26 septembre 2024 (voir les zones surlignées en gris)'. The main content area contains two paragraphs: 'Une messagerie prénom.nom@universite-paris-saclay.fr est disponible depuis le 30 août 2024, pour tous les personnels de l'Université Paris-Saclay, sans à ce stade de reprise de l'historique.' and 'Les étudiant.es ont reçu le 6 septembre un message sur leur adresse mail personnelle pour leur permettre d'activer leur adresse email d'établissement au format prenom.nom@etu-upsaclay.fr. Pour tout problème de création ou d'activation de l'adresse mail @etu-upsaclay.fr, les étudiants sont invités à le signaler en adressant un mail à compte_universite_paris_saclay@centralesupelec.fr.' A 'Français' button is visible at the bottom right.

Déroulé technique :

- Dimanche 11/08/24:
 - Accès à l'hyperviseur par des droits à privilèges;
 - Chiffrement de tous les SI portés par la virtualisation;
 - Perte des accès à la messagerie, intranet, espaces partagés, et certaines applications métiers.
- Conclusion:
 - Perte d'une grande partie des données,
 - Inscriptions scolaires complexes,
 - Réalisation des enseignements encore plus complexe,
 - Obligation de migration vers des infrastructures non recommandées (ex: O365),
 - A ce jour fonctionnement partiel des infrastructures,
 - Perte de confiance importante de la part de tous les corps composants PSL.

Source : M. Thuairé – RSSI UPCité

12/86

Le leader français de la santé privée visé par LockBit

Sécurité : A la mi-janvier, le siège du Groupe Elsan avait été victime d'un incident informatique. La franchise criminelle LockBit vient finalement de revendiquer l'attaque.



Par Gabriel Thierry | Jeudi 26 janvier 2023

Reactions 0 Share Tweet LinkedIn plus +



- L'établissement affirme qu'aucune donnée de patient n'a été diffusée



LEAKED DATA

TWITTER
PRESS ABOUT US

HOW TO BUY BITCOIN
AFFILIATE RULES

CONTACT US
MIRRORS

UNTIL FILES
5D12H16M36S
PUBLICATION

Deadline: 06 Feb, 2023 00:26:48 UTC



elsan.care

stolen: 821 GB.

data: marketing, finance, information of all departments of one of the company's clinics, numbers, personal data of employees, contracts, reports, internal and external contracts with policyholders, subsidiaries, etc.

Elsan is a major healthcare provider in France, operating hospitals and clinics. Elsan offers full-service hospital care, personalized care, and medical specialists.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 24 JAN 2023 12:20 UTC

UPDATED: 26 JAN 2023 07:21 UTC



Le domaine de la santé particulièrement visé

Deux semaines après la cyberattaque, "on est toujours au papier et aux crayons", décrit le directeur général du centre hospitalier de Versailles

L'hôpital André Mignot, situé dans les Yvelines au Chesnay-Rocquencourt, a été victime d'une cyberattaque il y a 15 jours. Deux semaines plus tard, l'établissement n'a toujours pas retrouvé un fonctionnement normal.



Publié le 21/12/2022 09:55 Mis à jour le 21/12/2022 11:40

Temps de lecture : 3



Après la cyberattaque, les données du Centre Hospitalier Sud Francilien dévoilées

Sécurité : A défaut d'enregistrer le versement de la rançon demandée, les pirates informatiques ayant visé le Centre hospitalier ont commencé à dévoiler les données volées à l'expiration de leur ultimatum.

Par Gabriel Thierry | Publié le lundi 26 sept. 2022 à 12:00 - Modifié le mardi 27 sept. 2022 à 08:54

Reactions 6 Tweet LinkedIn plus +



3 grand est

Accueil > Grand Est > Vosges

Les hôpitaux de Vittel et Neufchâteau dans les Vosges sont la cible d'une cyberattaque : les interventions chirurgicales sont suspendues

Publié le 07/10/2023 à 15h11
Mis à jour le 07/10/2023 à 17h11

Écrit par Jean-Christophe Panek



Les urgences de l'hôpital de Vittel (Vosges) • © Valentin Piovesan / FTV

Accueil > Finistère > Brest

Avis de décès Agenda des loisirs Infos pratiques Météo
Bénévolat Annonces légales

Le CHU de Brest-Carhaix relève la tête après l'attaque informatique

T Article réservé aux abonnés

Le 03 avril 2023 à 06h02

Trois semaines après l'attaque informatique, le CHU de Brest-Carhaix relève prudemment la tête. Le point sur l'enquête et les perspectives avec Jean-Sylvain Chavanne, le responsable de la sécurité des systèmes d'information de l'hôpital.

CYBERSECURITE

En Alsace, une attaque d'envergure paralyse un groupe hospitalier

by VICTOR MIGET le 11 SEPTEMBRE 2023



Après la cyberattaque, une facture de 7 millions d'euros pour l'hôpital de Corbeil-Essonnes

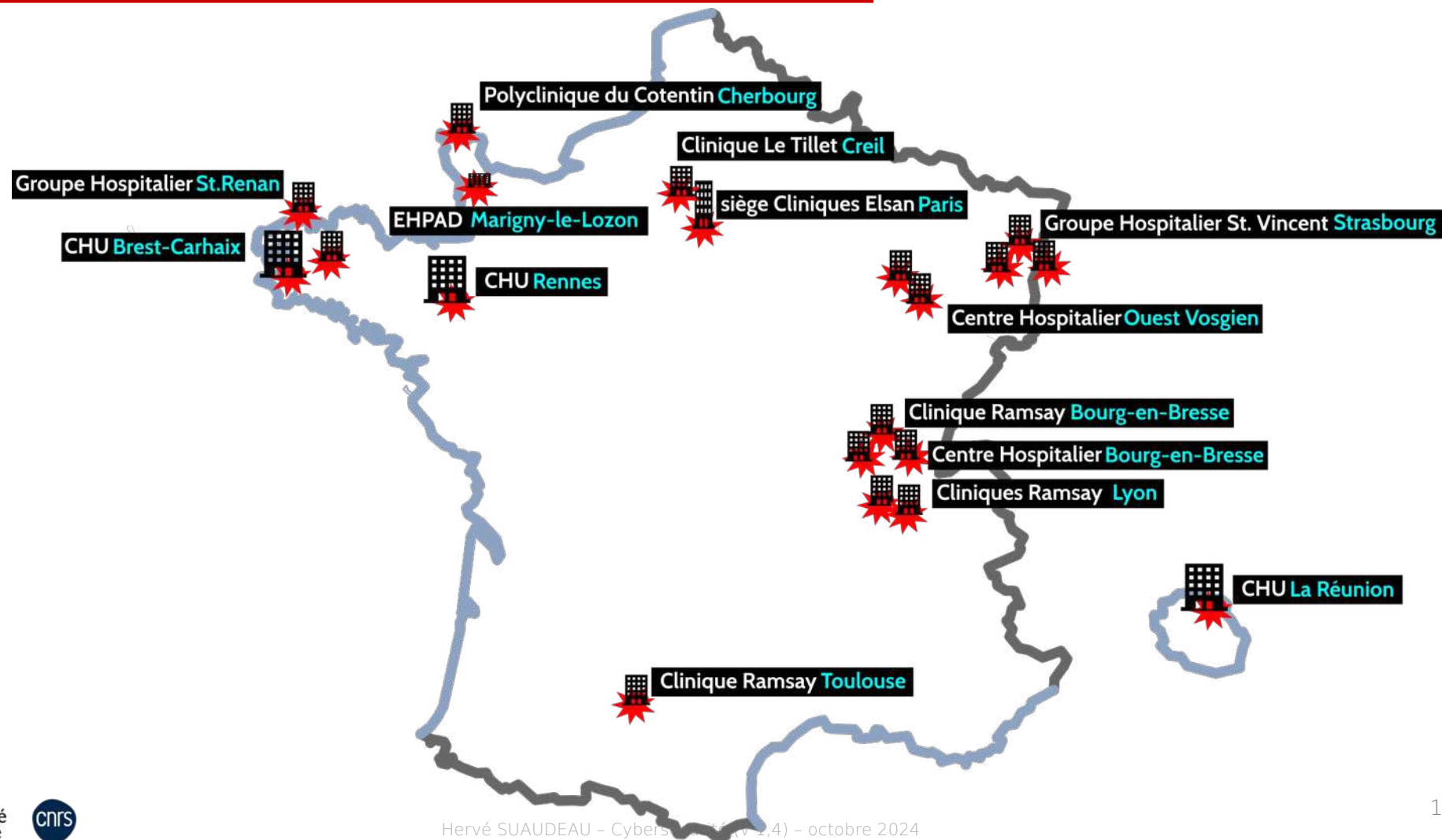
Sécurité : Outre deux millions d'euros déjà engagés dans la crise, le centre hospitalier de Corbeil-Essonnes va devoir dépenser cinq millions d'euros supplémentaires en 2023 pour rebâtir une infrastructure informatique solide.



Par Gabriel Thierry | Publié le mercredi 28 sept. 2022 à 17:00 - Modifié le jeudi 29 sept. 2022 à 08:44

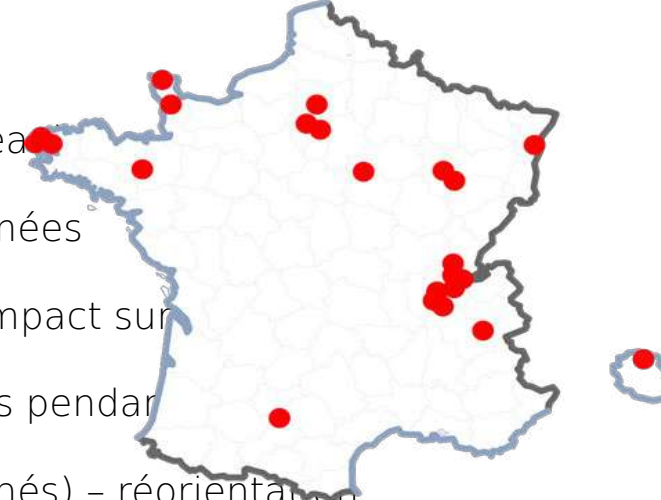
Reactions 8 Tweet LinkedIn plus +

Liste des hôpitaux français attaqués en 2023



Liste des hôpitaux français attaqués en 2023 (2)

- **Janvier 2023** : Siège du Groupe Elsan (137 établissements coupés du réseau) - 821 Go de données volées, rançon réclamée, données diffusées
- **Janvier 2023** : Cliniques Ramsay Santé (4 établissements) - urgences fermées - chirurgie et chimiothérapies repoussées
- **Février 2023** : CHU de la Réunion (4 établissements) - coupure réseau - impact sur l'organisation
- **Mars 2023** : CHU de Brest-Carhaix (9 établissements) - mail et wifi fermés pendant 3 jours - fuite de données
- **Avril 2023** : centre hospitalier de Bourg-en-Bresse (4 établissements touchés) - réorientation des soins non vitaux - mails fermés
- **Juin 2023** : CHU de Rennes (5 établissements) - 2M€ de coût - 3 mois de déconnexion - exfiltration de données
- **Septembre 2023** : groupe hospitalier Saint-Vincent à Strasbourg (30 établissements touchés) - retour 100 % papier pendant 10 jours
- **Septembre 2023** : centre hospitalier de Saint-Renan - rançongiciel - plus de mail ni internet - fuite de données
- **Octobre 2023** : centre hospitalier de l'Ouest vosgien (2 établissements touchés) - 100 % papier pendant plusieurs mois, activité de soin réduite, retour à la normale prévu en 03/24
- **Octobre 2023** : Ehpad de Marigny-le-Lozon - rançon - diffusion de données médicales
- **Décembre 2023** : Clinique le Tillet à Creil - fuite de donnée et rançon
- **Décembre 2023** : Polyclinique du Cotentin - fuite de donnée et rançon



Paiement des rançons? Vidéo ZATAZ du 11/12/2022 : <https://www.youtube.com/watch?v=JM8r3sGY1PY>

Exemples en janvier 2024 sur un site d'un groupe de rançongiciel (1)

coaxis.com

2D 18h 29m 45s

Coaxis provides CPA Firms with a fully-hosted and managed network solution designed to remove the complexities of federal and industry compliances, curb the demands of information

Updated: 26 Dec, 2023, 19:53 UTC

5718

polyclinique-cotentin.com

PUBLISHED

Medical clinic in Cherbourg-en-Cotentin, France

Updated: 22 Dec, 2023, 19:13 UTC

7211

labelians.fr

PUBLISHED

LABELIANS est concepteur, fabricant et distributeur d'équipements, d'ameublement, d'instrumentation, et de consommables pour les laboratoires

Updated: 03 Jan, 2024, 17:08 UTC

6935

isosteo.fr

PUBLISHED

Institut Supérieur d'Ostéopathie Lyon, ISOstéo Lyon a participé activement à la création du 1er enseignement de l'ostéopathie en formation initiale post-bac. Le Diplôme d'Ostéopathie

Updated: 01 Dec, 2023, 11:49 UTC

25093

elsan.care

PUBLISHED

next part of data 145gb

Updated: 16 Dec, 2023, 14:59 UTC

26596


letillet.btprrms.com


PUBLISHED


Updated: 27 Dec, 2023, 21:41 UTC

9635


Exemples en janvier 2024 sur un site d'un groupe de rançongiciel (2)

 MEDUSA BLOG

 TWITTER

 TELEGRAM

PUBLISHED






EHPAD

EHPAD is a French commercial institution for the accommodation of elderly dependents (nursing home). The company has several branches in France. The main office is located at 69 Rue République, Trun, Normandy, 61160, France

Download data now!

Oct 23, 2023, 02:08:20 PM

7863



File Explorer

📁 / 📁 ehpad - 📁 192-168-1-33_pc - 📁 Documents

- 📁 1er BOCAGE
- 📁 AFFICHE CHARIOT LINGE SALE
- 📁 EHPAD.fr

Liste des hôpitaux français rançonnés en 2022

- **Janvier 2022** : Clinique Léonard de Vinci de Chambray-les-Tours (500k€ demandés)
- **Janvier 2022** : Cité sanitaire de Saint-Nazaire. Les patients sont privés de TV, internet et téléphone et ne peuvent plus être joints par leur proches.
- **Mars 2022** : Centre hospitalier d'Ajaccio (Vice society)
- **Avril 2022** : Groupe Hospitalier Cœur Grand-Est (9 établissements, 3 370 lits et places, 5 831 agents, 287 000 habitants) piraté par Syp Industrial qui demandait 1,3M\$. Données mises aux enchères puis diffusion d'une partie.
- **Mai 2022** : Centre hospitalier de Macon. Seul le mail et les serveurs web impactés semble-t-il.
- **Août 2022** : Hôpital de Corbeil Essonne. 10M\$ de rançon, 1M\$ pour détruire, 10k\$ pour rajouter 24h. Les pirates affirment avoir volés 1M de dossiers médicaux. Pour faire pression, certains documents ont été rapidement révélés comme un arrêté concernant une admission en soin psychiatrique. Données finalement diffusées sur Internet 11.7 Go le 23/09/22.
- **Septembre 2022** : Maternité des Bluets (Paris). Plan blanc déclenché. Vice Society. Désactivation des systèmes de surveillance centralisés des fonctions vitales des bébés in utero. Données publiées depuis 4 mois.
- **Septembre 2022** : Hôpital de Cahors
- **Décembre 2022** : hôpital de Versailles. Patients transférés et redirigés. 17 j après l'hôpital ne tournait qu'à 60 % de sa capacité.



[https://esante.gouv.fr/espace-pr
esse/observatoire-des-incidents-
de-securite-si-pour-les-secteurs-
sante-et-medico-social-2023](https://esante.gouv.fr/espace-pr
esse/observatoire-des-incidents-
de-securite-si-pour-les-secteurs-
sante-et-medico-social-2023)

Multiplication des attaques dans les établissements sanitaires

- Impacts très forts sur la qualité et la sécurité de prise en charge des patients
- Développement croissant des usages du numérique dans les ES
- Augmentation générale de la cybermenace et professionnalisation des attaquants

4.1 Chiffres clés pour la période 2022-2023



x2 : nombre d'incidents déclaré par les ES depuis 2020

3ème secteur le plus touché par des attaques par rançongiciel

1,6 % : budget hospitalier dédié au numérique (part en diminution)

** Ici sont présentées les données de 2023 en gris et les données de 2022 en rose

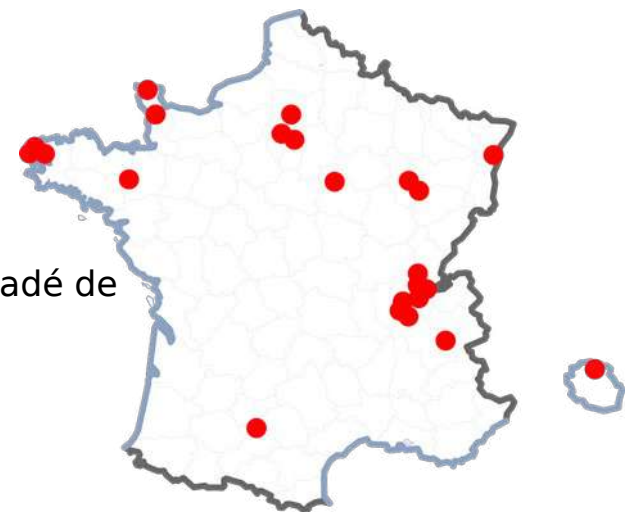
Attaques des établissements de santé en 2022

En 2022 :

- **290** structures ont déclaré au moins un incident (80 % d'hôpitaux publics)
- 50 % sont des dysfonctionnements, **50 %** d'origine malveillante
- **227** signalement de pertes de données, **117** divulgation (ou accès non autorisé) à des informations à caractère personnels, **51** atteintes à l'intégrité des données
- **113** structures contraintes de mettre en place un mode dégradé d'accès au soin
- 21 structures ont interrompu la prise en charge des patients

Pour les attaques par rançongiciel :

- **27** attaques déclarés
- **17** établissements ont été contraints de mettre en place un mode dégradé de fonctionnement
- **4 établissements sont restés dans ce mode plusieurs mois**
- **76 mises en danger avérées de patients**



Programme CaRE annoncé le 19/12/2023

- mise à niveau des systèmes d'informations hospitaliers
- 750M€ annoncés jusqu'en 2027

Buts :

- éviter que les attaques aboutissent,
- permettre aux établissements de s'en relever le plus rapidement possible.



**Le plan d'action pour protéger
nos établissements face à la menace cyber**

- Selon l'Agence nationale la sécurité des systèmes d'information (Anssi, 2023), chantage par « rançongiciel », qui consiste à chiffrer les données la victime puis à exiger rançon, majoritairement les entreprises (40 %), puis les collectivités territoriales (23 %) et les établissements publics santé (10 %) Les signalements réalisés auprès du CERT Santé démontrent que l'état de la menace ne faiblit pas.
- Ces derniers mois, des attaques massives ont ciblé certains établissements de santé et ont eu des conséquences directes sur l'organisation des services et la prise en charge des patients. Le retour à la normale peut prendre plusieurs mois et nécessite souvent des investissements importants, humains et financiers, pour les établissements victimes.
- On estime que les établissements de santé subissent 2 à 3 fois plus d'attaques que d'autres secteurs (2020 Healthcare Cybersecurity Report)
- UK : 2017 – 45 établissements de santé du NHS touchés par WanaCry. 200 000 ordinateurs !
- Le plan d'actions, appelé CaRE, annoncé en décembre 2023, vise à accélérer la mise à niveau des systèmes d'informations hospitaliers face à l'état de la menace et à renforcer durablement la résilience des structures de soins. Le programme doté de 250 M€ jusqu'en 2025, sur un objectif d'investissement total de 750 M€ d'ici 2027, poursuit le double objectif : éviter que les attaques aboutissent ; et permettre aux établissements de s'en relever le plus rapidement possible





- En 2022, l'ANSSI est intervenue au secours de 11 établissements publics de santé victime d'attaques par rançongiciel
- Des attaquants motivés car :
 - Données médicales vendues très chères sur le Dark web
 - Établissements traditionnellement mal protégés
 - Manque de moyens et de personnels
 - Effet psychologique puissant particulièrement en période de pandémie



- La santé est particulièrement visée par les pirates
- Les établissements de santé sont vulnérables
- Les données de santé valent cher
- La réponse à ces problèmes commence tout juste

La loi



Charte d'usage des Systèmes d'Information d'Université Paris Cité

I.	Objet et champ d'application	2
a.	Personnes concernées	2
b.	Systèmes d'information	2
c.	Usages concernés	2
II.	Principes d'usage	3
a.	Utilisation conforme aux lois et règlements en vigueur	3
b.	Usage général	3
i.	Usage professionnel ou étudiant	3
ii.	Usage à titre privé	4
iii.	Conditions d'accès et authentification	4
c.	Usage spécifique	4
i.	Mobilité et accès distant	4
ii.	Télétravail	4
iii.	Utilisation des outils informatiques par les organisations syndicales	5
iv.	Unités mixtes de recherche et spécificité défense	5
d.	Configuration du poste de travail	5
e.	Gestion des Média USB	6
f.	Messagerie électronique	6
g.	Téléphonie fixe et mobile	7
h.	Internet et intranet	7
i.	Gestion des absences et des départs	7
j.	Bonnes pratiques	8
III.	Protection de la propriété intellectuelle, des informations et des données	8
a.	Propriété intellectuelle, droit à l'image	8
b.	Secret et confidentialité	9
c.	Protection des données à caractère personnel	9
i.	Registre des activités de traitement et transparence sur les traitements	10
ii.	Finalité des données personnelles collectées	10
iii.	Confidentialité des données personnelles	10
iv.	Durée de conservation des données	10
IV.	Règles de sécurité	11
a.	Devoirs de signalement et d'information	12
V.	Mesures de contrôle	13
a.	Administration des systèmes d'information	13
b.	Les systèmes automatiques de filtrage	13
c.	Les systèmes automatiques de traçabilité	13
VI.	Sanctions	14
VII.	Glossaire des termes clés	14
VIII.	Modalités d'entrée en vigueur de la charte	15

- L'utilisateur est responsable de ses actions
- Toute information est réputée professionnelle.
- Utilisation privée raisonnable
- Ne pas :
 - Installer des logiciels non officiels
 - communiquer son mot de passe
- Devoir de :
 - Verrouiller son poste de travail
 - Protéger ses données

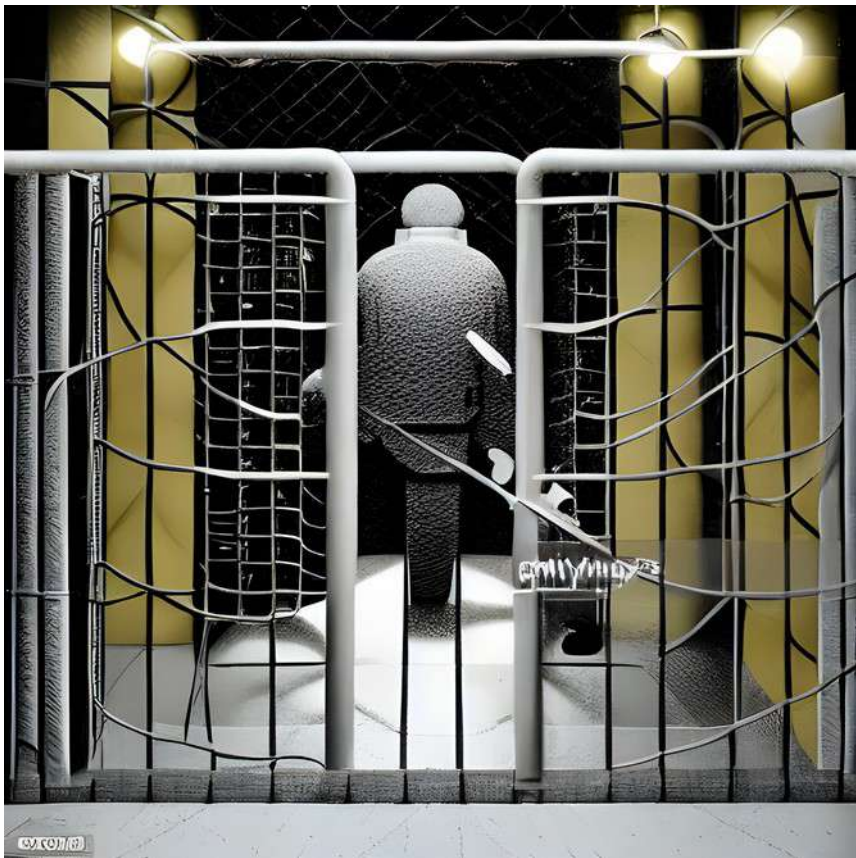


- Respect de la vie privée. Données strictement nécessaires
- Consentement explicite
- Extraterritorialité
- Sécurisation obligatoire des données
- Sanctions



- Extraterritorialité
- Supervision gouvernementale
- En conflit avec RGPD
 - Donc données sensibles (à fortiori médicales) interdites chez héberge





Délit d'intrusion

- **Article 323-1 - Code pénal**
- « accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données » **trois à sept ans** d'emprisonnement.

•

Délit de consultation

- **Article 227-3 - Code pénal**
- « consulter habituellement ... une telle image ou représentation [pédopornographique] par quelque moyen que ce soit est puni » **cinq ans** d'emprisonnement.
- **Article 421-2-5-2 - Code pénal**
- « consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes » **deux ans** d'emprisonnement (sans même manifester de l'adhésion à l'idéologie exprimée sur ce service).



Le directeur
Réf : DINUM-DIR-210901

Direction
interministérielle du
numérique

Paris, le 15/09/2021

NOTE

Aux secrétaires généraux des ministères

Objet : Doctrine "Cloud au Centre" et offre Office 365 de Microsoft

Référence : Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État

Certaines administrations étudient l'opportunité de recourir à l'offre Office 365, proposée par Microsoft sur ses propres infrastructures cloud (Azure), en remplacement des solutions bureautiques et de messagerie (MS Exchange notamment) déployées sur les serveurs de l'Etat.

La circulaire du Premier ministre citée en référence explicite la doctrine cloud de l'Etat, dite « Cloud au Centre ». Dans sa règle [R9], elle précise que pour un système numérique qui manipule des données sensibles, le recours à une offre de cloud commercial est possible uniquement si cette offre est qualifiée SecNumCloud et qu'elle est immunisée contre les réglementations extracommunautaires.

Les solutions collaboratives, bureautiques et de messagerie proposées aux agents publics relèvent des systèmes manipulant des données sensibles. Ainsi, la migration de ces solutions vers l'offre Office 365 de Microsoft **n'est pas conforme à la doctrine Cloud au Centre**. A titre transitoire, pour les éventuels projets très avancés au 5 juillet

2021, une dérogation pourra être accordée sous la responsabilité de votre ministre. Cette dérogation se limiterait aux seuls services de messagerie et de *drive* personnel, « pour une durée limitée à 12 mois après la date à laquelle une offre de cloud acceptable sera disponible en France ». En revanche elle ne peut concerner les services documentaires, collaboratifs, de messagerie instantanée, d'audioconférence, de visioconférence et de webinaire, qui sont couverts par l'offre interministérielle SNAP, déjà conforme à Cloud au Centre ou en passe de le devenir très prochainement.

1/2

Ainsi, dans le cas où vous envisageriez d'externaliser la construction et le fonctionnement de vos suites collaboratives hors de vos systèmes d'information ministériels, je vous invite :

- Renforce l'interdiction de l'usage du Cloud non européens
- Notamment pour les établissements publics et administrations ;



- La charte résume vos obligations
- Le RGPD vous protège et vous oblige
- Le Cloud Act vous empêche d'utiliser les GAFAM
- L'intrusion informatique est interdite
- La consultation de site publics est libre sauf exception

Qui sont les attaquants?



Les attaquants et leur motivations

- Les apprentis pirates (« script kiddies »)

- Les organisations mafieuses

- rançons
- vol de données
- recrutement de machines
- mercenariat



- Des entreprises (Ex. [Cambridge Analytica](#))

- Les États

- Intelligence économique
- Ingérence politique



- Autres exemples :

- Le « brouteur » (séduction, fausses annonces, faux comptes de stars...)
- Le collègue mécontent



Des États motivés par l'ingérence (1)

N° 1454
ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958
SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale
le 29 juin 2023

N° 810
SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat
le 29 juin 2023

RAPPORT PUBLIC

FAIT

AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

*relatif à l'activité de la délégation parlementaire au renseignement
pour l'année 2022-2023,*

Délégation parlementaire
AU RENSEIGNEMENT



<https://www.senat.fr/notice-rapport/2022/r22-810-notice.html>



Des États motivés par l'ingérence (2)



- « première [stratégie], l'infiltration »
- « attirer ... d'anciens dirigeants européens à travers leur participation aux conseils d'administration de grands groupes russes » (« François Fillon », « Gérard Schröder »)
- « manipulation de l'information de grande ampleur »
- « manœuvres d'ingérence dans les processus électoraux » : « tentatives d'intrusion dans l'infrastructure des systèmes de vote », « diffusion d'e-mails [...] volés », « piratage », « campagne massive sur les réseaux sociaux »
- « entreprises militaires privées »

- 250 000 membres de la « DGSE chinoise »
- Contraintes sur la diaspora : « tout ressortissant Chinois [est] un potentiel espion » (600 000 en France)
- « front uni » du PC chinois contrôlant « un réseau d'institutions publiques et privées et d'individus clés »
- « investissements chinois très dynamiques dans des secteurs stratégiques » en France
- Stratégie de mise en place d'une « dépendance financière » de nos « universités et le monde de la recherche »
- « les actions d'ingérences chinoises consistent autant à développer un narratif positif sur la Chine qu'à collecter des informations via des universités, l'espionnage, la compromission et l'achat de savoir-faire »



- « financement de lieux de culte » (« 2600 ») et « détachement d'imams » en France (« 120 »)
- « entrisme politique » : « le PEJ a présenté 52 candidats » aux législatives françaises de 2017
- « présence active sur les réseaux sociaux »
- « Cyberattaques [...] attribuées à des groupes turcs notamment au lendemain de l'adoption [de la] loi condamnant la négation du génocide arménien »



- « arrestation de ressortissants de différents pays pour s'en servir comme monnaie d'échange »
- « attaques informatiques »



- François Fillon affirme avoir été « écouté avec le président Sarkozy pendant cinq ans par la NSA »



- « Logiciel espion [Pegasus] développé par l'entreprise israélienne NSO Group »



- Ne pas confondre Hacking et cybercriminalité
- White hat et black hat
 - **Hackers White Hat** : Emploient leurs compétences pour renforcer la sécurité informatique, souvent en travaillant légalement pour des entreprises afin de trouver et de corriger les vulnérabilités.
 - **Hackers Black Hat** : Utilisent leurs compétences en informatique pour des activités illégales ou malveillantes, comme le vol de données ou la création de virus.



- Les attaquants ne sont pas toujours ceux que vous croyez
- Leurs intérêts et leurs moyens sont très divers

En libre achat !





INPUT DEVICES

Mouse Jiggler



\$20.00

-

1

+

ADD TO CART

SKU: EW-MJ

Category: Input Devices



KeyGrabber



\$40.00 - \$75.00

CLEAR

Model

USB WiFi Premium

▼

\$75.00

Out of stock

-

1

+

ADD TO CART



Rubber Ducky



https://www.youtube.com/watch?v=e_f9p-_JWZw



USB RUBBER DUCKY

\$119.99

NEW VERSION OF THE BEST SELLING I

With a few seconds of physical access, all bets are off...



USB RUBBER DUCKY
\$79.99



PRO BUNDLE
\$99.99



ELITE

Accessories



Advanced
DuckyScript...
\$49.99 USD



USB Rubber Ducky
Textbook
\$39.99 USD



CÂBLE O.M.G

€149⁰⁰

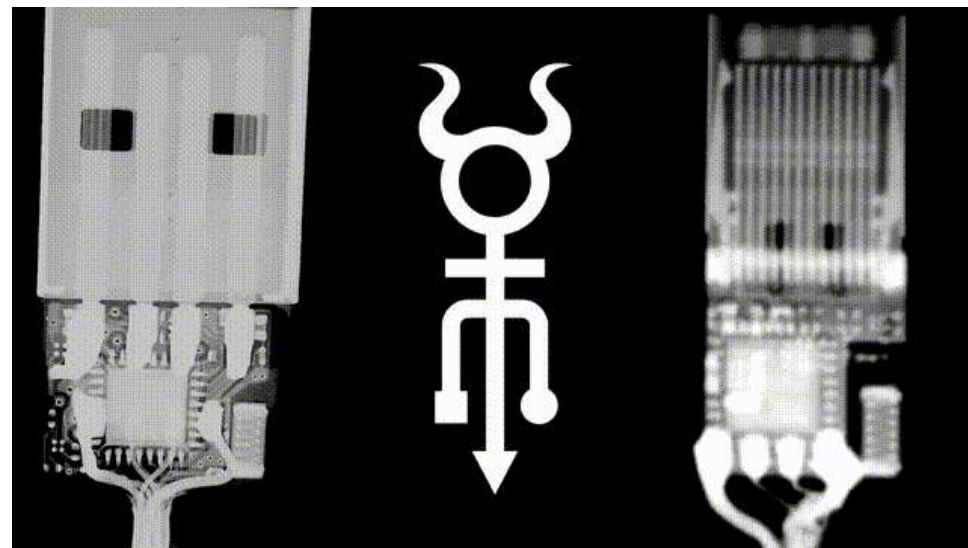
Version

Pro-Kit

Quantité

1

 SOLD OUT



<https://www.youtube.com/watch?v=XxIX7yn9lwU>



ICOPY-XS

€375⁰⁰

L'ICopy-X est un puissant dispositif de clonage RFID portable.

Construit sur le puissant Proxmark 3, son interface facile à utiliser simplifie le clonage RFID.

Il prend en charge la majorité des cartes HF et LF sur le marché, et est un must pour les pentesters et les chercheurs en sécurité.

Aucune connaissance experte n'est requise - mais les utilisateurs expérimentés peuvent toujours utiliser une console Proxmark pour effectuer des opérations avancées .

Paquet de cartes

De base

RFID PENTESTER TAG PACKS



PAC

€69⁰⁰ €90⁰⁰ SAVE €21

Packs d'étiquettes RFID pour tous les besoins : Économisez jusqu'à €160 !

Type d'emballage

Démarreur

Quantité

1

[HOME](#) / [ALL](#) / [WIFI PINEAPPLE](#)



WIFI PINEAPPLE

\$119.99

The industry standard WiFi pentest platform has evolved. Equip your red team with the WiFi Pineapple® Mark VII. Newly refined. Enterprise ready.

Basic edition includes antennas and USB-C power/ethernet cable.



MARK VII BASIC
\$119.99





FLIPPER ZERO

€169⁰⁰

Le Flipper Zero est le multi-outil ultime pour les geeks, les pentesters et les passionnés de matériel informatique qui glisse dans la poche.

Pack

De base

Quantité

1

 SOLD OUT

<https://www.youtube.com/watch?v=UQC4yKrLN7U>





- Les outils d'infiltration type « James Bond » sont facilement accessibles
- Ils illustrent de façon convaincante nos faiblesses
- ... mais ce n'est souvent pas ceux-là qui sont utilisés.

Types d'attaques





- Virus
- Vers
- Chevaux de Troie

Campagne Hack Academy : Ici, le candidat Martin nous montre comment la technique du cheval de Troie permet de soutirer les données personnelles des internautes.

<https://www.youtube.com/watch?v=SLeebIMR6H4&t=1s>

- Ransomwares



- Type Zeus

Godfather, le successeur du malware bancaire Anubis

Sécurité : Selon les chercheurs de Group-IB, ce trojan bancaire ciblant les utilisateurs d'Android partage une base de code commune avec Anubis.



Par Gabriel Thierry | Vendredi 23 Décembre 2022

Réactions

0

Share

Tweet

LinkedIn

plus +



Campagne Hack Academy : Ici, le candidat Willy nous raconte comment la technique du phishing permet de soutirer les données bancaires des internautes.

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

Campagne Hack Academy : Ici, la candidate Jenny nous montre comment il est possible de pirater les mots de passe les plus communs des internautes.

https://www.youtube.com/watch?v=jQ_BzKKSzqE

- Cyberattaques exploitant les failles humaines
 - Hameçonnage
 - Arnaque au président
 - Brouteur
 - Regarder un post-it
 - Ex

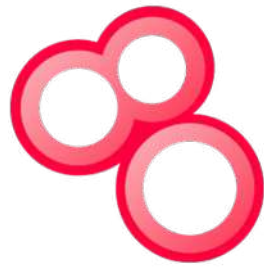




- <https://www.dailymotion.com/video/x1x7z3u>



SHODAN



SHODAN

- <https://www.shodan.io>
- <https://beta.shodan.io/search?query=u-paris.fr>
- <https://www.shodan.io/search?query=camera+web>
- <https://2000.shodan.io/#/>
- <https://beta.shodan.io/host/91.231.87.229>



Stable diffusion : « Deep learning, cybernetics, internet Hacking. PaperCut »

- Les États et les groupes mafieux s'organisent
- Attaques basées sur l'intelligence artificielle
 - DeepFake
 - Outils comme Chat GPT
 - ...



- Les attaques se passent généralement à distance
- Elles utilisent le plus souvent les faiblesses humaines

« Hygiène » numérique



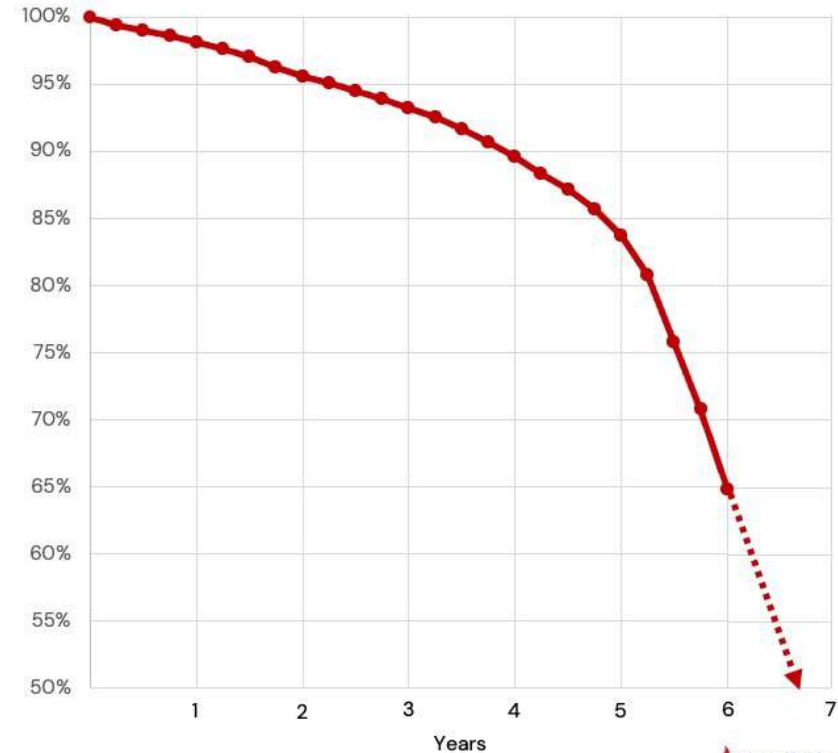
1 - Faire des sauvegardes

- Les disques durs ont une demie vie de quelques années
- Les SSD sont plus fragiles



Projected Backblaze Hard Drive Survival Rates by Quarter

Kaplan-Meier curve smooth for the reporting period ending 9/2021





- La Synchronisation cloud est-elle une sauvegarde ?

- Non ! Si un rançongiciel chiffre vos données, le cloud sera lui aussi chiffré.
- Il faut donc faire des « sauvegardes à froid »



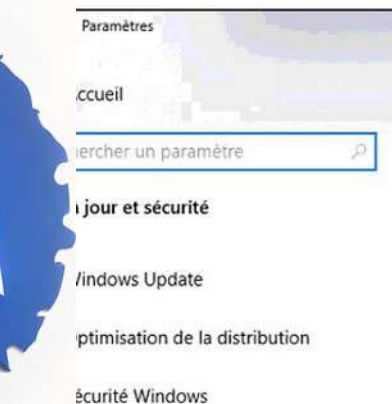
Non-souverains :



2 - Faire les mises à jour



Aucune raison valable ne justifie de laisser une machine connectée sans mise à jour



Windows Update



Vous êtes à jour

Dernière vérification : aujourd'hui, 08:50

Rechercher des mises à jour

Mises à jour facultatives disponibles

- 2019-10 Mise à jour cumulative pour Windows 10 Version 1903 pour les systèmes x64 (KB4522355)

Télécharger et installer maintenant



Suspendre les mises à jour pendant 7 jours

Consultez les options avancées pour modifier la période de suspension



Modifier les heures d'activité

Actuellement 08:00 à 17:00



Afficher l'historique des mises à jour

Voir les mises à jour installées sur votre appareil



Options avancées

Paramètres et contrôles de mise à jour supplémentaires



Mise à jour de logiciels

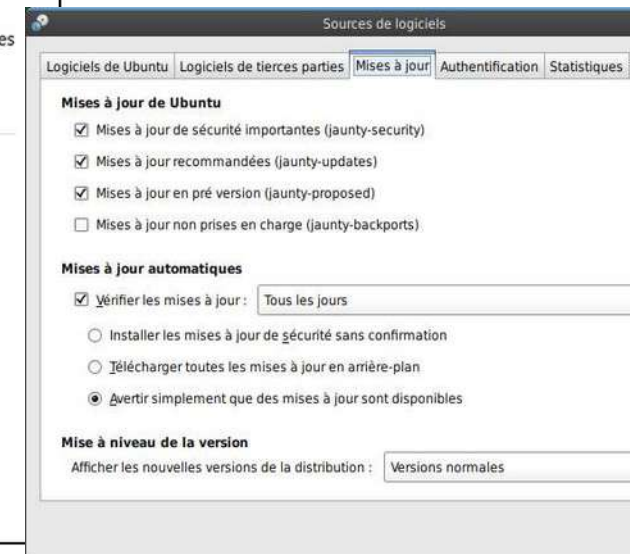
Une mise à jour est disponible pour votre Mac

- Mise à jour de macOS 10.14.3

[En savoir plus...](#)

L'utilisation de ce logiciel est soumise au contrat de licence d'origine de l'objet de la mise à jour.

☐ Mettre à jour automatiquement mon Mac



Mises à jour de Ubuntu

- ☒ Mises à jour de sécurité importantes (jaunty-security)
- ☒ Mises à jour recommandées (jaunty-updates)
- ☒ Mises à jour en pré version (jaunty-proposed)
- ☐ Mises à jour non prises en charge (jaunty-backports)

Mises à jour automatiques

- ☒ Vérifier les mises à jour : Tous les jours
 - ☐ Installer les mises à jour de sécurité sans confirmation
 - ☐ Télécharger toutes les mises à jour en arrière-plan
 - ☒ Avertir simplement que des mises à jour sont disponibles

Mise à niveau de la version

Afficher les nouvelles versions de la distribution : Versions normales

3 - Bien gérer ses mots de passe (1)

Vidéo de Jimmy Kimmel : <https://www.youtube.com/watch?v=opRMrEfAiiI>



NordPass® Business Perso Tarifs Fonctions Blog Aide

Résultats France

CLASSEMENT	MOT DE PASSE	TEMPS MOYEN
1	123456	
2	123456789	
3	azerty	
4	admin	
5	1234561	
6	azertyuiop	
7	loulou	
8	000000	
9	doudou	
10	password	
11	marseille	
12	motdepasse	
13	12345678	
14	chouchou	
15	soleil	
16	cheval	
17	12345	
18	Password	
19	bonjour	

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS > Learn more about this at hivesystems.com/password



Des mots de passe

- Solides
- Uniques
- Personnels

Gestionnaire de mot de passe ?



keepass.info



keepassxc.org

Voir atelier « haveibeenpwnd » à la fin du cours

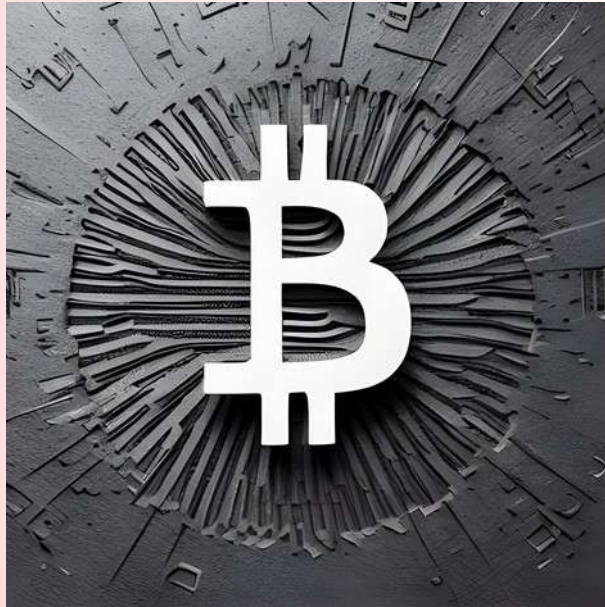
4 - Protéger l'accès physique à vos ordinateurs



- Fermer bureaux
- Ne pas laisser traîner de documents sensibles
- ~~Code sur Post-it~~
- Verrouiller session



Le technosolutionnisme



Se méfier de :

- Discours commercial
- Technologies magiques

5 - Attention aux messages ! (1)



Test sur <https://phishingquiz.withgoogle.com/>

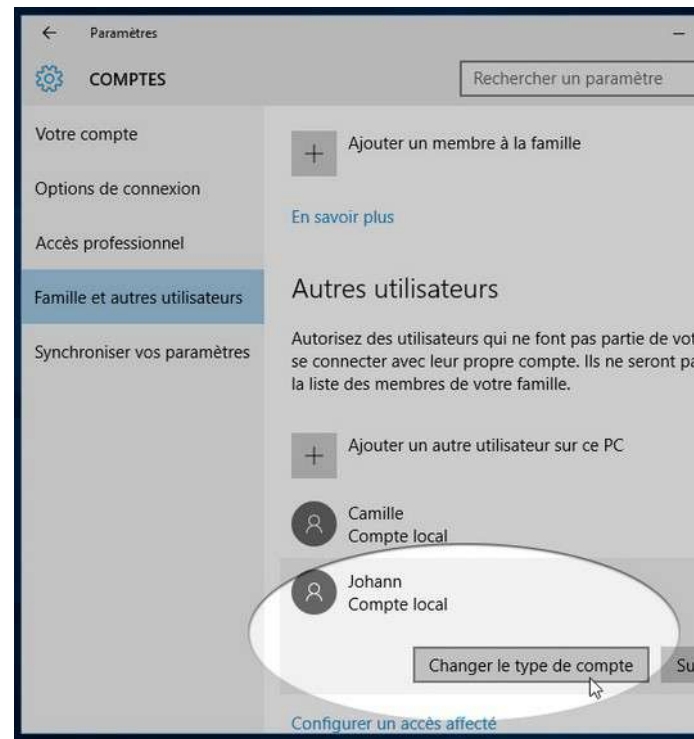
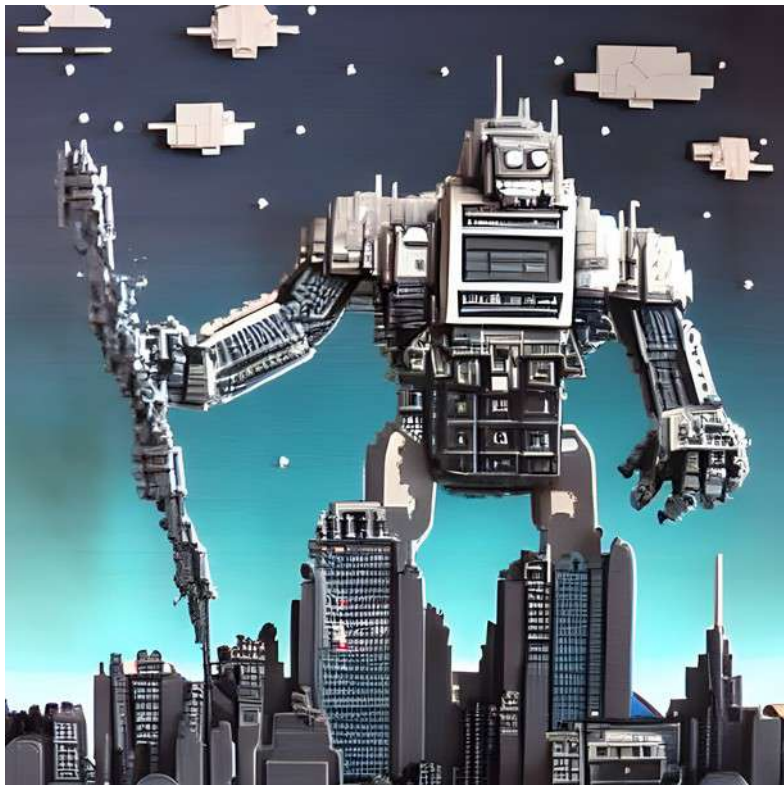
5 - Attention aux messages ! (2)



- Courriels, SMS, messages perso des réseaux sociaux etc.
- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone (identifiants, mots de passe, information bancaire etc...)
- Soyez attentifs à l'expéditeur mais pas trop
- Méfiez-vous des pièces jointes
- Demandez conseil devant tout mail suspect, contactez directement l'organisme en cas de doute.
- Numéros inconnus : ne rappelez jamais, ne répondez pas par SMS
- Soyez plus vigilants quand les sujets provoquent des émotions (peur, colère, pitié...) et confirment vos croyances
- URL menteuses et trompeuses : Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer)



6 - Ne pas travailler avec un compte administrateur



7 - Choisir une bonne solution de sécurité



- Ce n'est pas une protection totale !



8 - Télécharger sur les sites officiels et préférer le libre quand c'est possible



Moyen pour
obtenir une
URL fiable
d'un logiciel.
Éviter les
moteurs de
recherche car
il y a des
liens
trompeurs.

WIKIPÉDIA
L'encyclopédie libre

Rechercher sur Wikipédia

KeePassXC

12 langues

Sommaire [masquer]

Début

- Développement
- Applications alternatives
- Notes et références
- Annexes
- Liens externes
- Articles connexes

KeePassXC est un gestionnaire de mots de passe gratuit et open-source publié sous la licence libre GPL v2 ou ultérieure et disponible sur Linux, Windows et macOS. Il permet de sauvegarder un ensemble de mots de passe dans une base de données chiffrée. KeePassXC utilise le format de base de données de mots de passe KeePass 2.x (.kdbx) comme format natif¹. Il peut également importer (et convertir) la version 2 et les anciennes bases de données KeePass 1 (.kdb). Ce fichier de base de données s'ouvre avec un mot de passe principal et/ou avec d'autres méthodes d'authentification comme un fichier de clé, ou avec des clés de sécurité utilisant un jeton d'authentification. Les clés YubiKey sont compatibles^{3,4}.

Il a pour origine un fork communautaire de KeePassX^{3,5}, lui-même un fork multi-plateforme de KeePass.

L'Electronic Frontier Foundation mentionne KeePassXC comme « un exemple de gestionnaire de mots de passe open source et gratuit »⁶. Le collectif technologique PrivacyTools a inclus KeePassXC dans sa liste de logiciels de gestion de mots de passe recommandés en raison de son développement actif^{7,8}.

Développement [modifier] [modifier le code]

Il est développé à l'aide de bibliothèques Qt5, ce qui en fait une application multi-plateforme qui peut être exécutée sur Linux, Windows et macOS⁹.

Applications alternatives [modifier] [modifier le code]

Il existe de nombreuses implémentations multiplateformes de KeePass¹⁰ dont le format de bases de données est compatible car normalisé.

- KeePass le logiciel original à l'origine du format kdbx
- WinPass, portage pour Windows 8/10 Mobile.
- KeePassB pour BlackBerry.
- KeePassX, KeePassDroid et KeePass2Android, pour Android disponible sur F-Droid.
- KyPass pour iOS, un fork de MyKeePass avec prise en charge de Dropbox.
- MacPass pour macOS.
- KeeWeb, une application web pour accéder à la base de données KeePass depuis n'importe quel appareil et permettant la synchronisation avec Dropbox^{11,12}.

Notes et références [modifier] [modifier le code]

- ¹ « Release 2.7.4 » [archive], 29 octobre 2022 (consulté le 13 novembre 2022)
- ² « Documentation and FAQ » [archive], keepassxc.org (consulté le 18 juillet 2018)
- ³ ¹ ^a et ^b « The Project » [archive], keepassxc.org, 16 octobre 2016 (consulté le 13 janvier 2020)

KeePassXC

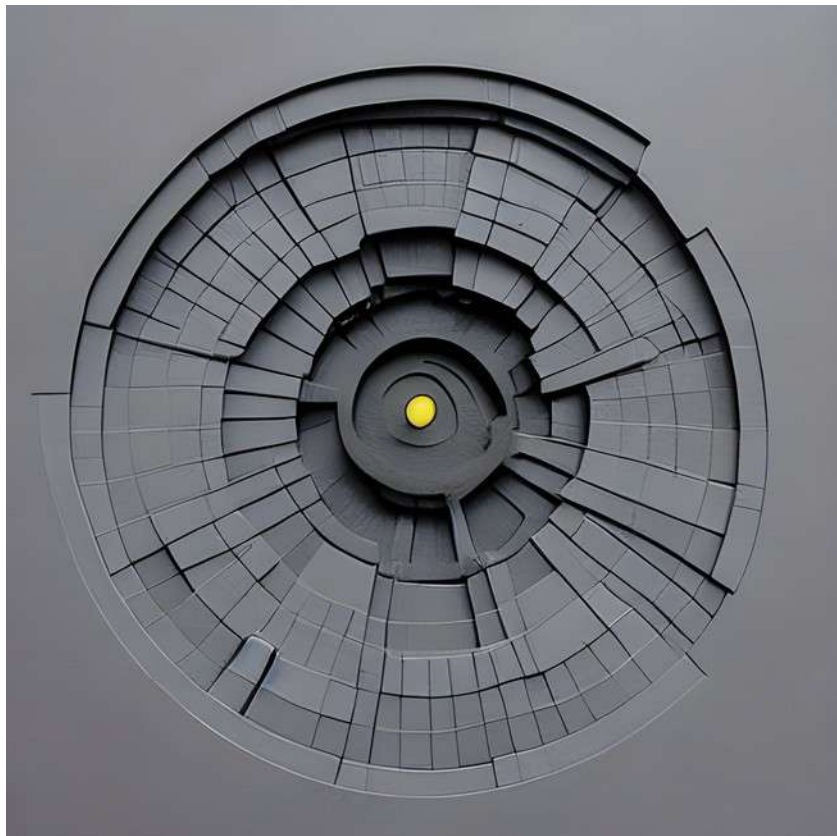
Lire · Modifier · Modifier le code · Voir l'historique

Informations

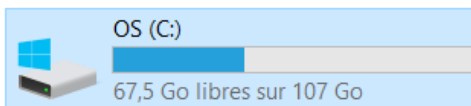
Dernière version	2.7.4 (29 octobre 2022) ¹ ✓
Dépôt	github.com/keepassxreboot/keepassxc ✓
Écrit en	C++ ✓
Interface	Qt ✓
Système d'exploitation	Linux, Microsoft Windows et macOS ✓
Formats lus	KDBX (4) et KDB (4) ✓
Type	Gestionnaire de mots de passe ✓
Licence	Licence publique générale GNU version 2 et licence publique générale GNU version 3 ✓ keepassxc.org ✓

modifier · modifier le code · voir Wikidata (aide)

9 - Chiffrer ses disques




✓ Périphériques et lecteurs (1)



Ouvrir

Ouvrir dans une nouvelle fenêtre

Épingler dans Accès rapide

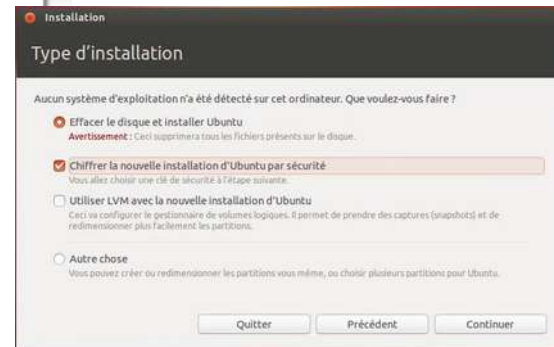
 Activer BitLocker

Partager avec

Restaurer les versions précédentes



élec

Facile à activer !




10 - Limiter ses traces



 **Firefox Monitor** [Accueil](#) [Fuites de données](#) [Conseils de sécurité](#)  

Que pouvez-vous faire pour protéger vos données personnelles


Bien que les mots de passe n'aient pas été exposés dans cette fuite de données, vous pouvez toujours prendre des mesures pour mieux protéger vos informations personnelles.

**Utilisez un service qui masque votre adresse IP**

Votre adresse de protocole Internet (adresse IP) identifie votre emplacement et fournisseur de services Internet. Avec un réseau privé virtuel (VPN), vous pouvez masquer votre position et masquer votre adresse IP.

**Évitez de partager votre numéro de téléphone**

Essayez de ne pas donner votre numéro de téléphone lors de la création d'un compte ou de l'inscription à un service. Si un numéro de téléphone n'est pas requis, ne le saisissez pas.

**Utilisez un alias de messagerie**

Fournir votre adresse électronique réelle permet aux pirates informatiques ou aux traqueurs de trouver vos mots de passe ou de vous cibler en ligne plus facilement. Un service comme Firefox Relay masque votre adresse électronique réelle tout en transmettant les messages à votre boîte de réception réelle.
[Essayer Firefox Relay](#)

**Évitez d'utiliser des informations personnelles dans votre code PIN**

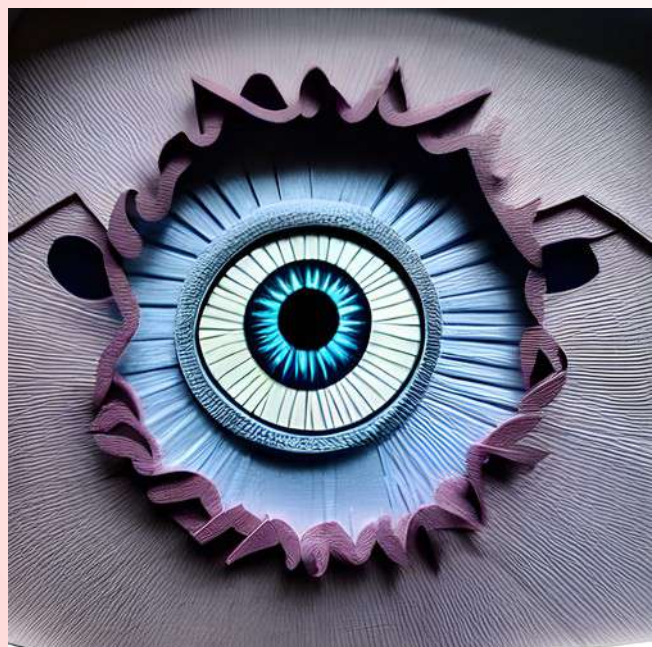
Puisque votre date de naissance est aisément trouvable dans des documents publics, il vaut mieux éviter de l'utiliser dans les mots de passe et les codes PIN. Les personnes qui connaissent votre date de naissance pourraient également deviner très facilement votre code PIN.

**Évitez d'utiliser des adresses dans vos mots de passe**

Utiliser des adresses ou bien la rue où vous avez grandi affaiblit vos mots de passe. Comme il est facile de trouver ces informations publiquement, cela rend ces mots de passe faciles à deviner.



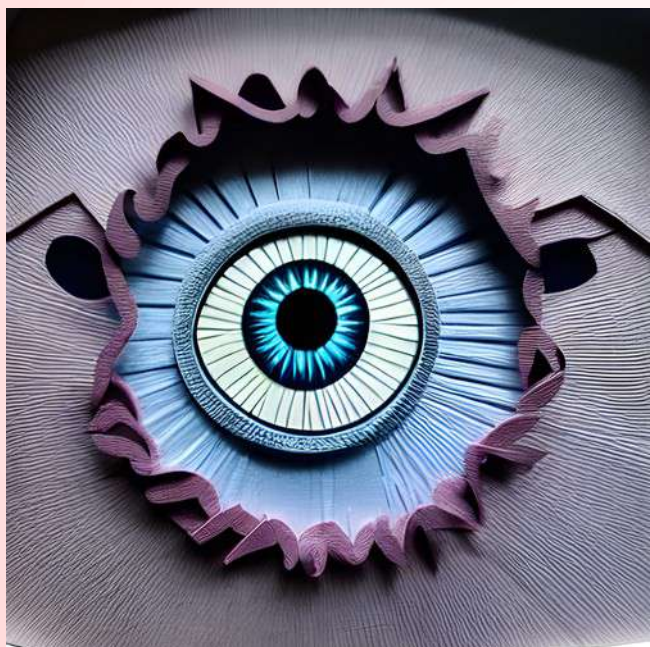
« Si vous n'avez rien à cacher, vous n'avez rien à craindre »



- Vraiment ?
- Témoignage d'Edward Snowden
- Vous ne fournissez pas que VOS données



« Si vous n'avez rien à cacher, vous n'avez rien à craindre »



- Vraiment ?
 - Numéro de CB, logins, habitudes privées...
- Témoignage d'Edward Snowden
 - La NSA va vous espionner avec 3 niveaux de relation. « Si vous connaissez quelqu'un qui connaît quelqu'un qui est le frère peut être perdu de vue d'un type barbu soupçonné de commettre des actes de terrorisme, si vous n'avez rien à voir avec cette personne, alors c'est potentiellement tous vos emails, toutes vos navigations, tous vos coups de fils, tous vos SMS qui sont espionnés par la NSA » (Jeremie Zimmerman ex-président de la Quadrature du net)
- Vous ne fournissez pas que VOS données
 - Quand vous donnez vos communications privées à Google, vous donnez aussi une partie de la communication de vos correspondants.

10 - Limiter ses traces (2)



Une bonne solution :



+



Chrome espionne
votre navigation

Ne nourrissons pas les GAFAM

Des alternatives existent, découvrons-les !

Office, Excel, Word

Adobe, Photoshop

Google, GoogleDocs, Doodle

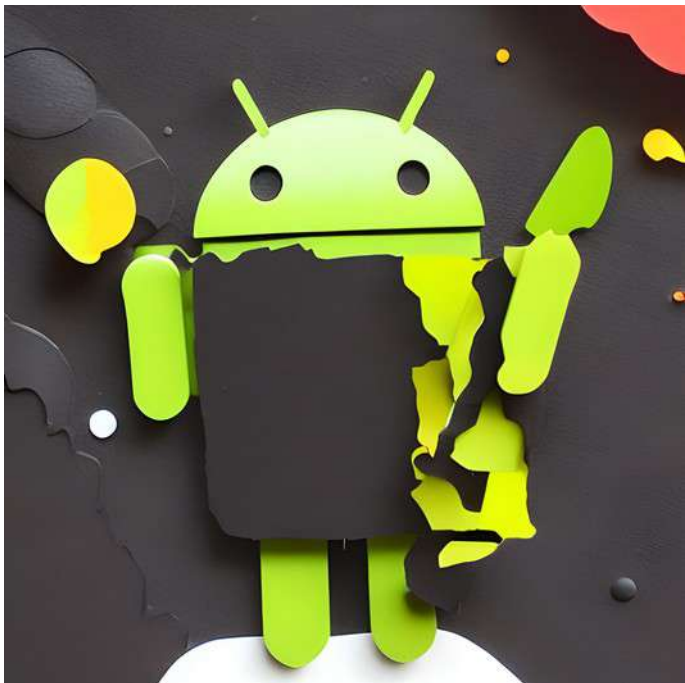
Les G(oogle) A(pple) F(acebook) A(mazon) M(icrosoft) :
Propriétaires, commerciaux, en situation de monopole...
Voulez-vous vraiment ne dépendre que d'eux ?

11 - Éviter les wifi publics



- Vos données sont potentiellement visibles
- Attaques Man in the Middle
- Préférer le partage de connexion 4G et sinon VPN





Très visés par les attaquants car vulnérables (surtout Android)

Avant de télécharger une application, recherchez des informations complémentaires sur celle-ci et validez sa provenance. La source de téléchargement doit être fiable.

Prenez aussi soin de sécuriser tous vos appareils mobiles, particulièrement lorsque vous en configurez un nouveau, en mettant en pratique quelques actions simples:

- Définissez un code d'accès à votre appareil et activez le verrouillage après un délai d'inactivité.
- Désactivez les connexions Bluetooth et le Wi-Fi lorsque vous n'en avez pas besoin.
- Mettez régulièrement à jour les applications et le système d'exploitation de vos appareils.
- Ne partagez pas d'informations sensibles par texto ou courriel.
- Bloquez les numéros de téléphone qui vous envoient des messages non désirés.
- Synchronisez vos appareils avec un ordinateur pour sauvegarder vos données.

Alerte de sécurité Android : un milliard d'appareils ne reçoivent plus de mises à jour

Sécurité : Si vous utilisez la version 6.0 d'Android ou une version antérieure, vous êtes vulnérable à des attaques via malware. Les mises à jour automatiques de sécurité ne sont plus livrées depuis au moins un an.



Par Steve Ranger | Lundi 09 Mars 2020

Réactions

3

Tweet

LinkedIn

plus +



Plus d'un milliard d'appareils Android dans le monde ne sont plus pris en charge par les mises à jour de sécurité, ce qui les rend potentiellement vulnérables aux attaques assure l'organisation britannique de protection des consommateurs Which?

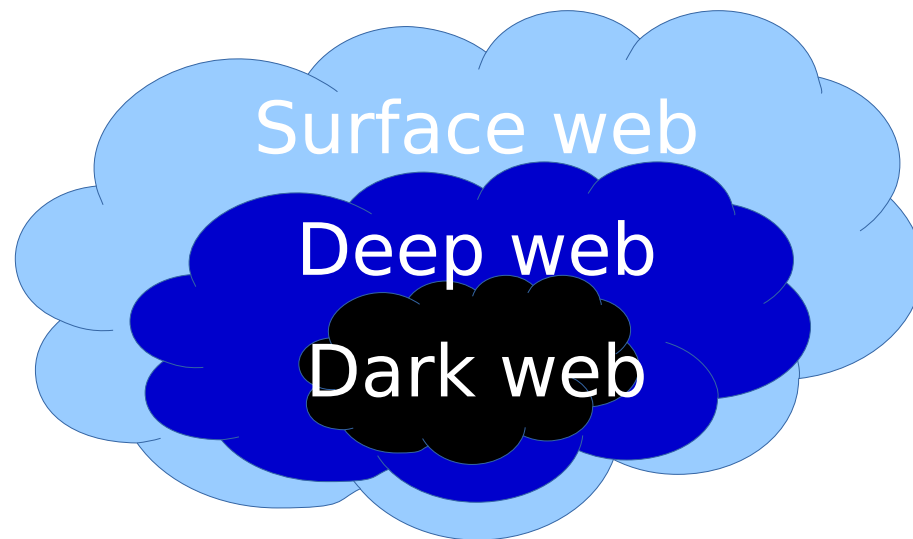


- L'hygiène numérique est un savoir de base indispensable
- Elle constitue la barrière la plus efficace pour les attaques les plus courantes
- Elle est peu efficace contre des moyens très sophistiqués... heureusement rares



Petit tour sur le DarkWeb





Tor | **Browser**



Surface web :

- Wikipédia
- Site web public
- Vidéos publiques
- ...

Deep web (>95%) :

- Webmail
- Intranet
- Banque en ligne
- Plateforme vidéo à la demande
- ...


Dark web (très minoritaire) :

- Journalisme non censuré
- Liberté d'expression
- Lanceurs d'alerte
- Confidentialité
- ... mais pas que légitime !



- NSA : <http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/>
- Secure Drop :
<http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/>
- Duckduckgo : <https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>







- Vérifier les liens .onion avant de cliquer
- Ne pas utiliser ton téléphone pour surfer
- Ne rien télécharger
- Ne pas communiquer d'infos perso
- Ne rien acheter
- Faire très attention à la légalité de ce que l'on consulte
- L'anonymat n'est pas garanti



LEAKED DATA

 TWITTER
 PRESS ABOUT US

 HOW TO BUY BITCOIN
 AFFILIATE RULES

 CONTACT US
 MIRRORS

azliver.com 13D 17h 20m 37s \$ 150 000 Our Mission Our mission is to provide state-of-the-art, innovative, and compassionate care to patients affected by liver diseases. Updated: 29 Jan, 2023, 10:52 UTC 114	ylresin.com 6D 04h 59m 32s \$ 30 000 Yuen Liang Industrial & Co., Ltd. is an enterprise in Taiwan, China, with the main office in Kaohsiung City. The company operates in the Automobile Dealers sector. The company was established on Updated: 28 Jan, 2023, 19:37 UTC 458	elsan.care 7D 09h 55m 05s stolen: 821 GB. data: marketing, finance, information of all departments of one of the company's clinics, numbers, personal data of employees, contracts, reports, internal and Updated: 26 Jan, 2023, 07:37 UTC 2795	xlntinc.com 14D 23h 47m 56s XLNT Software Solutions offers a variety of services to end-users of our Enterprise Application Software and developers. Located in Lancaster, Pennsylvania, United States. Updated: 24 Jan, 2023, 14:19 UTC 2586
miguelmechanical.com 3D 02h 03m 06s Miguel Mechanical Services Limited (MMSL) has been in existence as a service provider in the Oil and Gas Industry since 1988. With over 25 years experience as an Organization, we staff well Updated: 22 Jan, 2023, 06:34 UTC 3612	ibb-business-team.de 1D 00h 00m 58s Financing offers in Berlin for start-ups, SMEs and real estate IBB Business Team GmbH is a 100% subsidiary of the IBB Group. On behalf of the State of Berlin and the Investment Bank of Berlin Updated: 22 Jan, 2023, 06:32 UTC 3701	payroll2u.com PUBLISHED UPDATE!!! If you want to buy whole pack of source codes (Web, Mobile, etc) just pay for it! Hi to all! Let us introduce another IT company that provide super-secure payroll services in Asia :) Updated: 23 Jan, 2023, 10:55 UTC 4029	tvk.nl 9D 04h 30m 57s Ton van Kuyk (TVK) is your Volvo dealer in North Holland for new Volvos, used Volvos and maintenance. Company that operates in the Automotive industry. Updated: 18 Jan, 2023, 19:02 UTC 4633
duomed.com 3D 00h 28m 21s \$ 200 000 The Duomed Group is a dynamic organization with a well-established reputation and is active in consultancy, sales, integration, training and technical support of medical devices and Updated: 18 Jan, 2023, 18:01 UTC 4555	merlinpcbgroup.com 9D 21h 23m 46s \$ 500 000 Merlin PCB Group companies have been manufacturing and supplying PCBs to a global market for over 35 years with sustained growth based on continual investment in the very best Updated: 18 Jan, 2023, 11:55 UTC 1907	politriz.ind.br 4D 09h 22m 12s Fundada em 1989 EM UBERLÂNDIA/MG, em modestas instalações com a força de um jovem empreendedor que acreditou e viu a oportunidade de mudar sua vida e ao mesmo tempo mudar a Updated: 27 Jan, 2023, 04:44 UTC 6509	atcuae.ae 5D 15h 17m 07s Since its inception in 1965, ATCUAE has played a leading role in the development of motorsport on both the national and international level. Today, it governs approximately 140 competitive events Updated: 16 Jan, 2023, 11:48 UTC 4974

UNTIL FILES 2D23H29M25S PUBLICATION

Deadline: 01 Feb, 2023 15:00:04 UTC



duomed.com

The Duomed Group is a dynamic organization with a well-established reputation and is active in consultancy, sales, integration, training and technical support of medical devices and technology for hospitals and medical practices.
Local expert teams sell, install, integrate and maintain these products and solutions in high technological, critical medical environments in different European countries.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 16 JAN, 2023 18:00 UTC

UPDATED: 16 JAN, 2023 18:01 UTC

EXTEND TIMER FOR 24 HOURS

DESTROY ALL INFORMATION

DOWNLOAD DATA AT ANY MOMENT

\$ 3000

\$ 200000

\$ 200000

1-4 of 5





Les tâches à faire sont très nombreuses, il ne faut pas se décourager :

- Ne pas chercher à être parfait à court terme
- Adopter une démarche de progression continue
- On traite d'abord le maillon le plus faible

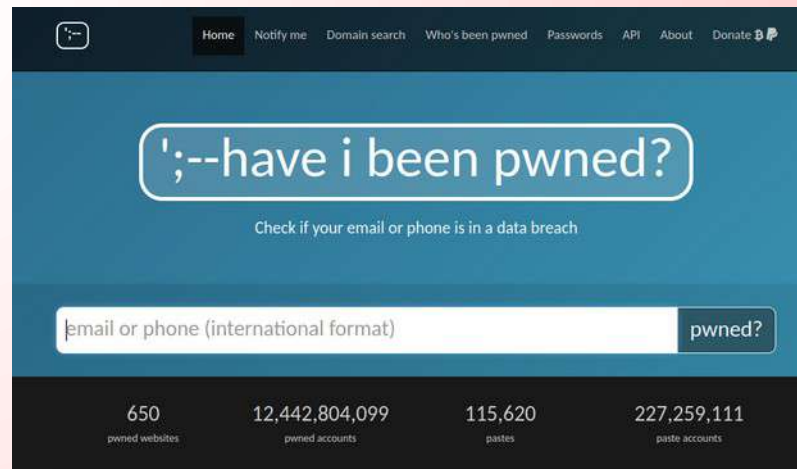


« Cela n'arrive qu'aux autres »

- L'actualité le dément (IUT de UPC)
- Les attaques sont très nombreuses chaque jour. Le hameçonnage par courriel en est une illustration visible
- Toujours pas convaincu ?



<https://monitor.mozilla.org>





haveibeenpwned.com

<https://haveibeenpwned.com/>

';--have i been pwned?

Check if your email address is in a data breach

email address

pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

739	12,864,327,356	115,766	228,881,584
pwned websites	pwned accounts	pastes	paste accounts



Firefox Monitor

<https://monitor.mozilla.org>

Récapitulatif des bonnes pratiques



1 – Faire des sauvegardes



2 – Faire les mises à jour



3 – Bien gérer ses mots de passe



4 – Protéger l'accès physique à vos ordinateurs



5 – Attention aux messages !



6 – Ne pas travailler avec un compte administrateur

Compléments « Les 10 mesures essentielles pour assurer votre cybersécurité »

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique>



7 – Choisir une bonne solution de sécurité



8 – Télécharger sur les sites officiels et préférer le libre si possible



9 – Chiffrer ses disques



10 – Limiter ses traces



11 – Éviter les wifi publics



12 – Se méfier des smartphones

You're an expert now !

