

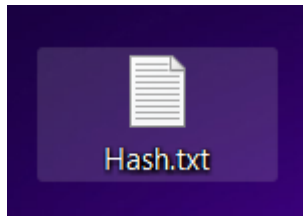
Objectif: Ce compte rendu a deux objectifs principaux. D'abord, apprendre à vérifier si un fichier a été modifié en utilisant des programmes de hachage comme HashCalc. Nous avons pu voir qu'une petite modification dans un fichier change complètement son empreinte numérique. Ensuite, comprendre les dangers des cyberattaques en étudiant 5 cas réels qui ont touché la France en 2024. Cela nous permet de voir comment les pirates attaquent et quelles protections mettre en place pour éviter le vol de données.

Partie 1: CyberSécurité Hachées.....	2
Étape 1 : Créer un fichier texte.....	2
Étape 2 : Installer HashCalc.....	2
Étape 3 : Calculer un algorithme pour le fichier Hash.txt.....	4
Étape 4 : Modifier le fichier Hash.txt.....	6
Étape 5 : Calculer un nouvel algorithme pour le fichier Hash.txt.....	7
Partie 2: CyberSécurité Volées.....	10

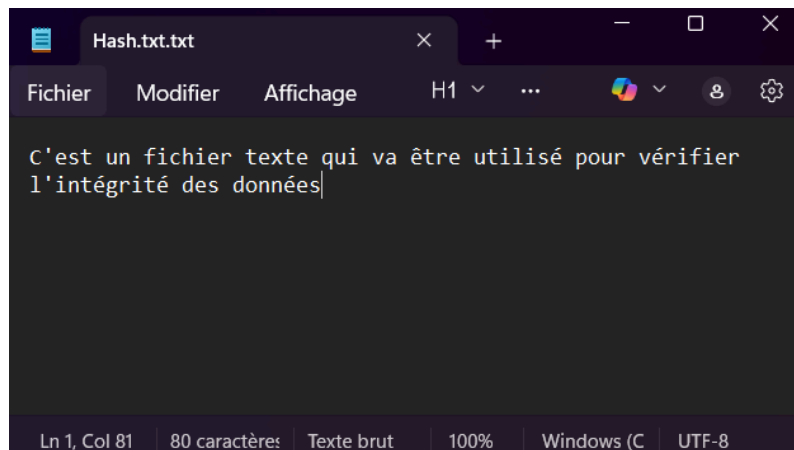
Partie 1: CyberSécurité Hachées

Étape 1 : Créer un fichier texte

1) Ouvrez le Bloc-notes (Notepad) sur votre ordinateur



2) Tapez un texte,




3) Enregistrez le fichier CTRL + S

Étape 2 : Installer HashCalc

Voici le lien en dessous pour télécharger,
<https://hashcalc.software.informer.com/download/>

Download the latest version from Software Informer

 Scanned by 76 antivirus programs on Feb 11, 2025.
The file is clean, [see the report](#).



Download now

Version: 2.02 (x86)

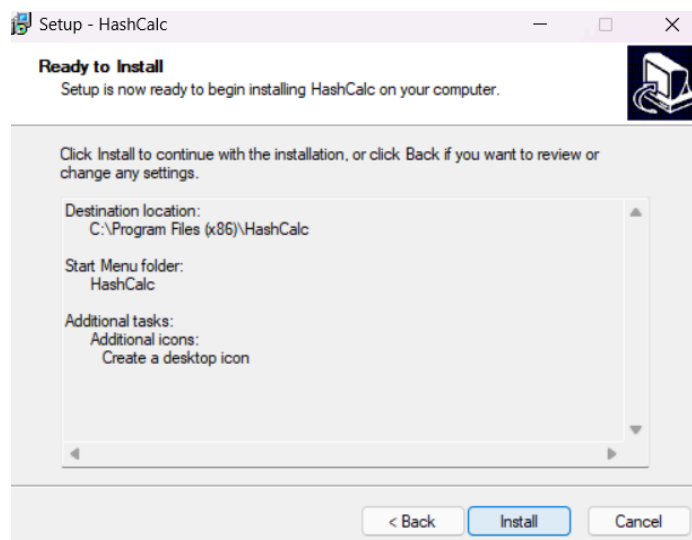
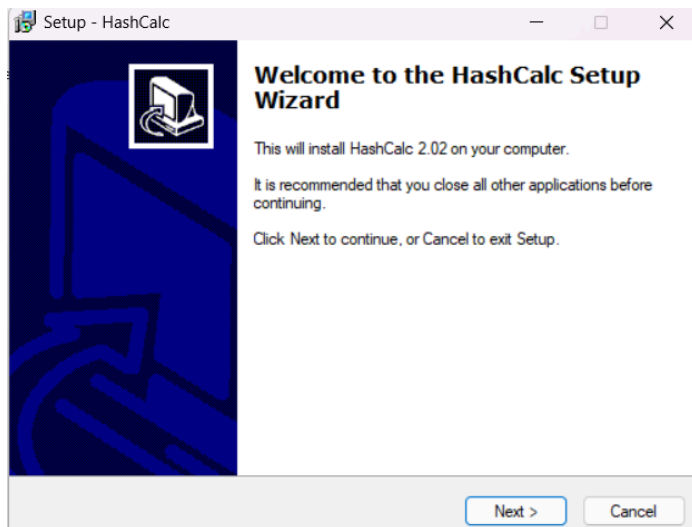
File name: hashcalc.zip

Size: 464 KB

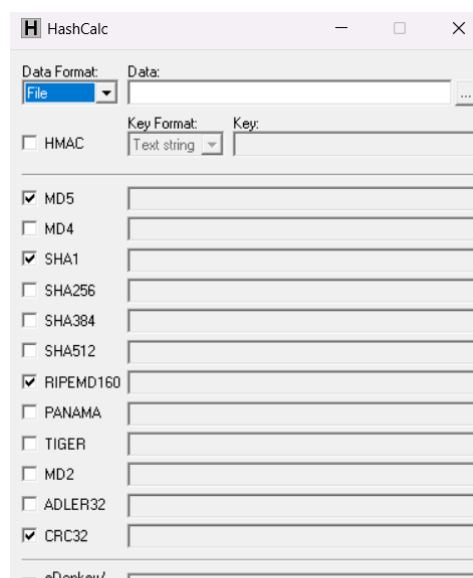


Visit the home page
slavasoft.com

Puis exécuter le fichier d'installation et suivre les instruction d'installation,

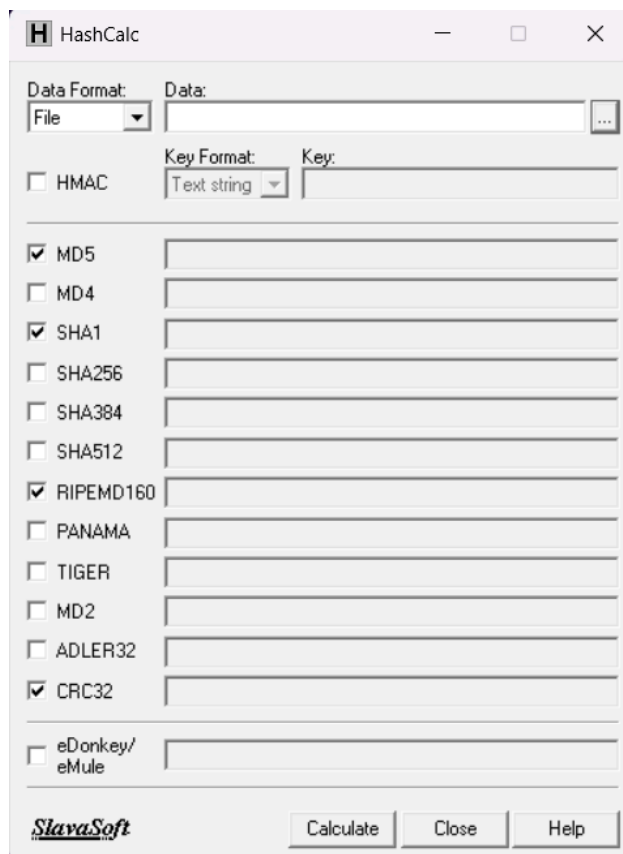


Et puis lancer

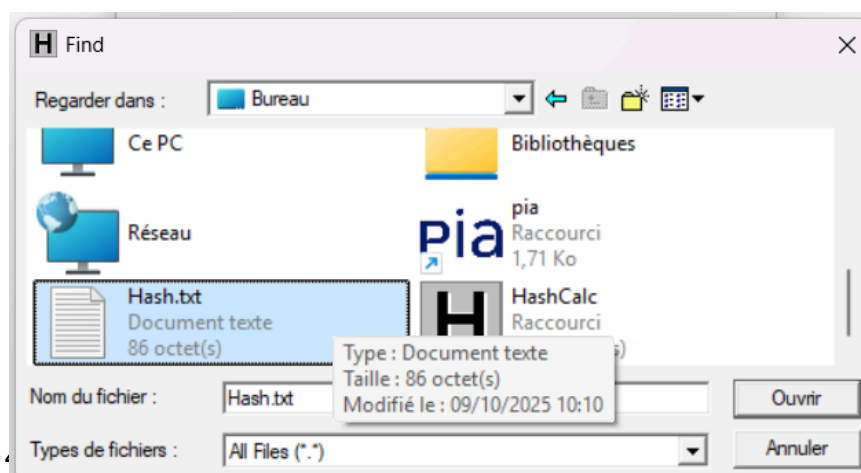


Étape 3 : Calculer un algorithme pour le fichier Hash.txt

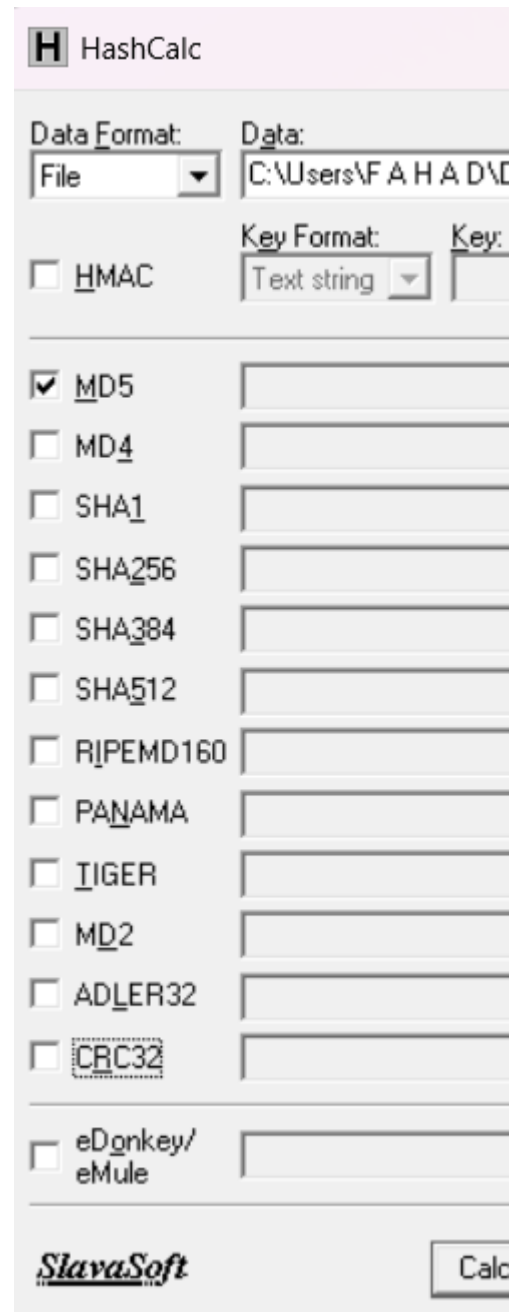
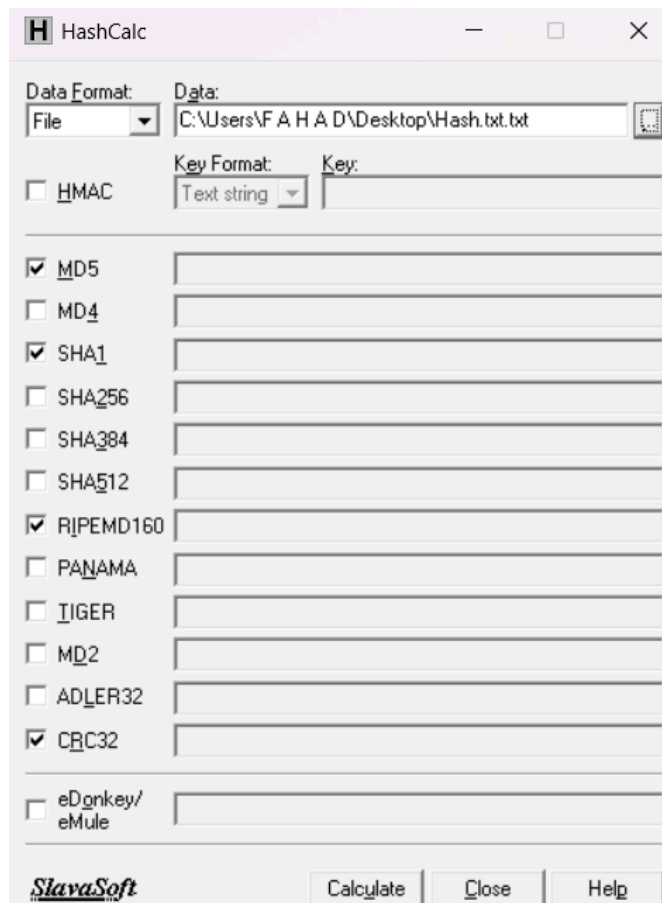
1) Ouvrez HashCalc et Configurez HashCalc,



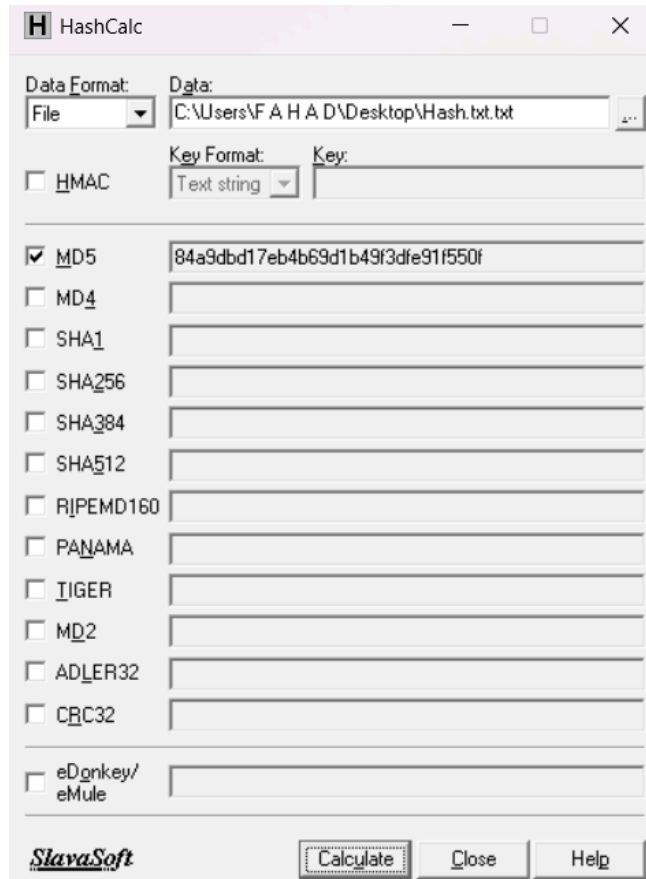
Pour configurer il faut bien verifier que **data format** est bien dans le file et puis juste a droite il y a **data** donc dans le data il faut aller chercher hash.txt dans le bureau,et l'ouvrir



Et puis on voit tout les algorithmes à gauche et il faut tout décocher et garder juste **MD5**,



Et puis il faut cliquer sur calculer,

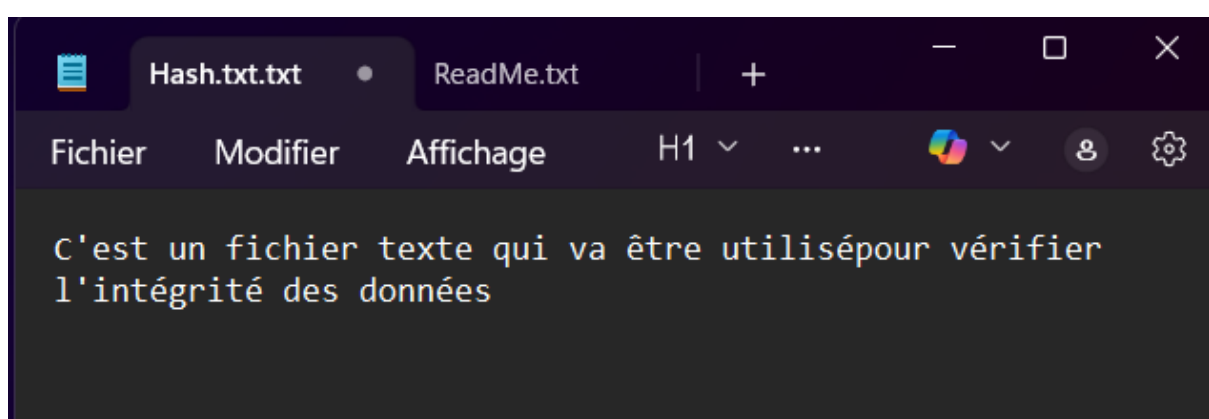


NOTEZ la valeur à côté de MD5 (c'est une longue chaîne de caractères) 84a9dbd17eb4b69d1b49f3dfe91f550f

Étape 4 : Modifier le fichier Hash.txt

Pour l'étape 4 il faut Retourner sur le Bureau et ouvrez le fichier Hash.txt,

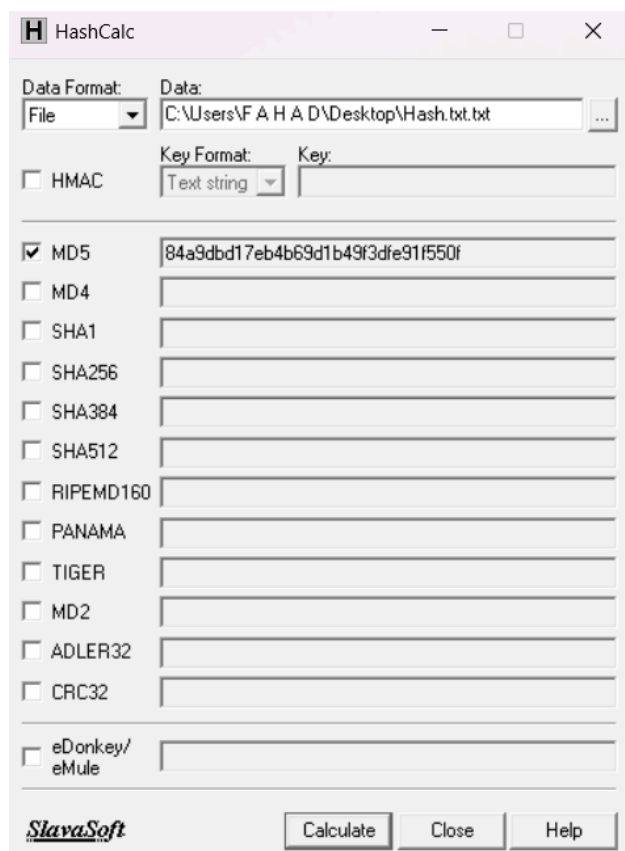
Modifiez légèrement le texte : Supprimez une lettre, OU un espace, et Enregistrez le fichier



Étape 5 : Calculer un nouvel algorithme pour le fichier Hash.txt

Donc maintenant,

Retournez dans **HashCalc** et refaire l'étape de calculer,

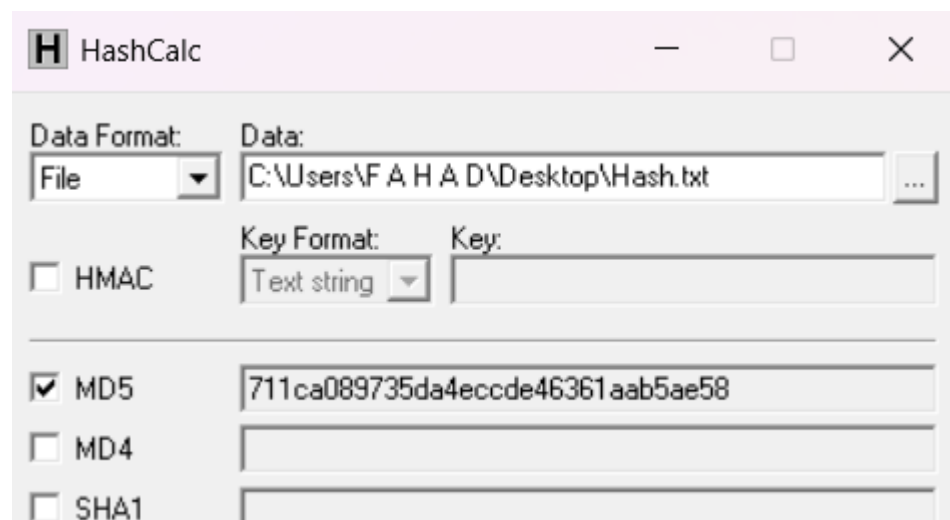


avant

84a9dbd17eb4b69d1b49f3dfe91f550f

apres

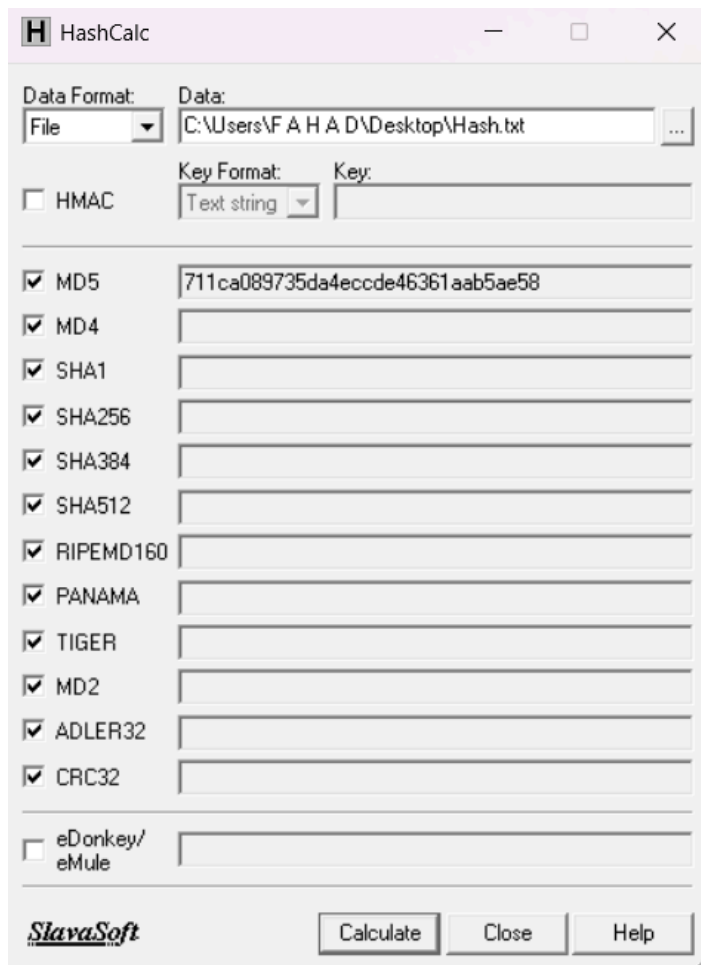
711ca089735da4eccde46361aab5ae58



On voit quoi en modifiant juste un peu le texte la valeur se change directement,

Donc l'étape suivante est de coucher tous les types de d'algorithme,et voir le resultat,

Et voici,



Après observation on voit que Certains algorithmes créent des valeurs plus longues que d'autres

The screenshot shows the HashCalc application window. At the top, the title bar reads 'HashCalc'. Below it, the 'Data Format' is set to 'File' and the 'Data' field contains the path 'C:\Users\F A H A D\Desktop\Hash.txt'. The 'Key Format' is set to 'Text string' and the 'Key' field is empty. A list of hash algorithms is shown with checkboxes and their corresponding hash values:

Algorithm	Hash Value
<input checked="" type="checkbox"/> MD5	711ca089735da4eccde46361aab5ae58
<input checked="" type="checkbox"/> MD4	701b26a6b792df915bd4f8dd77794406
<input checked="" type="checkbox"/> SHA1	d567b79bab306ab81e649b8e84a536cd3f3f9b08
<input checked="" type="checkbox"/> SHA256	16590c54e029ff2f419feaf674523eaad5cd5e3a6b134aa4
<input checked="" type="checkbox"/> SHA384	e375e289dbaaf08e17057b644abf6448c09e03dc476c85
<input checked="" type="checkbox"/> SHA512	e98f0d69c6d22bde6ed1748da729043f6e5c52ab3db1f0b
<input checked="" type="checkbox"/> RIPEMD160	8944369c8ccc0420f5c077412f4184d5f455e254
<input checked="" type="checkbox"/> PANAMA	5c7d89b57cbbb53ee7bb8a25738c0e4d8cec56bfe51a18
<input checked="" type="checkbox"/> TIGER	68865a91d89152bfa5f56e8643d0147e11d32943d9825ff
<input checked="" type="checkbox"/> MD2	c67d401f2b6f1540ad84b204d56f406d
<input checked="" type="checkbox"/> ADLER32	54a12533
<input checked="" type="checkbox"/> CRC32	d00c9210
<input type="checkbox"/> eDonkey/ eMule	

Partie 2: CyberSécurité Volées

ÉTAPE 1 : Rechercher des cas de failles récentes

1. Viamedis et Almerys - Santé - Janvier 2024
2. France Travail - Public - Février-Mars 2024
3. Free - Télécommunications - Octobre 2024
4. Intersport - Commerce - 2024
5. Hôpital Simone Veil de Cannes - Santé - Janvier 2024

TABLEAU DES 5 CAS DE FAILLES

Date de l'incident	Entreprise touchée	Nombre de victimes	Données volées	Méthodes utilisées	Source de référence
Janvier 2024	Viamedis et Almerys (prestataires de santé)	33 millions de personnes	Noms, prénoms, dates de naissance, numéros de Sécurité sociale, noms des assureurs santé	Compromission d'identifiants de professionnels de santé pour accéder aux systèmes	cybermalveillance.gouv.fr
Février-Mars 2024	France Travail (anciennement Pôle Emploi)	43 millions de personnes	Noms, prénoms, dates de naissance, numéros de Sécurité sociale, adresses, numéros de téléphone	Usurpation d'identité de conseillers Cap Emploi, malware sophistiqué	jedha.co
Octobre 2024	Free (opérateur télécom)	43 millions de personnes	Données personnelles, IBAN (coordonnées bancaires), 100 000 adresses publiées sur le Dark Web	Attaque via l'outil de gestion des abonnés, exploitation d'une vulnérabilité	kiwi-backup.com
2024	Intersport (commerce sportif)	Non précisé	52 Go de données : informations personnelles des clients et employés	Intrusion dans les systèmes informatiques, exfiltration de données	netexplorer.fr
Janvier 2024	Hôpital Simone Veil (Cannes)	Patients et personnel	Données médicales et administratives	Ransomware chiffrement de toutes les données	docs.cartographit.com

			tives	données	
--	--	--	-------	---------	--

Quelles sont les mesures à prendre pour éviter ces types d'intrusion ?"

- Pour éviter ces types d'intrusion, les organisations doivent d'abord renforcer l'authentification en mettant en place l'authentification multi-facteurs sur tous les systèmes critiques et en imposant des mots de passe complexes régulièrement renouvelés. La formation du personnel est également essentielle car de nombreuses attaques exploitent la négligence humaine, notamment à travers des campagnes de phishing. Les entreprises doivent maintenir leurs systèmes à jour avec les derniers correctifs de sécurité et mettre en place des sauvegardes régulières déconnectées du réseau pour pouvoir restaurer les données en cas d'attaque par ransomware. Il est crucial d'appliquer le principe du moindre privilège en limitant les accès aux seules personnes qui en ont réellement besoin et de surveiller activement les comptes à privilèges. Enfin, les organisations doivent déployer des outils de surveillance proactive pour détecter rapidement les comportements anormaux et préparer un plan de réponse aux incidents pour réagir efficacement en cas de cyberattaque. Ces mesures combinées permettent de réduire considérablement les risques d'intrusion et de limiter l'impact des attaques.

Conclusion

Ces deux exercices nous ont permis de découvrir des outils importants pour la sécurité informatique. Avec HashCalc, nous avons appris que les fonctions de hachage permettent de détecter si un fichier a été modifié, ce qui est très utile pour vérifier l'intégrité des données. L'étude des cyberattaques de 2024 montre que personne n'est à l'abri : entreprises, hôpitaux et services publics ont tous été touchés. Ces attaques ont affecté des millions de personnes et volé des données sensibles. Pour se protéger, il faut former les employés, utiliser des mots de passe forts, mettre en place l'authentification à double facteur et faire des sauvegardes régulières. La cybersécurité est aujourd'hui essentielle pour protéger nos informations personnelles et professionnelles.