e-santé Occitanie
Connecter pour mieux soigner

Les cryptolockeurs ou rançongiciels

Bruno POUJOULAT 07/09/2021

SOMMAIRE

Qu’est-ce que c’est ?

- Définition
- Comment se transmet-il ?
- Pourquoi les antivirus ne le détectent-ils pas ?

Comment s’en protéger ?

- Les mesures techniques
- Les mesures organisationnelles

Quel est le niveau de risque réel ?

- Qui est visé ?
- Qui est touché ?
- Avec quelles conséquences ?

Que faire si on est infecté ?

- Les mesures d’urgences pour limiter la propagation
- La désinfection
- Le retour à la normale

01

Qu’est-ce que c’est ?

Définition, fonctionnement

- Définition
  - Logiciel malveillant
  - Chiffrement des donnée (symétrique / asymétrique / hybride)
  - Rançon
  - Vol de données associé (évolution plus récente)

- Fonctionnement : Cheval de Troie
  - Web exploit (site web infecté qui exploite flash vulnérable)
  - Phishing mail (Word avec macro qui télécharge l'exécutable, Ryuk via Emotet et Trickbot)

- Quid des antivirus ?
  - Téléchargement en plusieurs étapes
  - Campagnes très courtes (signatures obsolètes)

Quel est le niveau de risque réel ?

Evaluation du risque, historique, actualité

- Menace n°1 pour les entreprises
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Traçabilité

- Tous les domaines sont touchés
  - Laboratoires, EHPAD, Hôpitaux (Ryuk, « le + rentable »)
  - Industrie (Ubisoft 10/2020, Colonial Pipeline 07/05/2021)
  - ESN (SOPRA-STERIA 11/2020)

- Actualités
  - Locky, Petya, WannaCry, NotPetya
  - CH Arles (08/2021), Memorial Health System (08/2021), Dordogne (2021), Dax (2021)
  - Décès en Allemagne (09/2020),
  - Lien malware/groupe malveillant (Maze => Egregor)

Comment s’en protéger ?

Mesures techniques, organisationnelles

- Infections : Droits sur les documents
  - Gestion fine
  - Désactivation des macros
- Transmission :
  - Cloisonnement
  - SIEM, EDR, XDR
  - Logiciels d'analyse comportementale
- Organisation :
  - Sensibilisation
  - Sauvegardes (déconnectées du réseau)

Que faire en cas d’infection ?

De l’alerte au retour à la normale

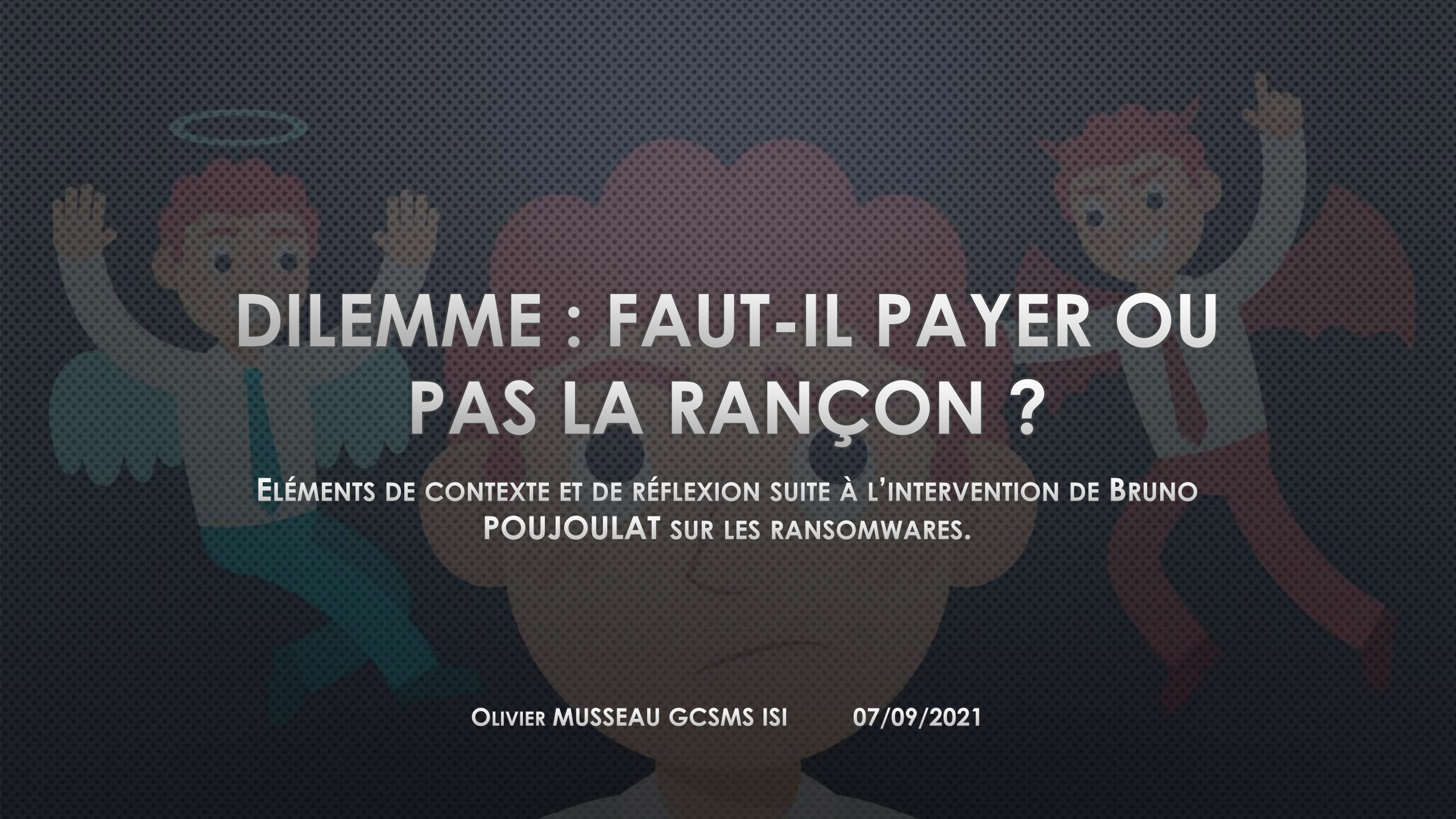
- L’urgence
  - Déconnection, isolement
  - Évaluation, appel à l’aide (sociétés spécialisées, OIV/OSE et ANSSI)

- La gestion de crise
  - Désinfection du SI
  - Communication
  - Archivage des données chiffrées

- Le retour à la normale
  - Restauration des données via sauvegardes
  - Payer la rançon ? (financièrement abordable/techniquement accessible/relativement fiable)

Merci de votre attention.

e-santé Occitanie
Connecter pour mieux soigner



DILEMME : FAUT-IL PAYER OU PAS LA RANÇON ?

Eléments de contexte et de réflexion suite à l'intervention de Bruno POUJOULAT sur les ransomwares.

Olivier MUSSEAU GCSMS ISI 07/09/2021

Avant toute chose, payer signifie-t-il récupérer ses données ?

Payer ne signifie pas toujours que l'on va récupérer ses données. C'est un peu la question que l'on se pose lorsque les personnes avec lesquelles on traite sont des pirates. Quelle est l'assurance de récupérer ses données une fois la rançon versée ? Si une personne veut vous nuire, seriez-vous prêt à lui faire confiance et lui attribuer en plus une récompense ?

Une étude menée sur les comportements de plus de 1 000 salariés confrontés à un ransomware, réalisée par l'entreprise californienne Intermedia, révèle que 19 % du temps les informations ne sont pas récupérées, même après le versement de la rançon.

La clé de déchiffrement n'est pas un remède miracle

Dans certains cas, il est impossible de restaurer les systèmes informatiques avec uniquement la clé de déchiffrement. Les fichiers peuvent avoir été corrompus. Lors de l'attaque ou de la réaction, d'autres composants peuvent avoir été endommagés. De plus, la clé vous permet uniquement de déchiffrer. Elle ne soigne pas le mal « profond » qui aura permis à l'attaquant de vous toucher… et de revenir dans le futur !

Les auteurs ont été assez corrects pour s'assurer qu'après le paiement de la rançon le système déchiffre automatiquement le contenu de votre ordinateur ? Mais du fait des activités des experts en sécurité et de la police, certains serveurs sur lesquels le système entier fonctionne ont été fermés, ce qui fait que le processus de déchiffrage ne marche pas toujours comme prévu…

Le double effet kiss cool !

La très grande majorité des entreprises qui payent reçoivent une seconde attaque dans la foulée. Et dans presque la moitié des cas, c'est le même ransomware qui frappe !

Les forces de l'ordre mettent en garde : il ne faut jamais payer de rançon, car cela finance la cybercriminalité et l'on n'est jamais sûr que les malfrats tiennent leur parole. Un sondage réalisé par Cybereason auprès de 1 263 professionnels de la cybersécurité semble leur donner raison :

Parmi ceux qui ont mis la main au portemonnaie, seuls 51 % ont pu totalement retrouver leurs données. 3 % n'ont rien pu récupérer du tout et 46 % se sont retrouvés avec des données partiellement altérées.
Mais ce n'est pas tout. 80 % des entreprises qui ont payé ont été frappées par une seconde attaque dans la foulée. Et dans 46 % des cas, il s'agissait du même ransomware ! Comme quoi la parole des cybercriminels ne mérite aucune crédibilité.

Quelques précautions d'usage

Certaines tactiques, comme demander une « preuve de vie » pour décrypter une partie de l'environnement avant le paiement, ou négocier les conditions de paiement (50 % immédiatement et 50 % une fois l'environnement décrypté, par exemple), peuvent parfois fonctionner.

Cependant, la première chose à faire dans cette situation est de s'assurer de la réalité de l'attaque en cours. Les tentatives d'escroqueries « au bluff » sont quotidiennes. Sur un malentendu ça peut toujours marcher…

Légalité et moralité

Aussi étrange que cela puisse paraitre, il n'y a rien d'illégal à verser la rançon demandée par un ransomware, même si le chiffrement des données d'un tiers sans son consentement et la demande de rançon qui s'en suit constituent des infractions pénales.

Il est néanmoins fortement déconseillé par les autorités de céder au chantage du ransomware. Derrière ces attaques se cachent souvent des groupes terroristes. La rançon payée pourrait donc servir à financer des activités criminelles, les entreprises peuvent faire face à des poursuites judiciaires le cas échéant. La décision de céder au chantage d'un ransomware ne doit jamais se faire à la hâte, encore moins sous le coup de la pression. Plusieurs paramètres doivent être pris en compte afin de ne pas être à nouveau victime d'un traquenard. Dans ce cas, l'entrée en scène d'un conseiller juridique, des forces de l'ordre ou de professionnels de la sécurité comme des cyber assureurs est nécessaire. Ces derniers pourront faire une évaluation minutieuse de la situation et proposer la meilleure attitude à adopter selon les cas.

L'interdiction de payer les rançons ne règlera pas le problème

Il est même à craindre que cela alimente un cycle sans fin. Bien que les gouvernements découragent les organisations de payer des rançons aux cybercriminels, cette pratique n'est pas illégale, même si des appels ont été lancés pour qu'une législation soit élaborée afin d'interdire le paiement de rançons.

« Vous interdisez les paiements, pas les personnes qui peuvent ou non faciliter les paiements. Interdire aux assureurs de couvrir les paiements, mais ne pas interdire aux entreprises de céder au chantage, n'a aucun sens. Soit on interdit les paiements, soit on ne les interdit pas. Ce n'est pas aux assureurs d'élaborer des politiques publiques, c'est aux gouvernements de le faire ! »

Ciaran Martin, ancien directeur du National Cyber Security Centre (NCSC), le gendarme britannique de la cybersécurité.

En synthèse

À l'heure actuelle, la décision de payer une rançon est entièrement entre les mains des entreprises privées, qui décident en fin de compte de ce qui est le mieux pour elles – et si cela signifie payer une rançon, elles la paieront. Reste que si l'idée d'interdire les rançons peut sembler séduisante, elle ne constitue pas une solution miracle contre les attaques par ransomware. Il est probable que les cybercriminels continueront à mener leurs campagnes, mais en sachant qu'ils peuvent toujours s'attaquer aux cibles faciles qui n'ont pas le choix lorsqu'il s'agit de payer une rançon – que ce soit illégal ou non.

Quelques chiffres actualisés sur le bizness du ransomware : https://ransomwhe.re/index.html

« Toutes les 40 secondes dans le monde, une entreprise est victime d'une attaque par ransomware. »

Entre payer rapidement pour voir ses données débloquées ou résister et prendre le risque de les perdre, quelle attitude adopter ?

En 2021 le mot de passe ne suffit plus !

Mais il n’est pas près de disparaitre pour autant…

Olivier MUSSEAU, GCSMS ISI

07/09/2021

« Un mot de passe aide les honnêtes gens à rester honnêtes, en protégeant un ordinateur ou un service web contre tout accès non autorisé ***occasionnel*** ».

Mais d'où vient ce problème de mot de passe ?

>Les sites se font pirater et voler les mots de passe stockés.

Il suffit de pirater la base de données du site ou d'acheter une liste de mots de passe compromis.

>Les utilisateurs se font voler leur mot de passe : social engineering.

Campagne de phishing, fausse intervention…

>Les pirates « devinent » les mots de passe.

Utilisation de dictionnaires, d'informations personnelles…

Comment les hackeurs volent-ils les mots de passe ?

Un peu d'ingénierie sociale

« La plus grande faille d'un système informatique se trouve entre le clavier et la chaise de bureau », dit l'adage. Parmi les techniques les plus simples et les plus efficaces de vol de mots de passe, on retrouve ainsi celles qui impliquent de tromper ou manipuler l'utilisateur. Le célèbre hameçonnage (ou phishing) consiste à créer un faux site Internet prenant l'apparence d'un service légitime, et à inciter l'utilisateur à s'y connecter. Son mot de passe en clair peut alors être volé en toute tranquillité.
Les méthodes les plus couramment utilisées sont les attaques de phishing, mais une approche moins courante est le "shoulder surfing" (qui signifie regarder par-dessus l'épaule) qui consiste, pour le pirate, à simplement regarder un utilisateur saisir son mot de passe, à son insu.

D'autres procédés touchant à l'ingénierie sociale permettent, dans le cas de services peu regardants sur leur sécurité, de parvenir au mot de passe de manière encore plus simple. Certaines plateformes posent des questions de sécurité à l'utilisateur comme « Quel était le nom de votre premier animal de compagnie ? » ou « Dans quelle ville avez-vous décroché votre premier emploi ? » lors de la procédure de recouvrement de compte (*account recovery*). Les réponses à ces questions peuvent souvent être dénichées sur les comptes Facebook ou Twitter, et les utilisateurs y ayant répondu sincèrement peuvent se trouver exposés.

La force brute, ou le nerf de la guerre

Un hackeur peut demander à un ordinateur de prendre un compte et potentiellement tester des milliers de mots de passe par seconde. Les mots de passe courts et dépourvus de caractères spéciaux sont ainsi particulièrement vulnérables. Mais dès que le mot de passe se rallonge, la difficulté pour l'ordinateur à le casser augmente de façon exponentielle.

Si la longueur et la complexité du mot de passe restent un gage de solidité, des techniques informatiques existent pour rendre la force brute plus efficace. Dans la variante de l'attaque par dictionnaire, l'ordinateur essaye en premier une série de mots courants, par exemple des mots du dictionnaire, ainsi que certains des mots de passe les plus fréquemment usités.

Nombreux sont les utilisateurs à recourir aux mêmes mots de passe extrêmement simples, tels que « 12345 » ou « azerty ».

Cela a inspiré certains hackeurs à mettre au point la technique de la force brute inversée. Elle consiste à prendre un mot de passe répandu et à l'essayer au hasard sur des utilisateurs, jusqu'à ce que cela marche. Pour faire une analogie avec des portes verrouillées, c'est comme si beaucoup de gens fermaient leurs maisons par des serrures ouvrables avec les mêmes clés. Il suffit alors de prendre une clé courante et de la tester sur diverses portes, pour voir lesquelles s'ouvrent.

L’homme du milieu

Pourquoi s’acharner à dépenser de la puissance de calcul pour casser un mot de passe, quand on peut tout simplement l’intercepter au vol ? C’est ce qu’on appelle les attaques par l’homme du milieu (man-in-the-middle, abrégé en MITM). C’est une famille d’attaques très utilisées pour espionner les communications d’un utilisateur à son insu. Le hackeur peut par exemple compromettre un point Wifi public (qui n’est pas protégé par un mot de passe ou qui ne chiffre pas ses communications) de façon à observer tout le trafic Internet qui passe par celui-ci — y compris les mots de passe saisis sur des sites Web.

On peut également envoyer un petit virus-espion à l’intérieur de la machine de l’utilisateur. Ce cheval de Troie peut par exemple enregistrer tout ce qui est tapé au niveau du clavier : on parle alors d’un keylogger. Mais à moins de vous égarer à la DEFCON, la convention annuelle de hackeurs à Las Vegas où les festivaliers se font un plaisir à se pirater mutuellement, ce genre d’attaques ne se produit pas tous les jours. Il reste tout de même conseillé de ne pas se connecter à n’importe lequel de ses comptes sur un réseau Wifi ou un ordinateur public.

Lorsque DEFCON rime avec AMAZON : https://yourls.gcsms-isi.fr/hztms

Piratage des services

Vous aurez beau prendre toutes les précautions possibles, le plus grand risque qu'on vous vole vos identifiants se trouve au-delà de votre volonté. Car du point de vue d'un hackeur, plutôt que de s'attaquer individuellement à quelques utilisateurs négligents, pourquoi ne pas plutôt pirater le site Web entier et dérober tous les mots de passe qui s'y trouvent ? Cela arrive très régulièrement, y compris pour les plateformes les plus renommées.

Petite consolation : le butin des voleurs se limite généralement aux versions *hachées* des mots de passe. Le hachage est une technique cryptographique très efficace qui prend un bout de texte, le passe à la moulinette, et le transforme facilement en quelque chose qui ne lui ressemble plus du tout. Toute plateforme en ligne ayant de bonnes pratiques de sécurité ne stocke pas les mots de passe de ses utilisateurs « en clair », mais uniquement les versions hachées.

Lorsqu'un internaute se connecte et qu'il entre son mot de passe, celui-ci est haché avant d'être comparé à celui listé dans la base de données du site. Il peut ainsi être identifié sans difficulté ; mais si des hackeurs s'introduisaient dans la base de données, ils ne pourraient *à priori* récupérer que du contenu illisible.

Enfin, le pire scénario survient quand la plateforme a commis la lourde négligence (ou le simple bug) de stocker les mots de passe en clair. Cela n'arrive malheureusement pas qu'aux sites Web les plus douteux ou négligents. En mai 2018, Twitter intimait à ses 330 millions d'utilisateurs de changer de mots de passe après qu'ils se soient trouvés exposés en interne. En mars dernier, c'était au tour de Facebook d'admettre avoir stocké des centaines de millions de mots de passe de manière parfaitement lisible. Si aucune brèche de sécurité n'était avérée dans les deux cas, il y avait véritablement de quoi s'inquiéter.

La sécurité des mots de passe, l'un des plus grands défis de l’informatique

80 % des fuites de données en entreprise sont causées par des mots de passe faibles ou volés… La statistique est éloquente. Les mots de passe ne forment qu’une seule couche de protection et sont très facilement usurpés. En effet, il faudrait potentiellement 52 secondes à un pirate pour usurper un mot de passe de 8 caractères, même aléatoires, contre 11 minutes pour un mot de passe qui inclut des chiffres.

La solution ?

Ce qu'il nous faudrait, c'est une deuxième clé, une donnée supplémentaire sans laquelle un voleur ne pourrait pas entrer.

Pas quelque chose que l'on mémorise, mais plutôt que l'on garde sur soi, vos empreintes digitales, votre scan rétinien, un porteclé ou un petit circuit intégré dans votre téléphone portable.

Pour se connecter, il faudrait, en plus du nom et du mot de passe, présenter également cette donnée.

Les spécialistes de la sécurité désignent cette procédure par le terme «de double authentification», car elle exige la présence simultanée de deux informations de nature différente, quelque chose que vous savez et quelque chose que vous possédez.

La double authentification n'a rien de nouveau, les grandes entreprises et les organismes d'État les utilisent depuis longtemps.

Le sésame supplémentaire consiste souvent en une petite carte à radiofréquence ou tout autre bidule électronique qu'il faut relier à l'ordinateur avant de se connecter au site concerné. Mais ces systèmes sont chers et représentent un surcroit de travail pour le service informatique (quelqu'un doit savoir où se trouvent tous ces porteclés).

De ce fait, la double authentification ne s'est pas immédiatement étendue aux sites d'usage courant comme le webmail ou la consultation bancaire en ligne.

La double authentification (two-factor authentication, ou 2FA en anglais) est une méthode qui protège efficacement l'utilisateur, elle commence donc à se démocratiser depuis quelques années/mois avec l'avènement du e-commerce.

Deux preuves d'identité sont requises pour accéder à un compte : le mot de passe et un code à usage unique. Celui-ci sera par exemple transmis par SMS, appel téléphonique, token ou encore une application comme « Authenticator ».

Avec la double authentification, le pirate devra donc disposer de davantage d'éléments que le simple accès à votre ordinateur. Et en cas d'intrusion, les utilisateurs seront directement prévenus.

Attention, toutes les solutions MFA ne sont pas fiables et efficaces. C'est le cas de la double authentification par SMS, que les pirates arrivent désormais facilement à intercepter ou à rediriger.

Vous l'aurez compris, les obstacles à la généralisation de la double authentification ne sont pas d'ordre technique, mais plutôt culturel et commercial. Beaucoup de gens n'ont aucune envie d'être obligés de s'identifier en deux temps pour se connecter, et les fabricants vont devoir collaborer pour créer un nouveau standard facilement déployable sur un large éventail d'appareils et de services.

Malgré tout, il est certain que ces difficultés seront surmontées et que la double authentification deviendra la norme. Tous les jours, on constate que les mots de passe ne suffisent plus pour nous protéger des cybercriminels. Pourquoi continuer à se cacher derrière une telle évidence?

Conseils pour sécuriser les mots de passe en attendant la généralisation de la double authentification

Créer plusieurs mots de passe (1 pour chaque compte)

Utiliser un générateur de mot de passe (https://www.dashlane.com/fr/features/password-generator)

Miser sur la longueur (>10c)

Varier les caractères (mM!#123)

Utilisez un mot de passe impossible à deviner

Préférer l'aléatoire

Changer de mot de passe régulièrement (90j)

Retenir ses mots de passe sans les écrire (bonne mémoire ou…)

Utiliser un gestionnaire de mot de passe

Testez votre mot de passe (https://howsecureismypassword.net/)

Changez votre mot de passe au moindre soupçon

Ne communiquez jamais vos mots de passe à un tiers

N'utilisez pas vos mots de passe sur un ordinateur partagé

Changez les mots de passe par défaut des différents services auxquels vous accédez

Choisissez un mot de passe particulièrement robuste pour votre messagerie

Ressources discutées

Ressources discutées

- Demande de supports de sensibilisation à la question de la cybersécurité
  - Proposition : touscybervigilants.fr il y a un très bon kit
- Entreprises spécialisées si on est victime d'attaque ?
  - L'ANSSI publie un annuaire d'entreprises spécialisées : https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/
  - En Occitanie : voir Cyber'Occ - Le portail de la Cybersécurité en Occitanie (cyberocc.com)
  - Il faut en parallèle déclarer l'incident à l'ANSI
- Solutions de filtres pour les mails
  - Vdsecure, mailcleaner. Efficaces mais chers.
- Chiffrage DD
  - Bitlocker (ne pas perdre la clé)
- VPN gratuit
  - Synology
  - Open VPN pour se connecter au SI. Gratuit mais demande des compétences Linux
- Coffre fort numérique
  - Keepass. Homologué ANSSI et gratuit.