Hackers – Les maîtres du monde

La santé est de plus en plus ciblée, les attaques en sécurité informatique ont explosé ces deux dernières années. Les failles sont nombreuses et les vulnérabilités des établissements de santé sont connus des pirates, mais les laboratoires, les centres de santé et les praticiens isolés sont aussi source d'inquiétude. Si ce risque par rebond est maintenant bien connu, il existe dorénavant le risque intégré avec le développement des objets connectés.

Pascal Wolff – *Le Cardiologue n° 446 – Mai-juin 2022*

A la suite d'une discussion avec un confrère, le Dr Cinécare a voulu installer un logiciel de prise en main à distance. Devant la pléthore de programmes, il a préféré essayer une version gratuite trouvée sur le net avant l'achat définitif d'une version payante.

Le Dr Cinécare clique sur les liens pour installer ce logiciel sans fournir bien sûr de numéro de carte ni de coordonnées bancaires.

L’installation se passe tout à fait normalement.

Une fois la version gratuite enregistrée, plusieurs emails sont arrivés dans une langue étrangère pour confirmation. Normal, le logiciel gratuit est en langue anglaise. Pour la langue française, il devra s’acquitter de la version payante.

Le programme d’installation lui demande d’éteindre sa machine et de la rallumer pour accéder au logiciel. Une fois fait et l’ordinateur rallumé, le Dr Cinécare transfère ses données dans le nouveau logiciel.

UNE PERTE DE CONTRÔLE

Subitement, l’ordinateur se met à ralentir sérieusement et certaines applications deviennent particulièrement difficiles à contrôler…

Le Dr Cinécare éteint une nouvelle fois sa machine puis la redémarre, pensant à un problème de connexion, comme cela lui arrive régulièrement. Mais l’ordinateur est toujours aussi difficile à gérer. Pire, le curseur de la souris se déplace tout seul et son PC se met à taper des lettres sans son intervention.

Le Dr Cinécare se rend subitement compte que sa machine a été piratée et est ainsi devenue un PC Zombie (botnet) [1]. Sans qu’il s’en aperçoive, ses mots de passe et toutes ses interventions vont pouvoir être lus et enregistrés. Le malware a introduit un trojan *(2)* qui ouvre la voie à d’autres programmes malveillants, prenant en otage l’ordinateur tout entier.

L’accès à ses logiciels devient impossible. Son agenda ne répond plus et, sans secrétaire extérieure informatisée, il ne sait pas quels patients ont pris rendez-vous et pour quels motifs. La série débute : Comment contacter les patients ? Comment annuler ou reporter les rendez-vous ? Quid des données et que vont-elles devenir si elles lui sont subtilisées ? Le malware prend également possession de son logiciel de messagerie et de ses mots de passe.

Le Dr Cinécar se sent soudain totalement perdu. Son informatique ne répond plus ; il n’a plus aucun moyen de récupérer sa comptabilité et donc aucune vue sur les versements perçus ou ceux en attente.

Heureusement, son informaticien (qu’il aurait dû contacter pour l’installation de ce logiciel… gratuit) lui avait installé un système de sauvegarde automatique avec deux disques durs en miroir. *(3)* Le but était d’en retirer un tous les soirs et de

l'interchanger avec un autre le lendemain, mais cela n'avait pas été fait depuis trois mois. Les données de la sauvegarde ont donc été également cryptées, à l'exception du disque dur interchangeable qui était resté dans sa boîte. Il peut donc retrouver une sauvegarde, certes avec un délai de trois mois en arrière, mais qui a le mérite d'exister. Ensuite, le Dr Cinécare a tout perdu.

Comme un grand classique, le piratage est intervenu au moment de l'installation du logiciel avec une prise en main à distance. Le fichier d'installation a été récupéré sur un site frauduleux et un logiciel de ransomware *(4)* a donc été installé au lieu du logiciel souhaité. Ce type de piratage est de plus en plus sophistiqué, les hackers s'adaptant au système antivirus en adoptant des méthodes évitant ainsi d'être détectés.

Mais les malwares peuvent venir d'autres sources, tels les mails, même ceux de vos connaissances (subtilisation des adresses mail), les sites frauduleux *(5)*, de votre portable subtilisé dans des réseaux publics (wifi), la liste est longue.

SE PROTÉGER DES VIRUS

Cela va de soi : le logiciel antivirus, votre première défense, à installer dans les plus brefs délais.

Il doit être également exécuté sur tous les appareils connectés au réseau. Il empêche les exécutables des logiciels malveillants de s'exécuter sur votre machine. Mais attention, il ne vous sauvera pas de toute attaque.

Les premiers gestes devant votre machine doivent devenir vos habitudes :

1. N'ouvrez jamais les pièces jointes insérées dans vos e-mails : de nombreuses attaques commencent ainsi.
2. Votre système d'exploitation doit toujours être à jour : les correctifs, outre les avancées techniques qu'ils procurent, corrigent les bugs et autres failles de sécurité découvertes.
3. Vous avez un doute sur un site : rebroussez chemin, vous éviterez les téléchargements par *drive-by* ou les redirections vers des sites hébergeant des logiciels malveillants qui ciblent la vulnérabilité spécifique de votre navigateur et/ou de ses plugins.
4. N'utilisez pas de logiciels piratés ou partagés. Tentants soient-ils, ils peuvent contenir des logiciels malveillants. En clair, téléchargez les logiciels uniquement à

partir de source officielle.

NOUS SOMMES TOUS DES CIBLES

Nous sommes tous des cibles, mais la réponse immédiate de quiconque est « *je suis trop petit, je n'intéresse personne et mes données n'ont pas de valeur* », ce qui est globalement vrai, mais la première règle est de ne pas se trouver dans les filets du chalut. Parce que toute personne a des accès à des systèmes plus larges et est donc potentiellement intéressante.

A l'heure du Covid, par exemple, les médecins victimes de piratage ont été nombreux. Activer par exemple sa carte e-cps via un compte piraté est facile, c'est ce qui était arrivé à un professionnel de santé à la retraite venant en aide dans un centre de vaccination. En se rendant sur son compte, il a découvert qu'il avait vacciné un millier de personnes, alors que ce n'était absolument pas le cas.

Le hacker est tout d'abord un prédateur, et si vous avez un niveau de résilience faible, vous serez une cible facile. On connaît la volonté de l'attaquant : l'argent, le pouvoir, l'information, la désinformation, la capacité à nuire, l'ego. On se retrouve forcément dans un de ces cas

IL FAUT AGIR

Il ne faut pas sous-estimer ces incidents qui peuvent avoir des répercussions dramatiques. Mais ceux-ci ne sont par forcément de nature malveillante, ils peuvent également être dûs à des problèmes matériels ou informatiques (incidents dans les data centers, coupures récurrentes chez des opérateurs…).

Nous verrons dans notre prochain numéro comment se prémunir pour éviter le pire et – surtout – travailler sur l'anticipation, car la sécurité se passe tout d'abord en amont afin de garder une marche d'avance sur les hackers…

LES DIFFÉRENTES FAMILLES DE VIRUS

On peut considérer le virus informatique comme son cousin biologique qui s'attaque à un organisme pour le détruire. Il y aurait plus de 50 000 virus en circulation aujourd'hui, des plus inoffensifs aux plus virulents, capables d'effacer les données d'un disque dur.

Les trois grandes familles

1. Le virus de fichier capable de corrompre des fichiers exécutables (fichiers contenant un programme identifié par le système d'exploitation) tels les .exe, .com; .bin,…

2. Le virus de boot. Son secteur : détruire les données utilisées pour démarrer le disque dur.

3. Le macro-virus (près de 80 % des virus). Attaque les documents contenant des macros afin de casser l'automatisation des fonctions des logiciels.

Les virus sont capables de se répliquer, de se développer et de se propager vers d'autres ordinateurs en s'insérant dans d'autres programmes ou documents.

Les vers

Le vers (worm) est un logiciel malveillant capable de se dupliquer et de propager via les réseaux. C'est un fichier qui se multiplie à l'infini, via par exemple les courriers électroniques (et épuisent ainsi l'espace de stockage). Il peut exploiter les carnets d'adresses et envoyer automatiquement à l'insu des propriétaires des fichiers word infectés.

Les chevaux de Troie

Le cheval de Troie (Trojan horse) transite également par courrier électronique et s'installe également à l'insu de l'utilisateur. Activé à distance, il permet le contrôle complet de la machine (système, configuration, mots de passe…)

Les maldocs

Le maldoc est un document informatique malveillant qui se partage deux mécanismes : la vulnérabilité (exploite une vulnérabilité préexistante ou exécute une charge utile à l'ouverture) et la fonctionnalité (accès direct aux ressources du système).

(1) « Botnet » (contraction des termes « robot » et « network »). Les cybercriminels utilisent des chevaux de Troie particuliers pour violer la sécurité des ordinateurs de différents utilisateurs, et d'en prendre ainsi le contrôle à distance.

(2) Le trojan (cheval de Troie en français) n'est pas un virus mais un programme

malveillant.

(3) Le système plus connu sous le nom de RAID sécurise automatiquement vos données en les dupliquant sur deux disques identiques.

(4) Un ransonware est un logiciel qui chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

(5) Utilisez la page de Google ***Safe Browsing*** *afin de savoir si Google a référencé un site comme douteux.*

Source : kaspersky.fr

Vérifiez vos adresses mails !

Il n'y a pas que votre ordinateur qui peut être piraté. Vos adresses mails on pu être subtilisées dans d'autres bases de données (Santé, Gafam, réseaux sociaux…). Pour le savoir et éviter une usurpation de votre identité, de l'hameçonnage ou autre méfait, vérifiez auprès du site haveibeenpwned s'il y a eu violation de vos adresses. Si tel est le cas, le site vous indique sur quels sites vos données ont été volées… et changez vos mots de passe.

la CNIL et vos données

Le médecin libéral doit donc protéger ses données personnelles et médicales. Pour ce faire, il doit passer par des protocoles précis : hébergement certifié données de Santé avec demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

La CNIL a récemment sanctionné deux médecins libéraux pour ne pas avoir suffisamment protégé les données de leurs patients, des milliers d'images médicales hébergées sur des serveurs étaient en accès libre. Toutes ces données pouvaient donc être consultées et téléchargées, et étaient, selon les délibérations de la CNIL, « *suivies notamment des nom, prénoms, date de naissance et date de consultation des patients* ». Le problème venait simplement d'un mauvais paramétrage de leur box

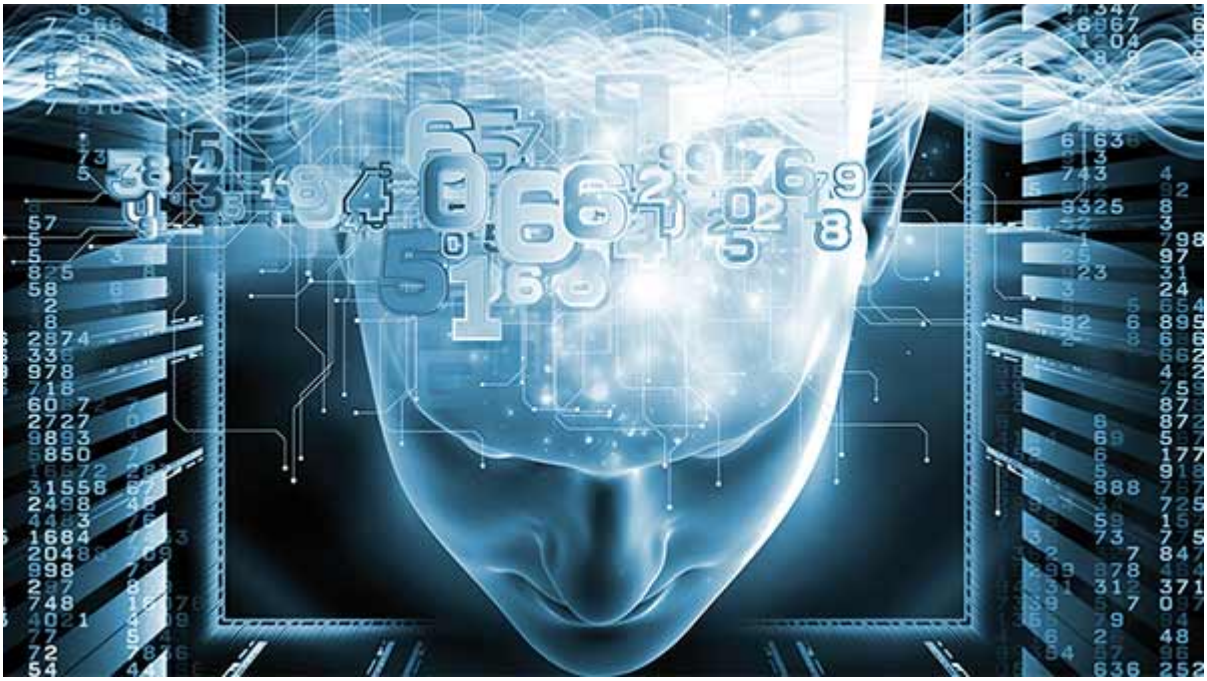
internet et du logiciel d’imagerie qui laissait en libre accès les images non chiffrées.

A lire également

Cybersécurité – banalisation sur toile

Intelligence artificielle – la santé au cœur du futur

L’intelligence artificielle – Introduction à la Santé

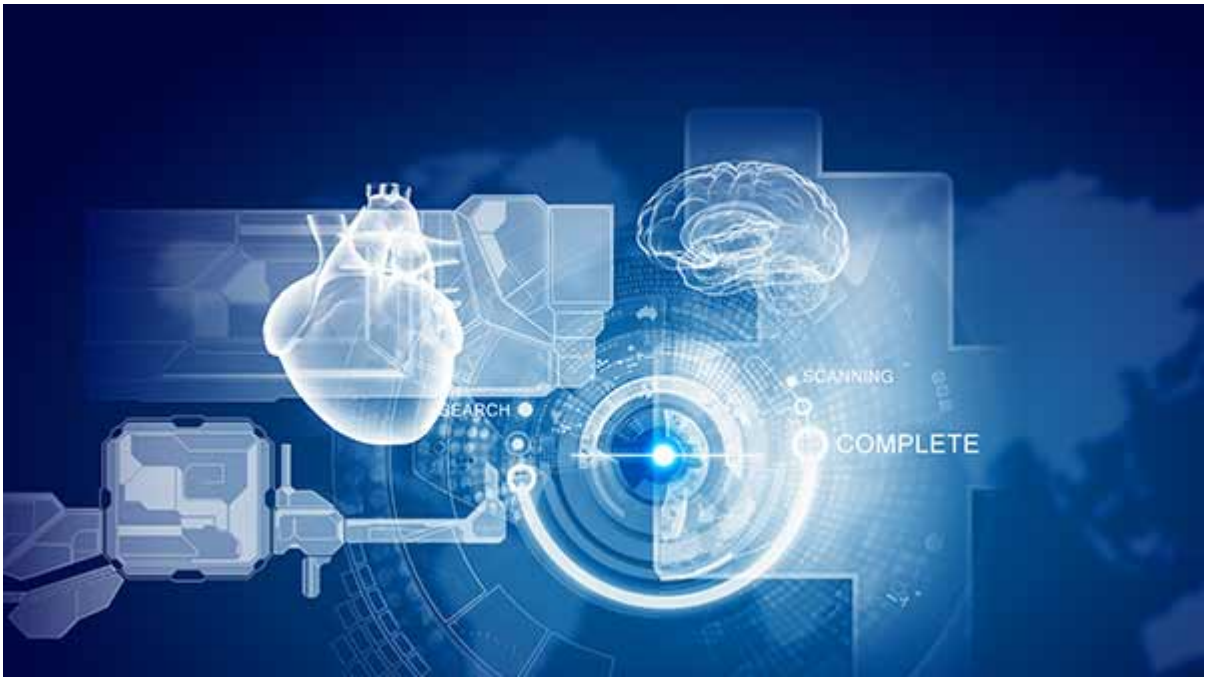


Les préoccupations liées à l’intelligence artificielle

Les 50 ans d’internet

Les virus

De l’impression 3D à la bio-impression



Retour vers le futur – les prédictions médicale dans les années 1950

LES NFT, C’EST QUOI EXACTEMENT ?

Les jetons non fongibles (NFT) sont des certificats de propriété stockés sur une blockchain. Ces jetons numériques permettent de certifier l’authenticité d’un objet qui lui est associé en achetant un code (ou un certificat)

Contrairement à la monnaie telle qu'on la connaît (ou aux cryptomonnaies), chaque NFT est unique ou non fongible, c'est-à-dire qu'il ne peut être échangé contre quelque chose de valeur égale.

Le marché de l'art est en pleine révolution grâce aux NFT. Mike Winkelmann (Beeple) a vendu une photo numérique pour plus de 69 millions de dollars chez Christie's. Et pourtant, cette photo est consultable et téléchargeable sur internet, contrairement à un tableau « réel ». Alors, pourquoi acheter une telle œuvre de cette manière ? Et bien tout simplement parce que celle-ci a été vendue avec son NFT qui la rend unique et traçable. Ce certificat signe bien sûr l'œuvre de l'artiste et indique qui l'a vendue, qui l'a achetée et pour quelle somme et à quelle date. Cette œuvre « numérique » peut donc être cédée en enchère… et si la valeur de la cryptomonnaie qui a permis d'acquérir le certificat NFT augmente, la valeur de cette œuvre augmentera pour le possesseur du NFT.