Cyber Menaces - Pour les Particuliers

La numérisation des documents et l'accélération de l'échange d'information entre les Interlocuteurs sont les conséquences de l'arrivée de l'informatique dans notre société. Si cette évolution a été une révolution des méthodes de communication et d'échanges d'informations, c'est aussi devenu un nouvel espace de criminalité. Des individus, experts en informatique, imaginent tous les jours de nouvelles techniques afin d'en tirer illégalement profit. Or le champ des infractions possibles est immense, car l'informatique qui évolue tous les jours est un enchevêtrement complexe d'interactions technologiques et chacune de ces interactions est un maillon ayant potentiellement une faille : Téléphones, Tablettes, Systèmes d'exploitation, logiciels…

Pour la petite Histoire le piratage informatique est apparu pour la première fois dans les années 1950/60, lorsque des experts, utilisant la technique « **Phreaking** [1] » ont trouvé le moyen de ne pas payer leurs appels longue distance grâce à une série de codes qu'ils tapaient sur leurs téléphones au moment de l'appel.

Les Cyber Menaces touchent les particuliers, les entreprises ou les institutions gouvernementales, avec différents enjeux [2] : Sabotage, Espionnage, Atteinte à la Notoriété, ou Vol. Il s'agit de Cybercriminalité. Je traiterai ici les Techniques de Cyber Menaces dirigées vers les personnes, c'est-à-dire [3/4] : **Rogues, Ingénierie Sociale**, **Phishing, Botnets**… Et pour vous rassurer, je rajouterai, que les attaques les plus complexes sont généralement réalisées et orientées vers des personnalités, des entreprises ou des institutions gouvernementales ciblées, et que ces attaques sont techniquement plus sophistiquées car le jeu en vaut plus la chandel : **Sniffing, Spoofing, Man-In-The Middle, DOS, Hijacking, APT, Worms…**

Les Cyber Menaces pour les Particuliers seront abordés via les termes Techniques. Et je commencerai par les Cyber Menaces du type arnaques : **Rogues** ou **Scareware**. C'est généralement en visitant une page internet infectée, et en cliquant sur une publicité ou un message vous alertant que votre ordinateur, téléphone ou tablette est lent, infecté d'un virus que le **Scareware** s'installe. Je précise des maintenant que de nombreux logiciels malveillants s'installent via un clic sur un bandeau publicitaire. Ils se clament être un antivirus ou un outil d'optimisation, mais ils ne sont que des outils complètement factices. Ils vous demandent pour réparer votre ordinateur d'acheter la « version complète », ce qui est une arnaque pour vous soutirer de l'argent, ou vous dérober vos numéros de carte bancaire au moment du paiement. **Parade** : N'utilisez que des antivirus connus, c'est-à-dire des logiciels de protection d'ordinateur comme : **Norton**, **McAfee**, **Kaspersky**, **Bitdefender**, **AVS**… Et ne pas cliquer sur les Publicités des sites internet non Officiels ou aux contenus douteux. **Pourquoi ?** Parce que généralement les sites officiels ont des équipes de sécurité informatique qui surveillent et remédient à ce type d'attaques…

Point d'eau où les animaux viennent se désaltérer : **Watering Holes**. Il s'agit des sites internet qui ont été attaqués et infectés par des Hackers parce qu'ils sont fréquentés par la population que les pirates informatiques veulent attaquer : Amateurs de voitures de luxe, d'objets d'arts ou fans de Tennis… etc... **Parade** : La parade est simple - Ne pas aller sur des sites non officiels ou des sites aux contenus douteux.

Les « **Joker** » sont des logiciels que l'on installe sur le téléphone portable, ou une tablette. Ils volent de l'argent aux utilisateurs en les souscrivant à des abonnements payant sans leur consentement. Il simule les interactions avec de fausses annonces envoyées à l'utilisateur, le vol via des messages SMS et subtilise ses moyens de paiements. **Parade** : La parade est simple - Ne pas installer des logiciels sur son téléphone qui ne sont pas connus.

Botnets – Sans que vous le sachiez, votre ordinateur appartient maintenant à un réseau d'ordinateurs compromis et contrôlés à distance par des pirates informatiques. Ces Hackers peuvent alors agir en effectuant des tâches malveillantes, récupérer vos identifiants, vos codes ou lancer des attaques partout dans le monde depuis votre ordinateur. **Parade** : Utiliser un antivirus connu, c'est-à-dire un logiciel de protection d'ordinateur comme : **Norton**, **McAfee**, **Kaspersky**, **Bitdefender**, **AVS**…

L'Ingénierie Sociale – Il s'agit aujourd'hui de la technique de base utilisée pour des attaques ciblées. Les hackers recherchent sur Internet des informations sur les personnes issues d'un type de population choisi. Ils utilisent pour cela toutes les ressources d'Internet à leurs dispositions : Facebook, Twitter, LinkedIn, tous les sites d'information ou des bases de données qui ont été volées et revendues sur le Darkweb - Marche Noir d'Internet. Après avoir repéré les informations nécessaires sur leurs cibles, plusieurs approches sont possibles pour les Cybercriminels :

- **Contact Direct** - Les Cyber Criminels vous contactent directement, habituellement par téléphone en se faisant passer pour un faux service technique, un service de clientèle ou votre banque, par exemple. Ils veulent gagner votre confiance afin que vous leur fournissiez les dernières informations dont ils ont besoin, généralement un mot de passe ou vos coordonnées bancaires. **Parade** : Il est important de comprendre que ces appels sont réalisés sans que vous ne les ayez sollicités. C'est cet appel non attendu qui doit être une alerte pour vous. D'autres part, ces cybercriminels trouvent les informations qu'ils veulent par internet et souvent tenteront de rentrer dans votre vie privée en vous ajoutant comme ami sur les réseaux sociaux. Il est donc important de bien vérifier les informations que vous laissez accessibles, sur Facebook par exemple. Et de n'accepter les invitations que des personnes que vous connaissez ou qui appartiennent à vos cercles ou associations.
- **Phishing** – Lorsque vos coordonnées se retrouvent dans une base de données utilisée par des Pirates Informatique, il est possible que vous soyez victimes d'une campagne de **phishing**. Vous recevez alors un courriel maquillé, reprenant le format et les caractéristiques d'une société ou d'une Institution connue afin que vous ne puissiez remettre en question l'authenticité de son origine, comme les Impôts ou la Sécurité Sociale… Ce courriel déguisé contient soit un document joint, soit un lien de connexion. Cette pièce jointe ou ce lien, lorsque vous cliquez dessus déclenche une ou des actions malveillantes sur votre équipement, comme l'‘installation d'un **Ransomwares** - **Parade** : Plusieurs possibilités… **A –** Vous utilisez un antivirus, c'est-à-dire un logiciel de protection d'ordinateur connu : **Norton**, **McAfee**, **Kaspersky**, **Bitdefender**, **AVS**… qui analyse vos courriels et vos pièces jointes. Mais dans tous les cas, les mêmes principes de base s'appliquent. **B –** Ne pas cliquer sur des liens ou ouvrir le document d'un courriel que vous n'attendez pas… Par exemple, vous recevez un courriel sur un colis que vous avez reçu et qu'on vous demande de venir chercher, mais vous n'avez rien commandé… **C –** Lorsque vous recevez un courriel ne pas hésiter à téléphoner à l'expéditeur pour en vérifier l'origine.

Les deux conséquences possibles et directes d'un **Phishing** issues de l'**Ingénierie Sociale** sont le **Vol d'Identité** et le **Ransomwares**.

Le Vol d'Identité - Lorsqu'un hacker a accès et possède vos informations personnelles, il est possible pour lui de vous voler de l'argent, de participer à des fraudes de tout ordre en votre nom.

Ransomwares - Les Ransomwares ou Rançongiciels. Ces des logiciels qui encryptent vos données et vous demandent de l'argent afin de vous les restituer décryptées. Malheureusement dans la grande majorité des cas le décryptage n'a jamais lieu, vous ne récupérez jamais vos données et vous perdez l'argent que vous avez envoyé aux hackers

Pour Conclure – Comme vous pouvez le constater, la majorité des Cyber Menaces peuvent être contenues et arrêtées si vous avez protégé votre ordinateur avec un Anti-Virus. Maintenant, la principale menace reste l'être humain - Vous… Car l'être Humain sera toujours le maillon faible de la chaine de Sécurité et il y a plusieurs raisons à cela : les techniques utilisées par les pirates informatiques sont complexes, il faut donc de se former continuellement pour que le risque d'une erreur diminue. D'autre part, les techniques sont nombreuses, ce qui nécessite de toujours rester à l'écoute des nouveautés. Mon message de fin sera donc celui-ci : Il faut envisager les Cyber Menaces comme une merveilleuse occasion pour tout un chacun de toujours rester éveillé, de continuellement se former, apprendre, de se remettre en question et donc de ne pas s'endormir sur ses lauriers !

- **1 - https://en.wikipedia.org/wiki/Phreaking**
- **2 - https://www.gouvernement.fr/risques/risques-cyber**
- **3 - Kaspersky Lab - Panorama-des-cybermenaces_2015Oct.pdf**
- **4 - https://www.intrinsec.com/tendances-2019-cyber-threat-intelligence**