h e g

Haute école de gestion
Genève

Études des cyberattaques de type ransomware et proposition de solutions adaptées aux particuliers et PME

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Sara LAGARE

Conseiller au travail de Bachelor :

David Billard

Genève, le 6 mai 2021

Haute École de Gestion de Genève (HEG-GE)

Filière informatique de gestion

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science en Informatique de Gestion.

L'étudiante a envoyé ce document par courriel à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : https://www.urkund.com.

L'étudiante accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteure, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seule le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 06.05.2021

Sara Lagare

Remerciements

Par ces quelques mots je tiens à témoigner toute ma gratitude à Monsieur Billard pour avoir accepté de prendre en charge l'encadrement et le suivi de mon travail de Bachelor.

Il m'a non seulement aidé à définir un sujet de travail de Bachelor, mais aussi il a su me guider et me rassurer par rapport à mes incertitudes concernant mon étude. Je le remercie encore pour m'avoir fourni des ressources utiles pour mes recherches.

Je remercie également mes parents et amis proches pour le soutien moral qu'ils m'ont apporté, ainsi que mes deux meilleurs amis pour m'avoir fait part d'un retour concernant le site internet que j'ai créé pour ce travail.

Résumé

Etant née en 1995, je considère faire partie de la génération qui a vue croître l'informatique, un essor technologique fascinant. De plus, je suis de nature prudente et ai choisi ce sujet car je trouve nécessaire de ne pas négliger les dangers accompagnant cette technologie, dangers qui se complexifient et progressent avec elle.

Parmi tous ces dangers, toutes les cyberattaques possibles, j'ai choisi de porter mon travail sur le ransomware, car c'est une menace qui frappe de plus en plus en ces temps de confinement à la suite du covid. Les entreprises qui, pour beaucoup, se sont retrouvées désemparées avec le confinement, mais aussi les particuliers et même les institutions telles que les hôpitaux et gouvernements se trouvent particulièrement touchés à travers le monde.

Ainsi, je commencerai ce mémoire par expliquer ce qu'est un ransomware, puis comment il parvient à se frayer un chemin chez leurs cibles, puis exposerai les différents moyens pour se prévenir d'une attaque, ainsi que les risques encourus d'accepter ou non la rançon demandée une fois attaqué. Je finirai par analyser ce que la Suisse propose en termes de protection juridique. Je présenterai également la plateforme web que j'ai créée, plateforme web qui a pour objectif d'être une source d'informations complète, compréhensible par tous, sur cette menace informatique en proposant diverses explications, recommandations et redirections vers les services appropriés, afin d'aider les particuliers ou PME qui cherchent de l'aide vis-à-vis de cette menace informatique.

Table des matières

Déclaration i
Remerciements ii
Résumé iii
Liste des figures vi
1. Introduction 1
2. Le ransomware 2
3. Son apparition sur les machines 4
3.1 L'ingénierie sociale 4
3.2 Les failles techniques 5
4. Exemples de ransomwares 7
4.1 WannaCry 8
4.2 Maze ransomware 9
5. Les principales cibles des attaques 10
5.1 Les conséquences par secteurs 11
6. Les auteurs des ransomwares 13
7. Quelques chiffres 14
8. Comment s'en protéger 15
8.1 Se protéger sur le plan humain 15
8.2 Se protéger sur le plan technique 18
9. Une fois attaqué 19
9.1 Réaction à la suite de l'attaque 19
9.2 Faut-il ou non payer la rançon 22
9.2.1 Les raisons de ne pas payer 22
9.2.2 Pourquoi certains payent la rançon 23
10. Contexte législatif 25
10.1 Peines encourues 25
10.2 Nouvelle Loi fédérale Suisse sur la protection des données 27
10.3 Protection et assurances 28
11. Plateforme web d'aide créée 29
11.1 Introduction du site Internet 29
11.2 Explication du design 30
11.3 Explication du contenu 34
12. Conclusion 37
12.1 Synthèse 37
12.2 Point de vue personnel 38

12.3 Proposition d'amélioration 40
Bibliographie 42

Liste des figures

Figure 1 : Capture d'écran : Demande de rançon d'un ransomware 2
Figure 2 : Nombre annuel d'attaques de ransomware de 2017 à 2020 3
Figure 3 : Exemple de matériel utilisé lors d'un hacking par force brute 6
Figure 4 : Capture d'écran : Trouver l'option « autres » sur Gmail 16
Figure 5 : Capture d'écran : Détails de la fenêtre « autres » sur Gmail 17
Figure 6 : Capture d'écran : Code source d'un e-mail sur Gmail 17
Figure 7 : Statistiques concernant le paiement ou non des rançons en 2020 24
Figure 8 : Site internet : Page d'accueil 30
Figure 9 : Site internet : Présentation sous format réduit et menu fermé 31
Figure 10 : Site internet : Présentation sous format réduit et menu ouvert 31
Figure 11 : Site internet : Illustration du set de couleur 33
Figure 12 : Site internet : Favicon du site 33
Figure 13 : Site internet : Barre de menu 34
Figure 14 : Site internet : Menu déroulant de la rubrique « prévention » 34
Figure 15 : Site internet : Menu déroulant de la rubrique « Agir » 34
Figure 16 : Site internet : Quizz 1 – Navigation sur le site 35
Figure 17 : Site internet : Quizz 2 – Test sur le niveau de sécurité personnel 36

1. Introduction

Depuis la montée en flèche de l'informatique via l'essor d'internet au grand public en 1990, on peut dire que l'informatique d'aujourd'hui, en 2021, a énormément évolué, ainsi que notre dépendance à celle-ci et les dangers qu'elle peut apporter.

En effet, le nombre de personnes dans le monde utilisant internet s'élève maintenant à 4.54 millions soit plus d'une personne sur deux au niveau mondial (KEMP 2020).

Par conséquent, plus il y a de personnes connectées, plus les risques de cyberattaques augmentent.

> « Une cyberattaque ou attaque informatique est une action volontaire et malveillante menée au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent (particuliers, entreprises, hôpitaux, institutions[...]). » (DELUZARCHE, Céline)

A côté de cela, nous sommes actuellement pris au piège d'une épidémie mondiale, le covid-19, qui force les gouvernements à imposer des confinements et quarantaines afin de restreindre les risques de contaminations au virus. Forçant de nombreuses entreprises, institutions et particuliers à faire du télétravail : « Activité professionnelle exercée à distance de l'employeur grâce à l'utilisation de la télématique » (LAROUSSE 2021) pour limiter les pertes de gains quand cela est possible.

Ce nouvel environnement de travail, souvent établit dans la hâte, est souvent moins sécurisé et offre une grande vulnérabilité aux cyberattaques. C'est pourquoi en cette période de pandémie, le ransomware, aussi appelé « rançongiciel » en français, fait partie des cyberattaques qui sont en augmentation de manière significative.

Il existe évidemment plusieurs types différents d'attaques informatiques dont les fameux : « hameçonnage (phishing) ; attaque par déni de service (DDoS) ; attaque par brute force (recherche du mot de passe en essayant toutes les combinaisons possibles) ; vol d'informations ; installation de programmes espion ou de malwares ; ransomware ; etc. ». On s'attardera uniquement sur ce dernier, le ransomware, le rançongiciel.

2. Le ransomware

Mais qu'est-ce qu'un ransomware ?

> « Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. » (ALTOSPAM 2021)

Figure 1 : Capture d'écran : Demande de rançon d'un ransomware

(BRIDEWELL CONSULTING, 2016)

Voici une image explicite qui montre à quoi ressemble une ransomware sur un appareil touché. Généralement, on y retrouve : un minuteur ayant pour but de stresser la victime afin de l'inciter à payer le montant de la rançon et une explication sur comment payer celle-ci. Le moyen de paiement est souvent une demande de versement de bitcoin, une monnaie électronique décentralisée, car c'est un moyen de paiement impossible à retracer et donc plus sûr pour les cybercriminels.

La toute première attaque de type ransomware remonte en 1989 avec le cas nommé « Cheval de Troie du Sida », « AIDS Trojan » en anglais, ou encore « PC Cyborg virus ». Un ransomware codé par un académicien d'Harvard prénommé Joseph L. Popp. Le virus a été codé dans des disquettes de manière à crypter les fichiers et cacher les

répertoires du lecteur C après 90 démarrages de l'appareil infecté. Pour signaler le déclenchement du ransomware, un message apparaissait pour demander une rançon de 189 USD à verser à l'association PC Cyborg Corporation dans une boîte postale au Panama. Ces disquettes ont été distribuées à 20'000 personnes ayant l'attention d'assister à la conférence sur le sida de l'Organisation mondiale de la santé, d'où l'attaque tire son nom.

Pour revenir aux ransomwares en général, il en existe principalement deux types : les crypto-ransomwares et les ransomwares de type « Locker ».

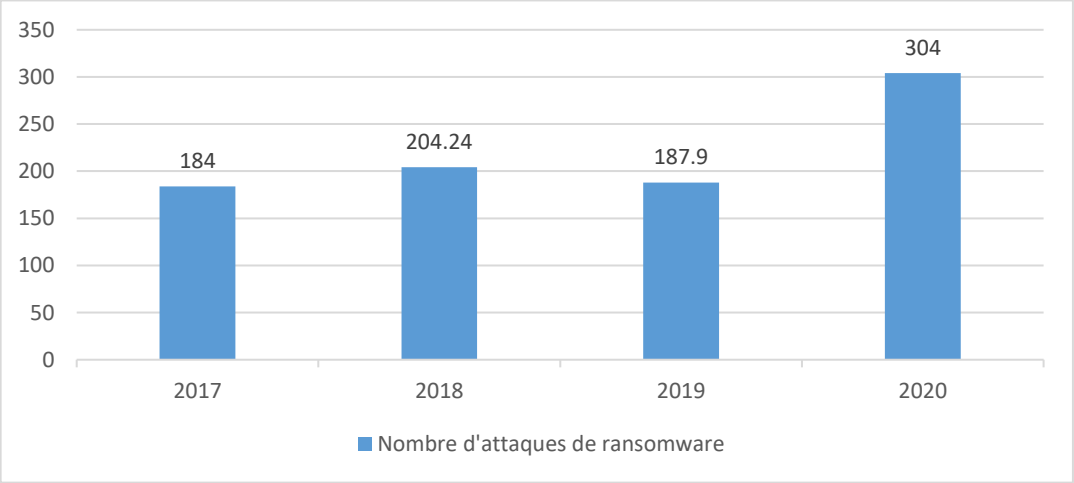
- Les crypto-ransomwares : le logiciel malveillant chiffre, crypte les données, fichiers de l'ordinateur de manière que l'utilisateur n'ait plus aucun moyen d'accéder à ceux-ci. La rançon est exigée contre la clé de déchiffrement qui permettrait le décryptage des données, fichiers.

- Les ransomwares « Lockers » : Comme son nom l'indique, ce ransomware va « lock », c'est-à-dire verrouiller l'accès entier à l'appareil, ce qui va le rendre inutilisable par son propriétaire. La rançon est exigée contre le déverrouillage de l'appareil. Dans ce cas, les données ne sont pas chiffrées, seul l'accès à la machine est bloqué.

Il ne faut pas oublier qu'il n'y a aucune garantie sur le fait de pouvoir récupérer ses données une fois la rançon payée, ni que les pirates informatiques ne gardent pas de copie de ces mêmes données.

Il y aurait eu en 2019, plus de 189 millions d'attaques de type ransomware. Et ce chiffre aurait même presque doublé en 2020 !

Figure 2 : Nombre annuel d'attaques de ransomware de 2017 à 2020



(JOHNSON, 2021)

Selon une enquête effectuée la même année par SOPHOS, une entreprise sur deux aurait été touchée par une attaque où les cybercriminels sont parvenus à chiffrer les données 73% de fois par attaques.

3. Son apparition sur les machines

Ce type de logiciel malveillant ne peut pas infecter n'importe quels appareils. Il doit y être invité ou bien trouver une brèche dans le système. Il ne peut en effet infecter un appareil uniquement à distance. Il doit réussir préalablement à y installer des lignes de code, qui elles se chargeront de télécharger le code manquant au bon fonctionnement du ransomware en allant les chercher sur des sites web prévus pour, le cas échéant. Ces lignes de code exécuteront automatiquement des fonctionnalités lui permettant par la suite d'exécuter sa tâche malveillante : le chiffrement des données, le blocage des accès, etc.

Pour ce faire, il existe deux moyens principaux parmi lesquels les ransomwares peuvent s'introduire dans les machines : En exploitant soit des failles humaines, soit des failles techniques.

3.1 L'ingénierie sociale

Dans ce premier cas qui concerne l'ingénierie sociale, c'est l'utilisateur de la machine qui a donné la possibilité à la menace informatique de s'y établir. Il y'a plusieurs moyens par lesquels un utilisateur peu malencontreusement faire entrer le ransomware. En effet, les cyberpirates exploitent principalement le manque de connaissances, la curiosité ou l'inquiétude de leurs victimes.

Le procédé souvent utilisé ici est appelé « phishing » ou en français « hameçonnage ». Cette méthode se concentre sur l'emploi de courriels frauduleux renfermant les précieuses lignes de code nécessaires au ransomware. Du code pouvant être dissimulé dans un document au format léger et transportable par courriels, du style : « .docx, .pdf, .jpg, etc. ».

L'auteur de l'attaque cherchera donc un moyen d'inciter l'utilisateur à lire le mail et à télécharger le logiciel caché mis en pièce jointe. Le danger n'est pas dû à l'ouverture du courriel, mais à la lecture de celui-ci, si la victime aura soit : téléchargé et ouvert le document piégé mis en pièce jointe ou cliqué sur un lien malveillant s'y trouvant.

En effet, le document peut contenir un script exécutable à l'ouverture, lecture de celui-ci et c'est ce script qui se chargera de finaliser la mise en place du ransomware sur l'appareil. En cliquant sur le lien malveillant se trouvant soit dans l'e-mail ou dans la pièce jointe, la victime peut déclencher un type d'attaque explicité plus loin dans le document appelé « drive-by download ».

Les criminels peuvent utiliser des informations personnelles et privées de la victime, récoltées préalablement, pour rendre le courriel le plus innocent et crédible possible. Pour les particuliers, la pièce jointe peut prendre l'apparence d'une fausse facture, amende, convention au tribunal etc. par exemple. Dans le cadre d'un employé d'entreprise, cela peut ressembler à un rapport top secret, un CV, un texte ou fichier à réviser, retoucher pour un supérieur ou collaborateur. Il est également possible que l'employé de l'entreprise soit soudoyé afin qu'il installe lui-même le logiciel.

Pour donner un cas concret d'ingénierie sociale, parlons d'un cas assez étonnant où un gouvernement est l'auteur même d'une telle attaque. En effet, le gouvernement britannique responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information, le « Government Communications Headquarters » ou GCHQ, a lancé une opération appelée « Opération Socialist ». Lors de cette opération, dont les toutes premières actions remontent à 2009, le GCHQ a réussi à s'infiltrer dans l'infrastructure de la compagnie belge de télécommunications Belgacom qui ne remarquera l'intrusion qu'en 2013. Pour faire simple, les espions britanniques ont fait parvenir des fausses pages de profile LinkedIn aux ingénieurs de Belgacom. Les pages truquées ressemblaient comme deux gouttes d'eau aux pages officielles à la différence qu'elles contenaient le code caché permettant aux cybercriminels de s'infiltrer dans les machines de Belgacom afin d'espionner la compagnie de l'intérieur.

3.2 Les failles techniques

Il existe également une multitude de procédés différents pour introduire le logiciel malveillant sans que cela provienne des talents des cybercriminels à berner leurs victimes afin de s'introduire dans la machine, système ciblé.

Ils vont tenter de trouver une faille technique, une vulnérabilité du système en exploitant un manque de protection, sécurité. Faille technique généralement dû au fait qu'une mise à jour du système principal, ou à celui d'un composant logiciel de la machine, n'a pas été faite créant une brèche dans la sécurité laissant ainsi la possibilité aux virus de s'y infiltrer. Ces mis à jour concernent également celles des navigateurs web ainsi que leurs

composants : « plug-in, thèmes de navigateurs, etc. ». À cet effet, si une brèche est trouvée, ils pourront effectuer une attaque appelée « drive by download ». Attaque qui consiste simplement à installer du code malveillant même si la victime n'a pas pris action à part entière en cliquant sur un lien, un pop-up ou une fenêtre de notification corrompue par exemple.

Les cyberpirates peuvent également tenter de s'introduire dans les systèmes eux-mêmes. Certains vont chercher à trouver les mots de passe, pour se connecter aux machines et systèmes ciblés, à l'aide d'ordinateurs dont la seule fonction est d'essayer des milliers de combinaisons de mots de passe par secondes. Le nombre de mots de passe par seconde utilisé dépend de la force de calcul de la machine utilisée pour hacker. Cette méthode d'hacking est appelée « hacking par force brute » ou « bruteforce ».

Pour vous donner une idée de la rapidité d'hacking de mots de passe, il a été démontré à la conférence « Passwords-12 Conférence » à Oslo, qu'il était possible de craquer, deviner, par force brute un mot de passe de Windows XP de 14 caractères en à peine 6 minutes.

> « Le déploiement qui était capable de 350 milliards de suppositions par secondes était un cluster d'ordinateurs de cinq serveurs avec 25 cartes graphiques AMD Radeon et un logiciel de virtualisation. » (OWANO 2012)

Figure 3 : Exemple de matériel utilisé lors d'un hacking par force brute

(DOCTOROW 2012)

N’oublions pas que la majorité des rançongiciels ne s’arrête pas à une seule machine mais cherchera à infecter le plus possible de machines, à s’infiltrer plus profondément dans l’entreprise ou au sein du foyer. Une fois avoir réussi à s’introduire dans la première machine via les méthodes explicitées précédemment, le malware va scanner l’appareil infecté afin de trouver des vulnérabilités du système qui lui permettront de se propager.

Le rançongiciel analysera la configuration du réseau et les « open SMB shares » (un protocole de partage de fichiers sur un même réseau). Ce protocole permet l’utilisation de ressources partagées distantes telles que les imprimantes, par exemple. Ce protocole rend également possible la communication avec n’importe quel programme conçut pour recevoir des requêtes d’un client SMB, client utilisant le même protocole.

Le malware cherchera également à examiner l’Active Directory pour trouver les permissions, comptes et domaines, jugés comme domaine de confiance.

> « Active Directory (AD) est un service d’annuaire destiné aux environnements Windows Server. Il s’agit d’une base de données distribuée et hiérarchisée qui partage des informations relatives à l’infrastructure permettant de localiser, de sécuriser, de gérer et d’organiser des ressources ordinateur et réseau ressources dont des fichiers, utilisateurs, groupes, périphériques et appareils réseau. » (PAESSLER)

Après avoir étudié la machine scrupuleusement sous ses deux aspects, le malware est en mesure de se propager sur d’autres machines du réseau en utilisant les accès des comptes utilisateurs trouvés à l’aide des scans effectués sur la machine initialement infectée. Le virus va faire ce qu’on appelle un « mouvement latéral » pour s’infiltrer plus profondément dans le réseau, la compagnie. Il va ainsi réitérer ses actions, scans afin de contaminer le plus possible.

4. Exemples de ransomwares

Pour comprendre plus en détails leur fonctionnement, nous allons analyser en profondeur les deux ransomwares suivant :

- WannaCry
- Maze ransomware

4.1 WannaCry

« WannaCry », aussi connue sous le nom de « WannaCrypt », doit être sans doute l'attaque mondiale la plus connue dans l'histoire d'internet vu son ampleur.

Le 12 mai 2017, le ransomware « WannaCry » a réussi à infecter plus de 230'000 ordinateurs dans 150 pays en une seule journée (LATTO 2020). Les pays les plus touchés étant l'Inde, les Etats-Unis et la Russie.

L'attaque aurait exploité une vulnérabilité de sécurité Windows appelée « MS17-010 », que possède les ordinateurs dont le système d'exploitation est plus ancien que Windows 10 et qui n'auraient pas effectué les mises à jour de sécurité adéquates. Les ordinateurs sous Windows XP ont été particulièrement touchés. En effet, Microsoft avait publié un correctif de sécurité justement palliant ces vulnérabilités environ 2 mois avant l'attaque. Cela démontre bien l'importance de garder ses appareils constamment à jour pour minimiser les risques d'attaques.

Le ransomware aurait pu avoir une ampleur beaucoup plus grande si toutes les machines du monde étaient interconnectées et si elles n'avaient pas effectué les mises à jour adéquates pour empêcher cette infection. En effet, pendant l'année de l'attaque « WannaCry », il a été établi que le système d'exploitation Windows 10, système protégé de l'infection du ransomware, était présent sur 500 millions d'installations que ce soit sur PC, smartphones, tablettes ou consoles de jeux (LEPINE 2017). Cependant, selon des statistiques concernant mai 2017, Windows 10 ne représentait alors que 34.25% des systèmes d'exploitation utilisés. Ce qui signifie que les cibles potentielles de ce rançongiciel, toujours dans l'hypothèse que les mises à jour de sécurité Windows en question n'auraient pas été faites, représentaient environ 65.75% des systèmes d'exploitation mondiaux, autrement dit, plus de 959 millions d'installations (SHANHONG 2021).

Il semblerait que l'origine de l'attaque proviendrait du fait que l'Agence nationale de la sécurité des Etats-Unis, la « NSA », aurait découvert cette vulnérabilité Windows et aurait développé un hack pour l'exploiter. Cependant, ce hack prénommé « EternalBlue » a malheureusement été dévoilé par un groupe de cyber criminels « The Shadow Brokers ».

La propagation du malware a été possible par le fait qu'elle affecte le protocole de Windows (SMB) qui est un protocole de partage de données, fichiers, à travers un même réseau. Ce qui fait que lorsqu'un ordinateur a été touché, le virus cherche également à affecter les autres appareils du même réseau.

4.2 Maze ransomware

Contrairement aux ransomwares classiques qui agissent uniquement de manière locale en s'infiltrant dans la machine de la victime pour y encrypter les données où en bloquer l'accès, les « Maze ransomwares » se distinguent par le fait qu'ils réussissent à récupérer les données sur des serveurs appropriés à leurs délits. De ce fait, ces cybercriminels font partis des premiers à avoir ce moyen de pression, celui de publier les données volées sur des sites prévus à cet effet si la victime refuse de payer.

Pour parler maintenant de quelques détails techniques du fonctionnement des mazes ransomwares, il est à relever que le code de leur malware est en général écrit en C++. De plus, pour sa façon d'encrypter les données, Maze utilise RSA et ChaCha20.

Etant donné la menace engendrée par le cryptage et l'extorsion des données, provoquée par le virus, il est intéressant de savoir que Maze ne tente pas de crypter l'intégralité des données mais ignore certains dossiers de la machine ainsi que certains types de documents.

Les dossiers ignorés par le virus sont :

- \\Program Files
- \\Windows
- \\Games\\
- \\Tor Browser\\
- \\ProgramData\\
- \\cache2\\entries\\
- \\Low\\Content.IE5\\
- \\User Data\\Default\\Cache\\
- \\All Users
- \\IETldCache\\
- \\Local Settings\\
- \\AppData\\Local
- AhnLab
- {0AFACED1-E828-11D1-9187-B532F1E9575D}

Les types de fichiers et extensions ignorés sont :

- DECRYPT-FILES.txt
- inf
- ini
- ini
- dat
- db

- bak
- db
- dat.log
- bin

5. Les principales cibles des attaques

En prenant comme secteur les Etats-Unis sur l'année 2019, environ 1'000 institutions gouvernementales, compagnies, etc., ont été touchées par un ransomware. Pour être encore plus précis, cela concernerait plus de 760 institutions fournisseuses de soins, plus de 110 agences gouvernementales étatiques et municipales, 90 universités, collèges, affectant plus de 1200 écoles individuelles (HAUK 2020). Par déduction, les parties les plus touchées sont les services publiques, professionnels de la santé et de l'éducation.

Le domaine de la santé a aussi été particulièrement touché avec une hausse de 75% en octobre 2020 selon une étude effectuée par « Kroll » (2021), le premier fournisseur mondial de services et de produits numériques liés à la gouvernance, aux risques et à la transparence.

Concernant les services professionnels, les cybercriminels choisissent d'attaquer de préférence les entreprises de taille petite et moyenne estimant que bien souvent elles ne possèdent pas une aussi bonne défense, sécurité, que les grandes entreprises. Cela en fait donc des cibles de choix pour les rançongiciels.

Avec l'apparition du Covid-19 et à la suite aux divers confinements et mesures imposées, beaucoup d'entreprises se sont adaptées et ont commencé à faire du télétravail. Ce qui a fortement favorisé les attaques de type ransomware car il faut facilement quelques jours à plusieurs semaines pour obtenir un environnement à distance complétement opérationnel et sécurisé. Toujours selon le constat effectué par Kroll, les cybercriminels exploiteraient les protocoles de bureau à distance (RDP), de communication réseau propriétaire de Microsoft et les réseaux privés virtuels (VPN). En effet, Kroll a remarqué que pour environ 47% des cas de ransomwares il y a eu une exploitation du RDP de l'entreprise. Les cybercriminels cherchent souvent les failles dans la configuration des RDP ou des vulnérabilités des VPN.

Le secteur de l'éducation est un secteur de choix car très vulnérable aux attaques de ce genre. En effet, à la suite du Covid-19, près d'1,2 milliards d'enfants suivent des cours

en ligne (LI, LALANI, 2020). Mais cela ne signifie pas que les écoles et leur personnel étaient entièrement préparés à ce nouveau système d'enseignement.

Selon D.SCOTT, Christopher (2021):

> « 60% des éducateurs et administrateurs nient avoir reçu un entrainement ou des informations concernant la sécurité informatique, alors qu'environ 80% d'entre eux donnent des cours en ligne. »

Et qu'en est-il des entreprises ciblées, comment les choisissent-ils ?

Lors d'une tentative d'attaque sur une entreprise préalablement choisie, du point de vue de l'ingénierie sociale, les cybercriminels chercheront toujours à atteindre et à piéger un employé ayant des droits d'administrateurs élevés. Ceci afin de pouvoir s'infiltrer plus profondément dans le système vu les accès plus étendus de ce dernier.

5.1 Les conséquences par secteurs

Les dégâts engendrés sont loin de concerner uniquement le côté financier lié à la rançon. Ils concernent surtout les dégâts relatifs au fonctionnement fondamental de l'entreprise concerné, ralenti ou mis à l'arrêt à la suite des données essentielles volées ou au blocage de l'accès aux divers systèmes utilisés. Les dégâts concernent également ceux engendrés à l'image de l'entreprise, à la perte possible de clients et partenaires à la suite de l'attaque.

En effet, une des conséquences les plus dramatiques outre l'échange et vente des données volées sur le marché noir, est sans doute les coûts liés aux dommages et à la réputation de l'entité affectée. Les clients souhaitent pouvoir recevoir les services auxquels ils se sont souscrits en tout temps, autrement ils risquent de perdre confiance en l'entreprise et celle-ci automatiquement aura une perte de gain. De plus, avec l'apparition des rançongiciels avec menace de publications des données volées, les entreprises qui cherchent à dissimuler ce genre d'incident en interne n'ont d'autre choix que d'en avertir ses clients. Ceux-ci auront légitimement le droit de douter de la sécurité de leurs informations confiées à l'entreprise après cela. Selon une étude faite par « Arcserve » sur près de 2'000 consommateurs, 60% d'entre eux refuseraient de faire confiance à une entreprise qui aurait subi une cyberattaque dans l'année qui a précédé (EL-JILALI 2020). Toujours selon la même étude, 45% auraient ou connaîtraient quelqu'un qui aurait déjà eu une mauvaise expérience en relation avec une cyberattaque. Néanmoins, 40% seraient prêts à payer plus pour une entreprise qui promet une bonne sécurité informatique.

Lorsqu'une attaque de type ransomware sévit sur une structure, celle-ci voit ces services soit complétement mis à l'arrêt soit grandement ralentis. Non seulement à cause du cryptage des données et/ou blocage des accès aux machines, mais également car la propagation du malware dans le réseau peut consommer un bon morceau de la bande passante.

En effet, selon une étude faite par le département du système d'information à l'Université Telkom en Indonésie :

> « un malware d'une taille de 15.17mo, une fois injecté, peut ralentir le trafic de la bande passante d'environ 16% à 75% » (MUHTADI, ALMAARI, 2020)

De plus, dès qu'une attaque de ce type est détectée, à cause du mouvement latérale de la propagation du virus, l'identification et l'isolation des machines infectées prend aussi un certain temps. Des services entiers peuvent être mis à l'arrêt et d'autre peuvent ne plus pouvoir se synchroniser correctement pour effectuer leurs tâches.

Dans le cadre du secteur de la sécurité, lors de ces ralentissements et arrêts de services, la police peut se voir couper l'accès à leur base de données, les empêchant de consulter des informations cruciales telles que l'historique de certains criminels et les mandats actifs. De plus, des systèmes de surveillances ont été rendus complétement inactifs. Également, des preuves digitales et autres données importantes peuvent être complétement détruites lors de l'infection. En effet, un cas de ransomware au département de la police au Texas a résulté en la perte d'au moins 1TB de preuves critiques de vidéos surveillances. Les données perdues comprenaient des preuves vidéo depuis 2009, des photos, des documents de la suite Office, des fichiers Word et Excel, des vidéos de tableau de bord de voitures, etc. La plupart de ces données étaient nécessaires pour prouver la culpabilité de criminels notoires.

Concernant le domaine de l'éducation, les écoles peuvent perdent accès aux données importantes comme celles concernant les allergies, les traitements et les soins spéciaux requis pas les élèves. De plus, l'attaque peut résulter à l'interruption ou au retardement des cours donnés par l'établissement. Un autre exemple de conséquence dans le milieu scolaire est le retardement du début des cours comme il l'a été pour les écoles américaines à Hartford au Connecticut. L'infection ransomware a bloqué l'accès aux données et a, en outre, rendu inutilisable pour un certain temps le système de communication que les écoles utilisent avec leur compagnie de bus, rendant impossible la tenue des cours le mardi. Les enjeux majeurs dans ce secteur sont les dégâts liés au retard et à la désorganisation qui nuisent gravement à l'éducation en général. Cette

désorganisation peut devenir très problématique lorsque l'on pense à un minutage synchronisé au niveau fédéral pour des examens fédéraux devant être passés au même moment, par exemple.

Dans le cadre du secteur de la santé, des dossiers médicaux ont été inaccessibles voir même perdus définitivement.

Un cas horrible de ransomware dans le secteur de la santé aurait même abouti, pour la première fois, à la mort d'une personne en Allemagne.

En effet, en septembre 2020, la clinique universitaire allemande « Duesseldorf » a été touchée par un ransomware qui a encrypté les données de 30 serveurs de l'hôpital (SECURITY 2020). Le système informatique de l'hôpital a été rendu progressivement non opérationnel à la suite de l'attaque. Ayant même eu pour conséquence le transfert d'une femme dans une condition de mort imminente dans une autre ville pour recevoir un traitement, mais qui est finalement morte juste après avoir été transférée. L'hôpital n'avait même pas reçu de demande de rançon claire à la suite de l'attaque, mais juste des coordonnées pour contacter les malfaiteurs. Coordonnées qui étaient adressées non à l'hôpital mais à l'université dont il est affilié. En outre, l'attaque visait l'université et non l'hôpital, ce qu'a expliqué la police qui est allée les contacter en leur demandant de rendre la clé de décryptage car l'attaque mettait en danger la vie des patients, demande exécutée par les malfrats, reporte « AP News ».

Finalement, selon un article écrit par Patrick Howell O'Neill (2020), un reporteur dans le domaine de la cybersécurité, la fameuse victime aurait succombée tôt ou tard face à sa maladie, qu'il y ait eu ou non cette attaque contre l'hôpital. Même s'il se pourrait que cette attaque n'ait pas été la cause de la mort de cette femme dans ce cas précis, cela ne change aucunement le fait qu'une telle action, un jour, pourrait réellement blesser, voir causer la mort de patients.

6. Les auteurs des ransomwares

Et que dire des auteurs de ces délits ?

Nous avons déjà mentionné plus tôt le promoteur de la toute première attaque de type ransomware : « Joseph L Popp ». Mais le nom que l'on retient le plus est sans doute le groupe de cybercriminels « MAZE ». Groupe s'étant spécialisé dans les maze ransomwares. En effet, c'est le groupe qui s'est rendu le plus populaire par le fait

d'utiliser son site web pour afficher les données volées à la suite d'une rançon non payée, ce qui a beaucoup fait parler d'eux. Comme en décembre 2019, en publiant un échantillon des 120 GB de données volées à « Southwire », une entreprise nord-américaine de confection de câbles ayant refusé de payer les 6 millions de rançon exigés (COBLE 2020).

L'explosion des ransomwares provient du fait indéniable que dans le domaine de la cybercriminalité, les attaques de ce type sont extrêmement lucratives. Les groupes comme « MAZE » le démontrent bien.

Nous avons donc une émergence de nouveaux acteurs qui se lance à leur compte et/ou qui vont employer des cybercriminels ayant les compétences en matière de rançongiciels. En effet, nous pouvons trouver maintenant tout un business autour des ransomwares et des cybercriminels qui mettent leurs talents en vente.

Il ne faut pas oublier que des cybercriminels connus dans d'autres domaines se mettent à la tendance du ransomware. Je parle par exemple du groupe « Emotet », Dridex ou encore « Trickbot » (AULD).

Ainsi on peut remarquer que les ransomwares peuvent être lancés par vraiment n'importe quel type ou groupe d'individu et peuvent cibler des particuliers isolés comme de très grandes entreprises et/ou gouvernements.

7. Quelques chiffres

Avant d'aller plus loin et de se renseigner sur comment se protéger contre de telles attaques, analysons quelques chiffres établit par KOCHOVSKI, Aleksandar (2020), concernant ces fameux ransomwares.

Les attaques ransomwares sévissent de plus en plus à tel point qu'en 2020 elles atteignent une ampleur conséquente :

En effet, selon les entreprises interrogées en 2020, 51% d'entre-elles ont déjà subi une attaque ransomware.

Le prix moyen d'une rançon tourne autour de 5'900 USD soit environ 5'240 CHF pour une petite entreprise et de 178'000 USD ou 158'100 CHF pour la somme moyenne des rançons demandées en 2020.

La plus grande somme demandée par les cyberpirates a été faite le 30 janvier 2020. Cette rançon s'élevait à environ 10 millions d'euros et a été exigée à la compagnie française « Bouygues Construction » pour la récupération d'environ 200GO de leurs données. La compagnie « Bouygues Construction » a cependant pris le bon réflexe de ne pas payer la rançon. Le temps estimé pour une récupération totale ne devrait pas prendre plus que 4 à 6 semaines environ, selon le ressenti du personnel de « Bouygues Construction » (BOHIC, 2020).

La compagnie danoise « Maersk », le plus grand transporteur maritime mondial a, elle aussi, subit une attaque qui lui a coûté très cher. Le ransomware responsable dans ce cas est dénommé « NotPetya malware ». Cette attaque survenant en juin 2020, n'aurait pas résulté en un vol de données, affirme la compagnie, mais en un grand et problématique arrêt des systèmes informatiques cruciaux pour le bon fonctionnement de la compagnie. Les dégâts ont résulté à une impossibilité de continuer le processus de transport de marchandise pour environ trois des neufs unités commerciales du conglomérat et s'est traduit en une perte de près de 300 millions de dollars américains de pertes financières (LORD, 2020).

Il faut garder en tête qu'une victime sur quatre continue de payer la rançon et que selon les statistiques pour 2021, une compagnie sera victime d'une attaque par ransomware toutes les 11 secondes.

8. Comment s'en protéger

Comme expliqué précédemment, les attaques surviennent sur deux différents niveaux majeurs, au niveau humain et technique.

8.1 Se protéger sur le plan humain

Il faut surtout travailler sur la vigilance et construire des bonnes pratiques :

<u>Les courriels électroniques :</u>

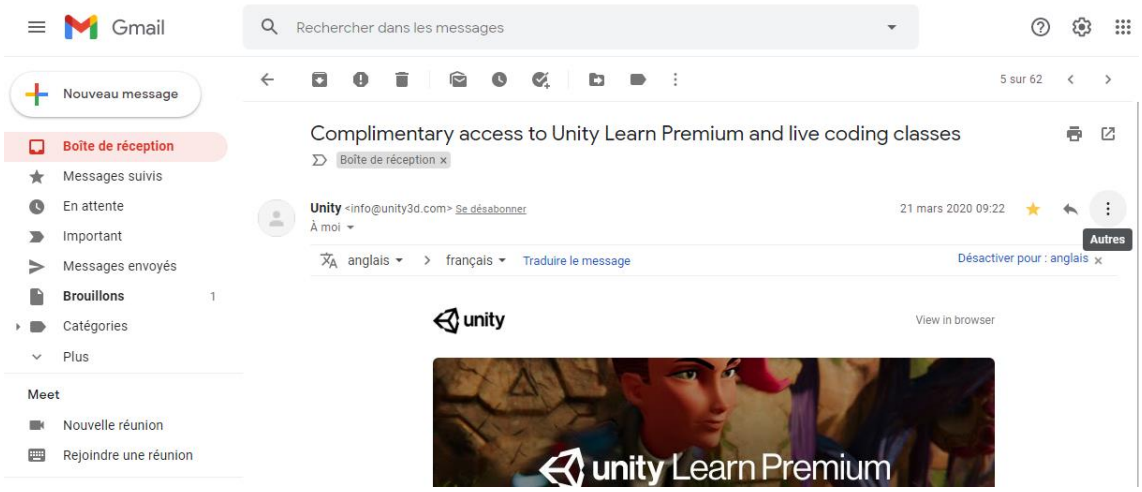
- Ne jamais cliquer sur un lien dont la source est inconnue et/ou l'adresse http ne commence pas par « https:// ».
- A la lecture du courriel, vérifier l'adresse électronique de l'expéditeur.
- Ne pas télécharger des pièces jointes par curiosité pour les lire.

- Lorsqu'à la lecture du contenu du courriel cela parait suspect d'en être le réceptionnaire, envoyer un e-mail de confirmation à l'expéditeur sans utiliser le bouton automatique « répondre » mais depuis le carnet d'adresse.
- Ne jamais donner ses informations de login.
- Pour s'assurer que le courriel ne contient aucun contenu caché malveillant, vérifier le code source de l'e- mail. Le code source étant le contenu réel du courriel avant interprétation de celui-ci (avant d'appliquer les diverses actions de mise en page). C'est dans le code source qu'il sera possible de voir les « balises » invisibles permettant les attaques (AROBASE, 2018).

  Comment afficher le code source depuis le Webmail Gmail :

  1) Sélectionner l'e-mail dont on veut afficher le code source.
  2) Cliquer sur l'option « autres » situer après le bouton flèche « répondre ».

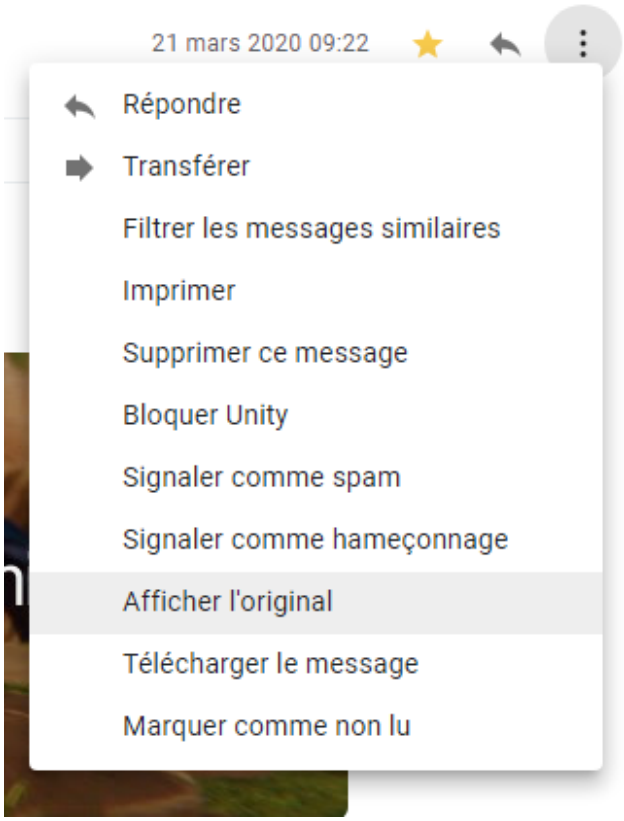
Figure 4 : Capture d'écran : Trouver l'option « autres » sur Gmail



(LAGARE SARA 2021)

3) Sélectionner « Afficher l'original ».

Figure 5 : Capture d'écran : Détails de la fenêtre « autres » sur Gmail



(LAGARE SARA 2021)

4) Le code source s'affiche dans une nouvelle fenêtre :

Figure 6 : Capture d'écran : Code source d'un e-mail sur Gmail

```
Delivered-To: yooooupi@gmail.com
Received: by 2002:a0c:fc45:0:0:0:0:0 with SMTP id w5csp655448qvp;
        Sat, 21 Mar 2020 01:22:46 -0700 (PDT)
X-Google-Smtp-Source: ADFU+vvVni8Zb7gGCK5FFGPXpnhtzzyuKoGTRJfSH3xhiW41pgRDcOTCKlEVfJjSq6oT9nIVBBNh
X-Received: by 2002:a17:906:c4f:: with SMTP id t15mr12163610ejf.193.1584778966052;
        Sat, 21 Mar 2020 01:22:46 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1584778966; cv=none;
        d=google.com; s=arc-20160816;
        b=fH/luqd4LOZtLbTt63kIWwNrgo0lVKHn7BZk0WWThy+P1GcNqkwdvlStv1FShqeTp7
         uYa6wG5iQQS4ZquP1sMMKdER0HGraSBnpA9RIR5V3+/zpFrPmS04Sj6jlkozBFwMsH7s
         j213zjFLfIe4LMKvP3/qaD+RmV+PfPzL1h5lB1mBt8J8+0tH9Dt9j0EWQlHi/KcPfJhP
         L9IZWSr9v6L88vgpcIWc9BTJdrJOi5Z89QAERE5nl+laHWW33P1cWhWj/jDVurn/N4NW
         4tmdHrrDn7MmXeDhANcFwsDUAligJMOUqADad7rxlu+vd5Kt+ga+nEi5TkaruyCC4/TZ
         JN6Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=subject:date:reply-to:to:from:mime-version:list-unsubscribe
         :message-id:dkim-signature;
        bh=2zdeBflx1mQd7o02dwz7fL/z9GXAN0zag4vbPlDK4Hc=;
        b=bmh5zGzQYh0p7/8Mxc19w7cUjJ8kL+wjGmWq4w8wlYEsO65lBU27+foIBQ8lomIL5o
         u2MM/l8vU1t45hJcUPH1ZRD9QuK5PrjoZFlz5YGcOKZyuTrgUkXD+BO8+O8K7IcSVL5f
         k43A5af6UP7X7FumBwVrbdd8ugq+iNQ3TR777CUQM+m6WgwOjHBnKMwAkO2xiBO9N697
         yG/5fXhO8EkveRTVkKF7yTCtCayK5G4zmpjD/vpGA7ooCNwvRc/w0j5Lz2laYU8hmg9H
         Kb5S7wmSmCcPKAOo+Ip2A9/seP1WYmA4A2sznG9apK4dUd2BwqqCFJnwtBTWB/QFpQIG
         JdQg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@unity3d.com header.s=dk1024-2012 header.b=Y9cYAcWe;
       spf=pass (google.com: domain of bounceback@response.unity3d.com designates 141.145.10.89 as
smtp.mailfrom=bounceback@response.unity3d.com;
```

(LAGARE SARA 2021)

La sauvegarde de données :

- Il est souhaitable et largement conseillé de faire des sauvegardes des données ne devant absolument pas être perdues.
- Suivre la bonne pratique de sauvegarde de données 3-2-1 : « 3 copies de vos données au moins, sur 2 supports différents, 1 sauvegarde hors site ». Il est important de faire au moins une copie hors site pour éviter de tout perdre en cas d'incendie, vol, etc. sur le lieu de travail (BURNEL, 2020).
- Il est important de créer des images systèmes afin d'être en mesure de restaurer les appareils si nécessaire.

8.2 Se protéger sur le plan technique

Drive-by download :

- Mettre à jour tout le contenu du site web, allant des thèmes aux add-ons.
- Retirer tout contenu obsolète qui n'est plus supporté par le site web.
- Utiliser un login et mot de passe de niveau fort pour les comptes administrateurs. (Un mot de passe d'une longueur d'au moins 12 charactères avec un mélange contenant au moins une majuscule, un symbole et un chiffre). Plus de détails concernant la protection de ses comptes via une bonne gestion de ces mots de passes sont disponibles depuis le site officiel tenu par la Confédération suisse à l'adresse suivante : https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-private/aktuelle-themen/konto-gehackt.html
- Installer des logiciels web pour la sécurité du site web et pour traquer plus efficacement les changements malveillants dans le code source du site.
- S'assurer de la sécurité des publicités recommandées affichées sur les différentes plateformes proposées. Beaucoup de drive-by downloads sont véhiculés au travers de publicités suspectes.
- Utiliser un compte administrateur uniquement pour l'installation de programme. Le problème est que le compte administrateur possède des droits privilégiés nécessaires aux drive-by download pour opérer. Etant donné que le téléchargement furtif s'effectue sans réel conscience de celle-ci par la victime, il est préférable alors d'utiliser un compte secondaire non-administrateur pour une utilisation basique de l'appareil.

- Garder le navigateur web et le système d'exploitation à jour.
- Il est conseillé de se débarrasser de tous logiciels superflus et inutiles afin d'éviter d'apporter plus de risques d'infections.
- Il est toujours utile d'adopter une solution de protection internet.
- Eviter les sites non officiels et ceux concernant le partage de documents.
- Toujours faire attention aux pop-ups et fenêtres d'avertissements sur les navigateurs, regarder l'orthographe de ceux-ci et la qualité des images utilisées, etc.
- Utiliser un logiciel antipublicitaire, « ad-blocker », permet d'éviter la possible infection via une fenêtre d'avertissement.

Autre :

- Eviter d'ouvrir des fichiers suspects en vérifiant aux préalables leurs extensions. Pour se faire, activer l'option dans les paramètres Windows « Afficher les extensions de fichiers » et éviter de préférence ceux de type « .exe, .vbs, et.scr. » (BINANCE ACADEMY, 2021).

9. Une fois attaqué

9.1 Réaction à la suite de l'attaque

Première étape : Déconnecter l'appareil

La première chose à faire si l'on est malheureusement victime d'une attaque par ransomware est de s'assurer d'éteindre l'appareil et de le déconnecter complétement du réseau internet. C'est-à-dire, débrancher le câble internet, éteindre le wifi et déconnecter tout type de partage de données avec l'appareil infecté.

Ceci est notre premier réflexe pour la simple raison que certaines cyberattaques, dont le ransomware, peuvent se propager depuis notre appareil aux appareils aux alentours via le réseau internet. D'où le besoin de tout déconnecter temporairement.

Une fois l'appareil isolé, on peut enfin se rendre compte de l'étendue des dégâts et cibler les appareils, fichiers et données touchés par l'attaque (DRUVA).

Deuxième étape : Trouver l'origine du problème et alerter les utilisateurs

Cette étape consiste principalement à se demander comment cela a-t-il pu arriver. L'attaque est-elle apparue juste après avoir cliqué sur un lien malveillant dans un mail ? Est-ce que j'ai utilisé des applications obsolètes car les mises à jour n'ont pas été faites ? Ai-je remarqué des fenêtres pop-ups de publicités inhabituelles dans mon navigateur internet ?

Lorsque l'on fait partie d'une compagnie, organisation, l'infection ransomware a pu se propager via le réseau internet comme expliqué précédemment. A ce moment-là l'interrogation de tous les membres de l'organisation pour identifier quelle personne en premier a remarqué les premiers signes de l'attaque est nécessaire. Il est également possible que l'attaque ne provienne pas uniquement d'une seule source, mais de plusieurs (SINGH, 2021).

Il est important de communiquer et d'expliquer à l'ensemble du personnel ce qui est en train de se passer et les raisons pour lesquelles cet incident a pu se produire. Rappelons-nous que bien souvent le problème se trouve entre la chaise et l'écran de l'ordinateur, et que la prise de bonnes pratiques à la suite de la compréhension des petits dangers quotidiens peut éviter bien des soucis. De plus, si cela est déjà arrivé une fois, il est important de comprendre pourquoi pour éviter que cela se reproduise une deuxième fois de la même façon.

Il nous est également possible et conseillé de relever l'attaque à l'autorité concernée. Plus les autorités recevront de comptes-rendus sur le nombre et type d'attaque, plus ils auront d'informations leur permettant d'identifier les auteurs de ces cybercrimes et de comprendre, déterminer les cibles de ceux-ci.

Troisième étape : Identifier le type de ransomware

L'identification du ransomware donne des indications utiles sur son mode de fonctionnement et la manière dont il se propage. Cela nous permet de mieux cerner l'étendue du problème et de savoir plus justement comment réagir face à la menace concernée.

Pour découvrir quel type de ransomware nous avons affaire, il est recommandé de prendre une capture d'écran du message d'avertissement de l'infection. En effet, le ransomware s'identifie par lui-même dans son message d'avertissement en déclarant

directement son nom, son id, ou en analysant la structure du message (procédé de paiement, adresse électronique, etc.) (VERRIER, 2020).

Il existe aussi des solutions pour découvrir plus justement le type exact du ransomware :

- No more ransom (https://www.nomoreransom.org/)
- ID Ransomware (https://id-ransomware.malwarehunterteam.com/)

Ces deux sites web représentent des solutions simples et gratuites pour trouver cette information.

Connaître la date exacte de l'infection aide à discerner le type de ransomware en question et peut également révéler si le malware était dans un état « dormant » dans l'appareil, ce qui veut dire qu'il était déjà présent dans la machine avant l'attaque mais qu'il a attendu un moment précis pour se déclencher.

Quatrième étape : Restaurer les appareils via la ré-imagerie

Dès que l'origine du problème est trouvée, erreur humaine ou brèche de sécurité au niveau informatique, il est temps de se débarrasser de l'infection. Malheureusement, la manière la plus sûre de le faire est d'opter pour une action drastique et de restaurer les appareils, serveurs, ainsi que les machines virtuelles touchés par l'attaque. En effet, l'utilisation d'un anti-virus pour éliminer les traces d'un rançongiciel peut être compliqué. La connaissance du rançongiciel exact utilisé est nécessaire, afin d'employer l'application de type anti-virus adéquate.

La manière la plus sûre d'opérer est donc de tout supprimer, de nettoyer les systèmes afin de les rendre comme neufs, puis de réimager pour la restauration des fichiers. La ré-imagerie est une méthode de restauration système utilisant une image disque qui se chargera de reconstruire un disque dur avec le contenu exact de l'image disque et de conserver l'arborescence des fichiers.

Cinquième étape : Récupération des données via des sauvegardes

C'est à cette étape finale que la prise de conscience est faite sur l'importance de la création de sauvegarde déjà citée précédemment qui reste l'unique façon de s'en sortir à tous les coups après le cryptage des données par le ransomware. Si la règle de sauvegarde 3-2-1 a été suivie, grâce à la copie hors-site, les appareils restaurés avec la

réimage seront donc fonctionnels à nouveau et complétement seins, nettoyés de tous virus. De plus la récupération des données et applications critiques et manquantes se feront via les sauvegardes sur le cloud.

9.2 Faut-il ou non payer la rançon

9.2.1 Les raisons de ne pas payer

Dans la mesure du possible, la rançon ne devrait jamais être payée et ce pour des raisons évidentes.

La première étant que : « **Payer la rançon ne garantit aucunement le déchiffrage des données ni le déverrouillage de l'appareil** ».

De plus, même dans l'optique ou la clé de déchiffrage a été échangée contre la rançon, les cyberpirates, ayant eu accès à vos données, ont pu les extraire et dans le cas des maze ransomwares, par exemple, ils ont les pleins pouvoir d'en faire des copies et de les échanger avec d'autre cyberpirates.

Selon une étude, lancée en 2016 faite par Kaspersky sur les risques informatiques en matière de sécurité, qui détermine que sur les 34% d'entrepreneurs disant payer la rançon, une compagnie sur cinq ne réussit pourtant pas à récupérer ses données.

Un exemple d'un cas de paiement de rançon infructueux est celui d'un hôpital en Amérique, le « Kansas Heart Hospital » (SIWICKI, 2016).

Celui-ci aurait été attaqué par un ransomware qui aurait encrypté certaines de ces données. Nous ne savons pas exactement la quantité et qualité des données touchées, ni la somme de la rançon demandée. Nous savons seulement que ces données encryptées ne dérangeaient pas au bon fonctionnement de l'hôpital et que la première rançon demandée ne représentait pas une somme exorbitante. Oui, « première » rançon, car dans ce cas il est intéressant de relever qu'une fois la première rançon payée, l'hôpital n'a pas récupéré la clé de déchiffrage de ces données, mais une deuxième rançon lui a été demandée à la place.

Cela montre bien que si ces malfaiteurs ont le pouvoir de demander une rançon, ils ont les moyens d'en demander autant qu'ils le souhaitent. Tout leur est permis. La seule vrai solution contre eux consiste à ne pas payer. D'où l'importance d'avoir un backup opérationnel en cas d'attaque et surtout de mieux se sécuriser pour ne plus être attaqué.

Deuxièmement : « **Payer la rançon finance la cybercriminalité** ».

En effet, non seulement il n'y pas de garantie de récupérer ses données dans un état opérationnel, mais aussi et surtout, payer les rançons incitent les cybercriminels à poursuivre leurs activités malsaines.

Continuer à payer les rançons favorisent l'essor des attaques de type ransomwares. Et cela se remarque également au niveau du montant moyen de la rançon, montant qui a quasiment doublé entre 2018 et 2020 passant ainsi de 4'300 à 8'100 USD.

Certains cybercriminels spécialistes dans les attaques de type ransomwares vont jusqu'à louer leurs services à d'autre pirates. Ceux à l'origine du rançongiciel nommé « GrandCrab », par exemple, affirment même avoir acquis un montant annuel de 150 millions de dollars américains via cette activité. Les ransomwares sont donc un revenu extrêmement lucratif dans le milieu de la cybercriminalité, ce qui contribue à leur essor dans le domaine.

9.2.2 Pourquoi certains payent la rançon

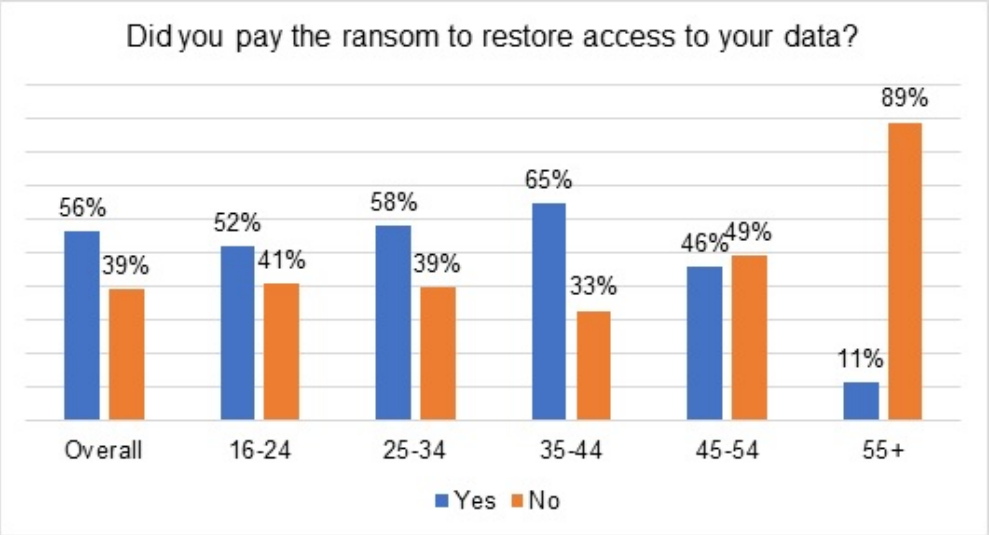
Après avoir expliqué l'importance de ne pas payer cette rançon au chapitre précédent, il est intéressant de nous questionner sur la raison qui poussent toujours certaines personnes à payer.

Rappelons-nous que les ransomwares cherchent à mettre une pression immense sur leurs victimes, visant à les prendre de court afin qu'elles ne puissent même pas considérer une autre option que celle de payer.

C'est à cet effet que dans le message d'avertissement fournit par le malware sur la machine est affiché généralement un chronomètre. Le fait de donner un temps limité pour réagir, pour payer la rançon, de pouvoir le visualiser, est un moyen pour stresser la victime. Pourquoi mettre un temps limite au paiement autrement ? Ce qui leur importe est la rançon (et les données elles-mêmes dans le cas des « maze ransomware » où les pirates réussissent à les extraire et peuvent les marchander). Bien que les pirates, dans le cas précis des ransomwares, ont majoritairement comme principal objectif d'être payés, certains peuvent toujours trouver un certain profit à simplement mettre hors de fonctionnement certains services fournis pour l'entité visée.

Selon une étude effectuée par Kaspersky, il est mentionné que parmi les victimes de ransomwares, les personnes plus jeunes ont une plus grande tendance à payer la rançon tandis qu'uniquement 11% décident de payer pour celles âgées de plus de 55 ans.

Figure 7 : Statistiques concernant le paiement ou non des rançons en 2020



(KASPERSKY 2021)

Les victimes plus jeunes sont en général moins conscientes du danger des ransomwares et des moyens de lutter contre. Pris sous pression et face à leur ignorance sur l'ampleur et la nature exacte de l'attaque, elles choisiront souvent de simplement payer.

D'autres chiffres donnés par Panda Security montrent que concernant les entreprises et spécialement les PME, 87% d'entre-elles sont préparées à faire face à une attaque ransomware. Les 17% restant ne se sentent pas prêtes, majoritairement pour des raisons de temps et de ressources (PANDA, 2020).

Pour de nombreuses entreprises, plus l'interruption de leurs services est longue, à la suite du vol de leurs données, plus cela peut être catastrophique pour leurs clients qui ont un besoin immédiat de leurs services. Les secteurs publics, comme celui de la santé ou de la sécurité, doivent évidemment pouvoir être opérationnels en tout temps.

Un autre point important à relever, c'est que le temps où l'entreprise est bloquée et mise à l'arrêt à la suite de l'attaque peut être long. Selon les cas cela peut même durer plusieurs jours. Tout dépend de comment la victime est préparée à rebondir sur ce genre d'attaques. Les entreprises utilisant des backups prennent en général 2 jours. Cependant les statistiques démontrent que 30% des entreprises prendraient environ 5 jours, si ce n'est pas plus, pour avoir à nouveau accès à leurs données. Certaines compagnies affirment que le coût total des dégâts engendrés à la suite de l'arrêt du bon fonctionnement de l'entreprise (perte d'opportunités commerciales, dommages liés à la réputation de l'entreprise, dédommagements face aux clients mécontents) est souvent énormément plus élevé que la rançon elle-même. Il semblerait selon « Tech

Transformers », qu'un simple accident de type ransomware peut facilement coûter en moyenne plus de 700'000 USD, 642'775 CHF (GRAHAM, 2017). Aussi, certaines victimes, si cela leur revient moins cher, choisissent de payer la rançon ne regardant ainsi que l'aspect financier de la situation.

De plus, selon des statistiques fournit par « Coveware », une entreprise dont la mission se concentre à aider les compagnies à récupérer leurs données en cas d'attaques ransomwares et ce de manière transparente, affirme que sur 98% des entreprises interrogées victimes d'un ransomware qui avaient payé la rançon et avaient reçu la clé de déchiffrage, cette clé n'avait fonctionné que pour 97% seulement des entreprises interrogées (COOK, 2021). Cet étonnant haut pourcentage de récupérations de données réussi à la suite du paiement aux cyberpirates conforte les victimes à choisir l'option du paiement se sentant plus en confiantes sur le succès obtenu par ce procédé.

10. Contexte législatif

10.1 Peines encourues

Pour ce qui est de la Suisse, voici ci-joint une liste des principaux articles du Code Pénal Suisse faisant référence aux infractions liées aux rançongiciels, et plus loin leurs détails :

- Art. 143 : « Soustraction de données »
- Art. 143bis : « Accès indu à un système informatique »
- Art. 144bis : « Détérioration de données »

Les infractions commises lors de rançongiciels peuvent concerner également quelques autres articles du code pénale listés comme suit :

- Art. 146 CP : escroquerie
- Art. 147 CP : utilisation frauduleuse d'un ordinateur
- Art. 156 CP : extorsion et chantage
- Art. 177 CP : injure
- Art. 179^{novies} CP : soustraction de données personnelles
- Art. 305bis CP : blanchiment d'argent

Ci-après le détail des trois principaux articles du code pénal suisse listés précédemment (CONFEDERATION SUISSE, 2020) :

Art. 143 CP : « soustraction de données »

> *1 Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.*
>
> *2 La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.*

Art.143bis CP : « Accès indu a un système informatique »

> *1 Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à au-trui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*
>
> *2 Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*

Art.144bis CP : « Détérioration de données »

> *1. Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*
>
> *Si l'auteur a causé un dommage considérable, le juge pourra pronon-cer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.*

2. Celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des indications en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Si l'auteur fait métier de tels actes, le juge pourra prononcer une peine privative de liberté de un à cinq ans.

10.2 Nouvelle Loi fédérale Suisse sur la protection des données

L'assaut des rançongiciels augmentant, la crainte concernant la sécurité des données personnelles grandit tout autant parmi la population. Il est ainsi bon à noter que la loi en Suisse sur la protection des données recevra bientôt quelques modifications.

En effet, une nouvelle Loi fédérale sur la protection des données a été adoptée en Suisse par le Parlement fédéral le 25 septembre 2020. Le délai référendaire étant en cours, son entrée en vigueur devrait se situer courant 2022 (SWISS BANKING, 2020). Pour ces nouveaux points les plus intéressants, voici en résumé :

- **Le concept de « données personnelles sensibles »** concernera également les données sur l'origine ethnique, les données génétiques mais aussi les données biométriques identifiant une personne physique de manière univoque.
- **Apparition de la notion de « profilage »,** traitement automatisé de données personnelles relatives par exemple à la santé de la personne concernée, à sa localisation, etc. Lors du profilage, l'accord de la personne en question ne sera pas requis.
- **Insistance sur le devoir d'informer** par la personne ou organe fédéral qui détermine la finalité et les moyens du traitement des données.
    - Devoir d'informer sur tout type de collection de données personnelles et non uniquement sur les données personnelles sensibles.
    - Devoir d'informer au minimum :
        - L'identité et les coordonnées du responsable du traitement des données collectées.

        - La finalité du traitement, le cas échant les destinataires ou catégories de destinataires des données personnelles. (Plus d'informations concernées si transmises à l'étranger).

- **Le droit à la remise et à la transmission des données personnelles** est maintenant octroyé à toute personne physique en étant à l'origine.

- **Les sanctions pénales** assurant la mise en œuvre de ces réglementations sont plus poussées dans la nLPD, elle y rajoute de nouvelles infractions et en augmente l'amende maximale encourue qui sera alors de 250'000 CHF.

    - La responsabilité pourra être également engagée non seulement par l'entreprise en question mais aussi par la personne physique responsable.

- **Le secret professionnel** sera imposé à toutes les professions et « sera ainsi puni d'une amende de 250 000 CHF au plus quiconque révèle intentionnellement des données personnelles secrètes portées à sa connaissance dans l'exercice de sa profession. ».

Le devoir d'informer jouera un rôle très important dans le cadre des rançongiciels, car malheureusement beaucoup trop d'attaques restent secrètes par les entreprises touchées, par craintes des conséquences à l'image qu'elles donnent. Environ seulement 10 à 20% des entreprises victimes déclarent publiquement avoir été attaquées, et ce même vis-à-vis de leurs partenaires d'affaires (CBC NEWS, 2020).

10.3 Protection et assurances

Les entreprises, comprenant le danger que représente ces cyberattaques grandissantes, cherchent soutien et protection auprès d'une toute nouvelle structure émergente. Je parle de l'apparition d'assurances qui dit couvrir les entreprises contre les dégâts provenant d'attaques par ransomwares. En réalité, cela apporte un autre type de problème, car ce genre d'assurance incite implicitement les entreprises à payer la rançon et à aller se faire rembourser, en partie, pour les dégâts engendrés. De plus, ces assurances ont pour habitude d'encourager activement les entreprises à payer la rançon ce qu'il est déconseillé de faire, car encore une fois, payer la rançon ne garantit pas la restitution en partie ou entière des données ou le déblocage et l'accès à l'appareil. Cela finance la cybercriminalité, favorisant son essor et rend la victime encore plus encline à subir une nouvelle attaque dans le futur pour avoir docilement payer la rançon la première fois. Cependant, cela reste favorable pour les assurances car plus il y a ce genre d'attaque, plus les entreprises auront peur et chercheront à se faire assurer contre

ce genre de danger. Evidemment, les assurances regardent ce qu'il est plus rentable de faire et financièrement parlant, c'est bien souvent de payer la rançon.

Un tel cas est arrivé en Floride dans la ville de « Lake City » en juin 2019. Victime d'un rançongiciel, le maire et le conseil de la ville, après avoir demandé des conseils sur la façon de gérer cette crise, en ont conclu qu'il était bien plus rentable de laisser son assurance « Beazley » s'occuper de payer la rançon s'élevant à 460 000 USD et d'ensuite, ne payer que 10 000 USD déductibles à celle-ci (NAIC, 2020).

Voici-ci des exemples de compagnies offrant une cyber assurance en Suisse, en faveur des entreprises :

- ZURICH CYBERASSURANCE
- AXA
- Allianz
- Vaudoise

Et celles visant plus spécialement les particuliers :

- Generali
- Allianz-travel (Assurance cyber)
- Baloise

11. Plateforme web d'aide créée

11.1 Introduction du site Internet

Pour conclure ce travail de recherche écrit, je vais maintenant vous présenter le site internet créé en complément.

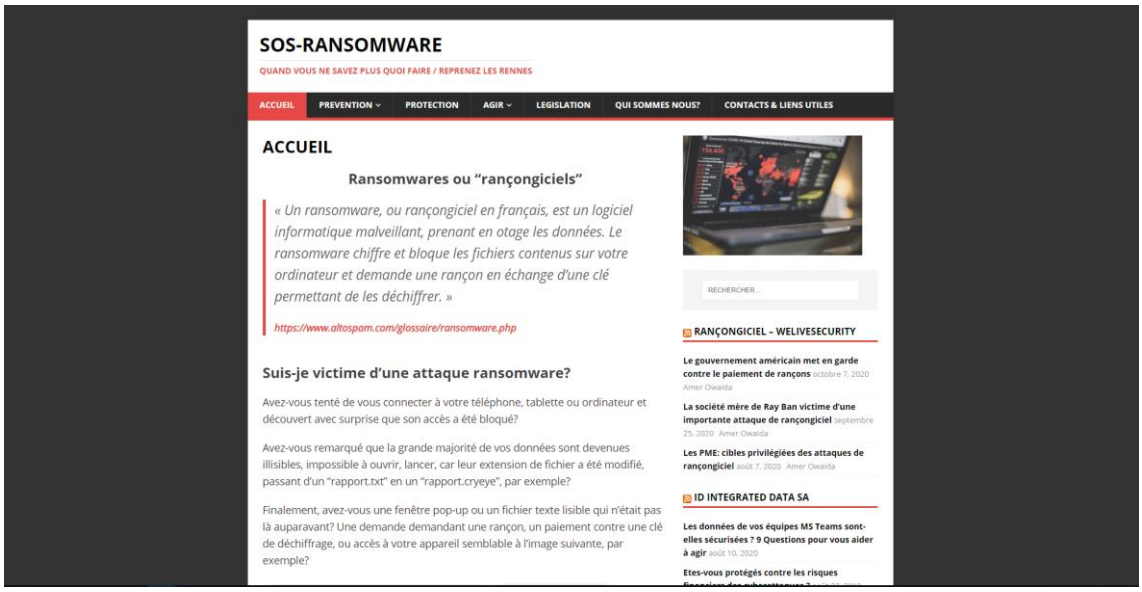
Je me réserve le droit de vous l'exposer d'une manière simple allant à l'essentiel car il sera ouvert et consultable jusqu'au 16 mars 2022 et vous invite à vous y rendre pour recevoir plus de détails le concernant.

J'ai nommé le site internet « sos-ransomware » et l'ai rendu accessible à l'adresse http suivante : https://sos-ransomware.site.

Le rôle de mon site internet est de fournir une source complète d'informations concernant les ransomwares sous une forme simple et accessible par tous ainsi qu'une aide pour les personnes atteintes du malware.

En demandant conseils à mon entourage et pour des raisons financières, je me suis finalement confiée à « Infomaniak » pour l'hébergement de mon site internet. Me demandant de ne payer uniquement pour le nom de domaine du site internet, j'ai obtenu gratuitement son hébergement et la création d'une adresse électronique, en profitant de leur offre étudiante (INFOMANIAK).

Figure 8 : Site internet : Page d'accueil



(LAGARE SARA 2021)

11.2 Explication du design

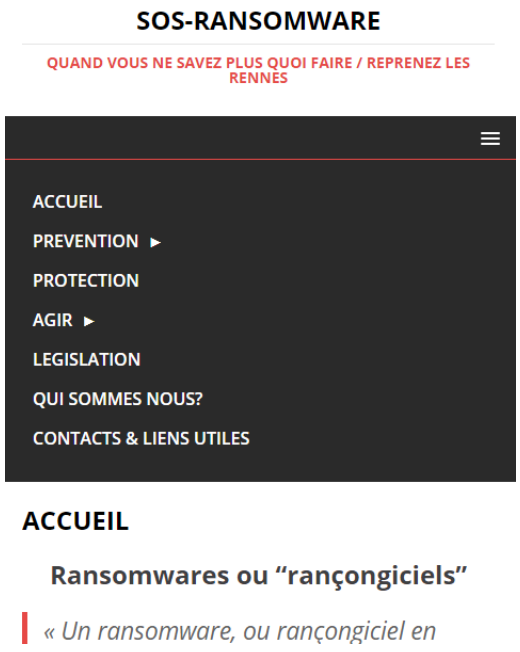
J'ai choisi de confectionner ce site internet en utilisant le logiciel libre WordPress. J'ai donc opté pour un thème de site internet simple avec un format qui permet, dans la plupart des formats d'écrans d'ordinateurs, d'être minimisé en ne s'étalant que sur la moitié de l'écran.

Le design du site est donc entièrement responsif et reste complétement fonctionnel même sous format mobile. En effet, il est lisible depuis un smartphone dans son intégralité, comme présentée plus loin aux figures 9 et 10. Ceci est un point important pour moi car dans le cas où l'appareil infecté par un ransomware serait un PC, par exemple, son propriétaire pourra facilement recevoir l'aide fournit par le site internet depuis son smartphone.

Figure 9 : Site internet : Présentation sous format réduit et menu fermé

(LAGARE SARA 2021)

Figure 10 : Site internet : Présentation sous format réduit et menu ouvert



(LAGARE SARA 2021)

Le site se compose visuellement de 5 parties :

L'en-tête du site, avec nom et slogan du site : « Quand vous ne savez plus quoi faire / reprenez les rênes ».

La barre de menu du site, permettant la navigation sur le site web et l'accès à l'ensemble du contenu du site.

Le corps du site internet hébergeant tout le contenu informatif du site web.

La partie latérale droite restant inchangée lors de la navigation du site, elle possède une image habillant le site internet suivi d'une barre de recherche permettant de faire des recherches par mots-clés sur l'intégralité du site web. Elle propose également une sélection de flux RSS.

Le bas de page exposant le copyright.

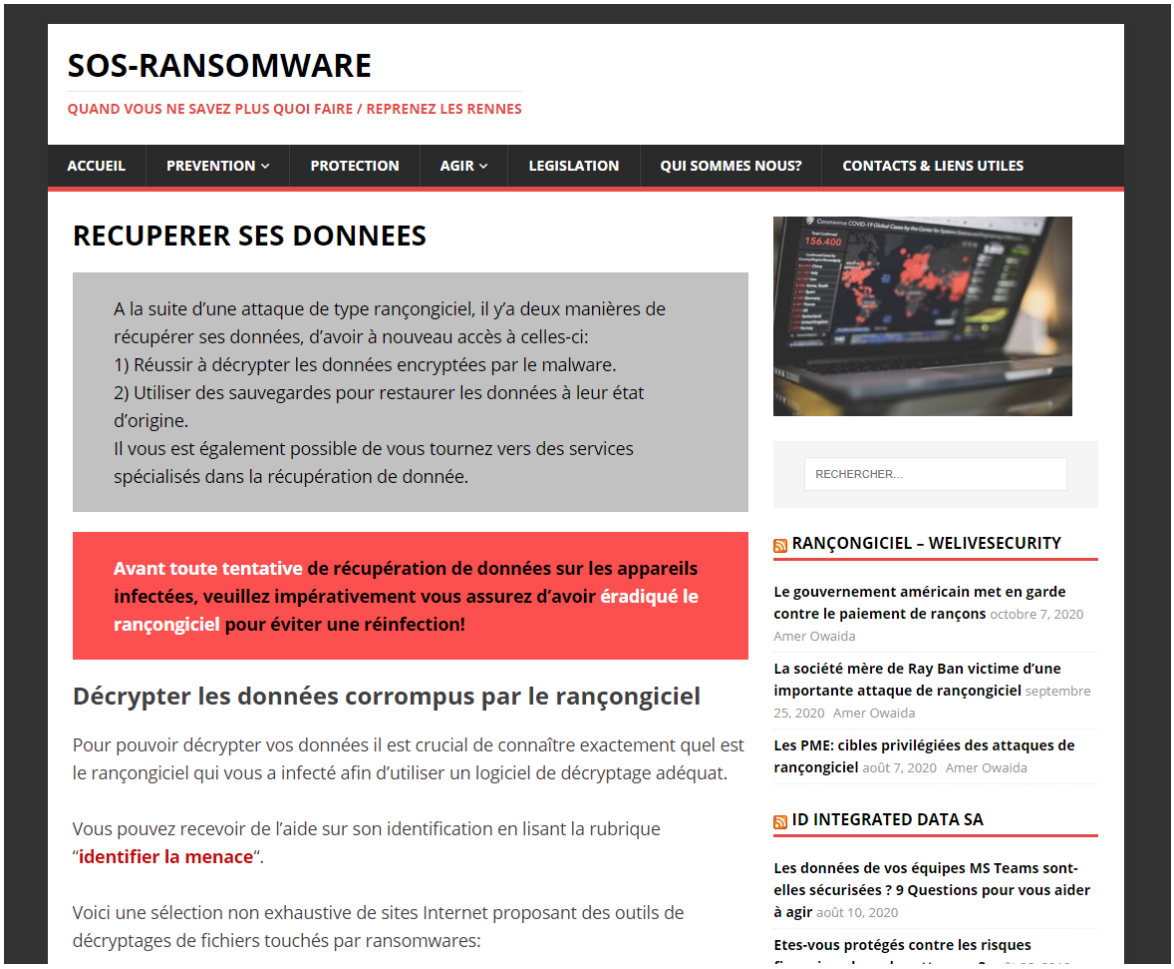
Explication du choix des couleurs utilisées :

Pour ne pas donner trop d'infos visuelles, ce qui risque d'engendrer de la confusion pour l'utilisateur, le site internet garde le même set de couleur dans différentes variations de gris, rouge, ainsi que du blanc.

L'écriture rouge sur fond blanc est destinée à donner une plus grande importance et si celle-ci est également en gras, cela signifie que le terme est cliquable pour rediriger l'utilisateur sur une autre page du site ou sur un site externe.

Les blocs d'écritures en gris sont là pour structurer l'information en y présentant des explications et des informations supplémentaires tandis que les blocs rouges maintiennent la fonction de représenter des informations importantes et des avertissements. Des mots-clés en gras blanc sont là pour attirer les yeux sur le bloc rouge.

Figure 11 : Site internet : Illustration du set de couleur



(LAGARE SARA 2021)

Pour ce qui concerne l'identité du site, je n'ai pas trouvé pertinent de réaliser un logo pour le site internet mais j'ai cependant confectionné moi-même, une favicon. Une icône qui est visible au niveau des onglets du navigateur. Elle est basique respectant le même set de couleur énoncé précédemment. Etant donné qu'elle ne sera affichée que sous un format très réduit, il était inutile de rajouter trop de détails.

Figure 12 : Site internet : Favicon du site

(LAGARE SARA 2021)

11.3 Explication du contenu

L'ensemble du contenu du site est articulé autour de la barre de menu déroulante de celui-ci.

Figure 13 : Site internet : Barre de menu

(LAGARE SARA 2021)

Elle a été agencée selon la façon logique d'une cyberattaque. Elle commence évidemment par la page d'accueil qui est également atteignable en cliquant sur le titre du site exposé dans l'en-tête.

Elle est ensuite suivie du menu déroulant « prévention » permettant de recevoir des informations importantes sur les bonnes pratiques à prendre au niveau humain et technique afin de limiter les risques d'infection au ransomware.

Figure 14 : Site internet : Menu déroulant de la rubrique « prévention »

(LAGARE SARA 2021)

La partie protection explicite les types de protections possibles face à la menace informatique tout en fournissant des redirections et exemples de protection.

Vient ensuite la partie « Agir », qui fait référence aux façons d'agir face à la menace si nous en sommes la victime :

Figure 15 : Site internet : Menu déroulant de la rubrique « Agir »

(LAGARE SARA 2021)

A cet effet, le menu « Agir » offre 3 sous-menus dans l'ordre logique nous permettant de savoir comment « stopper la menace », en sachant « identifier la menace » afin de pouvoir ensuite « récupérer ses données ».

En cliquant simplement sur « Agir », nous avons la possibilité d'effectuer deux quizz.

Le premier permet à l'utilisateur d'être guidé interactivement sur les pages du site étant plus susceptibles de lui être utiles. Le quizz est fait sous un format de « questions scénarios » ou la finalité des choix effectués redirige l'utilisateur sur la page du site adéquate.

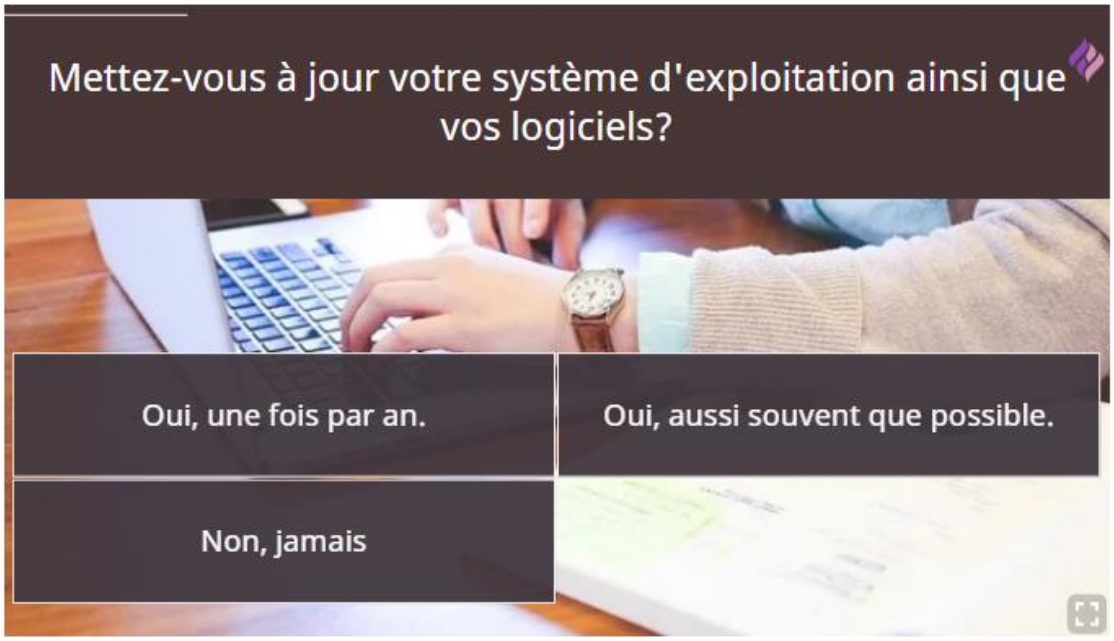
Figure 16 : Site internet : Quizz 1 – Navigation sur le site

(LAGARE SARA 2021)

Le deuxième quizz questionne l'utilisateur sur sa manière d'interagir avec son environnement informatique afin de le rendre conscient de son niveau de sécurité par rapport aux cyber-dangers.

Contrairement au premier quizz, celui-ci est sous un format de questions-réponses avec une seule bonne réponse possible. Une courte explication de la bonne réponse est affichée après chaque choix effectué.

Figure 17 : Site internet : Quizz 2 – Test sur le niveau de sécurité personnel



(LAGARE SARA 2021)

Parmi les dernières options du menu figure la partie « législation » qui permet aux utilisateurs d'avoir accès rapidement au code pénal relatif à une attaque de type ransomware.

Une rubrique « qui somme nous ?» arrive en avant dernière place afin de me présenter en tant que créatrice du site web. J'explique mes motifs pour sa création et donne la possibilité aux utilisateurs de me contacter en cas de besoin au courriel suivant : « support@sos-ransomware.site ».

Finalement, j'ai choisi de mettre en dernière position la rubrique « contacts & liens utiles » qui contient les liens et sites internet utiles dans le cas de ransomware.

Afin d'habiller le site et de le rendre un peu plus interactif, nous pouvons voir sur la barre latérale droite une multitude de flux RSS permettant d'avoir dynamiquement les dernières nouvelles sur la sécurité informatiques des sites en question.

12. Conclusion

12.1 Synthèse

En réalisant cette étude sur les ransomwares, il est apparu que ces cyberattaques étaient déjà présentes depuis 1986 avec le tout premier cas du PC Cyborg virus. Le procédé principal était déjà de berner les victimes en utilisant les supports de l'époque, à savoir des disquettes. Ces disquettes se sont dès lors transformées en courriels malicieux et transmissibles en une seconde.

Les méthodes de transmission du virus sont principalement orientées sur l'ingénierie sociale et la naïveté des gens. Beaucoup de trop de personnes utilisent internet et des environnements informatiques sans avoir conscience des cyber-dangers que ceux-ci peuvent apporter. La simple prise de conscience que tout liens http ou page web n'est pas libre de virus n'est pas présente chez tout le monde, bien que plus en plus d'entre-nous entrent dans un monde hyperconnecté. De la même façon, la majorité des failles techniques pourrait être évitée par la simple aptitude à garder ses applications à jour. Tout ça pour dire qu'une simple connaissance des dangers et la prise de certaines précautions et habitudes pourraient radicalement éviter bon nombre de désagréments.

Le constat a été fait que ces attaques peuvent prendre pour cible quasiment n'importe quel type d'entité, du particulier aux grandes entreprises, en passant par les services publics, de la santé et de la police. Personne n'est donc à l'abri des dommages causés par les ransomwares. En ce qui concerne le risque de perdre ces données définitivement, il n'y a qu'une unique et très simple solution, celle d'effectuer des sauvegardes régulières et sécurisées de ses données en suivant le principe 3-2-1.

La popularité de ce type de cyberattaque provient principalement de sa facilité à attaquer une cible. Comme énoncé dans cette étude, par rapport aux entreprises, il a été estimé qu'en 2021 une entreprise sur deux sera potentiellement victime d'un rançongiciel toutes les 11 secondes, ce qui est loin d'être anodin. Mais ce qui motive réellement les cybercriminels c'est le gain immense lié au paiement de la rançon. Car encore beaucoup trop de personnes choisissent de payer ces sommes qui parfois sont exorbitantes. A cet effet, Il ne faut pas omettre le fait qu'il existe tout un système de pression pour forcer la main aux victimes. Un temps limité pour prendre la décision de payer ou non et même dans certains cas, la menace de poster les données volées sur des sites de « shaming » si la victime refuse de payer.

Malgré tout, le paiement de la rançon continue d'alimenter ce système de cybercriminalité à tel point que les cybercriminels compétents dans le domaine des

ransomwares en viennent même à louer leurs services aux plus ignorants, désireux eux aussi de profiter de ces gains potentiels.

Les entreprises ont beaucoup à perdre, que ce soit en payant la rançon, avec les dommages liés à l'image et la perte de confiance de ses clients, ou bien même simplement à cause de ceux dû au temps d'arrêt de leur fonctionnement causé par le ransomware. C'est précisément à ce moment que les cyber-assurances apparaissent en promettant diverses couvertures pour pallier ces dégâts. Profitant également de ces cyberattaques, beaucoup d'entre-elles préconisent le paiement de la rançon en cas d'attaque, ce qui, encore une fois, est fortement déconseillé.

Bien qu'il existe également des lois suisses contre ces cybercriminels, il faudrait être au courant de ces attaques qui ne sont malheureusement pas toujours rapportées, car les entreprises ne veulent pas que cela se sache, surtout vis-à-vis de leurs partenaires. Cependant la nouvelle Loi fédérale Suisse sur la protection des données qui devrait entrer en vigueur d'ici 2022 forcera ces entreprises à divulguer ce genre d'incident auprès de leurs clients et partenaires, sous peine d'amende.

Enfin, j'ai confectionné une plateforme web permettant à tout un chacun de mieux appréhender la complexité des cyber-dangers en fournissant une source complète d'informations relatives aux ransomwares sous une forme simple et accessible à tous. Le site s'articule principalement autour des axes de la « prévention », de la « protection » et de l'« action » possible face aux ransomwares donnant ainsi une aide et des conseils aux personnes atteintes par le malware ou tout simplement désireuses de s'en protéger.

12.2 Point de vue personnel

Tenant à vous exprimer mon ressenti sincère pour ce travail de bachelor, je dois vous avouer que cela n'a pas du tout été facile pour moi. La situation de confinement due à la pandémie du COVID-19 a énormément joué en ma défaveur au niveau personnel et a directement impacté mes capacités de travail et ma motivation.

A ajouter à cela, que ce soit pour la recherche du sujet ou pour son élaboration, j'ai eu à plusieurs reprises des grands moments de doutes et d'incertitudes. Etant entrée dans la filière HEG sans aucun attrait pur aucune attirance particulière pour ce domaine ni de connaissances informatiques autres que celles apprises à l'ESIG « École Supérieure d'Informatique de Gestion », passerelle obligatoire pour mon admission à la HEG, cela a été très difficile de me projeter dans un travail de bachelor.

En discutant avec mon conseiller au travail de Bachelor Mr. Billard, j'ai partagé ma curiosité pour tout ce qui touche à la cybersécurité et j'ai ainsi accepté sa proposition de

porter mon travail sur le sujet des « ransomwares ». Un sujet très intéressant et qui est très présent de nos jours. Ma curiosité sur le domaine des cyberattaques s'explique par un fait personnel que je souhaite maintenant vous détailler.

En effet, je ne connaissais pas grand-chose à l'informatique, à l'exception des jeux vidéo sur PC, ce que je n'associe pas au fait d'être douée en informatique. Cependant, j'ai appris assez vite durant mon adolescence les dégâts que des virus pouvaient engendrer et j'ai surtout déjà vécu un cas de phishing qui, à l'époque, m'avait traumatisée. Je devais avoir 13 ans lorsque j'ai appris à mes dépends ce qu'était le phishing.

J'étais complétement conquise par un jeu en ligne gratuit qui offrait d'acheter des bonus en jeux. Ayant toujours refusé jusque-là de dépenser de l'argent réel pour ce genre de services, j'avais décidé que pour mon anniversaire je pouvais faire une exception tellement j'affectionnais ce divertissement. J'ai donc versé 20 CHF de mon argent de poche qui ont été ensuite convertis dans une monnaie virtuelle associé au jeu.

Le jeu proposait une fenêtre où défilaient régulièrement des messages. Naïvement, croyant que ces messages provenaient des créateurs du jeu et non de n'importe quel utilisateur, j'ai un jour cliqué sur un lien proposé par un de ces messages qui défilait. Message qui offrait d'obtenir une grande quantité de cette monnaie virtuelle à utiliser en jeu « gratuitement ». Oui, j'y ai cru.

Ce lien m'a redirigé sur ce qui, à première vue, ressemblait au site web principal auquel il était possible de se connecter avec son compte de jeu. Je suis entrée, ou devrais-je dire, j'ai donné mon identifiant et mon mot de passe au cybercriminel. En appuyant sur « l'envoi » j'ai remarqué que rien ne se passait, même en actualisant la page à de multiples reprises. J'ai cependant pu constater avec effroi sur la fenêtre de mon jeu, resté ouverte en fond d'écran sur mon ordinateur, que toute la monnaie virtuelle que j'avais acquise en dépensant mon argent la veille « disparaissait » assez rapidement jusqu'à ce qu'il n'en restât plus une trace.

Par ce simple incident j'ai compris que j'avais commis plus d'un geste d'insécurité. Tout d'abord, j'avais cliqué sur un lien dont je ne connaissais pas la provenance, ce lien ne devait sûrement pas être un lien « https ». Ensuite ce lien proposait une offre absurde. Néanmoins j'ai quand même entré mes identifiants de login sur une fausse page web qui avait l'apparence d'une vraie page web.

Même si ce n'était que de l'argent dépensé dans un jeu, pour une modique somme de 20 CHF et bien que cela m'a réellement dégoutée sur le moment, cela m'a également permis de prendre conscience de l'existence de ce genre de techniques malhonnêtes.

À la suite de cet événement malheureux, je n'ai plus jamais cliqué sur un lien sans être certaine qu'il ne contienne aucun danger. En y repensant, je suis reconnaissante que cela soit arrivé dans ces circonstances car cela a extrêmement forgé ma méfiance des cyberattaques et m'a appris à être très attentive à ce genre de détails.

J'ai choisi également de vous raconter cet événement précis car il démontre à quel point il est très facile de berner quelqu'un en faisant de l'ingénierie sociale et que, pour ma part, si je n'avais jamais été victime de phishing, je n'aurais jamais appris à m'en méfier.

C'est pourquoi, pour revenir au sujet des ransomware, je suis convaincue que le problème majeur concernant ces attaques de ransomware est le manque de connaissances des personnes sur ce sujet. Il existe une multitude de petites précautions et des pratiques simples à appliquer, mais trop peu de personnes ne les applique et ce parce que trop souvent elles ne sont pas au courant du danger auquel elles s'exposent.

Et je pense que, tout comme moi, beaucoup ne commencent à en prendre conscience qu'après avoir subi les dégâts d'une attaque. Dans mon cas ma perte financière ne s'élevait qu'à 20 CHF, alors que les ransomwares demanderont facilement 200'000 CHF. De plus, je n'ai pas perdu de données personnelles contenues sur mon PC, ces dernières n'étaient pas visées, alors que généralement ce sont la cible privilégiée des ransomwares qui en volent le plus possibles tout en tentant de rendre leur récupération impossible sans leur aide.

12.3 Proposition d'amélioration

En conclusion, je souhaiterais parler des diverses améliorations qui peuvent être apportées à mon travail écrit et à celui en ligne.

En ce qui concerne la partie écrite, je pense que l'ajout de questionnaires effectuées auprès d'entreprises apporteraient un plus. Portant sur leurs connaissances et gestion des problèmes de type ransomware ainsi que leurs habitudes d'utilisation de leur environnements informatiques, cela nous donnerait un exemple concret autre que les divers articles utilisés en références à mon travail.

Il faudrait donner et expliciter peut-être plus d'exemple de ransomwares. L'ajout de graphiques aux niveaux des statistiques rendraient la compréhension visuelle des données plus efficace. De même, l'explication détaillée du fonctionnement d'un ordinateur, des anti-virus et des pares-feux expliqueraient de quelle manière le ransomware réussit à s'infiltrer dans les machines puis à en crypter les données.

Concernant la plateforme web « sos-ransomware », j'ai pensé à quelques ajouts. La première étant d'ajouter une vidéo explicative concernant le ransomware afin d'en donner une description simple, visuelle et auditive aux utilisateurs du site. Une autre donnée visuelle qui ne serait pas négligeable serait l'ajout d'un graphique ou de statiques mis à jour en temps réel des attaques ransomwares ou le nombre de failles recensées dans le monde ou en suisse.

Pourquoi pas ajouter également une page réservée aux visiteurs qui leur permettrait de les laisser partager leur expérience vis-à-vis d'une attaque de ransomwares. L'idée étant, de recenser des témoignages sur le sujet donnant encore plus conscience aux visiteurs du site, qui n'ont encore jamais été victime d'une attaque, du danger que cela représente. Les questions du second quizz pourraient être plus nombreuses pour creuser encore plus le sujet. Enfin rendre le site multilingue, en ajoutant au minimum l'anglais et peut-être aussi nos langues nationales seraient un plus permettant d'aider un plus large public.

Bibliographie

ACADEMYBINANCE, 2021, Qu'est-ce qu'un Ransomware ? *Binance - academy*. [en ligne]. Mai 2021. [Consulté le 12 janvier 2021]. Disponible à l'adresse: https://academy.binance.com/fr/articles/ransomware-explained

ACRONIS, non daté, Understanding the true, hidden costs of ransomware attacks on the business, *Acronis*. [en ligne]. Non daté. [Consulté le 2 mars 2021]. Disponible à l'adresse: https://www.acronis.com/en-us/articles/costs-of-ransomware-attacks/

ALTOSPAM, non daté, Ransomware ou rançongiciel, vos données prises en otage, *Alto spam,* Non daté. [Consulté le 30.11.2020]. Disponible à l'adresse : https://www.altospam.com/glossaire/ransomware.php

AROBASE, 2018, Afficher et déchiffrer le code source d'un e-mail, *arobase : le guide de l'e-mail*. [en ligne]. 25 septembre 2018. [Consulté le 13 janvier 2021]. Disponible à l'adresse : https://www.arobase.org/bases/source.htm

AULD, Andy non daté, What's behind the increase in ransomware attacks this year?, *pwc : uk*. [en ligne]. Non daté. [Consulté le 8 mars 2021]. Disponible à l'adresse : https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

BOHIC, Clément, 2020, Ransomware : Bouygues tancé par les créateurs de Maze, *Silicon*. [en ligne]. 9 avril 2020. [Consulté le 27 janvier 2021]. Disponible à l'adresse : https://www.silicon.fr/ransomware-bouygues-maze-337856.html

BRIDEWELL CONSULTING, 2016, Crypto Ransomware, *The Bridewell of Knowledge*. [en ligne]. 9 décembre 2016. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://www.bridewellconsulting.com/crypto-ransomware

BURNEL, Florian, 2020, Sauvegarde : qu'est-ce que la règle du 3-2-1 ? *IT-connect*. [en ligne]. 20 octobre 2020. [Consulté le 13 janvier 2021]. Disponible à l'adresse : https://www.it-connect.fr/sauvegarde-quest-ce-que-la-regle-du-3-2-1/

CBC NEWS, 2020, Une compagnie d'assurance canadienne a payé une rançon de 950 000 $ US à des pirates, *Radio-canada*. [en ligne]. 30 janvier 2020. [Consulté le 29 mars 2021]. Disponible à l'adresse : https://ici.radio-canada.ca/nouvelle/1499133/une-compagnie-dassurance-canadienne-a-paye-une-rancon-de-950-000-us-a-des-pirates

COBLE, Sarah, 2020, Maze Relaunches “name and Shame” Website, *info security : strategy : insight : technology*. [en ligne]. 10 janvier 2020. [Consulté le 8 mars 2021]. Disponible à l'adresse : https://www.infosecurity-magazine.com/news/maze-relaunches-name-and-shame/

COMODO CYBERSECURITY, non daté, RANSOMWARE VIRUS, C*omodo Cybersecurity*. [en ligne]. Non daté. [Consulté le 30.03.2021]. Disponible à l'adresse : https://enterprise.comodo.com/forensic-analysis/how-to-remove-ransomware-virus.php#

CONFEDERATION SUISSE, 2020, Code pénal suisse, *Fedlex : La plateforme de publication du droit fédéral*. [en ligne]. 1 juillet 2020. [Consulté le 25 03.2021]. Disponible à l'adresse : https://www.fedlex.admin.ch/eli/cc/54/757_781_799/fr#a143

COOK, Sam, 2021, 2018-2021 Ransomware statistics and facts, *comparitech*. [en ligne]. 12 février 2021. [Consulté le 9 février 2021]. Disponible à l'adresse : https://www.comparitech.com/antivirus/ransomware-statistics/

DELUZARCHE, Céline, Non daté. Cyberattaque : qu'est-ce que c'est ? *Futura Tech* [en ligne]. Non daté. [Consulté le 30 novembre 2020]. Disponible à l’adresse : https://www.futura-sciences.com/tech/definitions/piratage-cyberattaque-18946/

DOCTOROW, Cory, 2012, Cracking passwords with 25 GPUs, *boingboing*. [en ligne]. 5 décembre 2012. [Consulté le 4 mai 2021]. Disponible à l'adresse : https://boingboing.net/2012/12/05/cracking-passwords-with-25-gpu.html

DRUVA, non daté, 6 key steps: what to do after a ransomware attack, *druva*. [en ligne]. Non daté. [Consulté le 25 janvier 2021]. Disponible à l'adresse : https://content.druva.com/all/ts-6-steps-what-to-do

D.SCOTT, Christopher, 2021, School’s Out for Ransomware, *Security Intelligence*. [en ligne]. 4 février 2021. [Consulté le 22 mars 2021]. Disponible à l'adresse : https://securityintelligence.com/posts/defend-against-ransomware-in-schools/

EL-JILALI, Oussama, 2020, The Link Between Customer Loyalty and Ransomware Attacks, *TotalRetail: The Retailer’s Source for Content & Community*. [en ligne]. 13 Juillet 2020. [Consulté le 10 mars 2021]. Disponible à l'adresse : https://www.mytotalretail.com/article/the-link-between-customer-loyalty-and-ransomware-attacks/

ENCRYPTION NEWS, 2020, HOW DOES THE MAZE RANSOMWARE WORK? *galaxy: Data protection for Enterprise*. [en ligne]. 13 juin 2020. [Consulté le 6 janvier 2021]. Disponible à l'adresse : https://www.galaxkey.com/blog/how-does-the-maze-ransomware-work/

FAWKES, Guy, non date, Histoire de la menace ransomware : passé, présent et futur, *vpn Mentor.* [en ligne]. Non daté. [Consulté le 17 décembre 2020]. Disponible à l'adresse : https://fr.vpnmentor.com/blog/histoire-de-la-menace-ransomware-passe-present-et-futur/

F-SECURE, non daté, Crypto-Ransomware, *F-Secure*. [en ligne]. Non daté. [Consulté le 31 mars 2021]. Disponible à l'adresse : https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml

GALLAGHER, Ryan, 2014, HE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO, *The Intercept_*. [en ligne]. 13 décembre 2014. [Consulté le 2 mars 2021]. Disponible à l'adresse :

https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story

GOUD, Naveen, non daté, Texas Police Department loses 1TB critical CCTV data due to Ransomware, *Cybersecurity : Insiders*. [en ligne]. Non daté. [Consulté le 22 mars 2021]. Disponible à l'adresse :

https://www.cybersecurity-insiders.com/texas-police-department-loses-1tb-critical-cctv-data-due-to-ransomware

GRAHAM, Luke, 2017, Ransomware can cost firms over $700,000; cloud computing may provide the protection they need, *CNBC*. [en ligne]. 4 août 2017. [Consulté le 2 mars 2021]. Disponible à l'adresse :

https://www.cnbc.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html

HAUK, Chris, 2020, Ransomware Statistics, Facts & Figures For 2021, *pixel privacy*. [en ligne]. 12 mai 2020. [Consulté le 9 février 2021]. Disponible à l'adresse :

https://pixelprivacy.com/resources/ransomware-statistics

HOWELL O'NEILL, Patrick, 2020, Ransomware did not kill a German hospital patient, *MIT Technology Review*. [en ligne]. 12 novembre 2020. [Consulté le 9 mars 2021]. Disponible à l'adresse :

https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/

HTTPC, non daté, Tout savoir sur les Ransomwares (rançongiciels), *HTTPCS by Ziwit*. [en ligne]. Non daté. [Consulté le 13 janvier 2021]. Disponible à l'adresse :

https://www.httpcs.com/fr/ransomware-rancongiciel

HUMANOID XP, 2019, Comment les hackeurs volent-ils les mots de passe ?, *numerama*. [en ligne]. 7 juin 2019. [Consulté le 21 décembre 2020]. Disponible à l'adresse :

https://www.numerama.com/tech/511984-comment-les-hackeurs-volent-ils-les-mots-de-passe.html

IACONO, Laurie, WOJCIESZEK, Keith, 2020, The year in ransomware: Key targets, extortion tactics, and what to do, *Security*. [en ligne]. 25 novembre 2020. [Consulté le 9 mars 2021]. Disponible à l'adresse : https://www.securitymagazine.com/blogs/14-security-blog/post/93936-the-year-in-ransomware-key-targets-extortion-tactics-and-what-to-do

INFOMANIAK, non daté, Infomaniak Student : hébergement web et mail gratuit pour les étudiant(e)s, *Infomaniak*. [en ligne]. Non daté. [Consulté le 4 mai 2021]. Disponible à l'adresse : https://www.infomaniak.com/fr/support/faq/2229/infomaniak-student-hebergement-web-et-mail-gratuit-pour-les-etudiantes

JOHNSON, Joseph, 2021, Annual number of ransomware attacks worldwide from 2014 to 2020, *Statista*. [en ligne]. 13 avril 2021. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

KASPERSKY, 2016, The Cost of Cryptomalware: SMBs at Gunpoint, *Kaspersky daily*. [en ligne]. 7 septembre 2016. [Consulté le 30.03.2021]. Disponible à l'adresse : https://www.kaspersky.com/blog/cryptomalware-report-2016/5971/

KASPERSKY, 2020, Reconnaître les ransomwares : quelles sont les différences entre les chevaux de Troie de chiffrement ? *Kaspersky*. [en ligne]. 28 avril 2020. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://www.kaspersky.fr/resource-center/threats/ransomware-attacks-and-types

KASPERSKY, 2020, What Is a Drive by Download, *Kaspersky*. [en ligne]. 28 avril 2020. [Consulté le 22 décembre 2020]. Disponible à l'adresse : https://www.kaspersky.com/resource-center/definitions/drive-by-download

KASPERSKY, 2021, Over half of ransomware victims pay the ransom, but only a quarter see their full data returned, *Kaspersky*. [en ligne]. 30 mars 2021. [Consulté le 31 mars 2021]. Disponible à l'adresse : https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

KASPERSKY, non daté, Ransomware Attacks and Types – How Encryption Trojans Differ, *Kaspersky*. [en ligne]. Non daté. [Consulté le 3 mars 2021]. Disponible à l'adresse :
https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

KASPERSKY, non daté, What Is a Drive by Download, *Kaspersky*. [en ligne]. Non daté. [Consulté le 13 janvier 2021]. Disponible à l'adresse : https://www.kaspersky.com/resource-center/definitions/drive-by-download

KEMP, Simon, 2020, DIGITAL 2020: 3.8 BILLION PEOPLE USE SOCIAL MEDIA, *we are social*. [en ligne]. 30 janvier 2020. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

KOCHOVSKI. Aleksandar, 2020, Ransomware Statistics, Trends and Facts for 2020 and Beyond, *Cloudwards*. [en ligne]. 11 novembre 20020. [Consulté le 27 janvier 2021]. Disponible à l'adresse : https://www.cloudwards.net/ransomware-statistics/#Sources

KROLL, 2021, Welcome To The New Kroll, *Kroll*. [en ligne]. Mars 2018. [Consulté le 9 mars 2021]. Disponible à l'adresse : https://www.kroll.com/en/about-us

LAGARE, SARA, 2021, Complimentary access to Unity Learn Premium and live coding classes [message électronique]. 3 février 2021.

LAGARE, SARA, 2021, *sos-ransomware*. [en ligne]. [Consulté le 4 mai 2021]. Disponible à l'adresse :

https://sos-ransomware.site/

LAROUSSE, 2021, *Larousse.* [en ligne]. 22 février 2021. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/t%C3%A9l%C3%A9travail/77159

LATTO, Nica, 2020, Qu'est-ce que WannaCry ?, *avast*. [en ligne]. 27 février 2020. [Consulté le 3 mars 2021]. Disponible à l'adresse : https://www.avast.com/fr-fr/c-wannacry

LEPINE, Bastien, 2017, Windows 10 est désormais installé sur 500 millions de PC, consoles et smartphones, *Phoneandroid*. [en ligne]. 10 mai 2017. [Consulté le 28 avril 2021]. Disponible à l'adresse : https://www.phonandroid.com/windows-10-desormais-installe-500-millions-pc-consoles-smartphones.html

LEROY, Philippe, 2020, Ransomware : les 3 infos sur l'attaque contre Bouygues Construction, *Silicon*. [en ligne]. 1 février 2020. [Consulté le 27 janvier 2021]. Disponible à l'adresse : https://www.silicon.fr/ransomware-3-infos-sur-attaque-bouygues-construction-333632.html

LESSING, Marlese, 2020, Case Study: AIDS Trojan Ransomware, *sdx central.* [en ligne]. 3 juin 2020. [Consulté le 17 décembre 2020]. Disponible à l'adresse : https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/

L'EXPRESS, non daté, Cyberattaque mondiale "WannaCry", le ransomware qui chiffre les données, *L'express*. [en ligne]. Non daté. [Consulté le 3 mars 2021]. Disponible à l'adresse : : https://www.lexpress.fr/actualite/monde/vague-internationale-de-cyberattaques_1907798.html

LI, Cathy, LALANI, Farah, 2020, The COVID-19 pandemic has changed education forever. This is how, *World economic forum*. [en ligne]. 29 avril 2020. [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

LORD, Nate, 2020, THE COST OF A MALWARE INFECTION? FOR MAERSK, $300 MILLION, *Digital Guardian*. [en ligne]. 7 août 2020. [Consulté le 30 mars 2020]. Disponible à l'adresse : https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million

LYNGAAS, Sean, 2020, Hartford Public Schools delay reopening amid ransomware attack, *cyberscoop*. [en ligne]. 8 septembre 2020. [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.cyberscoop.com/hartford-ransomware-attack-mayor-bronin-fbi/

MANENS, François, 2020, Rançongiciel (ransomware) : comment font les hackers, comment vous protéger, C*yberguerre*. [en ligne]. 29 juin 2020. [Consulté le 18 novembre 2020]. Disponible à l'adresse : https://cyberguerre.numerama.com/5873-rancongiciel-ransomware-comment-font-les-hackers-comment-vous-proteger.html

METEREAU, Caroline, non daté, RANSOMWARES : COMMENT ÇA MARCHE ?, *Compufirst*. [en ligne]. Non daté. [Consulté le 22 décembre 2020]. Disponible à l'adresse : https://www.compufirst.com/compufirst-lab/logiciels/ransomwares-comment-ca-marche/main.do?appTreeId=42807

MICROSOFT, 2016, Server Message Block Overview, *Microsoft*. [en ligne]. 31 août 2016. [Consulté le 10 février 2021]. Disponible à l'adresse : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831795(v=ws.11)

MUHTADI, Adib Fakhri, ALMAARI, Ahmad, 2020. Analysis of Malware Impact on Network Traffic using Behavior-based Detection Technique. International Journal of Advances in Data and Information Systems. 1 avril 2020. Vol. 1, No. 1, pages 23-24.

ISSN: 2721-3056, DOI: 10.25008/ijadis.v1i1.14
https://media.neliti.com/media/publications/300813-analysis-of-malware-impact-on-network-tr-85601df9.pdf

MUNDO, Alexandre, 2020, Ransomware Maze, *McAfee*. [en ligne]. 26 mars 2020. [Consulté le 3 mars 2021]. Disponible à l'adresse : https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

NAIC, 2020, RANSOMWARE, *Naic*. [en ligne]. 23 juin 2020. [Consulté le 29 mars 2021]. Disponible à l'adresse : https://content.naic.org/cipr_topics/topic_ransomware.htm

OWANO, Nancy, 2012, Password-cracking feats at blistering speed shown in Oslo, *Physorg*. [en ligne]. 11 décembre 2012. [Consulté le 4 mai 2021]. Disponible à l'adresse : https://phys.org/news/2012-12-password-cracking-feats-blistering-shown-oslo.html

PAESSLER, non daté, Qu'est-ce qu'Active Directory ?, *Paessler the monitoring experts*. [en ligne]. Non daté. [Consulté le 10 février 2021]. Disponible à l'adresse : https://www.fr.paessler.com/it-explained/active-directory

PANDA, 2020, 73% des PME décident de payer après une attaque par rançongiciel, *panda : a WatchGuard brand*. [en ligne]. 30 Juin 2020. [Consulté le 4 février 2021]. Disponible à l'adresse : https://www.pandasecurity.com/fr/mediacenter/business/attaque-par-rancongiciel/

PANOPTINET 2011, C'est quoi un Drive-by Download ?, *panopti net*. [en ligne]. 10 novembre 2011. [Consulté le 12 janvier 2021]. Disponible à l'adresse : https://www.panoptinet.com/cybersecurite-decryptee/cest-quoi-un-drive-by-download.html

PARRY, Tony, 2020, 9 Ways Ransomware Attacks Impact Your Bottom Line, *arcserve*. [en ligne]. 20 octobre 2020. [Consulté le 10.03.2021]. Disponible à l'adresse : https://info.arcserve.com/blog/9-ways-ransomware-attacks-impact-your-bottom-line

POUPARD, Guillaume, PIGNON, Catherine, 2020, *Agence Nationale De La Sécurité Des Systèmes D'information*. [en ligne]. Août 2020 [Consulté le 4 février 2021]. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

Operation Socialist, *Wikipédia : l'encyclopédie libre*. [en ligne]. Dernière modification de la page le 19 mars 2020 à 19:42. [Consulté le 2 mars 2021]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Operation_Socialist

ONTRACK FRANCE, 2016, Le blog Ontrack de la récupération de données, *Ontrack*. [en ligne]. 14 juin 2016. [Consulté le 18 décembre 2020]. Disponible à l'adresse : https://www.ontrack.com/fr-fr/blog/locky-cryptolocker-autres-ransomwares-devez-savoir

REDLEGG, 2020, 7 TYPES OF CYBER THREAT ACTORS AND THEIR DAMAGE, *Redlegg*. [en ligne]. 2 avril 2020. [Consulté le 31 mars 2021]. Disponible à l'adresse : https://www.redlegg.com/blog/cyber-threat-actor-types

ROBIN, Émilia, MADORE, David, NGUYEN, Marie-Lan, 2005, Brève histoire d'Internet. *Tuteurs* [en ligne]. 20 juin 2005. [Consulté le 27 novembre 2020]. Disponible à l'adresse : https://www.tuteurs.ens.fr/internet/histoire.html#s3

SECURITY, 2020, First ransomware-related death reported in Germany, *Security*. [en ligne]. 21 septembre 2020. [Consulté le 9 mars 2021]. Disponible à l'adresse : https://www.securitymagazine.com/articles/93409-first-ransomware-related-death-reported-in-germany

Server Message Block. *Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page le 29 mars 2021 à 11:20. [Consulté le 10 février 2021]. Disponible à l'adresse : https://en.wikipedia.org/wiki/Server_Message_Block

SHANHONG, Liu, 2021, Monthly market share held by Windows operating system for desktop PCs worldwide from January 2017 to March 2021, by version, *statista*. [en ligne]. 15 avril 2021. [Consulté le 28 avril 2021]. Disponible à l'adresse : https://www.statista.com/statistics/993868/worldwide-windows-operating-system-market-share/

SINGH, Amrit, 2021, Ransomware: How to Prevent or Recover From an Attack, *Backblaze*. [en ligne]. 27 avril 2021. [Consulté le 26 janvier 2021]. Disponible à l'adresse : https://www.backblaze.com/blog/complete-guide-ransomware/

SISA, 2020, MAZE.RANSOMWARE NEW DESTRUCTIVE MALWARE STRAIN, *Sisa*. [en ligne]. Mai 2020. [Consulté le 3 mars 2021]. Disponible à l'adresse : https://www.sisainfosec.com/downloads/advisory/maze-ransomware.pdf

SIWICKI, BILL, 2016, Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money, *Healthcare IT News*. [en ligne]. 23 mai 20016. [Consulté le 03.02.2021]. Disponible à l'adresse : https://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

SKPPSC, non daté, Piratage + logiciels malveillants, *Skppsc : Prévention Suisse de la Criminalité*. [en ligne]. Non daté. [Consulté le 25 mars 2021]. Disponible à l'adresse : https://www.skppsc.ch/fr/sujets/internet/piratage-logicielsmalveillants/

SOPHOS, 2020, Maze ransomware: extorting victims for 1 year and counting, *Sophos*. [en ligne]. 12 mai 2020. [Consulté le 3 mars 2021]. Disponible à l'adresse : https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

SOPHOS, non daté, ÉTAT DES RANSOMWARES 2020, *Sophos*. [en ligne]. Non daté. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://news.sophos.com/wp-content/uploads/2020/06/sophos-the-state-of-ransomware-2020-wpfr.pdf

SPIEGEL, 2013, GCHQ Used Fake LinkedIn Pages to Target Engineers,*SPIEGEL International*. [en ligne]. 11 novembre 2013. [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html

SWISS BANKING, 2020, La nouvelle loi sur la protection des données, *Swiss banking*. [en ligne]. 10 décembre 2020. [Consulté le 29 mars 2021]. Disponible à l'adresse : https://www.swissbanking.ch/fr/actualites-et-positions/actualites/la-nouvelle-loi-sur-la-protection-des-donnees

TCHEEKO, Blériot, 2016, Crypto-monnaies : avènement d'une monnaie digitale ?, *Digital Corner.* [en ligne]. 2016. [Consulté le 27 avril 2021]. Disponible à l'adresse : https://www.digitalcorner-wavestone.com/2016/12/crypto-monnaies-avenement-dune-monnaie-digitale/

TECHLIB, non daté, Reimage, *TechLib*. [en ligne]. Non daté. [Consulté le 26.01.2021]. Disponible à l'adresse : https://techlib.fr/definition/reimage.html

TRAYNOR, Joshua, et al., non daté,The Malware Threat to Law Enforcement, *Police Chief*. [en ligne]. Non daté. [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.policechiefmagazine.org/the-malware-threat-to-law-enforcement/

UNTERSINGER, Martin, 2020, Rançons exorbitantes, attaques ciblées : 2019, année « faste » pour le rançongiciel, Le Monde. [en ligne]. 31 janvier 2020. [Consulté le 4 février 2021]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2020/01/31/rancons-exorbitantes-attaques-ciblees-2019-annee-faste-pour-le-rancongiciel_6027913_4408996.html

VERRIER, François, 2020, Comment identifier le ransomware qui bloque mes données ? *clubic*. [en ligne]. 2 décembre 2020. [Consulté le 26.01.2021]. Disponible à l'adresse : https://www.clubic.com/antivirus-securite-informatique/logiciel-antivirus/article-891767-1-comment-identifier-ransomware-bloque-mes-donnees.html

WannaCry. *Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page le 5 avril 2021 à 10:48. [Consulté 3 mars 2021]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/WannaCry

WORLDOMETERS, non daté, POPULATION MONDIALE, *Worldometer.* [en ligne]. Non daté. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https://www.worldometers.info/fr/

ZINAR, Yaron, 2020, Maze Ransomware Analysis and Protection, *Crowdstrike*. [en ligne]. 14 décembre 2020. [Consulté le 10 février 2021]. Disponible à l'adresse : https://www.crowdstrike.com/blog/maze-ransomware-analysis-and-protection/