LES RANSOMWARES

03 AVRIL 2019

DOMINIQUE BRETON
CESI de Pau

Table des matières

1 Les ransomwares.

1.1 Définition.

Commençons par quelques définitions. Les ransomwares sont des logiciels malveillants de type malware conçus spécifiquement pour des gains financiers. Mais contrairement aux virus utilisés pour le hacking, le ransomware n'est pas conçu pour obtenir accès à un ordinateur ou un système informatique afin d'y voler des données. Ils n'essaient pas non plus de persuader ses victimes d'envoyer de l'argent de leur plein gré comme certains scarewares qui envoient de faux messages antivirus. Ils prennent en otage votre ordinateur ou les données de celui-ci et affichent des messages demandant de verser une certaine somme d'argent ou rançon (souvent en bitcoin, ou précédemment en Paysafecard et Ukash) afin que votre système fonctionne à nouveau. Cette catégorie de programmes malveillants est une arnaque lucrative et criminelle qui peut être installée en cliquant sur des liens trompeurs dans un email, via les messageries instantanées, en téléchargeant et exécutant une pièce jointe ou en se rendant sur un site Internet infecté.

À ce jour, on peut classer les ransomwares en deux grands types : ceux qui bloquent les programmes ou votre ordinateur et ceux qui chiffrent les fichiers. Ils sont parfois appelés à tort « virus » ou à raison s'ils se dupliquent et se propagent d'eux-mêmes. Bien entendu, il existe une multitude de variations de ransomwares dans le monde, qu'il est impossible de tous les citer de manière exhaustive. Dans la plupart des cas, une fois qu'un ransomware est en place sur un système, le message de rançon est envoyé automatiquement. Il peut apparaître sous forme de boîte de dialogue sur l'écran d'un système bloqué, ou dans le cas d'une crypto-attaque, envoyé par e-mail ou par message instantané à la victime.

1.1.1 Avant 2017.

Il y a quatre de cela les cybercriminels envoyaient des mails à des millions d'adresses, diffusant des variantes de logiciels rançonneurs via des liens infectés ou des documents Word sans logique ou ciblage en espérant trouver

au moins un utilisateur qui aurait des fichiers importants dans son ordinateur, et qui ouvrirait la pièce jointe malveillante.

Aujourd'hui la situation a changé. Les listes aléatoires des spammeurs ont été de plus en plus remplacées par les adresses des employés d'une entreprise qui avaient été trouvées en ligne, et spécifiquement collectées. Les cybercriminels ont clairement compris qu'il était beaucoup plus rentable d'attaquer les entreprises. Par conséquent, le contenu des messages a changé. Au lieu de se faire passer pour une correspondance personnelle, les messages semblent désormais être envoyés par des collaborateurs, des clients, les services fiscaux, des administrations ou des établissements bancaires.

1.1.2 Après 2017.

La situation a changé en 2017. Deux campagnes à grande échelle ont affecté des millions de personnes et ont montré que le ransomware pouvait avoir différents objectifs autres que l'extorsion. Le premier est le tristement célèbre ransomware WannaCry qui fût un pionnier technologique. Ce ransomware a exploité une vulnérabilité dans l'implémentation du protocole SMB sous Windows. Il s'agissait d'une vulnérabilité qui avait déjà été patchée, mais de nombreuses entreprises n'avaient pas pris le temps d'installer le patch. Cependant, cela n'était qu'une partie du problème.

WannaCry n'a pas eu de succès comme ransomware. Même s'il a infecté des centaines de milliers d'appareils, WannaCry ne rapportait que de modestes bénéfices à ses créateurs. Certains chercheurs ont commencé à se demander si l'objectif final était l'argent, ou s'il s'agissait plutôt d'un sabotage ou de la destruction de données.

La menace suivante a effacé tous les doutes. ExPetr ne pouvait pas récupérer les données cryptées. Il utilisait l'exploit EternalBlue (développé par la NSA). Pour récupérer les informations d'identification afin de se propager, ce ransomware utilisait des outils de type Mimikatz qui lui permettait d'extraire les informations d'identification du processus lsass.exe. Les informations étaient transmises par la suite aux outils PsExec ou WMIC pour la distribution sur le réseau local. Le ransomware attendait entre 10 et 60 minutes après l'infection pour redémarrer le système. Une fois redémarrer, le ransomware commence à chiffrer la table MFT dans les partitions NTFS en écrasant le MBR avec un chargeur personnalisé avec une demande de rançon. Il liste toutes les cartes réseau, tous les noms de

serveur connus via NetBIOS et récupère la liste des baux DHCP. Le ransomware vérifie alors sur chaque machine trouvée sur le réseau local si les ports TCP 445 et 139 sont ouverts afin de se propager.

1.1.3 En 2018.

Les événements qui se sont déroulés cette année ont montré que les ransomwares continuent d'évoluer. Des experts ont récemment étudié une menace assez nouvelle : la dernière modification du ransomware SynAck. Ils ont découvert qu'il contenait des mécanismes complexes pour contrer les technologies de protection, notamment de duplication de processus qui essaie de faire passer le processus malveillant pour légitime et s'assurer qui n'est pas surveillé dans un environnement contrôlé ainsi que le nettoyage des registres d'événement pour retarder l'analyse postérieure à l'incident. Il n'y a donc aucune raison de croire que les ransomwares ont fini d'évoluer. Leurs créateurs vont continuer de chercher comment l'améliorer.

1.2 Les Lockers.

Les ransomwares bloqueurs utilisent notamment des fenêtres pop-up par-dessus les autres programmes (ou applications dans le cas des smartphones), les bloquant ainsi et empêchant l'utilisateur de continuer dans sa tâche. Ces ransomwares vous accusent habituellement d'avoir commis des infractions imaginaires comme le fait le virus de la gendarmerie.

Il existe plusieurs variantes de ce ransomware, qui se fait passer pour des administrations françaises, comme HADOPI, utilisant toujours le même système pour provoquer la peur chez l'utilisateur infecté et le forcer à régler la rançon demandée.

1.3 Les crypto-malware.

Ceux sont des ransomwares qui chiffrent une partie ou l'intégralité des fichiers d'un ordinateur. Ils sont plus problématiques car agissent discrètement, puis affichent un message vendant la clé de déchiffrement suivie d'un compteur de temps, qui une fois arrivé à zéro détruit cette clé de déchiffrement. Plus l'ordinateur est puissant plus le chiffrage des données est rapide. À savoir que la rançon demandée peut doubler à chaque remise à zéro du compteur de temps. D'un point de vue cryptographique on a deux grandes façons de chiffrer des données : la façon symétrique et la façon asymétrique. La façon symétrique consiste à utiliser le même mot de passe pour chiffrer et déchiffrer. Le problème c'est que pour pouvoir déchiffrer des données chiffrées avec une clé donnée, il faut justement cette clé. Et on n'a pas de façon sécurisée de partager cette clé. La façon asymétrique règle ce problème, une clé dite "publique" est partagée, elle permet uniquement de chiffrer des données**.** La clé privée n'est pas partagée

et permet de déchiffrer les données**.** Cette clé privée est donc gardée sur un serveur distant, il faudra donc payer pour l'obtenir.

1.4 Marché de la cyber criminalité.

Ces dernières années, des attaques de ransomware très médiatisées, comme WannaCry et NotPetya ont fait les gros titres au niveau mondial pour avoir infecté des milliers d'ordinateurs en chiffrant les fichiers qui restent ensuite « tenus en otage » jusqu'au paiement d'une rançon par la victime. En plus de rapporter des millions de dollars aux cybercriminels, ces attaques malveillantes nuisent aux entreprises et aux particuliers du monde entier.

Une nouvelle tendance a vu émerger des plateformes dites de ransomware as a service (RaaS) qui permettent à des cybercriminels expérimentés de vendre leurs services au plus grand nombre. Cela permet à des malfrats novices en programmation, de s'associer à des experts de la création de ransomware qui codent pour eux.

Disponible sur le dark web, Satan & Co est la toute dernière plateforme RaaS à fournir un accès à du ransomware de qualité aux aspirants cybercriminels. Il suffit simplement aux utilisateurs de créer un compte et de payer un abonnement pour télécharger des fichiers malveillants exécutables prêts à infecter les PC de leurs victimes. Ils peuvent même personnaliser leurs codes et demandes de rançons en utilisant des modèles qui sont fournis. En échange, Satan facture une commission de 30 % sur l'argent récupéré lors des rançons.

2 Historique des ransomwares.

2.1 Le premier ransomware.

Le premier incident mondial impliquant un ransomware remonte à 30ans. En 1989, un académicien d'Harvard participait à une conférence de la World Health Organization sur le Sida. Il créa 20 000 disquettes pour les différents participants, qu'il nomma "AIDS Information – Introductory Diskettes" (Informations sur le Sida – disquettes d'introduction).

Ce que les participants ne savaient pas, c'est que les disquettes contenaient un virus informatique, qui, une fois la disquette lancée, restait caché dans l'ordinateur de la victime pendant un certain temps. Après 90 redémarrages, le virus prenait vie, cryptant rapidement les fichiers, et cachant les répertoires. Un message s'affichait, informant l'utilisateur que son système ne serait restauré que s'il envoyait 189 $ dans une boîte postale au Panama.

2.2 2005 : l'an zéro.

Internet a grandement facilité la distribution de tous types de malwares, et les années écoulées depuis le premier ransomware ont permis aux programmeurs de développer des méthodes de cryptage beaucoup plus puissantes.

Un des premiers exemples de ransomware distribués en ligne, le **GPCoder Trojan** fut identifié pour la première fois en 2005, le **GPCoder** infectait des systèmes Windows en ciblant les dossiers contenant plusieurs extensions**.** Une fois trouvés, les fichiers étaient copiés en crypté et les fichiers originaux effacés du système. Les nouveaux fichiers cryptés étaient illisibles, et l'utilisation d'un cryptage RSA-1024 solide limitait grandement les taux de réussite des tentatives de déverrouillage. Un message s'affichait alors sur l'écran d'accueil de l'utilisateur, le redirigeant sur un fichier .txt sur leur bureau, qui contenait les instructions pour payer la rançon et débloquer les fichiers affectés.

La même année où **GPCoder** fut identifié, un autre cheval de Troie avec le même cryptage 1024-bit RSA a également fait son apparition. Au lieu de cibler des

fichiers exécutables et des extensions de fichiers, **Archievus** se contentait de tout crypter dans le dossier Mes documents de la victime**.** En théorie, cela signifie que la victime pouvait continuer à se servir de son ordinateur et de tout stocker dans d'autres dossier. Mais puisque la plupart des gens stockent leurs fichiers importants, y compris des documents professionnels, dans le dossier Mes documents par défaut, les effets restaient dévastateurs.

Pour se débarrasser **d'Archievus**, les victimes étaient dirigées vers un site web où elles devaient acheter un mot de passe à 30 chiffres.

2.3 2009 – 2012 : l'heure de la paye.

Il a fallu un moment avant que ces formes précoces de ransomware en ligne s'imposent dans le monde de la cyber criminalité. La rentabilité des trojans comme **GPCoder** et **Archievus** restait plutôt basse, car facilement repérables et supprimables par les antivirus.

À l'époque, les hackers préféraient en rester au hacking, au phishing, et à tromper les gens avec des arnaques à l'antivirus.

Les premiers changements sont apparus en 2009. Cette année-là, un virus de type scareware appelé **Vundo** a changé de tactique et a commencé à fonctionner comme un ransomware. Auparavant, **Vundo** infectait les ordinateurs et déclenchait sa propre alerte de sécurité, guidant les utilisateurs vers une fausse solution. Toutefois, en 2009, des analystes ont remarqué que **Vundo** avait commencé à crypter les fichiers se trouvant sur l'ordinateur des victimes, et à vendre une solution efficace pour les déverrouiller.

C'était la première indication que les hackers commençaient à se dire qu'il y avait de l'argent à se faire avec les ransomware. Grâce à la prolifération des plateformes de paiement en ligne anonymes, il devenait également beaucoup plus simple de recevoir des rançons à grande échelle et la sophistication du ransomware était de plus en plus poussée.

En 2011, au premier trimestre, environ 60 000 nouvelles attaques ransomware avaient été détectées. Au premier trimestre 2012, ce chiffre dépassait les 200 000. Fin 2012, des chercheurs de Symantec ont estimé que le marché noir du ransomware avait une valeur monétaire d'environ 5 millions de dollars.

En 2011, une nouvelle forme de ransomware est apparue. Le cheval de Troie **WinLock** est considéré comme le premier exemple répandu des ransomware « Locker » (verrou). Plutôt que de crypter les fichiers de l'appareil de la victime, un verrou rend la connexion à l'appareil tout simplement impossible.

WinLock a lancé un genre de tendance chez le ransomware, en imitant de vrais produits, un peu comme l'ancienne méthode scareware. En infectant des systèmes Windows, et copiant le système d'activation de produit de Windows, il bloquait les utilisateurs jusqu'à ce qu'ils achètent une clé d'activation. Pour ajouter une petite touche d'ironie à peine masquée, le message affiché sur le faux écran d'activation indiquait aux victimes que leur compte devait être réactivé en raison d'une fraude, avant de les diriger sur un numéro international pour résoudre le problème. Le numéro de téléphone était présenté comme gratuit, mais finissait par vous coûter de grosses sommes, qui allaient directement dans les poches des criminels à l'origine du malware.

Une des variations sur le thème de l'imitation de produits logiciels, pour tromper les victimes et leur faire payer de faux abonnement, s'appelle le ransomware « Police ». Dans ces attaques, le malware cible des systèmes infectés avec des messages prétendant provenir d'agences gouvernementales ou d'autorités policières**,** qui disent que des preuves ont été trouvées sur l'appareil, attestant d'activités illégales. L'appareil est ensuite verrouillé jusqu'à ce que l'amende soit payée.

Ces malwares étaient souvent distribués par des sites pornographiques, des services de partage de fichiers, ou toute autre plateforme qui peut potentiellement être utilisée dans des buts illégaux. L'idée était, sans aucun doute, de faire peur aux victimes ou de les embarrasser pour qu'ils payent l'amende avant d'avoir l'occasion de réfléchir à tête reposée sur l'authenticité de ces menaces.

Pour que ces attaques aient l'air plus authentiques et plus menaçantes, les ransomwares police étaient personnalisés selon l'emplacement des victimes, avec leur adresse IP ou même parfois des images de leurs propres webcams, pour leur montrer qu'ils étaient surveillés et enregistrés.

Un des exemples de ransomware police le plus connu portait le nom de **Reveton**. Répandu en Europe à l'origine, **Reveton** a gagné assez de terrain pour commencer à envahir les USA, où les victimes apprenaient être sous la surveillance du FBI et devaient payer une amende de 200 $ afin de débloquer leur appareil. Les règlements étaient traités par des services prépayés comme

MoneyPak ou Ukash. Cette tactique fut récupérée par d'autres ransomware comme **Urausy** et **Kovter**.

2.4 2013 – 2015 : retour au cryptage.

Durant la seconde moitié de 2013, une nouvelle forme de ransomware à cryptage a émergé, lançant une nouvelle étape dans la lutte pour la cyber sécurité. **CryptoLocker** a changé la donne des ransomwares, de plusieurs façons. Déjà, il ne se préoccupait pas d'avoir l'air officiel, comme les scarewares ou les ransomwares police. Les programmeurs de **CryptoLocker** étaient très clairs sur leurs intentions, et envoyaient un message très direct à leurs victimes, expliquant que tous leurs fichiers avaient été cryptés et seraient effacés si la rançon n'était pas payée dans les trois jours.

Ensuite, **CryptoLocker** a prouvé que la puissance du cryptage que les cybers criminels pouvaient désormais utiliser était largement supérieure que lors de l'émergence du premier cryptoware, presque une décennie plus tôt. En utilisant des serveurs C2 sur le réseau Tor, les programmeurs de **CryptoLocker** purent générer des clés de cryptage publiques et privées 2048-bit afin d'affecter les fichiers aux extensions spécifiées**.** Cela agissait comme une double contrainte ; les gens à la recherche de la clé publique pour tenter de décrypter les fichiers rencontraient d'énormes difficultés vu qu'elles étaient cachée sur le réseau Tor, tandis que la clé privée, aux mains des programmeurs, restait très solide en elle-même.

Ensuite, **CryptoLocker** a innové dans sa manière d'être distribué. L'infection s'est répandue par le botnet Game over Zeus , un réseau d'ordinateurs « zombie » infectés, utilisés spécialement pour répandre des malwares sur internet. **CryptoLocker**, était donc le premier exemple de ransomware à se répandre par des sites infectés**.** Toutefois, **CryptoLocker** s'est également répandu par phishing, surtout par un système de pièces jointes d'e-mails envoyées à des entreprises, conçues pour ressembler à une réclamation de clients.

Toutes ces caractéristiques sont depuis devenues des traits dominants des attaques de ransomware, influencées par le succès de **CryptoLocker**. Facturant 300 $ le décryptage de systèmes infectés, on estime que ses développeurs ont gagné environ 3 millions de dollars.

CryptoLocker s'est retrouvé au chômage technique en 2014 quand le botnet Game over Zeus fut retiré, mais il y avait déjà de nombreux prétendants prêts à reprendre le flambeau. **CryptoWall** fut le plus significatif, utilisant les mêmes clés de cryptage RSA publiques-privées que celles générées par l'écran du réseau Tor, et distribué par phishing.

Le réseau TOR a commencé à jouer un rôle de plus en plus important dans le développement et la distribution de ransomware. Tenant son nom de la façon dont il route le trafic internet à travers un réseau mondial et complexe de serveurs, arrangés comme les couches d'un oignon, Tor est un projet sur fond d'anonymat, conçu pour aider les gens à garder leur confidentialité sur le net. Malheureusement, il attire aussi les cybers criminels, ravis de pouvoir maintenir leurs activités en ligne loin du regard des autorités, et c'est ce qui a donné à Tor un rôle aussi grand dans l'histoire du ransomware.

CryptoWall a également confirmé le rôle grandissant du Bitcoin dans les attaques ransomware. En 2014, cette crypto-devise était devenue la méthode de paiement préférée. Les autres méthodes nécessitaient du blanchiment, alors que le Bitcoin pouvait être utilisé en ligne comme une devise classique, et utilisé directement pour des échanges et transactions.

En 2015, on estime que **CryptoWall** a rapporté plus de 325 millions de dollars**.**

Autre étape majeure dans l'histoire du ransomware, le développement de versions ciblant les appareils mobiles. Visant exclusivement les appareils Android au début **;** ce système se servait du code open source d'Android.

Les premiers exemples sont apparus en 2014 copiant le format policeware. **Sypeng**, qui infectait les appareils par un message de mise à jour Adobe Flash contrefait, bloquait l'écran et affichait un faux message du FBI demandant 200 $. **Koler**, un virus similaire, fut l'un des premiers exemples de ransomware ver, un malware qui s'auto-reproduit et crée ses propres chemins de distribution. **Koler** envoyait automatiquement un message à tous les contacts des appareils infectés, avec un lien de téléchargement vers le ver.

Malgré son nom, **SimplLocker** fait partie des premiers crypto-ransomware pour mobiles, tandis que la majorité des autres prenaient la forme d'attaques de type verrouillage. Autre innovation, apparue avec les ransomware pour Android, les boîtes à outils DIY que des cybers criminels en herbe pouvaient acheter en ligne et configurer eux-mêmes. Un des premiers exemples fut un kit basé sur le cheval de Troie **Pletor**, vendu en ligne pour 5000 $.

2.5 2016 : la menace évolue.

2016 fut une année décisive pour les ransomwares. De nouveaux modes de distribution, de nouvelles plateformes, et de nouveaux types de malware se sont ajoutés à une menace en constante évolution, mettant en place les attaques mondiales massives qui allaient suivre.

Contrairement à de nombreux ransomwares qui ont connu de beaux jours et qui ont été ensuite neutralisés d'une façon ou une autre, la menace **CryptoWall** est encore là. Évoluant à chacune de ses 4 sorties distinctes, **CryptoWall** a lancé des techniques que les autres ransomwares ont imité par la suite, comme l'utilisation de clés de registres dupliquées pour que le malware charge à chaque démarrage. C'est une bonne technique, parce que les malwares ne se lancent pas toujours de manière immédiate, attendant de pouvoir se connecter à un serveur à distance, contenant la clé de cryptage. Le chargement automatique lors du démarrage maximise les chances d'y parvenir.

Avec sa distribution agressive basée sur le phishing, **Locky** a créé un précédent, repris par **WannaCry** et malwares similaires, pour la vitesse et l'échelle de sa répartition. Au plus haut de l'infection, plus de 100 000 nouveaux systèmes étaient touchés tous les jours, grâce au système de franchise d'abord utilisé par les boîtes à outils Android, pour inciter de plus en plus de criminels à rejoindre son réseau de distribution. **Locky** a aussi été un signe annonciateur de **WannaCry** en ciblant les prestataires de soin, puisque les gens qui l'ont créé ont vite compris que les services publics essentiels étaient très rapides à payer les rançons, afin que leur système se remette en marche le plus vite possible.

2016 a aussi vu l'arrivée du premier script ransomware à affecter les systèmes Mac. **KeRanger** était particulièrement malveillant, parce qu'il parvenait à crypter les sauvegardes de Time Machine, aussi bien que les fichiers ordinaires, empêchant les utilisateurs de Mac à revenir à des versions précédentes.

Pas longtemps après **KeRanger**, le premier ransomware capable d'infecter de multiples systèmes d'exploitation est apparu. Programmé en JavaScript, **Ransom32** était en théorie capable d'affecter des appareils sous Windows, Mac, ou Linux.

Grace aux exploit kits qui sont des protocoles de distribution de malwares qui ciblent les vulnérabilités connues dans des systèmes logiciels populaires pour y

implanter des virus, les choses se sont accélérées en 2016, avec un grand nombre de ransomware de qualité, ciblant les vulnérabilités d'Adobe Flash et Microsoft Silverlight – comme par exemple **CryptoWall 4.0.**

Suivant les innovations du virus **Koler**, les cryptoworms sont devenus une tendance très populaire chez les ransomwares en 2016. L'un des meilleurs exemples est **ZCryptor**, initialement découvert par Microsoft. Distribué à la base par des attaques de type phishing, **ZCryptor** put ensuite se répandre automatiquement par des appareils branchés sur réseau, en s'auto-multipliant et en s'auto-exécutant.

2.6 De 2017 à 2018.

Vu la progression rapide de la sophistication et de l'échelle des attaques de ransomware en 2016, de nombreux spécialistes de la cybersécurité sont arrivés à la conclusion que ce n'était qu'une question de temps avant qu'une attaque d'ampleur mondiale n'ait lieu. **WannaCry** a confirmé ces peurs, et a fait les gros titres dans le monde entier. Mais **WannaCry** est loin d'être le seul ransomware à menacer les ordinateurs cette année.

Le 12 Mai 2017, le ransomware qui deviendrait connu comme **WannaCry** faisait ses premières victimes en Espagne. En seulement quelques heures, il s'était répandu sur des centaines d'ordinateurs, dans des douzaines de pays. Quelques jours plus tard, ce chiffre atteignait le quart de million, en faisant la plus grosse attaque de ransomware de l'histoire et s'assurant que tout le monde prête désormais attention à cette menace.

WannaCry est un raccourci de **WannaCrypt**, référence au fait que **WannaCry** est un cryptoware. Plus spécifiquement, il s'agit d'un cryptoworm, capable de se reproduire et de se répandre automatiquement.

Ce qui a rendu **WannaCry** aussi efficace, et aussi choquant aux yeux du public, c'est sa répartition. Pas d'arnaque phishing, pas de téléchargement depuis un site compromis. **WannaCry** a marqué une nouvelle phase chez le ransomware, en ciblant les vulnérabilités connues des ordinateurs**.** Programmé pour patrouiller le net à la recherche d'ordinateurs tournant sous de vieilles versions de Windows Server – qui possède une faille connue – et les infecter. Une fois qu'il a infecté un ordinateur du réseau, il en cherche rapidement d'autres ayant la même faille et les infecte eux aussi.

C'est de cette façon que **WannaCry** s'est répandu aussi rapidement, et c'est aussi ce qui explique sa capacité à attaquer les systèmes de grandes organisations, comme les banques, les transports en commun, les universités et les services de santé publique. C'est aussi pour ça qu'il a fait tant de gros titres.

Mais ce qui a le plus choqué les gens, c'est que la vulnérabilité que **WannaCry** a exploité dans Windows avait été identifiée par la National Security Agency (NSA) il y a des années. Mais au lieu de prévenir le monde entier, la NSA a gardé cette faille sous silence et a trouvé le moyen d'exploiter cette faiblesse, s'en servant comme une arme. **WannaCry** a été conçu sur un système développé par une agence de sécurité nationale.

Directement après **WannaCry**, une autre attaque a touché des milliers d'ordinateurs aux quatre coins du monde. Appelée **Petya**, la caractéristique la plus notable de cette attaque, c'est qu'elle a utilisé la même vulnérabilité de Windows que **WannaCry,** montrant la puissance potentielle de la cyber arme de la NSA. Cet évènement nous a aussi montré que malgré le patch rendu disponible après l'attaque **WannaCry** , il est très difficile de maintenir les utilisateurs à jour au niveau sécurité.

Signe de la constance de la menace du ransomware, ce fut l'une des plus grosses attaques à faire les gros titres et à nous renvoyer à l'époque des scarewares et du chantage, mais avec une touche de modernité. Prenant pour cible les appareils Android, **LeakerLocker** menaçait d'envoyer l'ensemble du contenu du téléphone de l'utilisateur à toute sa liste de contacts. Donc, si vous aviez quelque chose de compromettant ou d'embarrassant sur votre téléphone, vous aviez intérêt à payer, ou vos amis, collègues et proches auraient vu ce que vous aviez à cacher.

2.7 De nos jours.

Un mois après son entrée en vigueur, le 25 mai dernier, le Règlement général européen sur la protection des données (RGPD), qui impose aux entreprises et aux organisations de revoir toute leur architecture de collecte et de traitement des données personnelles de leur utilisateurs/clients, n'en finit pas d'engendrer son lot de troubles.

Comme le RGPD est un véritable changement qui nécessite d'effectuer des investissements parfois conséquents pour la mise en conformité, que moins d'un

tiers des entreprises le sont, et que les sanctions en cas de non-respect de la législation peuvent atteindre jusqu'à 4% du chiffre d'affaires mondial, il y avait donc un terrain béni pour les cybercriminels et les arnaqueurs. La Commission nationale informatique et libertés (CNIL) avait d'ailleurs déjà sonné l'alerte pendant les mois précédant l'entrée en vigueur, mais les arnaques ont redoublé d'intensité depuis. De nombreux experts en cybersécurité dénoncent également sur les nouvelles pratiques des cybercriminels pour tirer profit de la panique autour du RGPD.

Le RGPD a ainsi donné naissance à un nouveau type de ransomware : le **ransomhack**. La différence ? Alors que le ransomware bloque l'accès aux données de l'utilisateur en les chiffrant et demande le paiement d'une rançon pour les rendre lisibles à nouveau, le **ransomhack** ne prend même pas la peine d'avoir recours au chiffrement : une fois infiltré dans le système informatique de sa victime, le hacker exige simplement le paiement de la rançon sous peine de rendre publique la fuite de données sur Internet.

Avec le RGPD, les entreprises qui protègent insuffisamment les données personnelles de leurs clients sont passibles de sanctions qui peuvent atteindre jusqu'à 4% de leur chiffre d'affaires. D'après l'article 33 du RGPD, en cas de violation des données, les entreprises doivent en informer les autorités de contrôle (la Cnil) au plus tôt et au maximum 72 heures après en avoir pris connaissance, sous peine de subir des sanctions supplémentaires.

Les cybercriminels utilisant des ransomhack parient sur la peur des sanctions pour pousser les entreprises hackées à payer la rançon sans sourciller. Les rançons demandées s'élèvent entre 1.000 dollars et 20.000 dollars. Tant que les entreprises qui exploitent des données personnelles n'auront pas sécurisé l'ensemble de leurs systèmes d'exploitation - face à l'urgence et aux coûts engagés, elles définissent des priorités -, elles seront vulnérables à ce type d'attaques. Cela ne signifie pas pour autant qu'une société victime d'un ransomhack sera sanctionnée par la Cnil : le régulateur devra déterminer si l'entreprise avait bien pris les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque avant de subir l'attaque.

Autre fléau lié au RGPD : les escrocs qui jouent sur la peur des sanctions pour facturer une fausse mise en conformité. La Cnil a publié le 7 juin 2018 une mise en garde contre la recrudescence de cette pratique et a appelé entreprises et organisations à la plus grande vigilance.

Ainsi, certains escrocs envoient un faux formulaire intitulé "Déclaration normale RGPD", qui reproduit frauduleusement le logo de la Cnil. La victime doit remplir le fichier, le renvoyer, et payer pour la démarche.

Un autre cas de fraude est le fameux courrier, email ou fax de "dernier rappel", qui présente également un logo usurpé de la Cnil. Le message invite à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen.

3 Les ransomwares en entreprises : mesures préventives.

3.1 Les mesures standards.

Selon le dernier rapport annuel du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), 8 entreprises sur 10 continuent d'être touchées par des ransomwares.

Ces entreprises déclarent que le Phishing est le mode d'attaque le plus fréquent tandis que le Shadow IT est le mode d'attaque le plus fréquent.

Attaques complexes, attaques sans malware, attaques sans fichier et infection de malware par accès physique. Les exploits zero-day tirent profit des nouveaux outils et techniques de cybercriminalité qui sont extrêmement agiles. Dans le contexte actuel et instable de menaces, les technologies préventives seules ne peuvent pas protéger les entreprises des menaces avancées. Si vous y ajoutez le fait que les pirates informatiques peuvent organiser une attaque ciblée efficace à un coût minimum, il n'est pas surprenant de voir que le nombre d'attaques réussies ne cesse d'augmenter dans le monde. Une approche traditionnelle n'est désormais plus suffisante mais reste nécessaire. Les premières mesures à mettre en place sont les suivantes :

- **Mettre systématiquement en place des sauvegardes de données** qui limiteront considérablement l'impact d'une attaque de malware, car les données chiffrées pourront être restaurées sans avoir à payer de rançon. Les entreprises doivent régulièrement tester leur stratégie de sauvegarde et de reprise d'activité après sinistre pour garantir sa fiabilité. Il convient, pour être efficace d'effectuer au moins 3 sauvegardes dont une à l'extérieur de l'entreprise (cloud, datacenter, etc)

- **Appliquer rapidement les mises à jour du système, du réseau et des applications**. Les mises à jour logicielles ou système d'exploitation contiennent généralement des correctifs. Installation obligatoire dès qu'elles sont disponibles.

- **Sensibiliser à la cybersécurité** : formez les employés à la détection et à la gestion d'attaques d'ingénierie sociale et phishing, et les informer régulièrement des menaces de sécurité connues du moment.

- **Désactiver l'exécution automatique sur tous les appareils connectés** : cela empêchera les logiciels malveillants de se répandre en toute autonomie, et c'est une étape importante pour contenir un logiciel malveillant en cas d'infection.

- **Désactiver les macros dans les applications Microsoft Office** : dans de nombreux cas, le ransomware se diffuse via des documents Microsoft Office infectés qui contiennent des macros malveillantes qui téléchargent et exécutent un malware si on les lance. La désactivation par défaut des macros peut contribuer à empêcher cela, même si un utilisateur ouvre un fichier infecté.

- **Désactiver les connexions de bureau à distance autant que possible :** cela empêchera les agresseurs ou les logiciels malveillants d'accéder à distance aux appareils et aux fichiers d'un utilisateur.

- **Limiter l'utilisation des outils administrateur du système :** les privilèges administrateur et l'utilisation des comptes admin doivent être limités pour garantir qu'un utilisateur infecté n'accorde pas accidentellement des droits administrateurs à un criminel ayant obtenu accès à son compte.

- **Déployer des logiciels de sécurité :** il existe de nombreuses solutions qui peuvent contribuer à lutter contre les infections de ransomware. Les logiciels antivirus et les pares-feux, par exemple, peuvent aider à bloquer des variantes de logiciels malveillants connus ou répandus. Pour plus de protection, les entreprises doivent envisager des solutions EDR (détection et réaction aux menaces sur les terminaux) et ATP (protection contre les menaces avancées) qui optimisent la détection des malwares et bloquent l'exécution du code malveillant. Le déploiement de mécanismes de sécurité multicouches comme la catégorisation des données, la segmentation du réseau, le contrôle ou la liste blanche des applications et le suivi des comportements, permettra une stratégie de sécurité supérieure pour préserver les données de l'entreprise.

Le modèle RaaS est une tendance révolutionnaire qui rend le ransomware facile à utiliser, en ne nécessitant que peu, voire pas de compétences techniques pour le configurer, le personnaliser et l'exécuter. Cela signifie que les criminels peuvent rapidement changer de vecteurs d'attaque et s'adapter aux défenses de sécurité. Les entreprises et organismes doivent donc déployer une approche multicouche de la sécurité pour ne pas devenir victime d'un logiciel malveillant.

De nos jours, l'utilisation d'un simple anti-virus et/ou pare-feu n'est plus suffisante, notamment aux vues des données traitées et des enjeux stratégiques de l'entreprise.

Chaque appareil se connectant à un réseau constitue un vecteur d'attaque potentiel, et chacune de ces connexions est un point d'entrée potentiel vers vos données. Avec la montée en puissance du BYOD (Bring Your Own Devices – apportez vos appareils personnels), les attaques mobiles et des techniques sophistiquées de piratage n'ont fait qu'augmenter les risques de voir vos données piratées.

Les solutions d'EDR contribuent à protéger ces points d'entrée dans votre réseau en surveillant vos terminaux pour y détecter les nombreuses menaces modernes qu'ignorent les logiciels antivirus. Elles peuvent contribuer à assurer une surveillance et une protection contre les APT (Advanced Persistent Threats), qui utilisent souvent des techniques de piratage sans malware et des failles de sécurité pour accéder à un réseau. Les anciens logiciels antivirus ne peuvent détecter un malware que lorsqu'ils trouvent une signature correspondante. Ils sont incapables de surveiller les activités d'un pirate pour déterminer qu'il a accès à un ordinateur.

L'association de menaces courantes avec des modèles malveillants uniques, et des activités qui reposent sur des techniques d'infiltration complexes élaborées par les pirates informatiques, font que les menaces avancées et les attaques ciblées sont extrêmement dangereuses pour n'importe quelle organisation qui n'utilise qu'une approche conventionnelle en matière de cybersécurité.

Les vols et les attaques sont une menace constante pour les entreprises ; données et finances, propriété intellectuelle, données commerciales sensibles, données personnelles spécifiques ou autres données sensibles, ainsi que processus d'entreprise, avantage concurrentiel, et ainsi de suite.

Les incidents causés par les menaces avancées ont un impact important sur l'entreprise : le coût de réponse et de récupération, l'investissement dans de nouveaux systèmes et processus, l'effet sur la disponibilité, les dégâts engendrés en termes de réputation et de marque, les pertes financières, et ainsi de suite. Les organisations doivent non seulement prendre en compte le nombre croissant de programmes malveillants courants, mais aussi la croissance des attaques complexes avancées et des attaques ciblées.

Cela signifie que les entreprises doivent étendre leur protection au-delà du réseau, des e-mails et du trafic Internet aux points de terminaison, ce qui inclut les postes de travail, les ordinateurs portables, les serveurs et les smartphones. Ces points de terminaison sont généralement utilisés comme points d'entrée dans l'infrastructure de l'organisation pendant les attaques ciblées, rendant ainsi la visibilité des points de terminaison critique dans le contexte actuel de menaces.

Il est certain que le blocage des menaces simples sur les points de terminaison n'est pas suffisant. De nos jours, les entreprises ont besoin d'outils qui les aident à détecter et à répondre aux dernières menaces et aux menaces les plus complexes.

A cause des spécificités des attaques ciblées que les pirates informatiques utilisent :

- Contournement des systèmes de sécurité. Les agresseurs réalisent des recherches approfondies sur l'infrastructure existante, ce qui inclut le système de sécurité utilisé pour les points de terminaison ;
- Vulnérabilités zero-day, comptes compromis ;
- Logiciel malveillant ou logiciel unique créé spécialement ;

- Objets compromis qui apparaissent comme normal et par conséquent restent fiables ;
- Approche avec plusieurs vecteurs qui cherche à s'infiltrer dans le plus grand nombre de points de terminaison possible : ordinateurs de bureau, ordinateurs portables, serveurs, etc. ;

- Ingénierie sociale et données obtenues par des connaisseurs.

Ensuite, c'est à cause des limites technologiques des produits traditionnels de protection des points de terminaison, qui :

- Veulent détecter et bloquer les menaces courantes (simples), les vulnérabilités déjà connues ou les menaces inconnues qui reposent généralement sur des méthodes connues auparavant ;
- Se concentrent sur la visibilité de chaque point de terminaison et ne sont pas conçus pour visualiser et contrôler en temps réel tous les points de terminaison de façon simultanée à partir d'une seule interface centralisée ;
- Ne fournissent pas les informations nécessaires sur les menaces aux administrateurs informatiques pour qu'ils aient un aperçu du contexte des menaces actuelles. Ils manquent également de visibilité totale sur l'activité individuelle des points de terminaison, et sur les processus, les historiques et les possibles relations entre chaque point de terminaison de l'entreprise ;
- Offrent un mappage qui n'est pas intégré, ou une corrélation de plusieurs conclusions proposées par différents mécanismes de détection en un seul incident unifié ;
- Ne comprennent pas une fonctionnalité qui permet de détecter une activité anormale, des déviations d'activités normales, ou d'analyser le travail des programmes légitimes ;
- Ne peuvent pas analyser rétrospectivement le mouvement latéral du malware ;
- Ont des capacités limitées pour détecter les attaques sans fichier, les injections dans la mémoire ou les menaces sans malware.

Le coût moyen des incidents, et les lacunes des fonctionnalités des solutions EPP traditionnelles qui ne sont pas conçues pour contrer les menaces complexes, montrent clairement qu'il faut aussi investir dans des produits spécialisés dans la détection et la réponse de menaces avancées. Les produits EPP doivent être plus flexibles, et inclure des fonctions de système de détection et de réponse sur les points de terminaison (EDR), ou pouvoir intégrer des solutions EDR autonomes de plein exercice, selon la taille et les besoins de l'entreprise.

L'EDR est une technologie en matière de cybersécurité qui répond au besoin d'avoir une surveillance en temps réel, et met fortement l'accent sur les analyses de sécurité et la réponse aux incidents sur les points de terminaison de l'entreprise. Cette technologie fournit une véritable visibilité de bout en bout de l'activité de chaque point de terminaison de l'infrastructure de l'entreprise. Tout est contrôlé à partir d'une seule console, avec de précieux renseignements sur la sécurité qu'un expert en sécurité informatique peut utiliser pour approfondir ses recherches et les réponses.

La plupart des plateformes de protection des points de terminaison reposent sur des modèles enregistrés et des fichiers signés pour arrêter les menaces connues. Les plateformes plus récentes de protection des points de terminaison de la nouvelle génération, utilisent l'apprentissage automatique et des mécanismes de protection d'un niveau plus approfondi pour chasser et découvrir les menaces, et cherchent aussi à offrir une protection contre les malwares.

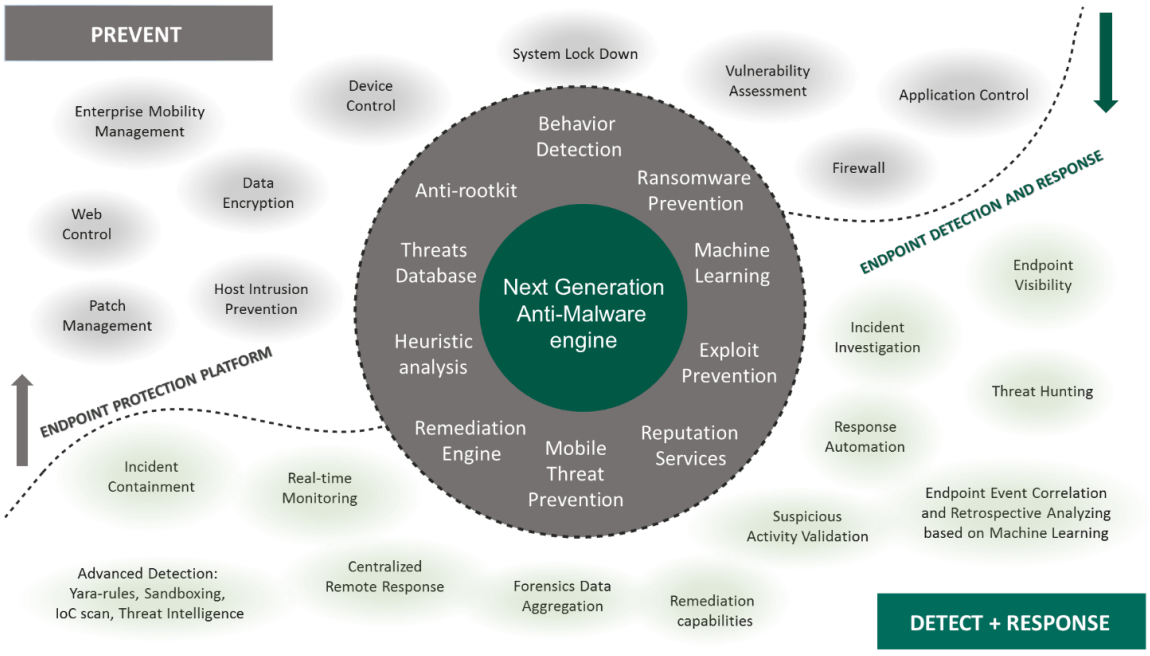
L'objectif principal d'EDR est la détection proactive de menaces nouvelles ou inconnues, mais aussi la détection d'infections non identifiées antérieurement et qui s'infiltrent dans l'organisation en passant directement par les points de terminaison et les serveurs. Cet objectif est atteint grâce à l'analyse des événements qui ont lieu dans les zones d'ombre ; berceau de ces objets ou processus non inclus dans les zones « fiables » ni « définitivement malveillants ».

Sans la fonction EDR, les EPP traditionnelles ne fournissent pas un soutien technique à la visibilité approfondie des points de terminaison, une analyse rétrospective de l'attaque sur plusieurs points de terminaison, la corrélation d'événements, ou l'habilité à choisir entre plusieurs détections celles qui sont pertinentes en matière d'attaques complexes pour établir la réponse appropriée. Toutes les solutions EPP disponibles sur le marché n'ont pas accès aux renseignements sur les menaces nécessaires pour comprendre les principales tactiques, procédures et techniques en matière de menace.

Toutes ces fonctions sont nécessaires pour lutter contre les menaces modernes et les attaques ciblées. Les entreprises doivent comprendre que la sécurité des points de terminaison ne peut plus être garantie par une seule solution EPP. EDR a de bien meilleures chances de détecter les souches d'un malware inconnu en zero-day, et les attaques au niveau de l'APT, parce qu'il utilise des technologies de détection avancées comme les règles YARA, le sandboxing, un scan des IoCs (indicateurs de compromission), la découverte et validation d'activités suspectes, une analyse rétrospective avec une corrélation des événements selon un apprentissage automatique dynamique, l'analyse et le confinement des incidents, l'automatisation de la réponse, des fonctionnalités de remédiation, et bien d'autres.

Pour avoir une protection fiable et efficace contre les menaces avancées, l'EPP et l'EDR travaillent ensemble. L'EPP gèrent les menaces connues, et l'EDR s'occupe des menaces inconnues plus complexes. Les plateformes EDR puissantes peuvent aider les analystes à étudier et améliorer leurs défenses, plutôt que de simplement réagir aux dégâts déjà causés par une menace avancée que les solutions traditionnelles de protection des points de terminaison pourraient ne pas détecter.

De plus, l'EPP fournit une protection, mais aussi un contrôle sur les applications, les dispositifs et les sites Internet, une évaluation de la vulnérabilité et la gestion des patchs, le filtrage des URL, le cryptage des données, un pare-feu et bien d'autres fonctions.



Chacun des systèmes décrits ci-dessus complète ce qui manque, ou est partiellement présent, dans un autre système. Cela signifie que les solutions doivent s'intégrer et interagir entre elles. L'EPP et l'EDR ont un même objectif qui consiste à contrer les menaces, mais il y a aussi de grandes différences. Ces deux solutions ont deux approches différentes de protection contre différents types de menaces et utilisent des outils différents.

Selon un rapport publié par Gartner, « Strategic Planning Assumption 2017 for Endpoint Detection and Response Solutions », d'ici 2021, 80 % des grandes entreprises, 25 % des moyennes entreprises et 10 % des petites entreprises auront investi dans des capacités EDR.

La présence de technologies préventives, comme l'EPP, pour la détection et le blocage automatique des menaces courantes et des objets malveillants, aide à éliminer le besoin d'analyser un grand nombre d'incidents mineurs qui ne sont pas pertinents en matière d'attaques complexes. Cela augmente l'efficacité des plateformes EDR spécialisées qui cherchent à détecter les menaces au niveau APT. Ensuite, l'EDR peut envoyer des conclusions à la plateforme de protection des points de terminaison après avoir détecté des menaces complexes. De cette façon, les deux solutions travaillent ensemble, et fournissent une approche réellement intégrée pour empêcher les menaces avancées.

3.2 Le Shadow IT.

Afin que l'entreprise ne soit pas mise en danger par le déploiement d'outils non validés, la DSI doit monitorer son réseau et mieux écouter les métiers pour proposer des alternatives satisfaisantes.

Selon une récente étude, un tiers des failles de sécurité seront dues au Shadow IT. Le déploiement de technologies par les collaborateurs sans passer par la DSI, à savoir la définition du Shadow IT, est un phénomène que l'on rencontre de plus en plus car les salariés et tout particulièrement les nouveaux entrants ont intégré ces usages dès leur enfance.

Pour être plus rapides, pour communiquer plus vite, les collaborateurs utilisent des applications, des services, des fonctions de stockage et de partage d'information sans passer par la DSI car ils estiment que ce sera plus efficace et moins cher. Mais cette pratique, a un impact évident sur la sécurité de

l'entreprise et rend plus complexe les actions de support, car on passe outre les mesures de gestion, d'intégration, de protection et de conformité nécessaires.

Pour résoudre cette problématique, les DSI peuvent mettre en place quatre mesures qui leur permettront de mieux collaborer avec les métiers et ainsi construire ensemble un plan d'action contre les failles et les coûts du Shadow IT.

- **Cherchez des solutions en monitorant le Shadow IT**

Il appartient à la DSI de faire l'inventaire de qui utilise quoi dans l'entreprise. Cet inventaire va permettre d'identifier les risques et de proposer des solutions plus adaptées. Pour y parvenir, il est possible de monitorer le réseau à l'aide de « sniffers » et autres outils de scan de sécurité. Même si ces scans ne résolvent pas les failles de sécurité, ils font apparaître les flux des applications inconnues ou nouvelles, lesquels constitueront une base de connaissances pour que la DSI puisse déterminer les meilleures alternatives possibles.

- **Proposer des solutions maîtrisées par la DSI, plus que des alternatives**

La volonté de la DSI étant surtout d'apporter des améliorations pour éviter les problèmes de sécurité, trouver une alternative à une solution déployée par les métiers eux-mêmes n'est pas forcément la solution. Parfois, il suffit juste de remettre un outil sous la responsabilité de la DSI, afin que celle-ci en contrôle la conformité technique et contractuelle.

Il est important que la DSI ne considère pas comme mauvais tout ce qu'elle va découvrir en menant des investigations au sujet du Shadow IT. Les outils et les applications révélées par cette investigation sont la voix des utilisateurs, ils sont ce dont les équipes ont vraiment besoin pour réussir dans leur travail. Ces solutions pourraient même bénéficier à d'autres directions métier.

- **Montrer une attitude d'ouverture**

Parallèlement, la DSI doit lutter contre sa tendance naturelle à se fermer quand il faut répondre aux nouvelles demandes des salariés. Il s'agit là du point de départ du Shadow IT : ne pas travailler ensemble, c'est s'interdire de savoir quelles technologies sont susceptibles d'être déployées, quels risques sont à éviter et quelles alternatives sont possibles. Prenons par exemple les télétravailleurs. Si la DSI ne leur propose pas spontanément les moyens pour collaborer à distance, ils en trouveront eux-mêmes, sans même se demander s'il

était pertinent d'en parler à la DSI. Et c'est à partir de ce moment-là que les complications commencent. La DSI doit plutôt anticiper incitant les métiers à la consulter pour partager leurs besoins. Les salariés de l'entreprise doivent être considérés comme les clients internes de la DSI. À ce titre, il est important de créer le dialogue en écoutant leurs retours d'expérience et les problèmes qu'ils essaient de résoudre.

- **Participer aux réunions des métiers sur la stratégie technologique**

Pour créer un climat de pleine collaboration entre les métiers et la DSI, cette dernière a tout intérêt à rencontrer régulièrement chaque direction afin de discuter avec elle de ses stratégies technologiques. Établir un dialogue ouvert avec les métiers est le meilleur moyen de rendre transparente la question des solutions à adopter et d'éviter le problème des technologies non approuvées en production. Participer aux réunions de planning stratégique réduit considérablement les surprises liées au Shadow IT.

3.3 La cyber-résilience.

La cyber-résilience fait référence à la capacité d'une entité à fournir en permanence le résultat souhaité malgré les cyber-événements indésirables. La cyber-résilience est une perspective en évolution qui est de plus en plus reconnue. La cyber-résilience se donne pour objectif de permettre à des organisations ou entreprises d'être les plus réactives possible face à une cyber attaque. Cela passe par une approche qui peut apparaître contre nature dans une cyberguerre puisqu'il est alors question pour les cibles potentielles de développer et de partager des outils et des informations afin de mutualiser les moyens défense.

Aujourd'hui la cybersécurité est devenue la première préoccupation des entreprises en France. Dans le top dix des préoccupations, les incidents cyber arrivent en première place suivi par les interruptions d'activité. Cette inquiétude sur la cybersécurité, est liée au fait que « Les entreprises françaises sont de plus en plus préoccupées par la fréquence et la gravité croissante des incidents cyber.

Pour ce qui est de l'arrêt d'activité, cyber-incident et interruption d'activité sont intimement liés. Devant la montée en puissance des coûts inhérents à ces problématiques, la cyber-résilience apparaît comme un enjeu majeur.

Pour faire face à ces risques, les entreprises s'organisent et entreprennent des démarches cyber-résilientes. En juillet 2018, par exemple, Orange et Europol ont signé un accord, au service de cette cyber-résilience. Ce partenariat porte sur le principe de partage de connaissances sur les cybermenaces pouvant peser au niveau européen.

Cela va dans le sens d'une meilleure connaissance de la cybercriminalité. Dans le même temps, la formation à la cyber-résilience devient de plus en plus performante au service des entreprises.

Altran a ainsi subi le 24 janvier 2019 une attaque au rançongiciel d'importance qu'elle a confirmée par un communiqué de presse « Information sur une cyber attaque » en date du 28 janvier 2019 , ce dernier met en avant sa capacité à réagir :

Pour protéger nos clients, employés et partenaires, nous avons immédiatement déconnecté notre réseau informatique et toutes nos applications. La sécurité de nos clients et des données est et sera toujours notre priorité absolue. Nous avons mobilisé des experts techniques et d'investigation indépendants mondialement reconnus, et l'enquête que nous avons menée avec eux n'a révélé aucun vol de données ni aucun cas de propagation de l'incident à nos clients. Notre plan de rétablissement se déroule comme prévu et nos équipes techniques sont pleinement mobilisées. Tout au long du processus, Altran a été en contact avec ses clients, les autorités gouvernementales et les régulateurs compétents.

Si la société Altran ne peut être qualifiée d'opérateur d'importance vitale, sa capacité à réagir et à mobiliser les acteurs internes et externes (investigations), le respect des exigences de transparence totale prévues par le Règlement Général sur la Protection des Données, ont été des éléments déterminants pour contenir la crise et la régler sans occasionner de potentiels dégâts collatéraux. Rappelons qu'Altran compte en effet parmi ses clients des organisations identifiées par l'État comme ayant des activités indispensables ou dangereuses pour la population telle qu' Orange, EDF, Engie.

La cybercriminalité est en constante évolution, elle ne disparaîtra pas, elle peut seulement se combattre de façon plus efficiente. Il s'agit donc d'intégrer que la cyber-résilience est l'affaire de tous et de toutes. C'est notamment celle des TPE/PME souvent moins armées et plus vulnérables, qui peuvent, sans être la cible finale , constituer des points d'entrée privilégiés vers de grandes entreprises, au même titre que l'est tout salarié peu ou mal informé des

principes de précautions les plus élémentaires lorsqu'il est connecté aux réseaux de son entreprise.

Pour conclure la cyber-résilience est un contrepoison, cela ne résoudra jamais tous les problèmes de sécurité à moins d'un changement généralisé de la nature humaine.

3.4 Ransomware et continuité d'activité.

La continuité d'activité permet d'assurer la résilience des entreprises en cas de sinistres majeurs. En se dotant de plans de continuité d'activité (PCA), les entreprises sont préparées à faire face à ces sinistres et assurer leur continuité. Ces plans de continuité prennent aujourd'hui assez peu en compte la gestion de cybercrises et interviennent surtout sur des scénarios d'indisponibilité des ressources humaines, logistiques et matérielles. Les cybercrises peuvent mettre en péril toute l'organisation. Se préparer à y faire face est donc une nécessité croissante et les entreprises doivent impérativement repenser leurs plans de continuité d'activité pour y intégrer les enjeux cyber. Les métiers vont devoir apprendre à gérer des solutions palliatives répondant non plus seulement à des problèmes d'indisponibilité des ressources mais aussi à des problèmes d'image, de confidentialité et d'intégrité nécessitant le recours à de nouveaux schémas de réponse.

Face à une cyber attaque, les réponses apportées ne peuvent plus se limiter au seul périmètre IT et technique. En effet la surface d'attaque s'étend aujourd'hui à l'entreprise entière, avec des conséquences sur les métiers qui peuvent se révéler tout aussi importantes. Les politiques de sécurité définies en réponse à ces attaques doivent donc tenir compte des aspects IT mais aussi des problématiques métiers impliqués. Le RSSI devra voir au-delà du problème technique et de l'aspect sécurité pour prendre en compte les enjeux métiers de certaines des décisions qu'il pourra prendre.

Les enjeux cyber une fois pris en compte, il sera important de tester le plan de continuité de l'activité et de le maintenir en conditions opérationnelles. Organiser des exercices en prenant en compte des scénarios de cyber attaque et ce à tous les niveaux, aussi bien techniques que décisionnels. Ce qui permettra de préparer l'ensemble des acteurs mais aussi d'apporter des modifications au PCA si nécessaire. De nouveaux acteurs, spécialisés dans les comportements individuels et collectifs, pourront aider les collaborateurs à mieux gérer les

situations de stress induites par de telles attaques (demande de rançon, médiatisation brutale et massive). Grâce à cette préparation, la cellule décisionnelle aura quant à elle toutes les cartes en main pour pouvoir prendre les meilleures décisions en cas de cyber crise.

Intégrer les scénarios cyber dans les plans de continuité d'activité permettra de répondre à une partie des crises cyber sous réserve que ce type d'évènement soit bien anticipé. Cependant, à la différence des scénarios habituels traités dans les PCA, ces cyber crises se distinguent par leur sophistication, vont souvent être difficiles à cerner et demanderont beaucoup d'investigations. Dès lors, il est primordial que le PCA prévoie le retour à la normale suite à un incident majeur. Ce retour à la normale, encore trop peu anticipé par les entreprises, constituera un point critique de la cyber-résilience et nécessitera à son tour de mobiliser l'ensemble des métiers aussi bien IT, que juridiques, financiers, commerciaux etc.

L'ensemble de ces actions devront s'articuler autour d'un dispositif de gestion de crise optimisant le pilotage de tous ces acteurs et de leurs enjeux, facilitant les échanges internes, établissant la communication externe et offrant un cadre décisionnel hors nome permettant de gérer tout ce qui reste de l'ordre de l'imprévisible.

4 Le futur du ransomware.

Une des plus grosses inquiétudes concerne le fait que le ransomware peut commencer à prendre pour cible des appareils numériques différents des ordinateurs et des smartphones. De plus en plus d'objets de la vie quotidienne sont connectés à internet, et cela créé un nouveau marché immense pour les cybers criminels, qui pourraient utiliser un ransomware pour empêcher les gens de rentrer dans leur voiture, ou en baissant le thermostat du chauffage des maisons au minimum en plein hiver tant que la rançon n'est pas payée. C'est de cette façon que le ransomware peut affecter directement nos vies quotidiennes de plus en plus facilement.

Une des autres possibilités, c'est que les ransomwares, plutôt que de viser les fichiers d'un ordinateur, utiliseront des injections SQL pour crypter des bases de données sur un serveur réseau. Le résultat serait catastrophique, l'ensemble de l'infrastructure d'une entreprise mondiale pourrait être corrompu en un seul

geste, ou des services internet entiers pourraient succomber, affectant une quantité incroyable d'utilisateurs.

Le chiffrement de fichier ne va pas disparaître de sitôt. La méthode fonctionne, le public potentiel d'attaques est large (personnes physiques et entreprises) et les solutions anti-virus ne sont pas efficaces à 100%.

Les entreprises ayant une grande base de clients continuent d'être des candidats attrayants pour les attaques. Plus il y a d'utilisateurs, plus il y a de contenu, plus l'opportunité financière est grande pour les pirates. Les attaquants peuvent planifier des attaques ciblées contre les technologies, le contenu et les utilisateurs uniques d'une entreprise, mais ils devront consacrer plus de temps (et d'argent) pour mener ce type d'attaque.

Le point d'entrée d'une attaque perturbatrice et ciblée peut provenir d'une vulnérabilité Web, l'un des moyens les plus simples d'infecter simultanément un grand nombre d'utilisateurs ou de périphériques connectés. La tendance Internet des objets (IoT) ne fait que rendre ce type d'attaque de plus en plus possible. Prenez les voitures connectées d'aujourd'hui et les voitures autonomes de demain, les deux ayant une connexion Internet, que ce soit via une application permettant aux propriétaires de contrôler les fonctions de la voiture ou de permettre l'envoi de mises à jour push du vendeur de voitures.

Une vulnérabilité du serveur Web communiquant avec l'application ou le mécanisme de mise à jour peut entraîner l'exécution de code à distance sur ces véhicules. Par exemple, les pirates pourraient prendre en otage un utilisateur et demander une rançon, tout en menaçant de désactiver les freins ou le système de direction de votre voiture. Le scénario encore plus chaotique est un pirate informatique qui prend le contrôle de toutes les voitures connectées d'un fournisseur spécifique et qui demande une rançon directement à ce dernier.
Il est raisonnable de penser que dans quelques années, la plupart des attaques évolueront en ransomware / extortionware, partageant cet ADN commun: attaque par corruption, exfiltration ou perturbation, puis en exigeant une rançon pour arrêter ou inverser l'attaque. Compte tenu de cela, les entreprises doivent continuer à protéger leurs données et leurs actifs en réponse à ces tactiques changeantes.

En outre, l'arrivée d'outils de piratage de protocole de très bas niveau, comme KRACK, va offrir aux hackers de nouveaux moyens de contourner l'infrastructure IoT et de la compromettre. Cela peut augmenter le risque d'attaques pour les équipements IoT à grande échelle comme le système de climatisation ou de

chauffage d'un bâtiment. L'accès à un protocole de bas niveau et sa prise de contrôle pourraient offrir la possibilité d'injecter ou de manipuler des données. Les implications peuvent être sérieuses si les équipements IoT nécessitent de se synchroniser avec une application Cloud ou d'en recevoir des messages faisant office de commandes. La manipulation des données pourrait entraîner l'envoi de la mauvaise action ou du mauvais paramètre à l'équipement IoT.

Il se peut que des attaques plus traumatisantes se produisent également. Des chercheurs ont apporté la preuve qu'il est possible de suivre un véhicule connecté à distance, de le contrôler et de le désactiver. Que se passerait-il si des criminels obligent un conducteur à les emmener jusqu'à une zone où il n'est pas possible d'obtenir de l'aide rapidement ?

Dans le meilleur des cas, si rien d'autre ne se produit, le conducteur sera embarrassé et cela lui prendra une journée pour réinitialiser et nettoyer le système embarqué de sa voiture pour pouvoir conduire à nouveau. Le pire des cas serait que les cybercriminels l'enferment dans sa voiture piratée, qu'ils le contactent par l'unité principale et lui demandent une rançon : le menaçant de le laisser enfermé là ou de lancer sa voiture à pleine vitesse contre un mur s'il refuse de payer. Cela peut paraître extrême, mais c'est complètement possible.

Les camions connectés de transport de marchandises pourraient exposer les entreprises à des risques. Tout retard pourrait provoquer de grosses pertes financières, si bien que les entreprises pourraient être tentées de payer plus pour débloquer les informations de suivi ou pour pouvoir réutiliser un camion.

La liste des scénarios potentiels est infinie, mais donne une idée d'ensemble : la connectivité est utile et nécessaire, mais elle peut aussi avoir des conséquences désastreuses laissée sans protection.

A ce jour de plus en plus d'entreprise sont touchées par des ransomwares. La plupart du temps, il s'agit de chiffrement de données et les entreprises décident de régler la rançon pour éviter une perte ou arrêt de production et être plus grandement impacté.

Mais on peut imaginer que demain, on parlera d'exfiltration de données, d'espionnage industriel ou de sabotage industriel.

Peu importe son évolution, nous devrions nous préparer à ce que cette menace soit de plus en plus présente au fil des années. Surveillez les e-mails que vous ouvrez, les sites que vous visitez, et faites attention à rester à jour, ou vous pourriez faire partie des tas de victimes du ransomware.

5 Glossaire

APT : Ce terme s'applique aux attaques concertées, furtives et continues dirigées contre des organisations spécifiques - par opposition aux incidents spéculatifs, isolés et opportunistes qui constituent l'essentiel de l'activité cybercriminelle. De telles attaques utilisent des logiciels malveillants très sophistiqués pour violer les défenses de sécurité d'une organisation de type gouvernementale.

Bitcoin : Le **Bitcoin** (de l'anglais *bit* : unité d'information binaire et *coin* « pièce de monnaie ») est une cryptomonnaie.

Botnet : Un **botnet** (contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.

Chiffrement : Le **chiffrement** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Chiffrement symétrique : Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. (Vernam, DES, 3DES, AES, etc.)

Chiffrement asymétrique : Pour résoudre le problème de l'échange de clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés : une publique, permettant le chiffrement et une privée, permettant le déchiffrement.

Chiffrement RSA : Le **chiffrement RSA** (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique qui utilise une paire de clé publique/privée, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

Cryptographie : La **cryptographie** est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de clés.

Cryptomalware : Logiciel de type ransomware qui chiffre les fichiers de l'utilisateur et demande une rançon. Les cryptomalwares sophistiqués utilisent des méthodes de chiffrement avancées afin que les fichiers ne puissent pas être déchiffrés sans une clé unique.

IOC : L'**IOC** ou indicateur de compromission est un ensemble de données sur les menaces (par exemple, lignes décrivant le chemin d'accès aux fichiers ou aux clés de registre) qui permet de déceler la présence d'une menace dans l'infrastructure grâce à l'analyse automatique à l'aide d'outils logiciels.

Malware : Logiciel malveillant créé délibérément pour exécuter une action non autorisée, souvent nuisible.

Ransomware : Ransomware est le nom donné aux programmes malveillants conçus pour extorquer de l'argent à leurs victimes, en bloquant l'accès à l'ordinateur ou en cryptant les données qui y sont stockées et proposant de restaurer le système en échange d'un paiement.

RaaS : Plateforme sur le dark web proposant l'achat ou la location de ransomware, la mise à disposition de botnet pour la diffusion de ransomware

Réseau TOR : Tor est un réseau informatique superposé mondial et décentralisé. Il se compose d'un certain nombre de serveurs, appelés nœuds du réseau et dont la liste est publique. Ce réseau permet d'anonymiser l'origine de connexions TCP. Cela peut entre autres servir à anonymiser la source d'une session de navigation Web ou de messagerie instantanée.

Sandboxing : Bac à sable qui fournit un environnement étroitement contrôlé dans lequel des programmes ou des scripts semi-fiables peuvent être exécutés en toute sécurité en mémoire (ou avec un accès limité au disque dur local).

Serveur C&C : Les serveurs de commande et contrôle, également appelés C & C ou C2, sont utilisés par les attaquants pour maintenir les communications avec les systèmes compromis au sein d'un réseau cible. Ces systèmes comprennent les ordinateurs, les smartphones et les objets IoT.

Shadow IT : **Shadow IT** est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information.

SMB(protocole) : Le protocole **SMB** (***Server Message Block***) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.

Solution EDR : Les logiciels **EDR** utilisent une technologie novatrice de détection des menaces sur le EndPoint (ordinateurs ...).Ce terme définit une catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes et les PC du réseau. Combiné avec un moteur basé sur de l'intelligence artificielle, le logiciel EDR est très réactif dans la détection et l'arrêt de menaces (Malwares, virus, attaques zéro Day, menaces persistantes avancées, ...). L'intelligence artificielle lui permet d'être auto-apprenant et de ne pas devoir se connecter sur internet pour mettre à jour des bases de données.

Solution EPP : **EPP** (Endpoint Protection Platform) est une solution déployée sur des terminaux pour empêcher les attaques malveillantes basées sur des fichiers, détecter les activités malveillantes et fournir les fonctionnalités d'investigation et de résolution nécessaires pour répondre aux incidents et alertes de sécurité dynamiques.

YARA : **YARA** est le nom d'un outil principalement utilisé dans la recherche et la détection de programmes malveillants. Il fournit une approche basée sur des règles pour créer des descriptions de familles de programmes malveillants basées sur des modèles textuels ou binaires.

6 Sources

www.ssi.gouv.fr

Agence Nationale de la Sécurité des systèmes d'information

www.cnil.fr

Commission Nationale de l'informatique et des libertés

www.forum-fic.com

Forum sur la cybersécurité

www.cesin.fr

Club des Experts de la Sécurité de l'Information et du Numérique

www.clusif.fr

Club de la Sécurité de l'Information français

www.kaspersky.fr

Editeur de solution de sécurité

www.eset.fr

Editeur de solution de sécurité

www.bleepingcomputer.com

Site de vulgarisation

www.cnetfrance.fr

Site de vulgarisation

www.assiste.com

Site de vulgarisation sur la sécurité

www.malekal.com

Site de vulgarisation sur la sécurité

www.zataz.com

Site sur la cybersécurité

www.datasecuritybreach.fr

Site sur la cybersécurité

www.unit42.paloaltonetworks.com

Site sur la cybersécurité