CYBERSÉCURITÉ 2019 :

à l'ère de la mondialisation, le respect de la vie privée et les intrusions au cœur de toutes les préoccupations

ESET CYBERSECURITY EXPERTS ON YOUR SIDE

INDEX

INTRODUCTION

Depuis plusieurs années déjà, notre rapport annuel regroupe les contributions d'experts ESET du monde entier. Offrant un aperçu des jalons atteints dans l'industrie de la cybersécurité, il s'intéresse également aux scénarios d'attaque susceptibles de se produire en 2019 et aux mesures à adopter pour se prémunir de ces menaces.

Les scénarios de base en la matière varient peu : les données des particuliers comme des entreprises sont encore et toujours au cœur de toutes les préoccupations. L'enjeu reste d'assurer leur confidentialité, leur intégrité et leur disponibilité et de les protéger contre les attaques répétées de hackers désireux d'y accéder, de les utiliser et/ou de les dérober. Pour ces raisons, nous insistons dans notre rapport 2019 sur l'importance croissante pour les entreprises de garantir efficacement la confidentialité des données, en particulier à la lumière du scandale Facebook-Cambridge Analytica et de la violation de données qui a conduit Google à fermer Google+.

En parallèle avec l'entrée en vigueur du Règlement général sur la protection des données (RGPD), ces incidents commencent à affecter les principaux acteurs du secteur. Cela soulève des questions sur l'impact potentiel des cas des GAFA (géants du Web) sur les entreprises plus petites qui n'ont pas les ressources nécessaires pour protéger comme il se doit la vie privée de leurs clients.

Par conséquent, compte tenu des volumes considérables de données personnelles gérées par ces services, certains organismes gouvernementaux prêtent désormais attention à la stratégie de traitement et de protection des données des géants du Web. En outre, ces institutions gouvernementales commencent à exercer des contrôles, tels que le RGPD dans l'Union européenne, qui est entré en vigueur le 25 mai 2018. *Dans une section dédiée*, nous examinons certaines des plus importantes questions relatives à cette législation. Parallèlement, nous évaluons aussi les éventuelles implications futures de cette initiative pour les nouveaux contrôles gouvernementaux mis en place aux quatre coins du globe.

Les questions de la protection des données et du respect de la vie privée sont d'ailleurs présentes en filigrane dans toutes les différentes sections de ce rapport. Alors que la technologie ne cesse de progresser, son utilisation évolue également, ce qui permet aux pirates de trouver de nouvelles stratégies. Ainsi, le présent document inclut une section sur les assistants connectés, sur les précautions à prendre avec l'Internet des Objets (IoT) et sur l'impact de ces appareils en termes de sécurité, aussi bien au travail qu'à la maison.

Nous abordons également un autre sujet connexe qui a beaucoup fait parler de lui l'année passée : les cryptomineurs. Tirant parti de la technologie légitime de la blockchain, cette menace vise à exploiter la puissance de calcul de l'ordinateur d'une victime, afin de miner des cryptomonnaies et de générer un retour financier pour l'auteur de l'attaque.

Bien sûr, ces progrès technologiques ne profitent pas seulement aux cybercriminels qui tentent de s'en emparer : ainsi, cette technologie sert aussi à protéger les utilisateurs et les organisations. Par exemple, le machine learning (ML) permet d'optimiser l'utilisation des gigantesques quantités d'informations générées par les interactions entre utilisateurs et systèmes, en traitant et en exploitant ces données pour améliorer les systèmes en question. Mais le machine learning n'est qu'un outil ; il ne s'agit pas d'une solution tout-en-un. Comme l'histoire nous a montré que toute technologie pouvait être utilisée à bon mais aussi à mauvais escient, dans la section dédiée au machine learning, nous tentons de répondre à la question suivante : cette technologie pourrait-elle être détournée ?

Pour protéger les informations des particuliers et des entreprises, il est indispensable de connaître les tendances à venir et les défis à relever en matière de sécurité informatique. Nous vous invitons donc à lire les différentes sections du présent rapport pour découvrir les prévisions des experts ESET pour 2019.

1

CRYPTOMINEURS : LE NOUVEL OUTIL DE PRÉDILECTION DES CYBERCRIMINELS ?

- Les successeurs des ransomwares
- Le cryptomining, un procédé lucratif
- La protection des systèmes

AUTEUR

David Harley
ESET Senior Research Fellow

Cryptomineurs : le nouvel outil de prédilection des cybercriminels ?

De nombreuses personnes ont découvert les *monnaies virtuelles* ou *cryptomonnaies*, lorsqu'une de leurs connaissances ou elles-mêmes ont été victimes d'un ransomware. Dans ce type d'attaque, les cibles doivent généralement payer une rançon en monnaie virtuelle, comme le *Bitcoin*, pour récupérer leurs données chiffrées.

Ce moyen de paiement est plébiscité par les hackers, car il préserve leur anonymat, surtout si le montant de la transaction est converti dans une autre cryptomonnaie avant d'être finalement échangé contre de l'argent comptant ou des articles « réels ». Ainsi,

pour créer un portefeuille Bitcoin ou tout autre moyen de paiement en vue de payer leur rançon, de nombreuses victimes de ransomwares ont dû suivre les instructions du pirate à l'origine de l'attaque.

Évidemment, cela ne signifie pas qu'elles connaissent les tenants et les aboutissants des cryptomonnaies ou comprennent le concept de cryptomining (parfois désigné sous le terme de « minage de cryptomonnaie »), même si elles ont déjà utilisé une monnaie virtuelle pour se sortir d'une situation délicate. Le présent article n'a pas pour but d'expliquer en détail le fonctionnement de la *blockchain*, *des cryptomonnaies et du cryptomining*. Cependant, nous pouvons dire en simplifiant que le *minage* consiste à exploiter une puissance de calcul et de l'énergie électrique pour « trouver» quelque chose. En d'autres termes, il s'agit de consacrer une puissance de traitement à un processus mathématique qui crée et distribue des pièces virtuelles.

Le cryptomining et les cryptomonnaies ne sont pas nécessairement *illégaux*. Cependant, de nombreux éditeurs d'applications et commentateurs présentent de manière inexacte les bénéfices potentiels du cryptomining. Pour certains, cet enthousiasme exagéré pour le minage rappelle *la pyramide de Ponzi* et le cas de la *Compagnie de la mer du Sud*.

Si le Bitcoin est la plus connue des cryptomonnaies, il y en a beaucoup d'autres. *Monero*, par exemple, est populaire auprès des cybercriminels, car elle est axée sur la protection de la vie privée, un aspect encore plus important pour les hackers que pour le reste d'entre nous.

En attendant, le minage de Bitcoin est *un processus coûteux*, uniquement rentable dans le cadre d'opérations de grande envergure et beaucoup trop exigeant pour les ordinateurs et appareils grand public, bien que certaines monnaies alternatives soient moins contraignantes. Cependant, comme la charge de traitement peut être répartie entre plusieurs machines et appareils, des applications légitimes (souvent payantes) permettent de se connecter à un « pool de minage ». Pour autant, les propriétaires des machines impliquées ne sont pas nécessairement conscients de leur rôle et les profits ne sont pas forcément partagés de façon équitable. Dans ce contexte, il est de plus en plus fréquent de fournir *des services légitimes* en échange de l'utilisation de la puissance de calcul de l'appareil d'un particulier à des fins de minage. Néanmoins, lorsqu'un appareil est détourné de façon illégitime (cryptojacking), il n'y a pas de contrepartie. Plus notoirement, (une partie de) la puissance de calcul du système de la victime est détournée grâce à un malware sur disque ou sans fichier (souvent appelé « cryptomineur ») ou grâce à des scripts *sur un site Web* (cryptojacking sur navigateur).

Des profils de victimes variés

Les systèmes dédiés au cryptomining ont tendance à ne pas s'appuyer uniquement sur les *cycles* de processeur (CPU) : ils tirent aussi parti de périphériques auxiliaires tels que les processeurs graphiques (GPU) et les puces ASIC (Application-Specific Integrated Circuit) dédiées. Faut-il s'attendre à une vague de malwares de minage destinés à exploiter ces différents composants ? Il est probable que les individus ou organisations qui font leurs premiers pas dans le domaine du minage et ont investi dans du matériel spécifique, relativement coûteux, veillent attentivement sur leurs cycles (peut-être même avec des logiciels de sécurité !). Mais les utilisateurs de machines de jeu haut de gamme, par exemple, sont susceptibles d'être moins prudents.

Dans tous les cas, un ralentissement sera probablement perceptible si les systèmes utilisés pour des applications exigeant beaucoup de ressources sont clandestinement détournés à des fins de cryptomining, d'autant plus s'il s'agit de systèmes relativement peu puissants, comme d'anciennes consoles de jeu ou des appareils mobiles.

Faut-il en conclure que les cybercriminels éviteront ces systèmes ? Pas nécessairement. Généralement, les hackers ne cherchent pas à préserver les ressources de leurs victimes, sauf s'ils souhaitent à tout prix rester incognito pour ne pas compromettre leurs efforts. En outre, comme le montre l'utilisation fréquente du minage sur navigateur, un appareil donné peut être utile même si sa puissance n'est pas élevée et même s'il n'est pas disponible à long terme.

Une utilisation sensiblement importante des cycles de CPU et de GPU peut donc suggérer la présence d'un malware de cryptomining. D'autres symptômes peuvent évoquer une telle attaque : surchauffe (ventilateur fonctionnant en permanence ou température inhabituellement élevée pour les téléphones et tablettes), pannes ou redémarrages inexpliqués et volumes inexplicablement importants de trafic réseau. Bien entendu, ces symptômes peuvent être le signe d'autres problèmes potentiellement sans rapport avec des malwares ou d'autres incidents de sécurité.

Début 2018, les malwares de cryptomining ont commencé à être présentés comme « les nouveaux ransomwares ».

Qu'est-il arrivé aux ransomwares ?

Ces dernières années, les ransomwares ont fait *les beaux jours* de la cybercriminalité. Les opinions et estimations quant à la part de marché et aux répercussions financières de ces types de menaces spécifiques sont si variables que leur valeur semble discutable. Cependant, il est clair que jusqu'à récemment, les ransomwares étaient la cybermenace la mieux connue des médias et du grand public. Pourtant, début 2018, les malwares de cryptomining ont commencé à être présentés comme « les nouveaux ransomwares » et les médias se sont désintéressés des incidents liés aux ransomwares.

Évidemment, cela ne signifie pas que l'épidémie de ransomwares s'essouffle, mais les cas médiatisés de personnes dont les données ont été dérobées ou qui ont dû payer des rançons ont diminué considérablement. Il est difficile de savoir si ce phénomène est dû à une perte d'intérêt des médias, avides de sujets plus accrocheurs ou moins éculés concernant les malwares, ou à une baisse importante des attaques par ransomwares.

Cependant, de grandes organisations continuent d'être ciblées par des menaces de ce type. Il est possible que cela indique un changement de stratégie de la part des cybercriminels : au lieu de tenter de faire de nombreuses victimes, dans l'espoir que l'accumulation de petits profits leur permette de retirer un bénéfice substantiel, les pirates semblent aujourd'hui préférer *cibler des proies moins nombreuses, mais très rentables.* Par exemple, *selon les estimations*, les créateurs du ransomware Sam-Sam engrangeraient chaque mois environ 330 000 dollars en ciblant des entreprises et des organisations du secteur public. De plus, les ransomwares se sont diversifiés, notamment avec les cas de *sextorsion.*

Des maux convergents

Bien entendu, les malwares peuvent rentrer dans plus d'une catégorie. XBash est un *exemple récent* de convergence de fonctionnalités, combinant un nombre surprenant d'attributs :

- Il peut être décrit comme un ransomware, même si le qualificatif de pseudo-ransomware serait plus juste, puisqu'il semble qu'aucune fonctionnalité ne permette aux hackers de restaurer les données des victimes qui choisissent de payer la rançon. Ainsi, si nous ne tenons pas compte de la demande de rançon, ce programme est fonctionnellement plus proche des malwares destructeurs appelés wipers.
- Il intègre également des fonctionnalités de botnet, de cryptomining et d'auto-propagation.
- Il s'agit d'un malware multiplateforme, dont la charge utile est susceptible de varier en fonction de l'environnement d'exécution (Linux ou Windows) et des services disponibles. Mais il existe aussi plusieurs extensions tierces pour Kodi, *qui servent* à déployer des cryptomineurs Linux et Windows. Et oui, il existe des malwares de cryptomining qui ciblent également macOS ou Android.

Après trente années dans le domaine de la sécurité, j'ai appris que la sophistication et la polyvalence n'étaient pas nécessairement synonymes de tendance majeure. Ces attributs peuvent simplement être révélateurs d'une transition entre différentes catégories de menaces. Ainsi, l'avènement de Melissa a été à la fois le point culminant des macrovirus et un signe avant-coureur du raz-de-marée des mass-mailers. Pourtant, il est probable que les cybercriminels continuent à miser sur des malwares expérimentaux, capables de générer des profits partout et à tout moment, tout du moins à court terme.

Nous pouvons également nous attendre à ce que de plus en plus de cryptomineurs *tentent de supprimer* des programmes concurrents sur les systèmes compromis, afin de pouvoir exploiter plus de ressources de traitement.

À quel point le cryptomining est-il lucratif ?

Une étude de l'Institut pour la sécurité des systèmes de l'Université technique de Brunswick *suggère* que le cryptojacking basé sur le Web est fréquent, mais reste modérément rentable. Pour autant, la tendance du cryptojacking ne montre pour l'instant aucun signe de ralentissement. Tomáš Foltýn d'ESET a récemment révélé qu'une *organisation britannique sur trois avait déjà été victime de cryptojacking en avril 2018*, tandis que près de

Le cryptomining a progressé de 956 % en un an et le nombre d'organisations touchées par le phénomène a doublé au cours du premier semestre 2018, permettant ainsi aux cybercriminels de générer 2,5 milliards de dollars pendant cette période.

deux cadres IT sur trois estimaient que leurs systèmes avaient été touchés, à un moment ou un autre, par des attaques de cryptojacking.

Selon un article de Phil Muncaster citant différents rapports, le cryptomining aurait augmenté de 956 % en un an et le nombre d'organisations affectées aurait doublé au premier semestre 2018, permettant ainsi aux cybercriminels d'engranger 2,5 milliards de dollars au cours de cette période. Au moment de la rédaction du présent rapport, *une autre étude* affirmait de son côté que le cryptomining avait progressé de 459 % en 2018 et imputait cette hausse à l'utilisation d'*EternalBlue.* Selon moi, cette tendance devrait perdurer encore un certain temps, même si je ne sais pas quelle est la part de responsabilité de la NSA en la matière.

Le mineur Coinhive a connu son heure de gloire en tant qu'extension de site Web, car il permet à un site d'utiliser les cycles du système d'un visiteur afin de miner du Monero. Il a *rapidement gagné en popularité* auprès des cybercriminels qui s'en sont servis pour pirater des sites légitimes, afin d'exécuter des scripts Coinhive, configurés pour miner du Monero, et de s'enrichir. Plus récemment, Crypto-Loot a *notoirement* été adopté par Pirate Bay, pour des raisons similaires.

Conclusion : il est indispensable de protéger vos systèmes

Les suggestions suivantes ne sont pas toutes spécifiques aux malwares (ou ransomwares) de cryptomining, mais elles pourront potentiellement limiter l'impact des autres menaces.

- Les logiciels de sécurité aident à lutter contre les malwares de cryptomining et autres menaces. Ils ne permettent pas uniquement d'éviter tout type de malwares : ils détectent spécifiquement les logiciels malveillants de cryptomining se présentant sous la forme de fichiers exécutables, susceptibles de compromettre vos systèmes et détectent ou bloquent les scripts de cryptomining dans les navigateurs.
- Ces malwares sont souvent détectés comme « potentiellement indésirables » ou « potentiellement dangereux » (voir *ceci* et *cela*). Veillez donc à ce que votre logiciel de sécurité soit configuré pour signaler les programmes de ce type.
- Malgré les allégations de certains fournisseurs de technologies concurrentes, les logiciels de sécurité grand public sont capables d'identifier de nombreux processus malveillants dans la mémoire principale ou à partir de scripts s'exécutant sur serveur.
- Pour limiter les risques liés à l'utilisation d'un navigateur, nous vous recommandons aussi d'installer un *bloqueur de publicités*, qui a beaucoup d'autres avantages, ou un bloqueur de script de confiance.
- Gardez à l'esprit que les cryptomineurs exploitent souvent des vulnérabilités comme EternalBlue, *faille pour laquelle un correctif* a été publié en mars 2017. Ne tardez pas à appliquer les correctifs, quel que soit votre système d'exploitation.
- Il y a toujours un risque que les cybercriminels provoquent des dommages, même si ce n'est pas nécessairement leur but (contrairement aux dommages infligés par les wipers et les ransomwares). Nous vous invitons donc à conserver des sauvegardes en lieu sûr (hors ligne), comme évoqué *ici*.
- Aucun produit ne peut tout détecter. Parfois, le bon sens et la prudence vous permettront d'échapper au danger, si la technologie ne suffit pas.

2

MACHINE LEARNING : L'INTERDÉPENDANCE DES HUMAINS ET DES MACHINES

- Fonctionnement du machine learning
- Technologie utilisée pour propager des malwares
- Contraintes pratiques du machine learning

AUTEUR

Lysa Myers
ESET Senior Security Researcher

Machine learning : l'interdépendance des humains et des machines

Les trois vertus d'un grand programmeur seraient la paresse, l'impatience et l'orgueil. Il est particulièrement important de garder cet adage à l'esprit pour évoquer l'avenir du secteur des malwares. De plus, pour élaborer des prévisions de cybersécurité, il convient également de se rappeler qu'en général (indépendamment du cadre légal), les gens essaient d'obtenir un retour sur investissement raisonnable, pour le temps et les efforts qu'ils consacrent à une tâche. Que peuvent nous apprendre ces règles sur l'avenir de la cybersécurité au regard de l'adoption du machine learning ?

Concernant le comportement des cybercriminels, nous pouvons affirmer que, sauf cas exceptionnels, ces derniers tentent de dérober de l'argent ou des produits précieux avec un minimum d'effort. Pour la plupart des hackers, inutile de développer ou de déployer des technologies de pointe, si des attaques basiques automatisées permettent d'obtenir le résultat escompté. C'est certainement le scénario le plus fréquent et le problème le plus important pour la plupart des individus qui cherchent à protéger leur domicile ou leur entreprise.

De leur côté, les groupes d'attaquants étatiques seront facilement enclins à employer des outils plus complexes pour atteindre leurs buts, puisqu'ils disposent d'un budget beaucoup plus confortable. Cette possibilité ne doit certainement pas être sous-estimée ou ignorée. Les grandes organisations, en particulier celles chargées de protéger des secrets industriels ou des données personnelles de millions de clients, doivent particulièrement se méfier des pirates pour qui le financement n'est pas un problème. Inéluctablement, ces outils plus complexes vont finir par être récupérés par les opérateurs de malwares.

Les spécialistes de la sécurité qui souhaitent obtenir le meilleur retour sur investissement cherchent une protection aussi efficace que possible, tout en respectant un budget donné, tenant compte à la fois des ressources financières et humaines. Si les fournisseurs de produits de sécurité ont eux aussi des préoccupations budgétaires, le facteur le plus important pour eux est la nécessité d'optimiser les solutions offertes aux clients, afin que les produits détectent autant de menaces que possible, avec un coût minimal en termes de puissance de calcul et de maintenance manuelle.

Dans cette section, nous allons discuter de l'utilisation du machine learning, qui continuera d'être adopté, aussi bien par ceux qui s'attaquent aux systèmes informatiques, que par ceux qui les défendent. Nous allons aussi évoquer certaines des contraintes pratiques du machine learning, ainsi que le rôle toujours crucial des humains dans la création de nouveaux outils d'attaque et de défense.

Machine learning et défense

Tout système de machine learning digne de ce nom dispose de volumes élevés de données utiles.
Sans informations pour apprendre, les machines n'ont pas les matières premières nécessaires pour définir des règles efficaces de prise de décisions.

Les systèmes utilisés pour identifier les fichiers et comportements suspects peuvent désormais s'appuyer sur un contexte et un vocabulaire beaucoup plus riches pour décrire les comportements indésirables.

Les lecteurs assidus de WeLiveSecurity savent que les produits de sécurité exploitent l'automatisation et le machine learning *depuis un certain temps déjà.* Depuis plus de 20 ans, ces techniques jouent un rôle actif dans l'arsenal d'ESET et leur importance ne fera qu'augmenter avec le temps.

Dans le domaine de la lutte contre les malwares, cela fait plusieurs décennies que les chercheurs recueillent et échangent des données sur les menaces. Ainsi, nous pouvons optimiser notre capacité à protéger les consommateurs contre les comportements malveillants. Depuis presque aussi longtemps, nous discutons avec un grand nombre d'éditeurs de logiciels pour collecter des données sur l'état actuel des fichiers propres. Grâce à cela, nous disposons de très nombreuses informations historiques et mises à jour permettant de former les systèmes de machine learning. Nous pouvons donc leur apprendre à identifier les fichiers et comportements considérés comme suspects, ainsi que les attributs les plus susceptibles d'indiquer une intention neutre. Cela nous aide à détecter les fichiers et comportements problématiques, tout en limitant autant que possible les faux positifs.

Aux débuts de l'industrie anti-malware, l'essentiel du travail d'analyse des menaces était réalisé manuellement et la quantité d'informations stockées était assez limitée. Les premiers systèmes de machine learning s'appuyaient sur les attributs de malwares connus et de fichiers propres pour évaluer le caractère suspect de futurs échantillons.

L'augmentation du nombre de nouveaux programmes malveillants a conduit à automatiser une grande partie de l'analyse initiale. Ainsi, les chercheurs consacrent moins de temps à des tâches répétitives et peuvent mettre à profit leur expertise pour identifier et analyser les schémas existants au sein d'échantillons individuels ainsi qu'entre des variantes et des campagnes de malwares entières. Ces tâches automatisées ont considérablement augmenté la quantité et les types de données stockées sur le comportement d'échantillons individuels et ont donc amélioré notre compréhension des cybermenaces. Aujourd'hui, les systèmes utilisés pour détecter les fichiers et comportements suspects peuvent s'appuyer sur un contexte et un vocabulaire beaucoup plus riches pour décrire les comportements indésirables.

Les fonctionnalités des produits de sécurité continuent de s'enrichir et les spécialistes de la sécurité impliqués dans les échanges d'informations sont toujours plus nombreux et présentent des profils de plus en plus variés. Cette accumulation d'informations continue de renforcer à la fois le potentiel et la portée des données que les experts de la sécurité collectent sur l'évolution des logiciels malveillants.

Le machine learning participe depuis longtemps à la protection contre les malwares et autres menaces de sécurité. À l'avenir, nous devrions observer une multiplication constante des méthodes utilisées pour identifier un problème ou un comportement anormal, pas seulement au niveau du fichier, du système ou du réseau, mais aussi à l'échelle du Web tout entier.

Machine learning et attaque

Comme nous l'avons vu précédemment, la majorité des attaques de malwares sont aussi simples que possible ; inutile de chercher de nouvelles technologies ou techniques si les anciennes garantissent un flux régulier de revenus illégaux. Cette tendance va probablement perdurer, car de plus en plus d'individus sans éthique se lancent dans la cybercriminalité, attirés par les faibles frais d'entrée sur le marché. Si les gens ne changent pas radicalement leur perception de la sécurité et leurs comportements dans ce domaine, nous ne pourrons ignorer l'impact d'attaques contre d'anciennes vulnérabilités et failles de sécurité basiques, qui constituent des cibles faciles.

Comme il y a de plus en plus d'acteurs (notamment soutenus par des états) sur le marché de la cybercriminalité, certains hackers seront probablement tentés d'utiliser de plus en plus l'automatisation pour maximiser l'efficacité de leurs programmes. Les cybercriminels *effectuent déjà* des recherches automatisées pour trouver des machines et comptes en ligne vulnérables et collecter d'importants volumes de données disparates, en vue de s'en servir ultérieurement à des fins de reconnaissance ciblée. L'automatisation va sans aucun doute s'accentuer afin d'optimiser la rentabilité des initiatives malveillantes et faire en sorte que celles-ci soient mieux adaptées aux attaques d'ingénierie sociale.

Et comme les organisations criminelles constituent des bases de données de plus en plus fournies, ces dernières pourront être exploitées dans le cadre du machine learning afin de créer des règles d'attaque boostant l'efficacité des campagnes. À l'heure actuelle, trois principaux domaines d'application se distinguent pour le machine learning : l'acquisition de cibles, l'exploitation des victimes et la protection des ressources pour éviter les perturbations.

Aujourd'hui, l'automatisation des opérations de reconnaissance semble avant tout axée sur la recherche de cibles vulnérables. En enrichissant une base de données de cibles vulnérables
avec de meilleures informations, les hackers pourraient mieux cerner la valeur de chaque victime potentielle. Par exemple, au lieu de demander l'équivalent de quelques centaines ou milliers de dollars en cryptomonnaie pour une base de données qui en vaut plusieurs millions, ils pourraient plus aisément déterminer le montant maximal de la rançon que la victime serait disposée à payer. De plus, une meilleure reconnaissance pourrait permettre aux cybercriminels de récupérer l'intégralité des ressources de valeur d'une organisation et de ne plus se contenter de prendre la première chose qui leur semble intéressante.

L'ingénierie sociale a toujours posé problème aux criminels qui souhaitent s'attaquer à une cible choisie, étant donné le caractère international de leurs efforts.

Les hackers pourraient employer des traqueurs Web qui suivent les victimes d'un site à l'autre ou obtenir des informations auprès de courtiers en données pour établir des profils.

Nous avons tous déjà reçu des e-mails ridicules de phishing ou d'escroquerie à l'orthographe et à la grammaire douteuses ou qui ne ressemblaient en rien aux messages attendus d'un expéditeur donné. Si certaines campagnes de phishing et autres attaques frauduleuses parviennent bien mieux qu'avant à imiter des sources légitimes, la plupart d'entre elles ne trompent personne. Dans ce domaine, le machine learning pourrait générer des gains d'efficacité.

Pour reprendre l'exemple de la publicité ciblée, les criminels s'appuient sur un modèle améliorant l'efficacité de leurs communications. Même s'il est peu probable qu'ils aient autant de données que les entreprises qui suivent régulièrement les achats d'une population donnée, les hackers pourraient employer des traqueurs Web qui suivraient les victimes d'un site à l'autre ou obtenir des informations auprès de courtiers en données afin d'établir des profils. Cela pourrait permettre de personnaliser les tentatives de hameçonnage et de fraude et les rendre ainsi plus convaincantes.

D'un point de vue technique, l'approche la plus complexe (et donc la moins susceptible de voir le jour à court terme) consisterait à exploiter le machine learning pour protéger les infrastructures des pirates et leur permettre d'échapper plus efficacement aux systèmes de détection. Cela impliquerait avant tout de renforcer la résilience des structures de commande et contrôle des cybercriminels et de créer de nouvelles variantes de malwares.

Machine learning et « course à l'armement »

Depuis la découverte des premiers fichiers malveillants, créateurs de malwares et spécialistes de la sécurité se livrent à une course à l'armement. Le machine learning ne mettra pas fin à ce conflit. Si les ordinateurs peuvent prendre des décisions à la place des humains, il y a, et il y aura toujours, des limites à ce phénomène. Il doit toujours s'agir d'une relation d'assistance mutuelle, et non de délégation totale de notre responsabilité.

La créativité des développeurs (qu'ils soient bien ou mal intentionnés) nécessitera toujours l'intervention d'experts capables de voir lorsqu'une initiative sort largement des cadres antérieurs. Si les humains étaient complètement écartés du processus d'analyse dans le cadre de la défense, les hackers prendraient l'avantage.

De nombreux cybercriminels qui cherchent à s'enrichir disposent actuellement d'un processus d'acquisition de données qui favorise l'obsolescence rapide des informations, puisque les coordonnées de carte de paiement et informations de connexion ont tendance à ne pas être valables longtemps. Pourtant, ils commencent à s'intéresser à des catégories de données moins variables, telles que les données médicales et d'assurance, dont la valeur est plus durable. Puisqu'elles sont de plus en plus présentes, les bases de données risquent de devenir de plus en plus détaillées et pourraient donc présenter un intérêt croissant pour les personnes mal intentionnées. Ainsi, comme leurs propres ressources sont amenées à devenir moins variables et plus précieuses, les cybercriminels auront peut-être besoin de méthodes de protection plus avancées.

Ironiquement, cela pourrait avoir un impact sur l'actuelle course à l'armement, qui ressemblerait moins à un conflit entre un attaquant et une victime, mais à une guerre à armes égales.

En fin de compte, nous allons probablement observer une confirmation graduelle de tendances qui existent déjà : le machine learning sera de plus en plus prévalent et sophistiqué et servira à défendre des machines ; et les cybercriminels disposant de financements considérables seront de plus en plus nombreux, ce qui permettra d'intégrer leurs outils et techniques dans les malwares grand public. Si les victimes potentielles ne doivent pas ignorer la puissance et l'importance des systèmes de machine learning (car il serait peu probable que les hackers les ignorent), ces systèmes ne constituent absolument pas une panacée, pour une partie comme pour l'autre.

La cybercriminalité s'avère très lucrative pour la majorité des acteurs du secteur, qui n'ont même pas à élaborer d'outils ultra-modernes (cependant, nous gagnerons quand même à nous préparer à affronter des menaces plus redoutables). Compte tenu de la complexité des mesures de sécurité défensive, les humains continueront à avoir besoin d'ordinateurs pour identifier les fichiers et comportements suspects et les ordinateurs auront toujours besoin d'humains pour identifier de nouveaux types d'armes.

3

RGPD : LE PREMIER PAS VERS UNE LOI INTERNATIONALE SUR LE RESPECT DE LA VIE PRIVÉE ?

- La valeur de la confidentialité des données
- L'UE contre les États-Unis
- La multiplication des réglementations sur le respect de la vie privée

AUTEUR

Stephen Cobb
ESET Senior Security Researcher

RGPD : le premier pas vers une loi internationale sur le respect de la vie privée ?

Les entreprises et consommateurs préoccupés par la confidentialité des données personnelles à l'ère du numérique se souviendront de l'année 2018 en raison de l'entrée en vigueur du Règlement général sur la protection des données (RGPD) dans l'Union européenne (UE). Cette législation a déjà un impact fort sur la confidentialité numérique, non seulement dans l'UE, mais aussi aux États-Unis et dans d'autres pays. Cette tendance va influencer le secteur de la cybersécurité en 2019 et même au-delà.

Une évolution inévitable ?

La plupart des délégués à la protection des données ont entendu parler du RGPD bien avant son entrée en vigueur. Le texte final de ce règlement a été approuvé en 2015 et adopté en 2016. Suite à sa promulgation, les entreprises ont bénéficié d'un délai de mise en conformité de deux ans. C'est à la fin de cette période, le 25 mai 2018 (date que nous avons tous retenue), que l'UE a commencé à appliquer les dispositions de cette réglementation.

À ce moment-là, la plupart des entreprises américaines avaient au moins pensé au RGPD. Si vous avez assisté à des séminaires ou conférences consacrés au RGPD aux États-Unis en 2017, vous avez peut-être remarqué que la question la plus fréquemment posée par les organisations américaines était la suivante : le RGPD va-t-il nous impacter ? Pour des raisons que nous avons listées dans *un article de WeLiveSecurity en 2016*, la réponse était quasi invariablement « oui ».
Les entreprises doivent se conformer au RGPD si elles :

- surveillent le comportement de personnes concernées se trouvant dans l'UE ; ou
- sont basées hors de l'UE, mais fournissent des services ou des biens au sein de l'UE (y compris des services gratuits) ou :
- possèdent un « établissement » dans l'UE, indépendamment du lieu où sont traitées les données personnelles (p. ex. tout traitement dans le cloud effectué hors UE, pour le compte d'une entreprise située dans l'UE, est soumis au RGPD).

Logiquement, la deuxième question qui revenait le plus dans les discussions au sujet du RGPD aux États-Unis était : comment pouvons-nous l'éviter ? Les réponses des consultants d'entreprises telles que Deloitte, PwC et KPMG ont été unanimes : ne perdez pas de temps à essayer de contourner le RGPD. Préparez-vous à aligner les stratégies de données de votre organisation sur le RGPD, car où que vous soyez implanté, vous serez inévitablement confronté, à un moment ou un autre, à une initiative similaire.

La confidentialité des données, un enjeu majeur

Les premiers analystes à prévoir le déferlement de législations similaires au RGPD ont d'abord été accueillis avec scepticisme. Puis la California Consumer Privacy Act (CCPA) a été votée en 2018. Cette loi a été promulguée moins de 40 jours après l'entrée en vigueur du règlement européen. Elle affirme qu'en matière de gestion de leurs informations personnelles par des entreprises, les Californiens ont le droit :

Préparez-vous à aligner les stratégies de données de votre organisation sur le RGPD, car où que vous soyez implanté, vous serez inévitablement confronté, à un moment ou un autre, à une initiative similaire.

- de connaître la nature des données personnelles recueillies, acquises ou obtenues à leur sujet ;
- d'accéder aux données personnelles les concernant, détenues par une entreprise, ou de les transférer ou de les supprimer ;
- de savoir si leurs données personnelles sont vendues ou communiquées par l'entreprise, et si oui, à qui ;
- d'interdire à l'entreprise de vendre leurs données personnelles ;
- de bénéficier de services et de tarifs équivalents, même s'ils exercent leurs droits au respect de leur vie privée.

Si la CCPA inclut de nombreuses exceptions et limitations, elle constitue un tournant majeur en matière de respect de la vie privée dans les Amériques.

Bien que la Californie ne soit que l'un des états constituant les États-Unis d'Amérique, elle serait la *cinquième puissance économique mondiale* si elle était indépendante (juste derrière l'Allemagne, le Japon, la Chine et le reste des États-Unis). Elle jouit donc d'une grande influence en termes de lois et de pratiques commerciales.

dans ce domaine. La Charte des droits fondamentaux de l'UE mentionne explicitement le droit à la protection des données à caractère personnel et interdit de collecter ou d'utiliser des informations personnelles sur des résidents de l'UE sans que ces derniers aient été avertis et aient donné leur autorisation.

Aux États-Unis, le droit constitutionnel au respect de la vie privée n'existe pas. Ainsi, les entreprises peuvent recueillir et utiliser des informations sensibles vous concernant, sauf si une loi ou une action en justice disent le contraire. Voici un exemple des implications de cet état de fait :

> Vous créez une entreprise qui propose des services de transport via une application comme Uber. Votre entreprise recueille des données sur les utilisateurs du service, telles que leur nom et les détails de leur voyage. Si votre entreprise opère dans l'UE, il y a des lois qui restreignent l'utilisation de ces données, même s'il n'existe aucune loi relative au respect de la vie privée, spécifique aux services de transport.

Deux approches différentes de la confidentialité

Pour comprendre en quoi l'adoption par la Californie de mesures de protection des données personnelles similaires à celles du RGPD peut jouer un rôle en matière de respect de la vie privée en 2019, nous devons examiner les approches que l'UE et les États-Unis ont employées jusqu'à présent

Aux États-Unis, les options qui s'offrent à votre entreprise de services de transport concernant le traitement des données dépendent d'un certain nombre de facteurs, tels que le lieu où votre entreprise a été constituée en société et les zones où elle opère. Mais dans la plupart des cas, vous pouvez en faire ce que vous voulez. Cette situation peut perdurer jusqu'à ce qu'un procès ou *une loi relative au respect de la vie privée* viennent réglementer l'utilisation des données personnelles recueillies par les entreprises de services de transport.

En d'autres termes, la protection accordée par les États-Unis aux données à caractère personnel varie selon leur type, selon la façon et le moment où elles ont été créées. Par exemple, la Video Privacy Protection Act de 1988 a été rédigée et adoptée dans les jours qui ont suivi la publication dans un journal de l'historique de location de vidéos d'un candidat à la Cour suprême.

Aux États-Unis, les dispositions qui protègent la vie privée découlent des lois fédérales, de la législation de l'état ou de décisions judiciaires au niveau de l'état ou du gouvernement fédéral. (Pour plus de détails sur la loi américaine relative au respect de la vie privée, consultez le livre blanc ESET : *« Data privacy and data protection: US law and legislation »* [« Protection et confidentialité des données : législations et lois en vigueur aux États-Unis »]).

Dans l'UE, les données qui vous concernent et permettent de vous identifier sont, par défaut, protégées dès leur création. C'est la définition pratique de l'expression « protection des données » selon l'usage européen. Toute personne souhaitant recueillir des données vous concernant doit légalement obtenir votre accord et est tenue de contrôler de façon stricte l'accès à vos données et leur utilisation, une fois votre accord obtenu. Cela vaut pour tous les nouveaux types de données à caractère personnel qui apparaissent. Ainsi, vous n'avez pas à attendre un procès ou un incident politique embarrassant.

Le raz-de-marée des réglementations sur le respect de la vie privée

En l'absence de loi fondatrice sur la confidentialité des données aux États-Unis, comment un seul état peut-il changer la donne en matière de protection de la vie privée ? Tout est question de richesse, d'influence et de volonté. La Californie est le plus riche état américain et peut se permettre de proposer des droits qui seraient plus difficiles à faire accepter ailleurs. Cela ouvre la voie à d'autres états, dont les résidents souhaiteront probablement bénéficier d'une meilleure protection de la vie privée, à l'instar des Californiens. Aujourd'hui déjà, beaucoup d'Américains aimeraient se voir octroyer les droits garantis aux Européens par le RGPD.

En matière de respect de la vie privée, l'histoire joue également un rôle : le premier pas vers la CCPA de 2018 date de 1972. Cette année-là, les électeurs de Californie ont voté l'amendement de la constitution de l'état pour rajouter le respect de la vie privée à la liste des droits « inaliénables » de toutes les personnes (outre la constitution fédérale, chaque état a sa propre constitution). À peine quelques années plus tard, en 1977, l'état a promulgué l'Information Practices Act, qui limitait la collecte, la gestion et la diffusion d'informations personnelles par les organismes d'état. Cette initiative était motivée par l'augmentation du traitement des données au sein des ministères.

Vingt-cinq ans après, en 2002, lorsque les business models reposant sur Internet ont entraîné une extension de la collecte d'informations personnelles et une multiplication des risques de divulgation non autorisée, la Californie a adopté la première loi étatique imposant le signalement des violations de données. Faisons un saut dans le temps pour nous retrouver en 2018. Aujourd'hui, chacun des 50 états américains comporte une loi similaire dans son arsenal législatif. Ainsi, il est plus que probable que de nouvelles mesures de protection des données s'inspirant du RGPD et de la CCPA voient voir le jour à travers les États-Unis.

Pourtant, certains facteurs pourraient entraver la concrétisation de cette prévision. En effet, divers lobbies luttent actuellement pour amender la CCPA avant son entrée en vigueur en 2020. Pour contrecarrer leurs efforts, les défenseurs du respect de la vie privée maintiennent la pression sur les législateurs (le mouvement pro-CCPA a son propre site Web, une stratégie qui pourrait facilement être adoptée dans d'autres états).

Les entreprises qui pensent que la loi leur

Il est difficile de réduire le droit au respect de la vie privée et à la protection des données à « une simple anomalie » européenne, alors que l'état américain où siègent des géants du numérique comme Google, Facebook, Apple, HP et Oracle a promulgué une loi allant dans le même sens.

nuira sont confrontées à un défi de taille : convaincre les consommateurs/électeurs qu'ils n'ont pas besoin de mesures de protection de la vie privée aussi strictes que dans d'autres pays. Il est difficile de réduire le droit au respect de la vie privée et à la protection des données à « une simple anomalie » européenne, alors que l'état américain où siègent des géants du numérique comme Google, Facebook, Apple, HP et Oracle a promulgué une loi allant dans le même sens. Ces sociétés exercent à l'international et la tendance mondiale suit clairement l'orientation définie par le RGPD en matière de protection de la vie privée.

Le plus grand pays d'Amérique latine, le Brésil, a adopté une nouvelle Loi générale sur la protection des données (LGPD) en 2018, pour remplacer un cadre sectoriel semblable à celui dont disposent actuellement les États-Unis. Selon *des analystes juridiques internationaux*, la « LGPD brésilienne fait écho à de nombreux aspects du RGPD ». En outre, cette loi aidera le Brésil à obtenir « une décision d'adéquation de la part de la Commission européenne, *comme cela a été le cas pour le Japon.* » Car effectivement, une autre grande économie, le Japon, devrait prochainement offrir des niveaux de protection de la vie privée équivalents à ceux dont jouissent les citoyens européens. La Chine emprunte également le même chemin. Même si la question de la censure sur Internet *complique la situation,* le fait que l'un des principaux sous-traitants mondiaux de données acquière les capacités et la technologie nécessaires pour gérer les données conformément au RGPD est très révélateur.

Deux approches différentes de la confidentialité

Fondamentalement, la cybersécurité vise notamment à contrôler l'accès aux informations afin qu'elles ne soient pas divulguées de façon non autorisée. Parallèlement, la réglementation sur le respect de la vie privée a entre autres pour but d'influencer la définition du concept de « divulgation non autorisée » en matière de données personnelles, puis de définir les sanctions encourues par les entreprises à l'origine d'une telle bévue. Par conséquent, il est possible qu'une violation de données ne se contente pas d'ébranler la confiance que les individus accordent à une organisation. Comme nous le verrons dans la section *« Respect de la vie privée »*, ce type d'incident peut également s'avérer coûteux s'il entraîne une violation des réglementations relatives au respect de la vie privée (ce qui peut être le cas s'il est mal géré).

En octobre 2018, le *Contrôleur européen de la protection des données* a annoncé que les premières amendes liées au RGPD pourraient, « dans certains cas, être imposées d'ici la fin de l'année ». À peu près au même moment, la Commission irlandaise pour la protection des données a commencé à enquêter sur Facebook. En cause : une violation des données *« pouvant faire l'objet d'une amende allant jusqu'à 1,63 milliard de dollars ».* Alors que les effets du RGPD se concrétisent, nous prévoyons qu'en 2019, de nombreuses entreprises vont activement se préparer en vue d'être conformes à la CCPA ou à toute autre loi similaire.

4

RESPECT DE LA VIE PRIVÉE : LE NOUVEAU MOTEUR DE RÉUSSITE DES ENTREPRISES ?

- Des millions de personnes exposées
- suite à des vulnérabilités et des bugs
- Le cas Facebook
- De nouveaux modèles de confidentialité

AUTEURS

Lysa Myers & Stephen Cobb

ESET Senior Security Researchers

Respect de la vie privée : le nouveau moteur de réussite des entreprises ?

Le nombre de personnes dont la confidentialité numérique a été remise en cause par un incident de sécurité des données en 2018 a probablement dépassé la barre des deux milliards avant même la fin du troisième trimestre. Si ce chiffre semble impressionnant, rappelez-vous qu'à elles seules, cinq organisations avaient déjà compromis près de 1,8 milliard d'enregistrements avant la fin du premier semestre : *Aadhaar*, *Exactis*, *Under Armour*, *MyHeritage* et *Facebook*. Ainsi, les statistiques pour 2018 pourraient être inférieures à celles de 2017 (7,8 milliards d'enregistrements) ou même au précédent record de 2016 (6,3 milliards d'enregistrements).

En étudiant les événements de l'année 2018, il ressort que de nombreux incidents liés au respect de la vie privée ne correspondent pas exactement à la définition classique du terme de « violation ». Nous avons généralement tendance à associer la violation de données à l'intrusion d'un pirate dans un système, dans l'espoir de dérober des informations. Pourtant, certains problèmes de confidentialité apparus en 2018 n'ont pas été clairement l'œuvre de hackers. Certains découlaient de vulnérabilités ou de bugs permettant un accès non autorisé, comme ceux qui ont mis en péril *les comptes de 90 millions d'utilisateurs* de Facebook ou de plus d'un demi-million d'utilisateurs de *Google* (cet incident ayant contribué à l'arrêt de cette plateforme).

Certains autres résultaient de produits ou services fonctionnant comme prévu et conformément aux accords de licence, mais se révélant cauchemardesques du point de vue de la confidentialité. Deux exemples illustrent parfaitement ce type de cas : *le scandale Facebook-Cambridge Analytica* et le *VPN espion Onavo*, promu par le réseau social. Les conséquences imprévues du partage de données agrégées ont fait les gros titres dès le début de l'année 2018, avec *les déboires de la carte d'activités de Strava.* Dans ce contexte, quelles sont les implications pour 2019 ? La réponse dépendra en grande partie de deux acteurs majeurs : Facebook et Google. À elles deux, ces sociétés ont constitué de gigantesques bases d'utilisateurs et accumulé des volumes impressionnants de données personnelles sur ces derniers. Il est essentiel que ces ressources soient protégées contre tout accès non autorisé. Les gens se demandent aujourd'hui si ces sociétés sont devenues *« trop grosses pour faire faillite ».*

Facebook et Google ont mis au point des plateformes extrêmement puissantes, qui permettent de mettre en contact un grand nombre de personnes, en vue de partager et de diffuser des informations, à bon et à mauvais escient. En conséquence, beaucoup de personnes dépendent des produits de ces deux géants du Web. Si certaines initiatives de ces plateformes représentent un risque ou un danger trop important pour certains utilisateurs, ces derniers se retrouvent isolés.

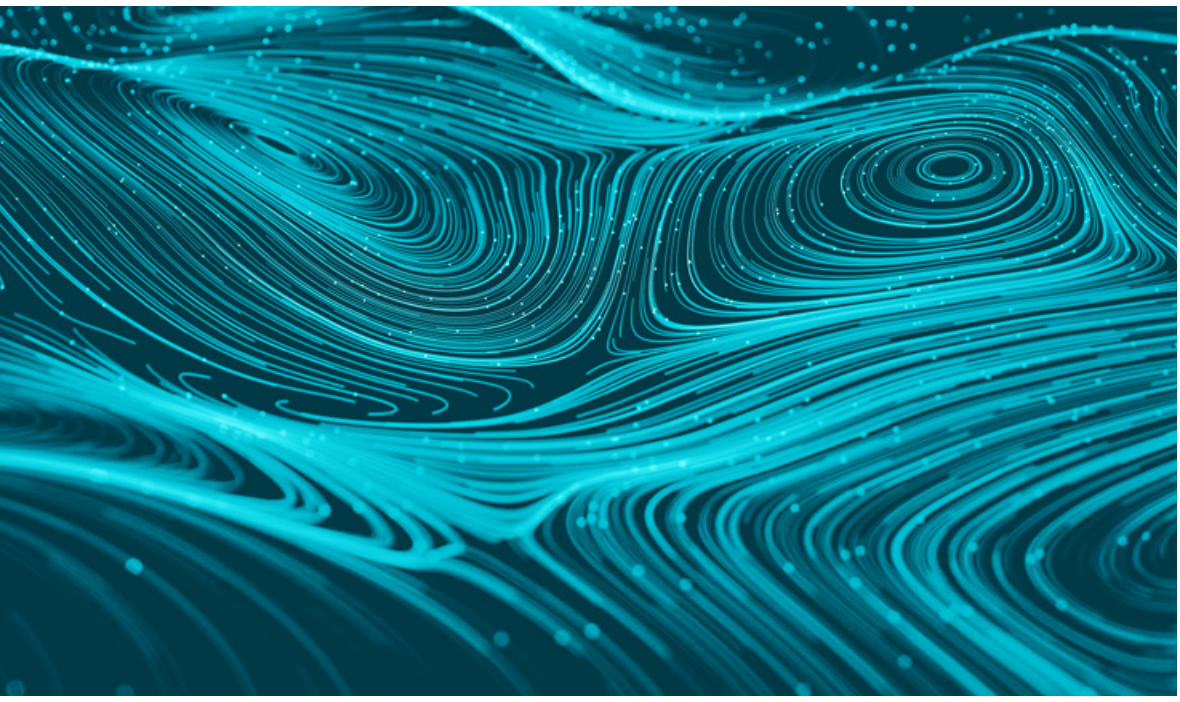
En d'autres termes, d'un point de vue social, choisir de ne pas utiliser une fonctionnalité offerte par Facebook ou Google reviendrait à s'éloigner de la vie moderne. Bien qu'il soit théoriquement possible de se passer complètement de ces deux outils, une telle initiative constituerait, à l'heure actuelle, un véritable frein dans la vie quotidienne, aussi bien personnelle que professionnelle. À tel point que pour la plupart des gens, le jeu n'en vaudrait pas la chandelle.

Les géants du Web vont-ils de l'avant ou visent-ils trop haut ?

Le nombre d'utilisateurs de Facebook reste colossal, malgré les deux grosses bévues de l'entreprise en matière de confidentialité des données en 2018. Cependant, les sentiments de nombreux utilisateurs se sont émoussés et ce phénomène est difficile à analyser à l'aide de statistiques. Alors que Facebook devrait être un outil incroyable pour rencontrer des gens et partager des histoires avec sa famille et ses amis, pour certains, il s'agit d'un réseau que l'on ne peut pas quitter sans perdre le contact avec son entourage.

Un certain nombre d'études récentes ont présenté une baisse de l'utilisation de Facebook, de ses taux d'engagement et de ses revenus publicitaires, ce phénomène s'étant accéléré ces dernières années. Pourtant, une étude approfondie de ces informations révèle des nuances de taille. Par exemple, alors que le nombre de personnes utilisant le service via un navigateur Web diminue, le nombre d'utilisateurs de l'application mobile progresse. De même, si les gens consacrent moins de temps et d'argent à Facebook, ils dépensent plus sur des plateformes appartenant à Facebook, comme Instagram, WhatsApp et Messenger. Même si Facebook peut laisser un goût amer à certains utilisateurs, ces derniers n'abandonnent pas pour autant complètement l'écosystème Facebook.

Ainsi, le lancement du Facebook Portal fin 2018 pourrait être un test intéressant pour mesurer l'opinion publique à l'égard de la société en 2019. En matière de respect de la vie privée, l'arrivée des assistants virtuels peut être décrite, au mieux, comme une opportunité discutable. Lorsque nous installons chez nous un appareil dont le microphone est toujours activé, nous pouvons légitimement nous attendre à ce que notre vie privée soit protégée.
Les assistants virtuels des enceintes connectées les plus populaires (Alexa, Google, Siri et Cortana) existent depuis plusieurs années et sont bien implantés sur le marché. Ils ont été testés, approuvés et sont plébiscités par les consommateurs qui les considèrent probablement comme des outils assez fiables. En 2019, Facebook Portal va devoir relever un défi de taille : gagner la confiance des consommateurs en dépit des récents incidents de confidentialité du réseau social. D'ailleurs, plusieurs analystes ont fait remarquer qu'en



Dans ce contexte, si les gens consacrent moins de temps et d'argent à Facebook, ils dépensent plus sur des plateformes appartenant à Facebook, comme Instagram, WhatsApp et Messenger.

lançant un système de surveillance à peine quelques jours après la compromission de millions de comptes utilisateur, Facebook semblait faire la sourde oreille aux inquiétudes de ses utilisateurs en matière de respect de la vie privée.

Si Facebook commence réellement à s'essouffler, le problème vient peut-être du fait que l'entreprise continue à exploiter la dépendance des utilisateurs vis-à-vis de sa plateforme, sans se rendre compte qu'elle est en train de perdre leur confiance.

Nous savons depuis longtemps que les violations et autres atteintes à la vie privée peuvent avoir de graves conséquences financières, même sur de très grandes entreprises. Il suffit de suivre le cours des actions d'une entreprise cotée en bourse à l'annonce d'un tel incident. Les actions de la société d'évaluation de cotes de crédit Equifax (qui dispose d'une mine d'informations personnelles) ont chuté de 30 % suite au piratage dont elle a été victime en 2017. Un an après, l'entreprise ne s'est toujours pas complètement remise des pertes qu'elle a subies pendant cette période. Facebook se trouve dans une position légèrement différente, car ses clients ne sont pas ses utilisateurs, mais ce sont les annonceurs. Ceci étant, la méfiance des utilisateurs peut avoir des répercussions si les annonceurs Facebook constatent que la plateforme n'est plus aussi rentable qu'avant pour promouvoir leurs produits.

Diversité défensive et nouveaux modèles de confidentialité

La clientèle des entreprises qui s'immiscent dans notre quotidien se rapproche d'un public captif. En 2019, les méga-entreprises vont-elles enfin nous prouver qu'elles ont suffisamment pris au sérieux la question de la confidentialité pour qu'il n'y ait pas d'incident dans ce domaine ? La réponse n'est pas claire, mais il ne fait aucun doute qu'en 2018, de nombreuses personnes se sont rendu compte que lier l'ensemble de leur existence sur Internet à une méga-entreprise représentait un danger.

Il est possible qu'en 2019, de plus en plus de gens cherchent des alternatives aux outils dominants actuels, en vue de diversifier leur écosystème en ligne. Cette diversification présente deux principaux avantages : le maintien de la « biodiversité » numérique et de « zones » numériques distinctes. Mettre en place un flux d'informations transparent entre chaque personne et entité connectée ou utiliser les identifiants d'une seule plateforme pour accéder à tous ses comptes en ligne peut sembler idéal. Cependant, les inconvénients de telles pratiques peuvent être difficiles à prévoir et sont potentiellement considérables.

Prenons l'exemple de la banane. La banane Cavendish est tellement omniprésente que la plupart des gens qui entendent le mot « banane » pensent immédiatement au clone jaune standard que tout le monde connaît. Les bananes achetées en Finlande et en Floride sont génétiquement identiques. Mais pour combien de temps ?

Les bananes Cavendish sont menacées par le champignon qui a déjà eu raison de la variété Gros Michel. Les bananes vendues en supermarché sont fragiles : l'absence de diversité génétique ne permet pas aux plantes de résister aux maladies et autres catastrophes naturelles. Une fois qu'une zone est infectée par le champignon pathogène, ce dernier reste dans le sol pendant plus de trois décennies, à tel point que les bananes ne peuvent plus y être cultivées. Seul l'établissement de procédures de biosécurité a permis de préserver la viabilité des cultures de bananes Cavendish. Pour cela, les différentes plantations ne sont pas seulement séparées géographiquement, elles le sont aussi sur le plan microbien.

Par comparaison, étudions le sort des grenouilles et crapauds touchés par *le champignon chytride*. Différentes populations d'amphibiens dans le monde ont été affectées de la même manière par un champignon souvent transporté par l'homme. Là encore, les scientifiques craignaient que cet agent pathogène ne décime des espèces dans le monde entier, si la progression de la menace n'était pas stop-

Il est possible qu'en 2019, de plus en plus de gens cherchent des alternatives aux outils dominants actuels, en vue de diversifier leur écosystème en ligne.

pée. Comme ces grenouilles ne sont pas des clones et sont génétiquement différentes, divers gènes leur permettent de s'adapter. Les populations de grenouilles et de crapauds ont donc commencé à développer une résistance à cette maladie ; aujourd'hui, certains individus infectés survivent.

Face à une menace, une population ou un écosystème homogènes - que ce soit dans le monde des molécules et des microbes ou dans le domaine des chiffres et des données - présentent un risque de contagion élevé. Si nous diversifions notre écosystème numérique, à la fois individuellement et en tant que population, nous réduirons les risques et faciliterons la résolution des problèmes. Par exemple, si nous utilisons l'authentification unique pour nos comptes en ligne, ces derniers risquent tous d'être compromis en cas de menace au sein de cet environnement. Même s'il est moins pratique de mettre nos œufs dans différents paniers, nos pertes seront limitées si l'un de ces paniers se renverse.

Résumé

En 2019, alors que les outils qui se sont révélés non sécurisés vont être de plus en plus délaissés, nous observerons peut-être une plus grande diversité de plateformes, ainsi qu'une poursuite de la baisse des taux de confiance et d'engagement des plateformes existantes. Nous pourrions même assister au déclin de certaines entreprises et/ou offres de produits, en raison de préoccupations liées à la confiance et au respect de la vie privée. Par ailleurs, tout au long de l'année, gardez en tête que les craintes des consommateurs ne sont pas le seul facteur qui influence les questions de confidentialité. Reprenons les scénarios de risques réglementaires décrits dans *la section consacrée au RGPD*. Il est possible qu'en 2019, le RGPD ne soit pas la seule source de sanctions pour les entreprises, en cas de non-respect de la vie privée. Des lois similaires ont déjà été récemment adoptées au *Brésil* et en *Californie* et il est peu probable que le phénomène en reste là.

5

ASSISTANTS CONNECTÉS : DES APPAREILS AUX DANGERS TOUJOURS EN VEILLE

- Maintien du rythme des attaques
- Alignement de la praticité d'utilisation et de la sécurité
- Progression de la sécurisation des données

AUTEUR

Camilo Gutiérrez Amaya

ESET Senior Security Researcher

Assistants connectés : des appareils aux dangers toujours en veille

Réfléchissez aux appareils électroniques que vous utilisez au quotidien. Lesquels sont les plus importants pour vous ? Avez-vous pensé à votre routeur ou modem Internet ? Ces petites boîtes noires cachées dans un coin jouent désormais un rôle critique et sont maintenant aussi importantes que nos ordinateurs ou téléphones portables pour les activités nécessitant une connectivité Internet.

Pourquoi ? Outre le fait qu'ils nous permettent d'accéder à Internet, ces appareils transmettent une grande partie voire la totalité de nos données sensibles. Ainsi, s'ils ne sont pas mis à jour correctement, ils peuvent être exploités par des cybercriminels, qui peuvent s'en servir pour compromettre d'autres périphériques connectés. En un mot, une fois compromis, ces systèmes peuvent se transformer en plateforme d'attaque permettant d'accéder à d'autres appareils sur le même réseau.

Cependant, ces dispositifs ne sont pas les seuls à collecter des informations provenant d'autres équipements électroniques. Récemment, *les assistants virtuels* (assistants connectés ou assistants vocaux) ont commencé à gagner en popularité. Comme ils sont connectés à différents périphériques qu'ils peuvent contrôler (par exemple : éclairage intelligent, capteurs, caméras et même des appareils ménagers), ils entraînent une extension du réseau des dispositifs interconnectés et de la surface d'attaque.

Selon un rapport d'IDC (International Data Corporation), le nombre d'appareils intelligents connectés à Internet devrait *atteindre 80 milliards d'ici 2020*. En 2019, nous nous attendons à une augmentation proportionnelle du nombre d'attaques. Ces dernières s'appuieront sur diverses méthodes, allant des scripts automatisés ciblant les vulnérabilités des appareils connectés, aux exploits conçus pour en prendre le contrôle. Les routeurs et assistants connectés étant les équipements qui interagissent le plus avec les autres appareils intelligents et avec le Web, ils constituent des proies de choix pour les pirates.

L'augmentation des attaques

Malheureusement, il n'est pas possible de prévoir avec exactitude l'ampleur de l'augmentation des attaques en 2019. Cependant, il est certain que les plus spécifiques d'entre elles vont se multiplier, comme l'illustre le botnet de spam, *BCMUPnP Hunter*. Apparu alors que cet article était en cours de préparation pour la publication, il regroupe 100 000 dispositifs et exploite une vulnérabilité découverte il y a 5 ans dans les puces Broadcom utilisées dans au moins 116 modèles d'appareils. Nous pouvons aussi nous attendre à des attaques plus variées visant les dispositifs fonctionnant en *hubs*, comme les routeurs ou les assistants connectés. Ces équipements peuvent permettre à un pirate d'accéder à un réseau entier, ainsi qu'à tous les autres périphériques connectés à ce réseau et, surtout, aux données qu'ils gèrent.

Nous ne devons pas oublier que, ces dernières années, les routeurs ont été victimes de différents types d'attaques, comme le « botnet Carna » qui cherchait à effectuer *un recensement du Web en 2012*, ainsi que d'autres événements de moindre envergure qui se sont produits avant la création de Mirai. En fait, Carna a en quelque sorte été le précurseur du *botnet Mirai*. Même s'il ne partageait pas les intentions malveillantes de ce dernier, Carna a réussi à exploiter divers appareils tels que des routeurs SOHO. Le cas du botnet Mirai est sans doute l'un des plus emblématiques. Reposant principalement sur des objets connectés compromis (il a infecté 600 000 appareils dans le monde), il a servi à mener des dizaines de milliers d'attaques DDoS et *notamment l'une des plus importantes de l'histoire*, celle qui a touché les

serveurs de Dyn en octobre 2016, entraînant l'interruption de services populaires comme Twitter, Netflix, Spotify, et PayPal, ainsi que plusieurs médias aux États-Unis et en Europe. Des études menées récemment sur les assistants vocaux ont démontré qu'il était possible d'envoyer *des commandes cachées, inaudibles par l'oreille humaine*, à des assistants tels que Siri (Apple), Alexa (Amazon) ou l'Assistant Google. Ces commandes peuvent demander aux systèmes de passer de coûteux appels internationaux, d'ouvrir des sites Web ou de contrôler d'autres équipements (changer le réglage du thermostat, etc.), sans que l'utilisateur ne s'en rende compte.

Si bon nombre de ces recherches ont été lancées dans le cadre de démonstrations de faisabilité, elles prouvent qu'il est possible pour un pirate de déverrouiller des appareils, d'effectuer des virements bancaires ou de faire des achats en ligne, simplement en cachant des messages malveillants au cours de la lecture d'un fichier audio normal.

À l'avenir, nous allons donc devoir relever un défi complexe : protéger ces hubs à l'ère du tout connecté. Par exemple, si l'un de ces composants était défaillant ou servait de plateforme dans le cadre d'une attaque, cela pourrait conduire à la compromission d'informations sur de nombreux périphériques.

Si les appareils intelligents sont appréciés en raison de leur praticité et de leur convivialité, ils peuvent également servir de porte d'entrée aux menaces. Alors que l'utilisation d'un assistant connecté regroupant et contrôlant plusieurs objets IoT ne cesse de progresser, les risques pour notre sécurité et notre vie privée se multiplient. Nous ne devons pas oublier que si la technologie évolue, il en va de même de la stratégie et du comportement des cybercriminels.

L'équilibre entre sécurité et convivialité

Si vous possédez déjà des appareils intelligents ou que vous envisagez d'en acheter, vous devez évaluer les nouveaux risques de sécurité potentiels auxquels vous vous exposez. En février 2018, des chercheurs d'ESET ont publié *un rapport analysant douze appareils connectés populaires, disponibles à la vente.* L'étude a révélé diverses vulnérabilités (dont certaines étaient sérieuses) et chacun des dispositifs passés au crible présentait des lacunes en termes de protection de la vie privée, la plus grande inquiétude étant liée au comportement des assistants intelligents. Par conséquent, il est important de se pencher sur les fonctionnalités offertes par chaque appareil et fabricant, afin de trouver un équilibre juste entre convivialité, facilité d'utilisation et sécurité.

Si les appareils intelligents sont appréciés en raison de leur praticité et de leur convivialité, ils peuvent également servir de porte d'entrée aux menaces.

Donc, si vous songez à acheter une solution Alexa (enceintes Amazon, Facebook Portal ou autres périphériques tiers), un Google Home, un HomePod d'Apple ou tout autre service similaire au cours des 12 mois à venir, vous devez impérativement vous renseigner sur les données personnelles que collectent et partagent ces appareils pour trouver la solution la mieux adaptée à vos besoins et exigences en matière de respect de la vie privée.

Les attaques qui sévissaient jusqu'à présent sur Internet vont désormais viser des appareils présentant des fonctionnalités de sécurité minimales. Dans cette optique, il est nécessaire d'examiner chacun des aspects de ces appareils, de leur emplacement physique aux modèles choisis, en veillant à ce qu'ils disposent de solides capacités de chiffrement et d'authentification. Ces mesures doivent être prises au sérieux, car nous sommes encore loin d'avoir des normes de sécurité pour l'IoT.

Il ressort clairement de ce rapport qu'en 2019, les menaces technologiques auxquelles nous serons confrontés seront assez complexes. Si les scénarios évoqués soulèvent un grand nombre de préoccupations autour de la sécurité et du respect de la vie privée, en tant qu'utilisateurs, nous devons agir maintenant et ne pas laisser le soin aux industriels de régler ces problèmes à notre place.

Les données au cœur de la sécurité

Concernant les équipements tels que les assistants connectés, sur quoi devrions-nous axer notre stratégie de sécurité en 2019 ? Avant tout, il faut connaître les données recueillies et échangées par ces appareils : informations d'identité, données permettant d'accéder à des profils en ligne, informations financières et toute donnée potentiellement sensible, de manière générale. Compte tenu de la variété des dispositifs, technologies, protocoles et fournisseurs existants, l'adoption d'un ensemble standardisé de mesures de sécurité semble bien lointaine. De fait, ce processus prendra du temps et aucune norme de ce type ne sera mise en œuvre en 2019.

D'ici là, les fabricants doivent donc s'efforcer d'implémenter des politiques de sécurité au sein de la couche d'application de leurs produits, pour renforcer la protection et la confidentialité des données. S'ils s'y refusent, les attaques dans lesquelles du code est injecté pour exploiter des vulnérabilités se multiplieront. En outre, les attaques qui sévissaient jusqu'à présent sur Internet vont désormais viser des appareils présentant des fonctionnalités de sécurité minimales.

Et pour la suite ?

À l'heure actuelle, nous observons une extension de la surface d'attaque. Dans certains cas, des cybercriminels ont accédé à des systèmes utilisant un large éventail de technologies et de protocoles de communication. Parallèlement, l'année 2019 sera émaillée de menaces s'appuyant sur différents vecteurs d'attaque et profitant de la diversité des options disponibles.

Nous avons déjà vu des hackers se servir d'objets connectés pour lancer des attaques par déni de service (DoS). Alors que ces équipements prennent de plus en plus de place dans notre quotidien, les pirates continueront d'explorer leurs caractéristiques afin de découvrir d'autres vulnérabilités (ils l'ont déjà fait pour les thermostats, les systèmes de vidéosurveillance, les jouets pour enfants, les véhicules, etc.)

En outre, les attaques qui sévissaient jusqu'à présent sur Internet vont désormais viser des appareils présentant des fonctionnalités de sécurité minimales.

et de les utiliser pour concevoir diverses menaces (escroqueries, ransomwares et cryptomining), diffusées via ces appareils. Compte tenu de l'adoption de plus en plus massive des cryptomonnaies et du nombre croissant de périphériques connectés à Internet, les appareils intelligents pourraient servir de porte d'entrée aux pirates et leur permettre de créer des fermes de cryptomining.

Certains s'inquiètent de cette situation et ont déjà commencé à agir. Par exemple, *la Californie a récemment adopté une nouvelle loi* exigeant qu'à partir de 2020, tous les objets connectés vendus sur le marché soient configurés par défaut avec des mots de passe uniques.

À la lumière de ces problèmes de sécurité décourageants, nous devons, en tant qu'utilisateurs, nous renseigner sur les dispositifs que nous achetons et les fonctionnalités proposées par les fabricants. Mais surtout, nous devons apprendre à utiliser la technologie en toute sécurité. De fait, il est tout à fait possible que des fabricants prêts à tout pour doper leurs ventes commercialisent des produits présentant des vulnérabilités et augmentent ainsi leur risque d'exposition. Dans ce contexte, prendre conscience des risques est le meilleur moyen de se préparer, pour pouvoir ensuite prendre des mesures en vue de protéger les appareils et les informations transmises.

CONCLUSION

2018 aura permis de mettre en avant l'importance de la confidentialité des données. À titre d'exemple, les révélations concernant la mauvaise gestion des données utilisateur de Facebook par Oxford Analytica et l'entrée en vigueur du Règlement général sur la protection des données (RGPD) ont largement contribué à la médiatisation de la confidentialité et de la sécurité des données.

Tout au long de ce rapport, nous avons souligné la criticité des données client pour les entreprises, les particuliers, les entités qui protègent ces données, mais aussi les cybercriminels.

Comme nous l'avons vu, l'évolution des menaces reflète l'évolution de la technologie et des habitudes des utilisateurs d'outils informatiques. Tout comme les responsables marketing cherchent à mieux comprendre le comportement en ligne de leurs prospects afin de mieux personnaliser les publicités, les cybercriminels vont probablement commencer à utiliser des technologies telles que le machine learning pour recueillir des données pouvant être ensuite utilisées afin de concevoir des campagnes d'ingénierie sociale plus personnalisées et donc plus convaincantes.

À l'ère du numérique, chacune de nos actions sur Internet laisse des traces. Alors que les incidents liés au respect de la vie privée vont sans aucun doute se multiplier et affecter aussi bien les entreprises que les particuliers, la mise en œuvre du RGPD est une lueur d'espoir, d'autant plus que des initiatives similaires ont vu le jour dans différents pays et régions à travers le monde. En outre, si le RGPD a soulevé beaucoup de questions pour les entreprises, en particulier hors UE, les événements dont nous avons été témoins cette année semblent avoir provoqué un changement d'état d'esprit, impossible jusqu'alors.
Cela suffira-t-il ? Probablement pas.

L'émergence de nouvelles réglementations de protection des données va constituer un nouveau défi : comment les nouvelles normes de chaque région ou pays vont-elles coexister, sachant que par nature, Internet ne tient pas compte des frontières géographiques ? Et que se passera-t-il en cas de conflit entre deux législations ou en cas de scénarios imprévus, non couverts par les règlements en vigueur ? Il est nécessaire d'établir des règles et de mettre en place un système pour suivre l'apparition de nouvelles exigences et anticiper les changements, afin de pouvoir actualiser les réglementations au fil du temps. Il est temps que les entreprises et les gouvernements démontrent leur engagement et ne s'en remettent pas uniquement aux entreprises de sécurité et aux propriétaires individuels d'équipements informatiques, comme c'est le cas actuellement.

Alors que les progrès technologiques s'accompagnent d'une extension de la surface d'attaque, il va falloir sensibiliser divers publics à la question de la sécurité informatique, dans divers domaines. Aujourd'hui, l'interconnectivité est omniprésente et tous les services sont reliés dans le cloud. Ainsi, assistants connectés, routeurs et autres appareils intelligents peuvent servir de porte d'entrée pour dérober des informations et un site Web peut être infecté par un code malveillant pour miner des cryptomonnaies. Plus que jamais, les consommateurs doivent veiller à utiliser la technologie de façon responsable et prudente, non seulement pour

savoir comment se protéger, mais aussi pour connaître les risques et responsabilités liés au téléchargement d'informations personnelles dans le cloud, ainsi que les informations qu'ils fournissent et partagent avec des services en ligne légitimes.

Parallèlement, organisations, entreprises et fabricants vont devoir eux aussi apporter leur pierre à l'édifice, s'ils ne veulent pas perdre la confiance de leurs clients à cause d'un incident de sécurité.
Même les entreprises comme Facebook, dont la valeur principale dépend d'un service reposant sur le traitement d'un volume considérable d'informations personnelles, ne sont plus perçues comme auparavant par leurs utilisateurs.

Cependant, toutes les organisations ne se verront pas accorder une seconde chance pour démontrer que la protection de ces données est une priorité pour elles. Un seul incident compromettant les données personnelles des clients peut ruiner complètement la confiance de ces derniers et entraîner la disparition du service ou de l'entreprise.

L'année 2019 sera ponctuée d'incidents : violations de sécurité, dispositifs sortant de l'usine sans contrôles de sécurité suffisants, campagnes malveillantes sophistiquées visant des infrastructures stratégiques, etc. Dans le même temps, les cybercriminels continueront à envoyer des e-mails de phishing pour tenter d'abuser les internautes les moins technophiles, ceux qui ne sont pas méfiants ou ceux qui n'ont tout simplement pas de chance. Compte tenu de la diversité et de la complexité des attaques possibles, il y a beaucoup de différents domaines dans lesquels les membres de la société (entreprises, particuliers, industriels, gouvernements, groupes sociaux indépendants) ont la responsabilité de veiller à la confidentialité des données et au respect de la vie privée.

Nous espérons que ce rapport sera utile à toutes les parties prenantes impliquées dans le processus de prise de décisions et que nous pourrons tous travailler main dans la main pour profiter d'une technologie plus sûre.

www.eset.com