CYBERSÉCURITÉ 2018 : LE PRIX À PAYER DE NOTRE HYPERCONNECTIVITÉ

ENJOY SAFER TECHNOLOGY™

INDEX

INTRODUCTION

2017 : la cybersécurité à la une des medias

Dans le rapport « Cybersécurité 2018 : Le prix à payer de notre hyperconnectivité », les experts en sécurité d'ESET présentent les domaines qui devraient constituer des priorités absolues en matière de sécurité au cours de l'année à venir et proposent des solutions pour réduire les éventuels risques associés. Nous aborderons les ransomwares, les attaques contre les infrastructures critiques, l'importance de l'analyse des logiciels malveillants dans la lutte contre la cybercriminalité, les cybermenaces qui planent sur les campagnes électorales et les prévisions 2018 en matière de protection de la vie privée.

Tout d'abord, revenons sur ce qui s'est passé en 2017, une année noire pour notre monde numérique durant laquelle la sécurité – ou plutôt le manque de sécurité – informatique a fait les gros titres et s'est installée durablement dans les colonnes de la presse grand public internationale. Parmi les principaux incidents de cybersécurité de l'année figure un certain nombre de cas très médiatisés qui ont non seulement eu un impact sur des millions d'utilisateurs dans le monde entier, mais aussi causé des pertes financières considérables à de grandes multinationales et à des organismes publics.

Deux des attaques qui ont le plus marqué 2017 sont sans doute les infections massives par les ransomwares : WannaCryptor (également connu sous le nom de WannaCry) et DiskCoder.C. Dotés de capacités de type « ver », ces rançongiciels ont attaqué les données de milliers de postes de travail et de serveurs partout dans le monde à une échelle et à une vitesse sans précédent. En outre, ces menaces ont soulevé auprès d'un vaste public d'importantes préoccupations sur les problèmes de sécurité.

Ces attaques ne sont pas les seuls incidents à avoir attiré l'attention des médias. Prenons par exemple les failles de sécurité chez Equifax, qui ont probablement touché plus de la moitié de la population aux États-Unis ainsi que de nombreux clients dans d'autres pays. Ou encore, le piratage de HBO qui a entrainé la divulgation d'informations confidentielles sur les acteurs de la chaîne, ainsi que du matériel lié à la production tels que des scripts et des épisodes de la série « Game of Thrones ». Même Yahoo! a reconnu, avec un peu de retard, que l'intégralité de sa base de données utilisateurs a été infiltrée lors d'une intrusion datant de 2013, ce qui signifie que les données de trois milliards de comptes comprenant les noms, adresses e-mail, dates de naissance, mots de passe et, dans certains cas, les questions de sécurité et les réponses associées – ont été compromises.

Et ce n'est pas tout. L'année dernière, les spéculations sur d'éventuelles interférences dans l'élection présidentielle américaine de 2016 ont été nombreuses. Il y a également eu la découverte de KRACK, une faille dans le protocole de chiffrement WPA2 pouvant compromettre la sécurité des connexions WiFi.

Enfin, n'oublions pas Industroyer, la menace la plus importante pour les systèmes de contrôle industriels depuis Stuxnet, avec sa capacité de s'attaquer à différents types d'infrastructures critiques telles que les réseaux de distribution d'eau, d'électricité et de gaz.

Sans l'ombre d'un doute, l'année a été chargée en matière de sécurité. Plusieurs prédictions identifiées par les experts en sécurité d'ESET et soulevées au cours des dernières années se sont malheureusement produites en 2017. Les incidents de cybersécurité sont de plus en plus répandus dans tous les domaines de notre quotidien et touchent désormais un éventail plus large de cibles à l'échelle mondiale.

Les avancées technologiques et leur adoption accélérée ont rendu possibles des scénarios qui semblaient encore improbables il y a quelques années seulement. Cela devient de plus en plus évident avec la découverte de failles de sécurité qui s'expliquent par le fait que de nombreux systèmes et protocoles que nous utilisons au quotidien n'ont pas été conçus dans l'optique d'une connexion généralisée à Internet. Comment résoudre alors ce paradoxe sans revenir à des capacités techniques inférieures ?
Revenons à notre rapport « Cybersécurité 2018 : le prix à payer de notre hyperconnectivité ». S'il n'est pas certain que les prévisions abordées dans les articles suivants se réaliseront, nous espérons que l'année 2018 sera plus calme en matière de cybersécurité et que ce rapport sensibilisera les lecteurs aux problèmes potentiels.

Nous espérons que nos prévisions pour 2018 offriront à tous ceux qui s'intéressent à la cybersécurité, l'occasion d'examiner, d'aborder et de relever les défis présents et futurs.

1

La révolution des ransomwares

- Des ransomwares qui se comportent comme des vers
- Épidémies mondiales
- Des rançons sans contrepartie
- Autres types de ransomwares
- RaaS: Ransomware as a Service

AUTEUR

David Harley
Chargé de recherche principal chez ESET

La révolution des ransomwares

C'est là que ma carrière a commencé, il y a près de 30 ans. La première attaque de logiciel malveillant sur laquelle j'ai apporté mon expertise était celle de l'incroyable cheval de Troie AIDS, du Dr Popp, qui rendait inaccessibles les données de la victime jusqu'au paiement d'une « licence logicielle ». Suite à cette affaire, les ransomwares n'ont plus beaucoup fait parler d'eux pendant longtemps, à l'exception des attaques par déni de service (DDoS) réalisées contre les entreprises.

Déni plausible

Si les attaques par déni de service ont été amplifiées par la multiplication de l'utilisation de réseaux de botnets à la fin du siècle dernier, les menaces d'extorsion par attaques DDoS ont de leur côté pris de l'ampleur (bien que de façon moins spectaculaire) parallèlement à l'augmentation des ransomwares ces dernières années. Cependant, il se peut que les statistiques soient faussées en raison du silence de certaines entreprises victimes et d'une progression simultanée des attaques DDoS à visée politique plutôt que financière. D'autres interactions complexes régissent les différents types de logiciels malveillants : des variantes de ransomware intégrant un bot DDoS ont été rapportées, tandis que plus récemment, les auteurs du botnet Mirai ont dirigé des attaques DDoS contre le « coupe-circuit » de WannaCryptor (alias WannaCry) afin de réactiver les copies inactives du malware.

Le ver se transforme

Le logiciel malveillant baptisé Win32/Filecoder.WannaCryptor par ESET est évidemment bien plus complexe que le simple facteur Mirai. La combinaison d'un ransomware avec un ver a permis d'accélérer la propagation du malware, bien que l'ampleur de l'infection ne soit pas aussi impressionnante que pour certaines des attaques de vers des années 2000, notamment parce que sa diffusion reposait sur une faille déjà largement corrigée. Cependant, son impact financier sur de grandes entreprises a attiré l'attention des médias dans le monde entier.

Une seule règle du jeu : payer !*

L'une des particularités de WannaCryptor était que les victimes payant la rançon avaient peu de chances de voir toutes leurs données déchiffrées. Ce n'est évidemment pas spécifique à ce ransomware : il existe malheureusement de nombreux exemples de rançongiciels dont les auteurs étaient incapables de rétablir tout ou partie des données par incompétence en écriture de code, ou n'avaient jamais eu l'intention de permettre la récupération des données. Ranscam et Hitler, par exemple, ne chiffraient pas les fichiers, mais les supprimaient tout simplement, sans aucune possibilité pour le cybercriminel de pouvoir les rétablir. Ces ransomwares ne se sont heureusement pas trop propagés. L'exemple le plus célèbre est sans doute le semi-clone de Petya qu'ESET a détecté sous le nom de DiskCoder.C, qui chiffre bien les données. Étant donné le professionnalisme avec lequel le malware a été conçu, l'absence d'un mécanisme de restauration des données ne semble pas accidentelle, mais traduit plutôt l'intention du pirate de disparaître avec la rançon.

Wiper

Si le logiciel malveillant DiskCoder.C parfois appelé NotPetya extorque de l'argent aux victimes en se faisant passer pour un ransomware, d'autres « wipers » (effaceurs de données) ont clairement d'autres objectifs, comme le malware Shamoon qui a récemment repris du service. Parmi les logiciels malveillants effaceurs de données visant l'Ukraine figurent KillDisk (associé à BlackEnergy) et, plus récemment, l'un des contenus malveillants déployés par Industroyer.

Quels enseignements tirer de ces tendances ?

La prise en otage de vos données contre une rançon est un moyen facile pour les cybercriminels de vous soutirer de l'argent, tandis que la destruction de données pour d'autres motifs (politique par exemple) semble devenir de plus en plus fréquente. Au lieu de spéculer sur tous les moyens possibles et imaginables d'altérer les données, passons plutôt en revue quelques mesures permettant de réduire les risques de manière générale.

1. Nous sommes conscients que les victimes choisissent de payer dans l'espoir de récupérer leurs données, même si elles savent que cela encourage les cybercriminels. Toutefois, avant de mettre la main au portefeuille, demandez conseil à votre éditeur de logiciel de sécurité :

    a. Il est peut-être possible de rétablir vos données sans payer de rançon
    b. Certaines variantes de ransomwares ne permettent pas de récupérer les données malgré le paiement de la rançon.

2. Il est préférable de protéger vos données de façon proactive plutôt que de faire confiance à la compétence et à la bonne foi des cybercriminels. Sauvegardez régulièrement toutes vos données importantes, en conservant au moins certaines sauvegardes hors ligne, sur des supports non exposés aux ransomwares et autres logiciels malveillants et en lieu sûr (de préférence à plusieurs endroits). De toute évidence, les sauvegardes protègent également vos données contre d'autres risques et doivent donc faire partie d'un plan de reprise d'activité.

3. De nos jours, de nombreux particuliers et entreprises délaissent les sauvegardes sur supports physiques (tels que les disques optiques et les mémoires flash) pour le stockage dans le Cloud, le plus souvent hors site. Cependant, gardez à l'esprit que de telles solutions de stockage sont « actives » en permanence et que leurs contenus sont vulnérables aux ransomwares de la même façon que tout périphérique de stockage local ou réseau. Il est important qu'une solution de stockage hors site réponde aux critères suivants :

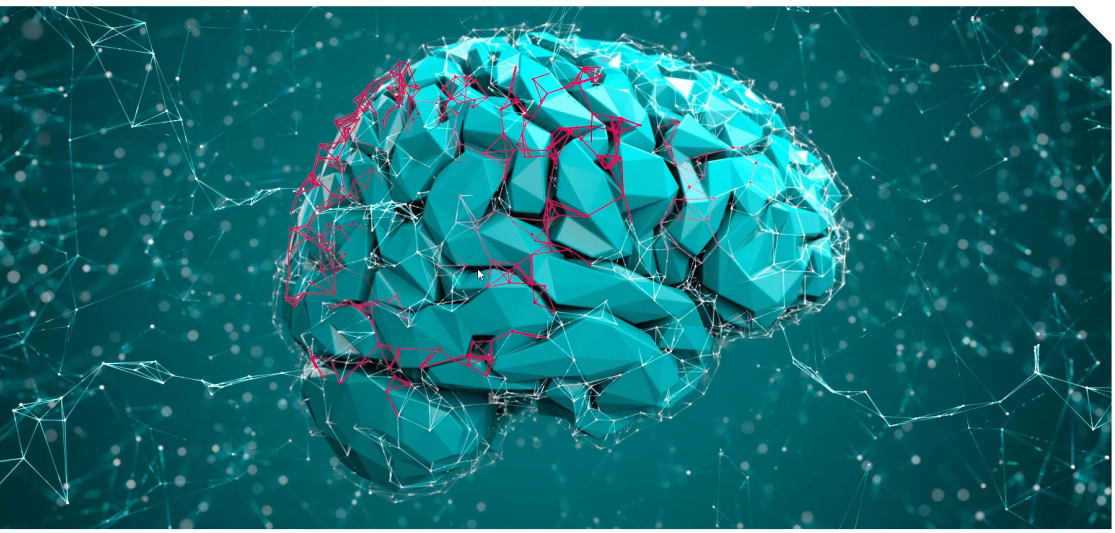
    a. Ne pas être en ligne en permanence
    b. Protéger les données sauvegardées contre toute modification automatique et silencieuse ou tout écrasement par un logiciel malveillant lorsque l'installation à distance est en ligne
    c. Protéger les sauvegardes précédentes, afin que vous puissiez les récupérer en cas de compromission des dernières sauvegardes
    d. Protéger le client en spécifiant les responsabilités juridiques/contractuelles du fournisseur, les modalités en cas de cessation d'activité du fournisseur, etc.

Sauvegardez régulièrement toutes vos données importantes, en conservant au moins certaines sauvegardes hors ligne, sur des supports non exposés aux ransomwares et autres logiciels malveillants et en lieu sûr (de préférence à plusieurs endroits).

4. Ne sous-estimez pas l'utilité des supports de sauvegarde non réinscriptibles/réutilisables. Si vous ne pouvez pas en modifier le contenu, alors les ransomwares non plus. Vérifiez de temps en temps que votre opération de sauvegarde/restauration fonctionne correctement et que vos supports (lecture seule, écriture désactivée ou écriture activée) restent lisibles (et que ceux en écriture active ne sont pas systématiquement inscriptibles). Et pensez à sauvegarder vos sauvegardes.

Prévisions pour le futur

« N'effectuez pas de prévisions informatiques qui puissent être vérifiées de votre vivant », comme l'a très justement affirmé Daniel Delbert McCracken. Nous pouvons tout de même prendre le risque de faire quelques extrapolations à partir de l'évolution récente des ransomwares afin de formuler quelques réflexions prudentes sur leur évolution future.



5. Je ne vous recommanderai certainement pas de compter sur des sauvegardes plutôt que d'utiliser un logiciel de sécurité, mais gardez à l'esprit que l'élimination de ransomwares actifs à l'aide d'un anti-ransomware n'équivaut en aucun cas à la récupération des données : si vous supprimez le ransomware puis décidez de payer la rançon, vos données risquent de ne plus pouvoir être rétablies même avec la coopération des cybercriminels, car le mécanisme de déchiffrement fait partie du logiciel malveillant. D'un autre côté, vous ne devez pas restaurer vos données sur un système où le ransomware est encore actif. Heureusement, grâce aux sauvegardes sécurisées, vos données restent intactes lorsqu'un malware passe outre votre logiciel de sécurité.

Attaques ciblées

Le cheval de Troie AIDS avait une cible relativement spécifique. Malgré cela, rares étaient ceux qui s'intéressaient aux détails de la recherche sur AIDS, et la distribution du cheval de Troie par disquette était assez coûteuse et le mécanisme de paiement de la rançon ne jouait pas vraiment en faveur de l'attaquant. (Bien entendu, en 1989, le Dr Popp n'avait pas accès aux cryptomonnaies, au Dark Web, aux moyens simples d'utiliser Western Union [le mode de transfert d'argent préféré des escrocs de la fraude 419] ou à la monétisation des photos de nu.) Le logiciel malveillant en soi était un ransomware classique, qui privait la victime de ses données. Par la suite, les attaques DoS et DDoS empêchaient les entreprises de bénéficier des services fournis : si les clients étaient privés de tels ser-

vices, c'était en revanche au fournisseur que la rançon était demandée. Cependant, avec l'essor de l'utilisation personnelle et individuelle d'Internet, la surface d'attaque a augmenté et le type de cibles potentielles s'est diversifié, ce qui a probablement une influence sur la distribution peu sélective de la plupart des ransomwares actuels.

Attaques non ciblées

La presse et les services marketing des éditeurs de solutions de sécurité ont tendance à s'emballer lorsque l'identité d'une victime célèbre ou importante (établissements de santé, universités, opérateurs téléphoniques, FAI, etc.) est dévoilée. Pour autant, il est inexact de supposer que ces institutions sont toujours ciblées de façon spécifique. Comme le vecteur d'infection utilisé dans une campagne donnée n'est pas toujours connu, il est impossible d'affirmer que ce n'est jamais le cas. Mais les maîtres-chanteurs du web semblent tirer pas mal de profits des rançons payées par les grandes institutions compromises par des attaques latérales à partir de comptes professionnels d'employés piratés. Au Royaume-Uni par exemple, NHS Digital nie que le secteur de la santé soit ciblé de façon spécifique – un point de vue que je partage de manière générale – tout en reconnaissant que les établissements de santé sont souvent victimes de cyberattaques.

La situation pourrait-elle changer ?

À l'heure actuelle, certaines entreprises semblent prêtes à payer des rançons relativement importantes. Dans certains cas, il s'agit d'une solution de repli raisonnable consistant à former une réserve d'argent pouvant servir en cas d'échec des dispositifs de sécurité informatique face aux ransomwares. Dans d'autres cas, les sociétés espèrent que le paiement des rançons sera moins coûteux que la mise en place de systèmes de défense complexes et pas toujours efficaces à 100 %. Cette mentalité risque d'encourager les criminels à viser les entreprises perçues comme des cibles faciles ou particulièrement aptes à payer la rançon (institutions financières, casinos). Le nombre croissant d'attaques de wipers et de ransomwares sans restitution des données permettra sans doute d'enrayer cette tendance malsaine, mais les sociétés qui ne renforcent pas au mieux leurs défenses pourraient alors constituer des cibles privilégiées. En effet, une attaque réussie dirigée contre une grande entreprise sera plus rentable plus rapidement que des attaques dispersées lancées au hasard contre des utilisateurs et adresses e-mail lambda.

Attaques de données vs attaques d'appareils

Concernant les attaques contre les smartphones et autres appareils mobiles, elles ont tendance à affecter davantage l'utilisation de l'appareil et de ses services que les données. En ne payant pas la rançon, les utilisateurs risquent de perdre leurs paramètres et d'autres données, ce qui est déjà suffisamment grave. De plus, comme les appareils mobiles remplacent de plus en plus les ordinateurs, de nombreuses données pourraient ainsi être menacées. Avec l'essor de l'Internet des objets (IoT – Internet Of Things) inutilement interconnectés et son lot d'appareils et de capteurs intelligents intégrés à des éléments insolites dans des contextes inattendus (routeurs, réfrigérateurs, compteurs communicants, téléviseurs, jouets, centrales électriques, stations-service, pacemakers, etc.), la surface d'attaque augmente considérablement. À l'heure du « tout connecté », le nombre de services pouvant être interrompus par des logiciels malveillants (contre rançon ou non) explose. Ces dernières années, nous avons évoqué ce que mon collègue Stephen Cobb appelle le Ransomware des Objets. Il y a moins d'exemples concrets de telles menaces à ce jour que ce à quoi l'on pourrait s'attendre,

Concernant les attaques contre les smartphones et autres appareils mobiles, elles ont tendance à affecter davantage l'utilisation de l'appareil et de ses services que les données.

étant donné l'attention qu'elles attirent. Cette situation pourrait toutefois changer si les ransomwares traditionnels perdaient leur efficacité en tant que moyen de s'enrichir rapidement, mais je pense que cela n'est pas près de se produire...

En revanche, la sécurité de l'Internet des objets ne semble pas progresser au même rythme que la croissance de l'Internet des Objets. Les pirates informatiques s'intéressent déjà à la monétisation de l'insécurité de l'IoT. Le développement et la propagation d'un logiciel malveillant affectant de nombreux objets connectés n'étant pas aussi simples que ce que suppose parfois les medias, il n'y a aucune raison de céder à la panique, mais ne sous-estimons pas pour autant la ténacité des cybercriminels ni leur capacité à nous surprendre.

*Mes excuses au défunt Henry Newbolt dont j'ai déformé le poème Vitaï Lampada : https://en.wikipedia.org/wiki/Henry_Newbolt.

2

Les attaques contre les infrastructures critiques en progression

- Le piratage des infrastructures critiques ne cesse d'augmenter
- Étude de cas ESET : Industroyer et BlackEnergy
- Attaques contre les chaînes d'approvisionnement
- Pourquoi votre pays n'est-il pas épargné ?

AUTEUR

Stephen Cobb
Chercheur senior
en sécurité chez ESET

Les attaques contre les infrastructures critiques en progression

Les cybermenaces visant les infrastructures critiques ont fait la une des journaux en 2017, à commencer par un article de Reuters en janvier attribuant une coupure d'électricité récente en Ukraine à « une cyberattaque ». Dans le rapport sur les tendances en cybersécurité de l'année dernière, nous nous attendions à ce que les attaques contre les infrastructures « continuent à faire les gros titres et à perturber le quotidien des populations en 2017 ». Nous avions hélas raison, et cette même tendance devrait malheureusement se poursuivre en 2018 pour les raisons énoncées dans ce rapport. Rappelons que les infrastructures critiques ne se limitent pas au réseau électrique et englobent également la défense, la santé, les usines de production et l'alimentaire, le réseau de distribution d'eau et les transports.

Coupures d'électricité

Voyons comment les choses ont évolué dans le temps. Fin décembre 2015, des cyberattaques contre des fournisseurs d'énergie ukrainiens ont privé d'électricité des centaines de milliers de foyers de cette région du monde pendant plusieurs heures. Le premier article publié par les chercheurs d'ESET en 2016 sur cet incident était l'analyse de Black Energy, le code malveillant utilisé dans cette attaque, par Anton Cherepanov. Le malware en question n'affectait pas directement les appareils du système de contrôle industriel (ICS), mais il permettait aux pirates d'infiltrer les réseaux des fournisseurs d'électricité et de désactiver les logiciels utilisés par les équipements ICS. Les articles de presse de l'époque – dont certains affichaient des titres accrocheurs tels que « Un logiciel malveillant coupe le courant » – ne faisaient pas clairement cette distinction.

L'attaque de fin 2016, mentionnée pour la première fois en janvier 2017, était très différente, comme les chercheurs d'ESET Anton Cherepanov et Robert Lipovský l'ont indiqué sur leur blog WeLiveSecurity. Selon leur analyse, il s'agissait d'un nouveau logiciel malveillant capable de contrôler directement les disjoncteurs et les commutateurs des sous-stations électriques, en les éteignant et rallumant littéralement dans certains cas (ce qui peut gravement perturber l'alimentation à cette échelle). Les chercheurs ont nommé ce malware « Industroyer » et ont montré que l'on avait affaire à la menace la plus importante pour les systèmes de contrôle industriels depuis Stuxnet. Lorsqu'ils ont présenté leur analyse au Black Hat USA 2017, la salle était comble, et pourtant, on aurait pu entendre une mouche voler.

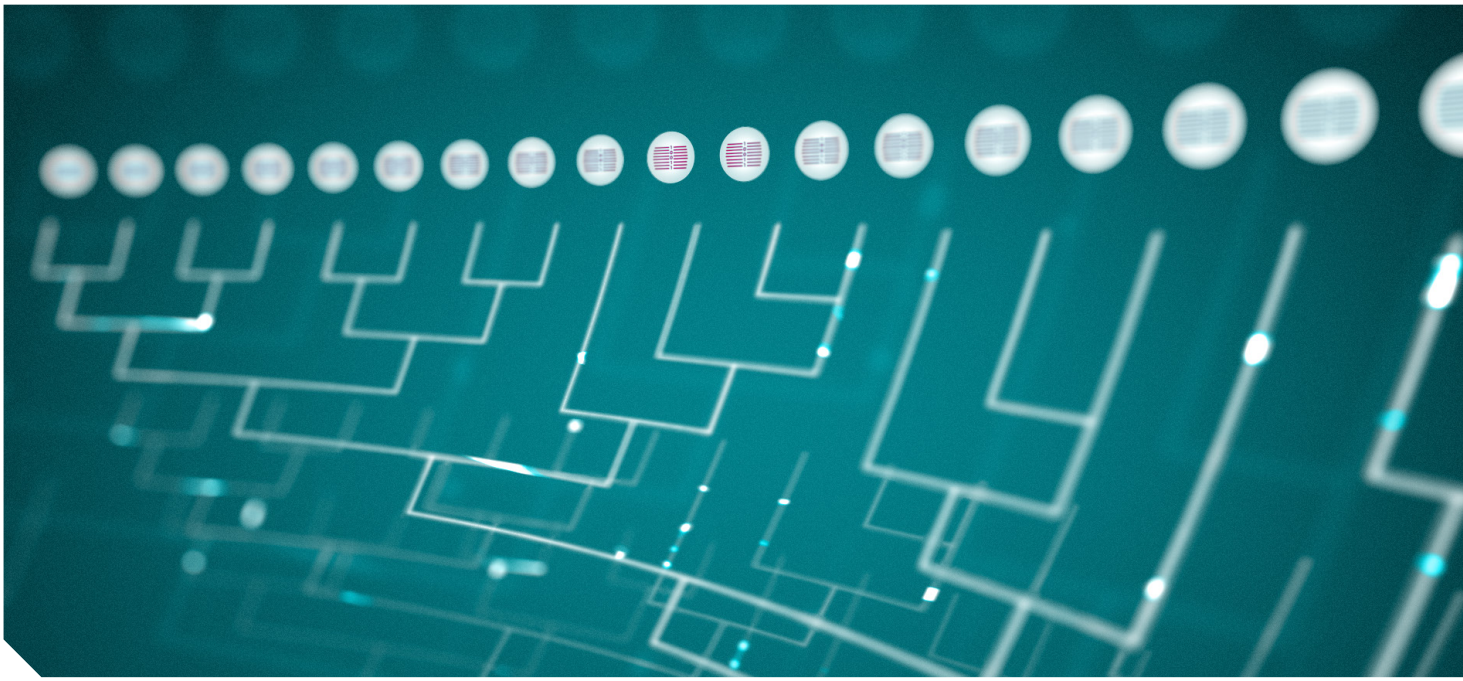
Les implications d'Industroyer pour les futures menaces visant les infrastructures critiques sont pour le moins inquiétantes, comme on peut en juger par le ton de cette interview de Robert Lipovský. Les équipements industriels ciblés par Industroyer sont couramment utilisés, bien au-delà de l'Ukraine (au Royaume-Uni, dans l'UE et aux États-Unis, par exemple) et dans plusieurs secteurs critiques. En outre, de nombreux équipements ICS encore en service aujourd'hui n'ont pas été conçus pour être connectés à Internet, ce qui rend les mesures de protection rétroactives difficiles à mettre en œuvre.

Les équipements industriels ciblés par Industroyer sont couramment utilisés, bien au-delà de l'Ukraine (au Royaume-Uni, dans l'UE et aux États-Unis, par exemple) et dans plusieurs secteurs critiques.

La plupart des opérateurs d'infrastructures critiques s'efforcent bien entendu de sécuriser leurs équipements. Par ailleurs, les études d'ESET suggèrent que toute future cyberattaque reposant sur Industroyer devra être adaptée à des cibles spécifiques, ce qui pourrait limiter les éventuelles attaques aux pirates suffisamment financés et empêcher les vastes campagnes visant à couper l'électricité, à paralyser les transports ou à interrompre une chaîne de production critique. Cependant, il n'est pas rare que de telles conditions évoluent dans le temps, avec le perfectionnement du code d'attaque et le recueil d'informations. En d'autres termes, les cyberattaques sur le réseau électrique auront tendance à augmenter en 2018, à moins d'être contrées par des mesures préventives telles que les mises à jour des systèmes, la détection précoce d'un sondage du réseau et l'amélioration de la détection et de la prévention des attaques par phishing.

Infrastructures et chaîne d'approvisionnement

Malheureusement, le simple remplacement des anciens équipements ICS par du matériel conçu pour être connecté à Internet n'améliorera pas automatiquement la sécurité. En effet, comme le souligne Stephen Ridley, fondateur et directeur de la technologie de Senrio (une entreprise spécialisée dans la sécurité des appareils connectés), les industriels sont en train d'abandonner les circuits intégrés à application spécifique (ASIC) en faveur d'une architecture générique moins coûteuse (SoC), pour laquelle des bibliothèques de code sont disponibles.



Bien que la nouvelle approche permette de réaliser des économies, elle ajoute des points faibles à la chaîne d'approvisionnement, tels que des puces présentant des failles difficiles à corriger et la réutilisation de code entraînant des vulnérabilités logicielles. En 2017, nous avions les exemples de la faille Devil's Ivy découverte dans plus de 200 modèles différents de caméras de sécurité d'Axis Communications et des failles BlueBorne qui ont touché plusieurs milliards d'appareils utilisant les systèmes d'exploitation les plus répandus (Windows, Linux, iOS et Android). Selon les prévisions, d'autres exemples de ce type seront découverts en 2018.

Un autre type de problème lié à la chaîne d'approvisionnement a fait les gros titres en 2017, en partie parce que l'industrie du spectacle a été touchée. Bien qu'il ne s'agisse pas d'un secteur critique, les enseignements que l'on peut tirer de l'incident de 2017 sont utiles aux acteurs essentiels de l'économie. La tentative d'extorsion à l'encontre de Netflix en échange d'épisodes de la série « Orange is the New Black » et le piratage du dernier volet de Pirates des Caraïbes mettent en évidence des aspects inquiétants de la sécurité de la chaîne d'approvisionnement.

Alors que les grandes entreprises prennent la cybersécurité bien plus au sérieux de nos jours, en accordant aux équipes de sécurité le budget et le soutien de la direction dont elles ont besoin pour effectuer le travail correctement, les petits sous-traitants qui leur fournissent des biens et des services peinent à relever le défi. Ces derniers deviennent ainsi une cible privilégiée si, par exemple, un blockbuster est en postproduction dans leurs systèmes de traitement audio connectés à leur réseau d'entreprise dont les utilisateurs n'ont pas été formés pour reconnaître des e-mails de phishing.
En 2017, nous avons eu la confirmation que les points faibles de ces petits prestataires en matière de sécurité pouvaient représenter un moyen efficace de compromettre des cibles plus importantes, telles que de grandes sociétés de production cinématographique. Après plusieurs affaires très médiatisées, j'ai rassemblé quelques conseils sur la sécurité des chaînes d'approvisionnement, qui peuvent également être utiles aux opérateurs d'infrastructures critiques. Après tout, il peut être difficile pour un pirate d'infiltrer directement le réseau d'un fournisseur d'énergie, mais qu'est-ce qui l'empêche d'attaquer son prestataire de services de nettoyage ?

Par le passé, on se méfiait de l'agent d'entretien mal intentionné et doué en informatique, craignant qu'il ne profite d'une pause pendant qu'il fait le ménage la nuit pour obtenir un accès non autorisé au réseau. Si ce risque n'a pas totalement disparu, il s'y ajoute désormais la menace d'une agence de nettoyage non cybersécurisée se connectant aux systèmes de la centrale électrique via un portail fournisseur (par exemple) mal isolé du réseau ICS.

Conséquence : les opérateurs d'infrastructures critiques doivent continuer à renforcer leur sécurité en 2018 en réduisant l'efficacité des attaques de phishing (qui reste l'un des principaux vecteurs d'attaque), en isolant et contrôlant l'accès au réseau, en vérifiant et testant le matériel et les logiciels, et en effectuant une due diligence sur les fournisseurs. Ils doivent également faire attention et réagir aux différents types de sondage et de surveillance du réseau, qui sont des signes potentiels d'une cyberattaque imminente.

Il peut être difficile pour un pirate d'infiltrer directement le réseau d'un fournisseur d'énergie, mais qu'est-ce qui l'empêche d'attaquer son prestataire de services de nettoyage ?

3

Cybercrime : collaboration des forces de l'ordre et chercheurs en malwares

- Démantèlements, condamnations et lutte d'ESET contre la cybercriminalité
- Étude de cas : comment la recherche sur Windigo a contribué à l'arrestation d'un cybercriminel
- En quoi cette lutte est importante

AUTEUR

Alexis Dorais-Joncas
Chercheur senior
en sécurité chez ESET

Cybercrime : collaboration des forces de l'ordre et chercheurs en malwares

L'objectif principal de l'analyse des logiciels malveillants est de comprendre le fonctionnement d'un malware, d'extraire les indicateurs de compromission (IOC) et de déterminer d'éventuelles contre-mesures. Il s'agit d'un travail de nature presque exclusivement technique, reposant sur des fichiers binaires et leurs propriétés. Les résultats de l'analyse de logiciels malveillants sont essentiels aux entreprises, car ils leur permettent de se défendre contre une attaque ou de remédier à une infiltration en cours. Ils sont également cruciaux pour les éditeurs de logiciels de sécurité, qui les utilisent pour offrir de meilleures capacités de détection et mesures de protection à leurs clients.

Cependant, d'autres questions se posent parfois. Ces deux fichiers sont-ils liés ? Quelle est l'architecture de l'infrastructure de commande et contrôle (C&C), et comment le protocole de communication fonctionne-t-il ? Comment les activités du botnet sont-elles monétisées : par facturation à l'installation, envoi de courrier indésirable ou redirection de trafic ?

La recherche sur les logiciels malveillants répond à ces questions et offre une meilleure compréhension du tableau général qui se cache derrière chaque malware individuel en établissant les liens nécessaires.

Bien évidemment, la recherche sur les logiciels malveillants profite aussi aux éditeurs d'antivirus, puisqu'elle les aide à développer de meilleures solutions de sécurité. Mais les informations qui en découlent sont également utiles aux forces de l'ordre dans le cadre de la lutte contre la cybercriminalité. Pourquoi ? Voyons quelques exemples de travaux d'ESET ayant contribué à mettre fin à des opérations malveillantes.

Campagne de démantèlement de Dorkbot

En 2015, ESET a participé à la campagne d'éradication de logiciels malveillants (CME) de Microsoft dans le cadre de la lutte contre la famille de malwares Win32/Dorkbot. Dorkbot était un kit en vente sur les forums clandestins, qui avait infecté plus d'un million de PC couvrant plusieurs réseaux de botnets indépendants. L'objectif de cette campagne CME était de démanteler autant de botnets que possible en faisant tomber les infrastructures C&C associées simultanément.

Dorkbot était un kit en vente sur les forums clandestins, qui avait infecté plus d'un million de PC couvrant plusieurs réseaux de botnets indépendants.

Afin de soutenir cette opération, les chercheurs en logiciels malveillants d'ESET ont automatisé le processus d'extraction d'informations C&C à partir des fichiers binaires de Dorkbot. Nous avons appliqué ce processus à notre flux d'échantillons Dorkbot existants et nouveaux. Nous avons ensuite nettoyé manuellement les résultats en supprimant les sinkholes connus et les domaines/adresses IP sains afin de limiter le risque de faire tomber des ressources légitimes. Microsoft a fusionné ces informations avec leurs propres données pour créer une liste exhaustive de tous les nœuds C&C actifs à cibler. Cette liste complète a alors été transmise aux autorités compétentes partout dans le monde, telles que le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), l'Équipe d'intervention en cas d'urgence informatique du Département de la Sécurité intérieure des États-Unis (DHS/US-CERT), Europol, le FBI, Interpol et la

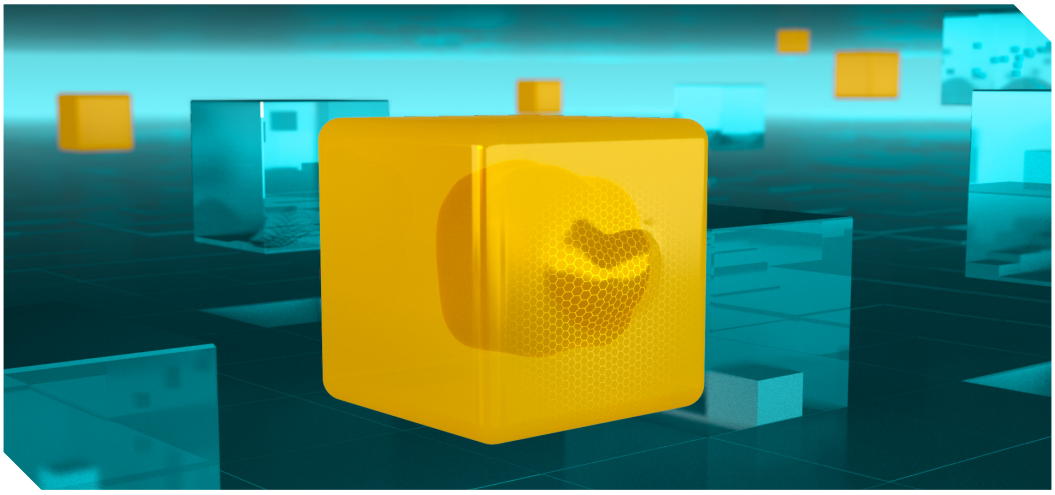
Gendarmerie royale du Canada (GRC). Le jour de l'opération, les mandats et les avis de démantèlement ont été exécutés de façon coordonnée.

L'activité de Dorkbot a depuis chuté brutalement dans le monde entier, ce qui témoigne de la réussite de la campagne CME.

Windigo et le botnet Ebury

tels que les adresses IP infectées, les données issues des messages indésirables envoyés par le botnet, ainsi que d'autres informations publiques pertinentes (registre de noms de domaine, par exemple).

Grâce à ces informations, le FBI a pu mener son enquête, doucement mais sûrement. Début 2015, un citoyen russe nommé Maxim Senakh a été identifié comme l'un des auteurs de l'Opération Windigo et officiellement mis en examen aux États-Unis. Par la suite, Maxime Senakh a été



ESET a publié pour la première fois une analyse technique exhaustive de ce que nous appelons l'Operation Windigo. En résumé, Windigo reposait sur une backdoor capable de voler les informations d'identification qui a infecté des dizaines de milliers de serveurs Linux, sur lesquels un ou plusieurs autres composants malveillants étaient installés et utilisés pour la monétisation du botnet, par exemple via l'envoi de courrier indésirable ou la redirection du trafic HTTP. Après la publication du rapport, nous avons collaboré avec le FBI dans son enquête sur les cybercriminels à l'origine de l'Opération Windigo.

Notre collaboration avec les forces de l'ordre a consisté à leur fournir nos résultats de recherche sur les logiciels malveillants, arrêté par les autorités finlandaises à la frontière russe alors qu'il retournait en Russie après des vacances. Il a ensuite été extradé vers les États-Unis. en février 2016. Maxime Senakh a fini par plaider coupable de fraude informatique, en violation du Computer Fraud and Abuse Act (loi américaine sur les fraudes et abus informatiques). Il a été condamné à 46 mois de prison.

Pour plus d'informations, consultez https://www.welivesecurity.com/2017/10/30/esets-research-fbi-windigo-maxim-senakh/.

En quoi cette lutte est-elle importante ?

Il faut du temps et de l'énergie pour lutter contre les cybercriminels, mais le jeu en vaut la chandelle. Pour nous, c'est l'un des meilleurs moyens de mettre un frein à la cybercriminalité et de rendre Internet plus sûr, et c'est la meilleure chose à faire.

Il existe différentes théories classiques de prévention de la délinquance et nous ne prétendons pas être des criminologues. Cependant, on peut établir un parallèle intéressant entre nos mesures de lutte contre la cybercriminalité et la théorie de la « prévention situationnelle de la délinquance », dont la définition est la suivante :

« La prévention situationnelle de la délinquance repose sur l'idée que le crime est souvent opportuniste et a pour objectif de modifier les facteurs contextuels afin de limiter les occasions pour les criminels de passer à l'acte. »

Les techniques de prévention situationnelle peuvent être regroupées en plusieurs grandes catégories, dont trois ont un lien avec notre travail.

1. *Augmenter l'effort nécessaire pour commettre un acte de délinquance*
   Les campagnes de démantèlement coordonnées, telles que celle dirigée contre Dorkbot, obligent les cybercriminels à se réorganiser et à se tourner vers de nouvelles stratégies et techniques, telles que la création de nouveaux logiciels malveillants ou la modification des protocoles de communication, ce qui augmente de toute évidence l'effort nécessaire pour poursuivre l'opération criminelle en cours.

2. *Réduire les gains pour ceux qui viennent de commettre un crime*
   (un corollaire du point 1), a pour conséquences de perturber les activités malveillantes. Le coût d'exécution augmente forcément, ce qui réduit le bénéfice net de façon proportionnelle.

3. *Rendre l'acte de délinquance plus risqué*
   Les informations techniques aident les forces de l'ordre à faire avancer l'enquête dans la bonne direction et à étayer la plainte. Une coopération accrue entre les enquêteurs et les chercheurs en logiciels malveillants permettra d'arrêter et de condamner davantage de cybercriminels, ce qui rendra leurs attaques plus risquées.

Certains croient que la raison pour laquelle si peu de cybercrimes sont punis est qu'il est facile de commettre de tels actes sur Internet de manière anonyme, sans être repéré. Au contraire, il est en réalité assez difficile de maintenir une parfaite sécurité opérationnelle (OPSEC) en permanence. Pensez à tout ce qu'il faut faire pour exploiter une opération malveillante : lancer des campagnes d'infection, surveiller le statut du botnet, mettre à jour les composants malveillants, enregistrer des noms de domaine ou des services d'hébergement, monétiser l'opération, etc. Pour un cybercrime parfait, chaque étape doit être exécutée à la perfection, à tout moment. Les cybercriminels sont des êtres humains, et l'erreur est humaine. Il suffit que l'attaquant se connecte une fois au mauvais serveur avant d'activer une connexion VPN ou TOR pour qu'il soit fiché dans un fichier journal, en attente d'être démasqué.

D'autres jettent l'éponge face aux cybercriminels car même lorsqu'ils sont identifiés, ils restent hors d'atteinte. Peut-être vivent-ils dans un pays qui ne dispose pas de lois efficaces contre la cybercriminalité ou qui n'a pas signé de traité d'extradition avec les pays enquêtant sur les criminels ? Là encore, l'erreur est humaine. Il suffit qu'un cybercriminel connu parte en vacances à l'étranger pour qu'il soit arrêté.

Pour un cybercrime parfait, chaque étape doit être exécutée à la perfection, à tout moment.

L'année 2017 a été marquée par un grand nombre d'arrestations dans diverses opérations cybercriminelles, comme le souligne Stephen Cobb dans son excellente synthèse. Avec la collaboration croissante entre les forces de l'ordre et les sociétés privées telles qu'ESET pour traquer les cybercriminels, nous sommes confiants quant à l'année 2018, qui sera le théâtre de nombreuses enquêtes fructueuses rendant Internet plus sûr pour tous. Sauf pour les cybercriminels.

4

Piratage de la démocratie : les processus électoraux peuvent-ils être protégés ?

- Vote électronique et en ligne
- Hacktivisme et attaques durant les campagnes électorales
- Comment la sécurité peut changer la direction d'un pays

AUTEUR

Camilo Guttierrez
Chef de la sensibilisation et de la recherche chez ESET Amérique latine

Piratage de la démocratie : les processus électoraux peuvent-ils être protégés ?

Ces deux dernières années, des élections ont été organisées dans plusieurs pays qui occupent le devant de la scène internationale. Elles ont soulevé toute une série de questions, dont la plus pressante est de savoir si une cyberattaque peut influencer un processus électoral au point de changer le cours politique d'un pays.

Personne n'oserait avancer une réponse définitive à une telle question, qu'il s'agisse de politologues ou de chercheurs en cybersécurité. Néanmoins, la situation dans laquelle nous nous trouvons actuellement pose de toute évidence un certain nombre de défis. Il est clairement établi que les résultats d'un vote électronique sont loin d'être sécurisés, comme nous allons le démontrer ici.

Par ailleurs, deux autres facteurs essentiels requièrent de l'attention : premièrement, l'influence des réseaux sociaux sur l'opinion publique notamment en matière de politique, en particulier la façon dont ils soutiennent l'hacktivisme ; et deuxièmement, la nécessité de faire figurer la cybersécurité parmi les préoccupations politiques.

Des systèmes de vote électronique non sécurisés

Ce n'était qu'une question de temps avant que la technologie de l'information ne soit intégrée au processus électoral. Certains pays (tels que l'Argentine, le Brésil, l'Allemagne et les États-Unis) ont décidé de mettre en place un vote électronique partiel dans le but de mettre fin aux fraudes, de normaliser et d'accélérer le dépouillement, et de compléter le système de vote papier sans le remplacer. Il est indéniable que la technologie progresse inexorablement, mais mieux vaut concentrer les efforts sur la mise en œuvre de davantage de mécanismes de contrôle, plutôt que d'adopter une approche qui ne fait qu'ajouter des vulnérabilités au système sans en éliminer les risques.

À l'image des responsables politiques, activistes et autres acteurs clés peu scrupuleux qui ont trouvé au fil des années des moyens de frauder le système électoral, les cybercriminels apprendront à exploiter les failles du système numérique, en particulier s'ils reçoivent le soutien de quelque commanditaire.

En 2006, Harri Hursti, programmeur finlandais cofondateur de ROMmon, avait déjà démontré dans le célèbre documentaire Hacking Democracy, que le système de vote Diebold utilisé à Leon County en Floride pouvait être facilement et entièrement compromis à l'aide d'une simple carte mémoire.

En deux temps trois mouvements, il a réussi à changer tous les votes sans que personne ne s'en rende compte.Malgré cela, ce même logiciel – avec quelques modifications mineures, un nouveau nom et un changement de propriétaire – continue d'être utilisé aux États-Unis pour l'enregistrement et le dépouillement des votes.

En dix ans, peu de choses ont changé, si ce n'est que des preuves supplémentaires ont été mises au jour. L'urne électronique du Brésil est au cœur d'une controverse depuis qu'il a été découvert en 2012

qu'il était possible de violer le secret du vote. Après des années d'allégations de vulnérabilité fondées, le Tribunal électoral supérieur revient au vote papier (dans un format hybride) et seuls 5 % des urnes seront utilisés pour les élections de 2018. Entre-temps, les procédures de vote électronique en Argentine et Allemagne ont également montré leurs limites.

À la lumière des preuves disponibles à ce jour, nous ne pouvons pas être tributaires de la technologie pour une chose aussi importante que le processus électoral ; elle doit uniquement servir d'outil complémentaire. Si l'idée est de limiter tous types de fraudes afin de donner plus de crédibilité aux résultats et à nos démocraties, nous devons alors recourir à des systèmes hybrides alliant votes papier et bulletins électroniques.

Un hacktivisme qui peut changer l'opinion publique

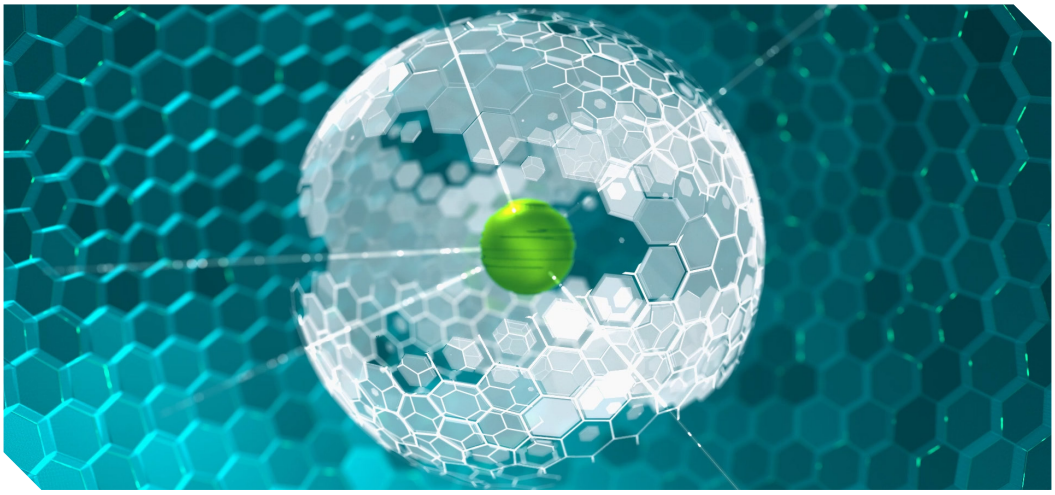
Nouvelles frontières de la scène politique, les réseaux sociaux sont utilisés par les politiciens pour toucher un public de plus en plus vaste. Comme nous le savons maintenant, ces mêmes réseaux ont également été utilisés pour saboter les campagnes électorales à coups de mensonges et de fausses informations, sans compter les vastes attaques contre la réputation de personnages publics.

Un certain nombre de ces attaques repose sur des menaces informatiques telles que les bots ou d'autres formes de logiciels malveillants, qui peuvent être combattues en mettant en place des protocoles de gestion de la sécurité adéquats. Ce qui semble traduire une tendance pourrait en réalité être la manifestation d'un groupe de pirates informatiques.

Si de telles attaques peuvent aider à manipuler ou à fausser l'opinion publique, elles ne signent pas pour autant la fin de la démocratie. Cependant, elles posent tout de même d'importants défis en matière de cybersécurité, si l'on veut garantir la bonne représentation de la voix du peuple dans les élections.

Annoncé en juillet dernier, le programme « Defending Digital Democracy » est soutenu et cautionné par des entreprises telles que Facebook et Google, ce qui montre l'importance qu'elles accordent à la sécurisation des mécanismes démocratiques.

Les réseaux sociaux ont également été utilisés pour saboter les campagnes électorales à coups de mensonges et de fausses informations, sans compter les vastes attaques contre la réputation de personnages publics.



Si les parties concernées ne prennent pas les choses en main, ces types d'incidents continueront de se produire à l'avenir.

Cybersécurité nationale

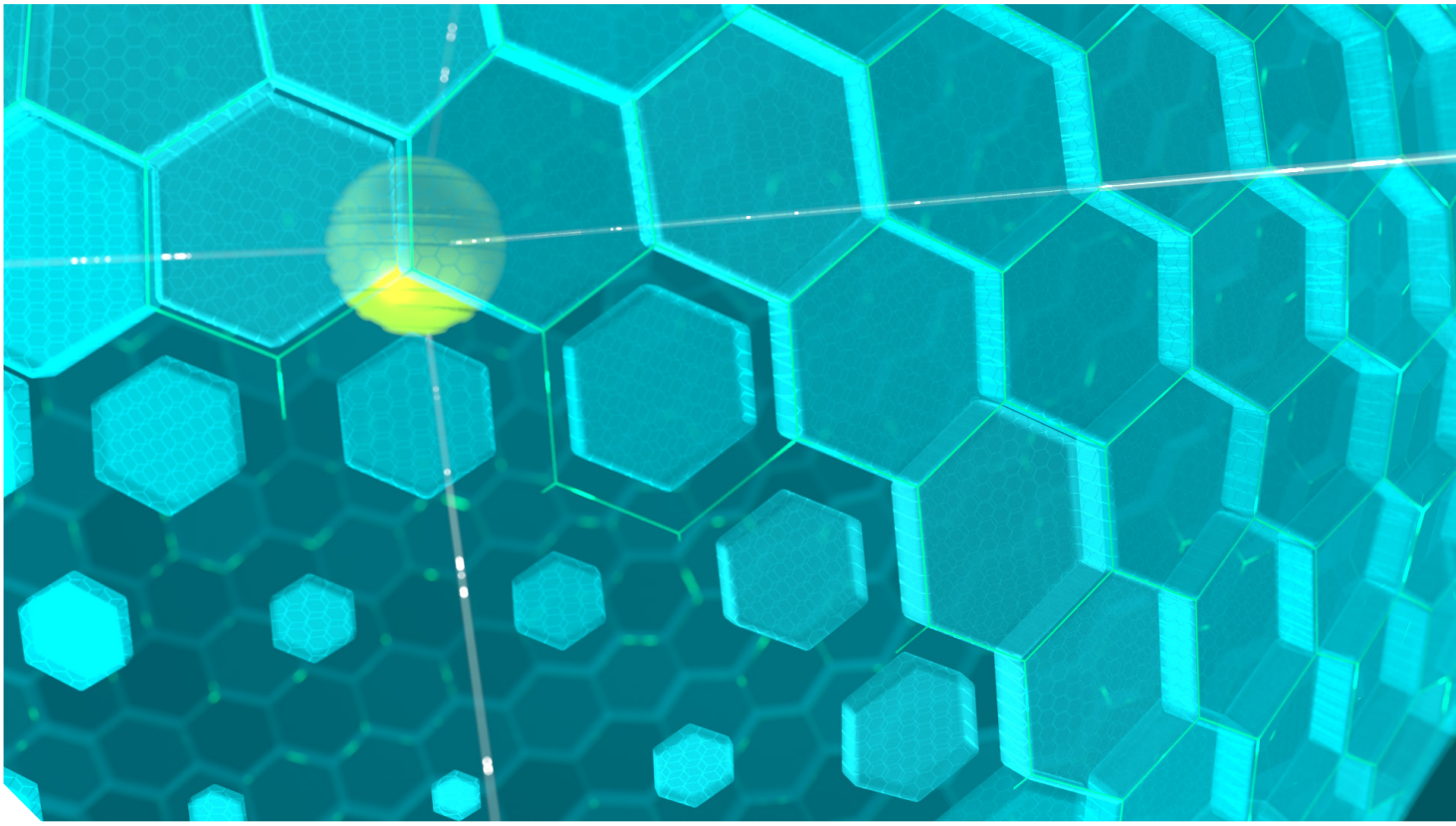
La technologie fait partie intégrante de notre quotidien. Par conséquent, il appartient aux gouvernements de garantir des interactions sécurisées entre les utilisateurs et celle-ci, en mettant en œuvre des programmes de cybersécurité nationaux en collaboration avec des acteurs clés tels que les responsables de la sécurité des systèmes d'information et les auditeurs.

Et si les pouvoirs publics, tels que les autorités judiciaires ou la commission électorale, sont amenés à prendre des décisions relatives à la mise en œuvre de certaines technologies, alors les décisionnaires doivent suivre une formation en cybersécurité adaptée à la situation, afin de pouvoir faire un choix en connaissance de cause.

Chaque avancée apporte son lot de risques. Si nous voulons nous servir de la technologie pour améliorer notre quotidien, nous devons l'empêcher de créer plus de problèmes que de solutions. Tous les éléments d'un système électoral doivent être considérés comme faisant partie des infrastructures critiques du pays et bénéficier d'une protection adéquate à ce titre.

Les défis sont là. Il est temps de prendre des mesures préventives pour assurer la sécurité numérique des informations, et tous les acteurs impliqués doivent contribuer à la recherche de solutions garantissant le bon déroulement des processus démocratiques.

Chaque avancée apporte son lot de risques. Si nous voulons nous servir de la technologie pour améliorer notre quotidien, nous devons l'empêcher de créer plus de problèmes que de solutions.



5

Données personnelles dans la nouvelle ère technologique et législation sur la protection des données

- L'Internet des Objets, un monde « public » peuplé de données personnelles
- Profilage sur réseaux sociaux et assimilation croissante des utilisateurs à des « produits »
- Les comportements utilisateurs exploités par certains éditeurs d'antivirus dans le cadre des solutions gratuites

AUTEUR

Tony Anscombe
Évangéliste de la sécurité et ambassadeur des partenariats industriels chez ESET

Données personnelles dans la nouvelle ère technologique et législation sur la protection des données

La vie privée est – ou devrait être – un droit fondamental de l'homme. Aujourd'hui, la notion de vie privée de l'utilisateur final tend à être assimilée à celle de protection des données ou des informations. Cette déviation rend de plus en plus difficile pour l'utilisateur final le maintien d'une position neutre vis-à-vis des données. D'un côté, des technophiles défenseurs de la vie privée visent le « zéro empreinte numérique » ; de l'autre la grande majorité des utilisateurs finaux laissent des traces un peu partout, offrant aux cybercriminels une Toile pleine de données sensibles qui ressemble à une plage de sable un jour d'affluence.

Moteur de la nouvelle révolution technologique, les données alimentent les nombreux systèmes d'intelligence artificielle (IA) en développement. La question qui se pose est la suivante : lorsque des données sensibles sont mises en ligne, combien de processus de prise de décision automatiques seront capables d'appliquer le droit à l'oubli, et les entreprises collectant ces données sauront-elles où et comment celles-ci sont utilisées par leurs systèmes IA ?

Si la plupart des utilisateurs finaux ont conscience de fournir leurs données aux réseaux sociaux ou aux entreprises via des formulaires et des applications, d'autres fournisseurs et services collectent des données de façon beaucoup moins transparente.

Logiciels et services gratuits

Comme les consommateurs s'attendent à avoir accès à des logiciels gratuits ou à très faible coût, certains éditeurs ont décidé de se lancer dans la collecte et le partage de données. Les éditeurs de logiciels gratuits ne disposent que de quelques méthodes de monétisation de leurs produits, dont la moins intrusive – du moins du point de vue de ce que perçoit l'utilisateur final – pourrait bien être le recueil et la vente de données à des tiers.

L'année dernière, des fournisseurs de solutions de sécurité réputés se sont mis à proposer des produits antivirus gratuits. Bien qu'ils n'aient pas ouvertement déclaré leurs intentions en matière de monétisation de leurs nouveaux produits gratuits, certains d'entre eux auront probablement recours à des méthodes indirectes telles que la collecte de données.

La tendance à proposer des solutions de sécurité gratuites et leur probable monétisation indirecte semblent s'être accélérées lorsque Microsoft a intégré l'antivirus Windows Defender à son système d'exploitation en tant qu'option gratuite par défaut. Comme bon nombre d'utilisateurs sont passés à l'option par défaut de Microsoft, le nombre d'opportunités commerciales a naturellement diminué pour les autres éditeurs d'antivirus, qui ont donc dû se tourner vers un autre moyen de monétisation en offrant leur propre logiciel gratuit plutôt que d'opter pour la concurrence directe.

Les risques associés à la protection des données augmenteront car les logiciels gratuits, qui n'utilisent généralement

pas les méthodes de monétisation traditionnelles, comportent des déclarations complexes conçues en partie pour dissimuler la nature des données collectées et leur éventuelle commercialisation. En effet, de nombreuses entreprises affichent des politiques de confidentialité interminables et illisibles que seuls les juristes comprennent.

Par conséquent, pour tout produit gratuit, il est important que l'utilisateur sache comment l'entreprise réalise des profits : un jeu mobile comportera par exemple des publicités ou vous fera payer pour accéder aux niveaux supérieurs. Si ce point n'est pas clair, la monétisation du produit risque fort d'impliquer vos données et votre vie privée.

L'Internet des Objets

Si les produits et applications gratuits savent tout de nos habitudes en ligne, l'Internet des Objets (IoT) rend possible la collecte et l'exploitation de données encore plus sensibles.

Pendant que vous rentrez du travail en voiture, votre smartphone partage les conditions de circulation avec d'autres conducteurs, vous permettant peut-être de faire des détours intelligents ou de prendre des décisions pour regagner votre domicile plus rapidement. Votre thermostat connecté communique avec votre téléphone, qui lui transmet votre position actuelle ainsi que l'heure. Vous êtes sur le chemin du retour. En arrivant dans votre rue, la porte du garage s'ouvre automatiquement, prenant une décision sur la base de votre proximité. Les lumières s'allument et votre sélection de musique actuelle est transférée de votre voiture à votre domicile automatiquement. Les objets connectés sont conçus pour fonctionner ensemble afin de nous simplifier la vie.

Avec toutes les données qu'il collecte, chaque objet connecté a une histoire à raconter. En combinant ces différents flux de données, n'importe quel pirate informatique pourrait dresser un tableau complet de votre vie : votre lieu de travail, votre restaurant préféré, votre salle de sport, votre salle de cinéma habituelle, vos magasins de prédilection, etc. L'association de ces données et des progrès de l'apprentissage automatique et de l'intelligence artificielle pourrait faire de nous des pantins de la technologie, qui prend de plus en plus de décisions pour chacun d'entre nous.

Selon les prévisions du cabinet Gartner, le nombre d'objets connectés dans le monde atteindra 11,2 milliards en 2018 et 20,4 milliards d'ici 2020. Prenez garde, le soulèvement des machines est proche ! Nous devons inculquer aux utilisateurs finaux la nécessité, à chaque demande de connexion d'un appareil, de lire la politique de confidentialité et de décider en connaissance de cause s'ils doivent ou non accepter les conditions de collecte de données qui y figurent.

Législation

À compter de mai 2018, le Règlement Général sur la Protection des Données (RGPD) de la Commission européenne, une directive renforçant le droit des citoyens en matière de traitement et d'utilisation de leurs informations, entrera en vigueur. Cette législation concerne toute entreprise traitant ou collectant les données d'un citoyen de l'Union européenne, quel que soit le pays où elle est basée.

Le non-respect du RGPD pourrait entraîner des amendes importantes, mais la manière dont celles-ci seront appliquées aux sociétés situées hors UE n'est pas claire. Il se peut que la

Avec toutes les données qu'il collecte, chaque objet connecté a une histoire à raconter.

Commission européenne sanctionne une entreprise extracommunautaire à titre d'exemple, potentiellement peu après l'entrée en vigueur du règlement le 25 mai. Sans un tel exemple d'application de la loi, de nombreuses sociétés internationales risquent de ne pas s'y conformer. La Commission européenne pourrait donc prendre les choses en main et agir dès 2018.

Aux États-Unis, la protection de la vie privée a fait un pas en arrière en 2017, lorsque la nouvelle administration a abrogé des mesures empêchant les fournisseurs d'accès à Internet (FAI) de collecter les données des clients sans leur consentement. Si certains FAI se sont engagés d'eux-mêmes à ne pas vendre les données à des tiers, cela ne signifie pas pour autant qu'ils ne les utiliseront pas dans leur propre intérêt commercial.

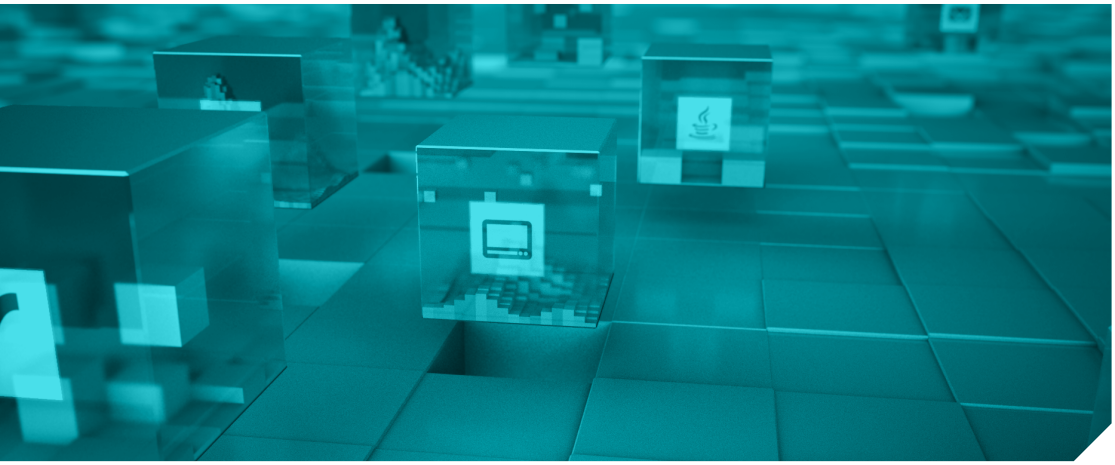
À partir des nombreuses données collectées à notre insu sur nos habitudes en ligne, il est facile de créer des profils montrant nos centres d'intérêt, des informations qui peuvent être considérées comme extrêmement personnelles.
Les profils clients pourraient devenir la cible de pirates informatiques, comme en témoignent les violations de données personnelles au niveau des bases de données, des sites commerçants et autres. Un cybercriminel parvenant à dérober des données sur nos comportements en ligne gagnerait le gros lot, puisqu'il pourrait les utiliser pour nous faire du chantage.

La possibilité de manipuler des quantités astronomiques de ce type de données pour les exploiter ensuite est une option relativement récente pour la plupart des éditeurs de logiciels et prestataires de services, car les coûts de stockage et de traitement associés ont baissé considérablement. L'écosystème du Big Data permet désormais à de nombreuses entreprises de collecter, de corréler et de commercialiser leurs données.

La facilité avec laquelle les entreprises peuvent collecter et vendre les données, notre propension à accepter les paramètres par défaut et notre tendance à ne pas lire les politiques de confidentialité font de notre identité, nos modes de vie et nos données personnelles des actifs d'entreprise.

J'espère que 2018 sera l'année d'une meilleure sensibilisation des utilisateurs, mais pour être réaliste, je pense qu'encore plus de données seront collectées à leur insu. Chaque appareil qui se connecte sans notre consentement éclairé érode davantage notre vie privée, jusqu'au jour où elle ne sera plus qu'un lointain souvenir.

Nous devons inculquer aux utilisateurs finaux la nécessité, à chaque demande de connexion d'un appareil, de lire la politique de confidentialité et de décider en connaissance de cause s'ils doivent ou non accepter les conditions de collecte de données qui y figurent.



CONCLUSION

Conclusion

L'analyse de la progression des ransomwares et des attaques récurrentes contre les infrastructures critiques dans les chapitres précédents indique clairement que le nombre de cyberattaques et leur portée continueront d'augmenter au cours de l'année à venir. Cependant, n'oublions pas que ces scénarios complexes ne constituent qu'un aspect – et pas forcément le plus important – de la cybercriminalité. Bien que les cyberattaques sophistiquées attirent davantage l'attention, elles ne représentent qu'une faible fraction des cybermenaces que nous analysons au quotidien dans nos laboratoires de recherche sur les logiciels malveillants.

En réalité, les menaces les plus réussies que nous rencontrons sont les plus simples : il s'agit généralement d'attaques malveillantes déployées via l'envoi de courrier indésirable ou l'hameçonnage et de campagnes de téléchargement direct pouvant être enrayées en sensibilisant les utilisateurs finaux. Le problème réside dans l'allocation des ressources nécessaires à la sensibilisation du public aux cybermenaces.

Les événements de 2017 montrent que les avancées technologiques et leur adoption accélérée par les utilisateurs finaux partout dans le monde ont rendu possibles des scénarios auparavant inconcevables.

Si l'on fait abstraction des spécificités de chaque événement, les données personnelles sensibles sont le dénominateur commun de toutes ces situations. Qu'elles appartiennent à une entreprise, au gouvernement ou à des particuliers croyant que leurs données ont peu d'importance, les informations constituent de nos jours une denrée précieuse à tous les niveaux. Elles peuvent être utilisées comme une monnaie (par exemple lorsque les entreprises monétisent des applications et des contenus gratuits en proposant aux internautes d'y accéder en échange de profils utilisateurs), ou par les organismes publics dans la gestion des dossiers et des opérations.

Dans la plupart des cas, le recueil de ces données personnelles sensibles est une activité transparente et légitime, souvent décrite dans les « conditions générales » que peu d'entre nous prennent le temps de lire. Mais que se passe-t-il lorsque de nombreuses parties sont impliquées dans la protection de ces informations ? Les risques augmentent avec le nombre et la complexité des processus sujets à l'erreur.

Les données personnelles d'un utilisateur final peuvent être compromises par un incident spécifique (tel qu'une infection par un logiciel malveillant ou une campagne de phishing), une intrusion systémique au niveau de l'entreprise, voire une cyberattaque contre un organisme public ou une institution financière.

Dans ce cas, pourquoi n'est-il pas demandé à chacune des parties d'assumer sa part de responsabilité afin que les mesures de cybersécurité soient mises en œuvre correctement sur tous les fronts ? Il n'appartient pas uniquement aux entreprises de cybersécurité de gérer ou d'éliminer la cybercriminalité – cela reviendrait à exiger des médecins qu'ils éradiquent les maladies ou de la police qu'elle mette fin à la délinquance.

Les escroqueries numériques et les menaces pesant sur la sécurité des informations continueront d'exister aussi

longtempsqu'ilexisteradanslasociétédes personnes prêtes à nuire aux autres par simple opportunisme ou malhonnêteté.

Il est temps que les utilisateurs à tous les niveaux et, à terme, le grand public, prennent conscience que la cybersécurité ne doit pas être assurée uniquement par les prestataires qu'ils ont choisis mais aussi par eux-mêmes, et qu'il reste encore beaucoup à faire.

La première étape consiste à comprendre la valeur des informations de nos jours et les raisons pour lesquelles tous les acteurs du monde numérique en ont besoin pour atteindre leurs objectifs. Il est impossible de protéger quelque chose sans savoir de quoi il s'agit et pourquoi il faut le protéger.

Il est essentiel de connaître ces menaces et les moyens de les repousser pour protéger la confidentialité, l'intégrité et la disponibilité des informations des différents acteurs de notre société, des informations qui constituent aujourd'hui la pierre angulaire d'un certain nombre d'activités (légales ou non).

Les perspectives sont prometteuses : depuis que WannaCryptor (WannaCry) a pris le monde au dépourvu, la sensibilisation à la cybersécurité a bien progressé dans divers secteurs et a régulièrement fait la une des journaux.

Le piratage des comptes de réseaux sociaux de célébrités et de clubs de football (tels que le Real Madrid et le FC Barcelone) ainsi que des systèmes internes de sociétés prestigieuses (telles que HBO, Disney et Equifax) a également eu un impact sur l'opinion du grand public, qui pour la plupart commence à peine à comprendre ce qui se passe.

Nous espérons que ce rapport sur les tendances 2018 éclairera les lecteurs sur les problèmes clés devant être résolus pour mener le monde vers un avenir plus sûr.

ENJOY SAFER TECHNOLOGY™