WannaCry, une frayeur à l'échelle planétaire

Par Jean-Luc AMINOT
Commissaire divisionnaire honoraire – Université de Paris (Master Ingénierie des risques)

Le 12 mai 2017, le monde entier découvrait le rançongiciel WannaCry, utilisé dans le cadre d'une cyberattaque massive sans précédent. Ce logiciel malveillant, de la famille des rançongiciels, touchait en quatre jours plus de 200 000 ordinateurs dans 150 pays différents. En Europe, le système informatique du NHS, le service de santé britannique, était quasiment paralysé. Plusieurs grandes entreprises privées européennes étaient également impactées.
Le défi posé à nos sociétés développées par WannaCry est celui de l'insécurité latente des réseaux par lesquels transitent chaque jour des milliards de données. Par conséquent, une véritable attitude de vigilance, de protection et de résilience s'avère aujourd'hui nécessaire, et ce malgré une connaissance perfectible des patrimoines informatiques, une hétérogénéité croissante des systèmes, et du fait des obligations liées à la protection des données personnelles.
C'est une véritable stratégie d'ensemble que les organisations se voient conviées à déployer, laquelle doit permettre de construire un état d'esprit de vigilance, une protection technologique efficiente et une résilience authentique.

Le 12 mai 2017, le monde entier découvre le rançongiciel WannaCry (« envie de pleurer »), utilisé dans le cadre d'une cyberattaque massive sans précédent. Nul ne le sait encore, mais rien ne sera plus comme avant : c'en est fini d'une relative tranquillité et d'une apparente sécurité dans la navigation sur la Toile, non seulement pour les individus, mais aussi, et peut-être avant tout, pour les organisations, qu'il s'agisse d'entreprises privées ou d'administrations publiques.

WannaCry, une attaque d'un genre nouveau

Ce logiciel malveillant fait partie de la famille des rançongiciels (*ransomwares*, en anglais). Lorsqu'il a pénétré une première machine (ordinateur de bureau, portable, serveur d'entreprise…), la charge virale qu'il renferme s'active, elle « prend en otage » les données présentes sur l'ordinateur en les chiffrant avec une clé cryptée, les rendant inaccessibles à l'utilisateur. Ce dernier, en allumant sa machine, ne voit alors plus qu'un message lui demandant de payer une rançon à envoyer à une adresse de paiement en monnaie virtuelle, en bitcoins… Invisibilité et opacité de la transaction garanties.

Des conséquences rapides et notables

Ce qui distingue WannaCry des autres types d'attaques jusque-là rencontrées, c'est l'extrême rapidité de sa diffusion. Ce logiciel malveillant, particulièrement virulent, mais d'une conception somme toute assez rudimentaire, se réplique et se propage très rapidement.

Initiée le 12 mai 2017, l'attaque se poursuit jusqu'à la découverte d'une solution provisoire, le 15 mai suivant. Pendant ces quatre jours, au moins plus de 200 000 ordinateurs dans 150 pays sont affectés, avec des pertes économiques estimées entre quelques centaines de millions et plusieurs milliards de dollars. D'après Kaspersky Labs, le pays le plus touché aurait été de très loin la Russie, suivie de l'Ukraine, de l'Inde et de Taïwan.

En quatre jours, WannaCry a eu le temps de causer des dommages conséquents. En Europe, la Grande-Bretagne a été sévèrement affectée : le système informatique du NHS, le service de santé britannique, a été quasiment paralysé. Dans de nombreux hôpitaux, les opérations non urgentes ont dû être repoussées. Aucun patient ne semble avoir été mis en danger ; mais avec 19 000 rendez-vous annulés ou perturbés, le service a enregistré des pertes de 92 millions de livres, dont 73 millions au titre du nettoyage et de la mise à jour des systèmes informatiques.

Plusieurs grandes entreprises privées européennes ont été touchées, dont l'opérateur Telefonica en Espagne, la Deutsche Bahn, et Renault, qui a connu des perturbations sur des chaînes de montage. Selon une source syndicale, l'usine de Sandouville (Seine-Maritime), qui emploie 3 400 salariés, a notamment été touchée.

Fleuron français du bâtiment, Saint-Gobain a aussi été fortement impacté par WannaCry, avant de subir les coups de l'autre grand *ransomware*, NotPetya, en juin 2017. La firme estimera à 220 millions d'euros de chiffre d'affaires, et à 80 millions d'euros de résultat d'exploitation, ses pertes dues aux cyberattaques sur la première moitié de 2017.

Les origines de WannaCry

Bien qu'il soit particulièrement ardu de nos jours d'attribuer avec certitude la paternité d'une attaque informatique d'une telle ampleur, nombre de chercheurs et de services d'intelligence, au sens anglo-saxon du terme, se sont penchés sur la question.

Il semble qu'à l'origine, la NSA (National Security Agency) se soit fait dérober, dans des circonstances restant à définir, un « exploit » (un élément de programme informatique permettant d'exploiter une faille de sécurité dans un système), dénommé EternalBlue. Il s'agissait d'un programme malicieux permettant d'exploiter dans le plus grand secret une faille latente dans la suite logicielle Windows. De telles failles, lorsqu'elles sont ainsi activées, sont dites *zero day*, car elles ne possèdent aucune antériorité ; de ce fait, la mise au point d'une contremesure s'en trouve largement complexifiée, et l'exploit peut générer très rapidement des dégâts irréversibles.

Selon le CERT-FR, la faille exploitée par WannaCry a été documentée par Microsoft dans son bulletin de sécurité MS17-010 du 14 mars 2017 accompagnant le *patch* corrigeant cette vulnérabilité considérée comme critique.

Les créateurs de WannaCry se revendiquent comme un groupe de hackers activistes répondant au nom de Shadow Brokers (« les courtiers de l'ombre »). Diverses hypothèses ont circulé quant à leur identité ; l'analyse du code de WannaCry a mis en évidence que certains caractères avaient été obtenus à partir d'un clavier à caractères coréens, mais rien d'avéré n'a pu être établi, si ce n'est qu'une telle organisation, quelle que soit sa taille et son origine, possédait un pouvoir de déstabilisation majeur à l'échelle de la planète.

Les concepteurs de WannaCry ont donc couplé EternalBlue à quelques lignes de code, aux fins de créer ce que l'on appelle un ver, c'est-à-dire un virus auto-répliquant et autonome, une fois lancé dans l'univers des réseaux. Un ver comme WannaCry contamine tous les ordinateurs connectés au réseau auquel appartient la première machine infectée. Il se propage ensuite sans aucune intervention humaine : nul besoin d'ouvrir la pièce jointe d'un *e-mail*, ni même de brancher physiquement une clé USB contaminée à une machine. Au-delà du seul réseau local, WannaCry scanne Internet pour trouver des ports réseau semblables et vulnérables à EternalBlue.

En général, les systèmes d'exploitation les plus vulnérables aux « exploits » sont aussi les plus anciens, parce qu'ils ne sont plus ou peu mis à jour. Or, dans le cas de WannaCry, l'écrasante majorité des victimes avaient installé sur leurs machines (98 %), sous Windows 7, la version alors la plus récente de ce système d'exploitation.

WannaCry, un révélateur salutaire

Le défi que l'attaque WannaCry (et celles qui ont suivi) pose à nos sociétés développées est celui de l'insécurité latente des réseaux par lesquels transitent chaque jour des milliards de données, le plus souvent en clair. Or, ces données sont source de valeur, en raison de leur nature (données personnelles, données de transactions, données sensibles liées à des brevets…).

La grande leçon à tirer de Wannacry est simple : même en l'absence de signes précurseurs, ou d'impératif réglementaire ou légal (ce qui tend à devenir rare), une véritable attitude de vigilance, de protection et de résilience s'avère de nos jours nécessaire pour qui veut emprunter Internet pour faire transiter des données, quelle qu'en soit la teneur.

Une nouvelle forme d'insécurité créée par trois défis majeurs

Les défis ainsi posés sont immenses et imposent tout d'abord de maîtriser au sein de chaque structure, quelle que soit sa dimension et sa dispersion à travers le monde, l'ensemble des architectures, des flux et des implantations matérielles et logicielles.

Le défi de la connaissance du patrimoine organisationnel

Avec l'émergence d'Internet, puis le développement des capacités de stockage en *cloud* (nuage), le nombre d'applications informatiques utilisées au sein des entreprises a explosé. Si les responsables de la sécurité informatique « traditionnelle » sont particulièrement sensibilisés à l'importance des opérations de maintenance, telles que les mises à jour des postes clients et serveurs, ce n'est pas forcément le cas des équipes opérationnelles, qui, par définition, se concentrent davantage sur la continuité de l'activité.

C'est ainsi qu'une étude récente de la société de conseil Tanium (2019) a montré que les directeurs de services informatiques interrogés se disaient freinés dans cet exercice de mise à jour par les directions opérationnelles : 94 % des DSI français prétendent ainsi avoir déjà renoncé à une mise à jour de sécurité par peur de son impact sur l'activité commerciale de l'entreprise.

Or, plus les établissements sont imposants et donc potentiellement « riches », et plus la migration vers un nouveau système peut s'avérer complexe : dimension du parc à migrer, capacité financière à absorber les coûts induits… Autant de raisons qui freinent les opérations de migration vers des systèmes plus modernes et donc, en théorie, mieux sécurisés. La tentation est alors grande pour un groupe de hackers de chercher à exploiter une ou plusieurs failles dans un tel environnement.

Jusqu'à ce que survienne l'épisode WannaCry et ceux qui l'ont suivi (NotPetya, notamment), qui s'appuient justement sur les systèmes d'exploitation non mis à jour ou obsolètes, ce type de situation ne posait pas à proprement parler de problèmes de sécurité. C'est ainsi que de nombreuses entreprises ont vu leurs systèmes d'information devenir inopérants en quelques heures seulement.

Le défi de l'hétérogénéité croissante des systèmes

Les systèmes informatiques des entreprises sont de nos jours équipés de nombreux systèmes d'exploitation différents, on y trouve les principales versions de Windows, de Mac OS X, sans oublier les différentes distributions de Linux. Chaque version de chaque OS ayant ses propres mises à jour, il est aisé d'imaginer la complexité que cela apporte dans la bonne gestion des mises à jour.

De plus en plus, les entreprises possèdent de multiples sites et sont présentes sur plusieurs continents à la fois ; leur architecture informatique suit la même logique. Ce qui conduit les informaticiens à gérer des environnements distribués dans le monde entier, avec un accès plus ou moins aisé selon le réseau et le pays d'implantation.

De nos jours, quelles que soient les études considérées, il appert qu'un ordinateur ou serveur sur 6, voire 5, est masqué aux cartographies opérationnelles des grandes DSI. Comment, dans ces conditions, opérer l'intégralité de toutes les mises à jour de toutes les machines participant au même réseau ? Les hackers se sont fait forts d'exploiter largement ce type de failles.

Aujourd'hui, la menace de type WannaCry demeure endémique : des millions de tentatives d'infections sont stoppées tous les mois ; plusieurs milliers de variantes éphémères parcourent encore la Toile. Dans un article récent (2019), l'éditeur Sophos confirmait que 12 480 variantes uniques avaient été observées fin 2018, et 6 963 en août 2019 (dont 80 % étaient nouvelles).

La persistance de la menace WannaCry est en grande partie due à la capacité de ces nouvelles variantes à contourner le premier antidote mis au point le 15 mai 2017. Toutefois, lorsque les chercheurs de Sophos ont analysé et exécuté un certain nombre de ces maliciels, ils ont constaté que leur capacité à chiffrer les données avait été neutralisée : la conséquence *a priori* d'une corruption de code.

Le défi de la protection des données personnelles

Au-delà de la difficulté de maintenir à jour des parcs informatiques fortement hétérogènes, dispersés, sous-traités… une révolution récente, liée à l'avènement de la préoccupation majeure que constitue aujourd'hui en Europe la protection des données personnelles, est venue complexifier encore la tâche des managers privés et publics : il s'agit de l'entrée en vigueur du Règlement général pour la protection des données (RGPD), le 15 mai 2018, dont les dispositions ont été complétées par la loi du 20 juin 2018 sur la protection des données personnelles.

Tous les organismes qui traitent de telles données doivent mettre en place des mesures pour prévenir les violations des données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu'une violation cause des dommages ou des préjudices aux organismes, comme aux personnes concernées.

Les nouvelles obligations concernant les violations de données sont prévues par les articles 33 et 34 du RGPD. Elles précisent l'obligation générale de sécurité que doivent respecter les organismes qui traitent des données à caractère personnel.

Au titre de ce principe essentiel, ces organismes doivent mettre en place des mesures visant à prévenir toute violation de données et à réagir de manière appropriée en cas de violation, c'est-à-dire mettre fin à celle-ci et en minimiser les effets.

Ces dispositions visent à préserver à la fois les responsables du traitement, afin de protéger leur patrimoine informationnel, en leur permettant notamment de sécuriser leurs données, et les personnes affectées par la violation, afin d'éviter que cette dernière ne leur cause des dommages ou préjudices, en leur permettant notamment de prendre les précautions qui s'imposent en cas d'incident, dans le plus grand secret.

Il est dès lors recommandé que les organismes qui traitent des données personnelles (responsables du traitement ou sous-traitants) prévoient et mettent en place des procédures globales en matière de protection de ces données.

Ces procédures doivent être envisagées selon un mode global : la mise en place de mesures visant à détecter immédiatement une violation, à l'endiguer rapidement, à analyser les risques engendrés par l'incident et à déterminer s'il convient de notifier celui-ci à l'autorité de contrôle, voire aux personnes concernées. Ces procédures participent ainsi à la documentation de la conformité au RGPD.

La nécessaire construction par les organisations d'une stratégie de résilience

Finalement, c'est une véritable stratégie d'ensemble que les organisations se voient conviées à déployer, laquelle doit permettre de construire un état d'esprit de vigilance, une protection technologique efficiente et une résilience effective.

Cette stratégie est à bâtir au plus haut niveau de la pyramide hiérarchique, ce qui implique que le haut management soit sensibilisé et convaincu de la nécessité de constituer une véritable stratégie de prévention et de résilience liée à l'utilisation des réseaux de communication (et pas seulement d'Internet).

Il importe que les décisions prises soient appuyées au plus haut niveau, et qu'un *reporting* de qualité, clair et fiable, soit institué entre les différentes entités de l'organisation (technologique, juridique, opérationnelle, ressources humaines, direction générale), de bas en haut, et inversement. Seuls une réelle transparence de l'information, de tous les instants, et l'emploi de messages de communication exempts de jargon technique, et donc aisément assimilables par les sphères dirigeantes, sont de nature à permettre la mise en œuvre d'une telle stratégie, pour des résultats gagnants.

Un état d'esprit général de vigilance doit ensuite être créé au sein des structures, lequel doit être entretenu et régulièrement testé.

Il est essentiel de convaincre chaque utilisateur qu'il est un maillon à part entière de la chaîne des systèmes d'information. À ce titre, et dès son arrivée dans l'entité, il doit

être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information, au travers d'actions de sensibilisation et de formation.

Ces dernières seront régulièrement reconduites et aborderont à chaque occasion l'évolution des risques, des menaces, mais aussi des parades disponibles. Un utilisateur averti peut à lui seul éviter beaucoup de risques.

La formation des collaborateurs aux bons réflexes en matière de sécurité informatique peut s'appuyer sur une charte informatique – pour formaliser et partager les bonnes pratiques –, des sessions d'*e-learning* – pour former chaque collaborateur à son rythme –, des formations de groupe – pour le partage d'expérience et l'émulation –, des dispositifs ludiques et participatifs, comme des tests sous forme de quiz, des tests d'intrusion en *social engineering* et autres *serious games*.

Quel que soit le choix du ou des vecteurs, ce travail de sensibilisation doit être encouragé et porté par la direction générale, proposer des contenus pratiques et liés aux usages réels des utilisateurs, se limiter à quelques sujets importants, les plus pertinents dans le contexte de l'organisation, mais les traiter en profondeur. Il ne doit pas être réservé à certains collaborateurs, mais être mené auprès de l'ensemble du personnel, et doit s'accompagner d'un contrôle des acquis en fin de formation. Enfin, il est primordial de procéder à des « piqûres de rappel » régulières, du fait de l'évolution permanente des menaces.

En termes de protection des structures et des systèmes, la meilleure politique passe par une attitude proactive, centrée sur les possibilités prometteuses que recèlent les derniers développements de l'intelligence artificielle. Plus que guérir le mal lorsqu'il survient, il convient d'organiser sa détection et son confinement en dehors des structures de l'organisation. À titre d'exemple, en matière de détection, Saint-Gobain s'est tourné vers l'intelligence artificielle, recourant à un IDPS (*Intrusion Detection and Prevention System*) : un système qui scrute le réseau à la recherche d'activités anormales, en avertit les administrateurs et tente de bloquer les menaces.

Plus globalement, l'avenir est aux plans d'action globale, impulsés depuis le *top management*, à la fois complets, explicites, ancrés dans la durée et dotés de leur propre dispositif d'évaluation pérenne. La sécurité des réseaux empruntés par nos organisations ne relève pas d'un effet de mode, mais d'un défi permanent. Aussi les réponses doivent-elles se montrer à la mesure ; citons par exemple le plan d'action pour la sécurité des systèmes d'information mis en œuvre par une instruction ministérielle des Affaires sociales et de la Santé en novembre 2016 [1], soit six mois avant l'épisode WannaCry. Si le NHS britannique a beaucoup souffert à cette occasion, il n'en a pas été de même en France… Ce n'est sans doute pas un hasard.

(1) Ministère des Affaires sociales et de la Santé, instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés.

Bibliographie

BONVOISIN G. (2018), « Ransomware : 9 mesures pour se protéger et récupérer ses fichiers », CNET, disponible en ligne : https://www.cnetfrance.fr/produits/guide-protection-fichiers-ransomware-39836850.htm

BOYDRON M. H. (2018), « WannaCry, son histoire », *Cybercover*, disponible en ligne : https://www.cyber-cover.fr/cyber-documentation/cyber-criminalite/wannacry-son-histoire

CASTRO V. (2019), « WannaCry, un an après : les mesures prises par les acteurs touchés », *Cyberguerre-Numérama*, disponible en ligne : https://cyberguerre.numerama.com/648-wannacry-un-an-apres-les-mesures-prises-par-les-acteurs-touches.html

CERT-FR (2017), Bulletin d'alerte CERTFR-2017-ALE-007, disponible en ligne : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-007/

CNIL (2018), « Les violations de données personnelles », disponible en ligne : https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

DGSI – Intelligence économique (2017), « Les risques cyber liés aux rançongiciels », Flash n°34, http://auvergne-rhone-alpes.direccte.gouv.fr/sites/auvergne-rhone-alpes.direccte.gouv.fr/IMG/pdf/fi_n34_juin_-_risques_cyber_lies_aux_rancongiciels.pdf

F-SECURE blog (2017), « Ce que le RGPD dit à propos des ransomwares », disponible en ligne : https://blog.f-secure.com/fr/ce-que-le-rgpd-dit-a-propos-des-ransomware/

LIBÉRATION-AFP (2017), « Renault parmi les cibles d'une cyberattaque mondiale », disponible en ligne : https://www.liberation.fr/planete/2017/05/12/renault-parmi-les-cibles-d-une-cyberattaque-mondiale_1569124

MACKENZIE P. (2019), "WannaCry Aftershock", Sophos, disponible en ligne : https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf

MANACH J. M. (2017), « "WannaCry" n'est pas une cyberattaque, mais une escroquerie », *Slate*, disponible en ligne : https://www.slate.fr/story/145575/wannacry-cyberattaque-epicfail

MICROSOFT Corporation (2017), Bulletin de sécurité Microsoft MS17-010 – Critique, disponible en ligne : https://docs.microsoft.com/fr-fr/security-updates/SecurityBulletins/2017/ms17-010

MICROSOFT Corporation (2017), « Commencer la mise en application du Règlement général sur la protection des données (RGPD) pour Windows 10 », https://docs.microsoft.com/fr-fr/windows/privacy/gdpr-win10-whitepaper

NAO – National Audit Office (2018), "Investigation: WannaCry cyber attack and the NHS", disponible en ligne : https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

PASSWORDREVELATOR.NET (2019), « WannaCry, toujours la bête noire des responsables de la sécurité informatique ? », disponible en ligne : https://www.passwordrevelator.net/blog/tag/wannacry/

TANIUM (2019), "Disruption by Bridging the Resilience Gap Report", disponible en ligne : https://info.tanium.com/l/286192/2019-03-26/55dm6h

VIE PUBLIQUE (2019), « L'essentiel de la loi du 20 juin 2018 sur la protection des données personnelles », direction de l'Information légale et administrative, disponible en ligne : https://www.vie-publique.fr/eclairage/19591-protection-des-donnees-personnelles-essentiel-loi-cnil-du-20-juin-2018