Note numéro 26
août 2017

# Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

## WannaCry et la diffusion des « zero day exploits »

### Que s'est-il passé?

Le vendredi 12 mai 2017, WannaCry a commencé à affecter les ordinateurs dans le monde entier. L'épidémie a commencé en Asie au début de la matinée et s'est répandue dans la journée. Plus de 200 000 ordinateurs auraient été infectés.[1] A titre d'exemple, seize hôpitaux britanniques n'ont pas pu accéder à leurs systèmes. Des entreprises comme Renault, Deutsche Bahn et Telephonica ont également été touchées. Le 14 mai, les effets de WannaCry se faisaient sentir sur tous les continents.

L'origine de l'incident peut être attribuée à la National Security Agency (NSA). L'agence américaine chargée du renseignement via l'analyse des signaux électroniques a développé un outil, appelé EternalBlue, pour exploiter une vulnérabilité dans les anciennes versions du système d'exploitation de Microsoft. Ces versions ne bénéficient plus du support technique de l'entreprise américaine mais sont encore couramment utilisées. Par exemple, Windows XP, commercialisé en 2001, fonctionne toujours sur plus de 5 % des ordinateurs Windows. EternalBlue permet aux machines de recevoir des fichiers sur des ports réseaux censés être bloqués. Ce logiciel peut désactiver les machines, collecter du renseignement et atteindre d'autres objectifs en exploitant des vulnérabilités non connues des éditeurs de logiciel (ces vulnérabilités sont connues sous le nom de «« zero day exploits »).

Naturellement, les outils tels que EternalBlue devaient rester confidentiels mais la NSA a connu plusieurs fuites au cours de ces dernières années. Par exemple, le Federal Bureau of Investigation (FBI) a arrêté Harold Martin en 2016. Cet employé de Booz Allen Hamilton, un sous-traitant pour la NSA, a été mis en examen pour la détention illégale dans son garage de téraoctets de données et de codes informatiques confidentiels. En avril 2017, les Shadow Brokers, un groupe ayant des liens supposés avec les services de renseignement russes, mirent les outils de la NSA en ligne. Dès lors, toute personne possédant un minimum d'expertise technique pouvait les utiliser pour ses propres besoins. En réponse, Microsoft a développé un patch de sécurité pour combler la faille mais celui-ci n'a pas toujours été déployé par les utilisateurs. Par exemple, certains logiciels obtenus illégalement ne peuvent pas le télécharger.

D'autres logiciels tels que Wannacry et Adylbuzz ont ensuite été développés pour profiter d'EternalBlue. WannaCry est un rançongiciel (« ransomware »), un type de logiciel malveillant qui bloque l'accès aux données de la victime jusqu'à ce qu'une rançon soit payée. Le 12 mai 2017, lorsque WannaCry a commencé à affecter les ordinateurs en Asie tôt le matin, les victimes ont été invitées à payer 300 dollars en bitcoins dans les trois jours (le prix augmentant ensuite à 600

1Cependant, l'estimation semble avoir été faite en examinant le nombre de machines qui ont accédé à une URL liée à WannaCry, ce qui a pu conduire à une exagération significative du nombre de machines réellement infectées.

dollars). Le logiciel malveillant (« malware ») s'est ensuite répandu dans le monde entier. Cependant, un expert indépendant britannique a rapidement identifié une faille critique dans le programme : WannaCry essayait systématiquement d'accéder à une URL particulière (qui était directement codée dans le logiciel malveillant) et se désactivait s'il ne pouvait pas y accéder. Il est possible que cette procédure ait été conçue comme un dispositif de sécurité pour empêcher un examen du logiciel dans des environnements stériles (« sandboxes ») où l'accès à l'URL aurait été impossible. Dans le cas où le logiciel ne pouvait accéder à cette URL, il se désactivait pour empêcher l'examen du code. Lorsque l'analyste britannique a acheté l'URL (pour moins de 11 dollars), il a réussi à ralentir considérablement la propagation de WannaCry. Le 14 mars 2017, Microsoft a publié un patch de sécurité en urgence qui protégeait les utilisateurs de la version XP de son système d'exploitation. Le 15 mai 2017, l'attaque était essentiellement contenue. Le 18 mai, trois chercheurs français identifièrent un moyen de décrypter les fichiers infectés par WannaCry dans certains cas.

En parallèle du développement de WannaCry, un logiciel distinct baptisé Adylkuzz exploitait aussi la vulnérabilité EternalBlue. Le but de ce deuxième logiciel malveillant était différent de celui de WannaCry. Les crypto-monnaies telles que Bitcoin ou Ether sont des actifs numériques créés par des communautés décentralisées grâce à la mise en œuvre d'algorithmes sur des ordinateurs individuels. Ce processus (appelé « extraction minière » ou « mining ») nécessite du temps informatique et de l'électricité et coûte donc cher. Adylkuzz s'est concentré sur l'extraction de Monero (une crypto-monnaie axée sur la protection de la vie privée) dont la capitalisation boursière augmente régulièrement depuis 2014. Cependant, Adylkuzz s'assurait que les bénéfices de l'extraction allaient aux pirates informatiques. Ironiquement, l'une des fonctionnalités d'Adylkuzz était de combler la faille exploitée par EternalBlue. En d'autres termes, Adylkuzz a complètement protégé les machines infectées de WannaCry.

**Quelles ont été certaines des conséquences de WannaCry?**

WannaCry a été la plus grande attaque de rançongiciel de l'histoire. Son effet a été global avec, selon les estimations, des ordinateurs infectés dans plus de 150 pays en seulement 72 heures. La Russie, l'Ukraine et plus généralement les pays de l'ancienne Union Soviétique ont été particulièrement touchés. Les ordinateurs des ministères de l'Intérieur de la Russie et de la Chine ont été infectés. Cependant, les autorités conseillèrent le public de ne pas payer la rançon et ce conseil a été largement suivi. Les comptes Bitcoin mis en place par les pirates informatiques ont reçu un peu plus de 100 000 dollars et ce montant n'a pas été transféré jusqu'à présent. Si la motivation était financière, WannaCry a été un échec.

Les autres coûts sont difficiles à estimer. Aucun effet sur les infrastructures critiques et aucun effet durable majeur n'a été signalé. Par exemple, les hôpitaux britanniques ont récupéré des données sauvegardées et ont rapidement repris leurs opérations. Malgré l'ampleur de l'attaque, ses effets semblent être relativement peu importants pour l'économie mondiale et même pour les pays les plus touchés.

En réaction à WannaCry et à l'exploitation des actifs de la NSA, les législateurs des États-Unis ont décidé d'examiner la politique concernant la divulgation des «zero day exploits». La décision de publier une vulnérabilité identifiée par les services de renseignement américains est actuellement prise dans un cadre administratif, le



Rédacteur : Gilles Hilary,
Chaired Professor, Houston Term Professor,
Department of Accounting and Control, Georgetown University,
chercheur associé du Centre de recherche
de l'École des officiers de la gendarmerie nationale

Vulnerability Equities Process (VEP), qui suit une approche basée sur une analyse coût-avantage. Maintenir le secret autour des « zero day exploits » préserve un avantage certain pour les services de renseignement ou même pour les forces de l'ordre mais rend l'écosystème cyber plus vulnérable en préservant des failles de sécurité. Le 17 mai 2017, cinq jours seulement après l'émergence de WannaCry, les législateurs américains ont présenté un projet de loi, le Patch Act, pour formaliser le processus de décision et garantir l'examen des « exploits » par un conseil indépendant. Si elle est adoptée, la loi Patch créerait un cadre légal et non plus seulement administratif (et donc soumis au bon vouloir du pouvoir exécutif).

**Qui était derrière WannaCry?**

L'attribution de la responsabilité de WannaCry reste incertaine à ce stade et repose largement sur des preuves circonstancielles. WannaCry possède deux composantes, le vecteur d'infection des réseaux (la partie qui installe le logiciel malveillant dans les ordinateurs) et le crypto-verrouilleur (la partie qui crypte les fichiers). La première composante peut être attribuée directement à la fuite provenant de la NSA. Divers acteurs ont noté des similitudes dans la deuxième composante avec des codes informatiques qui ont été utilisés dans le passé par un groupe baptisé « Lazarus ». On a déjà attribué la responsabilité d'incidents cyber à ce groupe, probablement lié aux services de renseignement nord-coréens. Par exemple, Lazarus a été accusé d'exécuter différentes attaques par déni de service (DDoS) visant des organisations sud-coréennes dès 2009. Une attaque DDoS tente de rendre un service en ligne indisponible en le submergeant par du trafic provenant de sources multiples comme des chapelets d'ordinateurs préalablement infectés. Le groupe a aussi été accusé en 2014 d'avoir organisé le piratage de Sony Pictures qui entraîna la fuite d'un grand volume d'informations confidentielles et de films inédits. En 2016, Lazarus a été accusé d'avoir orchestré des cyberattaques contre trois institutions financières. En particulier, une attaque sophistiquée et intégrée sur la banque centrale du Bangladesh a presque conduit au vol d'un milliard de dollars (les paiements ont été arrêtés après la disparition de 80 millions de dollars).

Ces épisodes ont mis en évidence un degré croissant de sophistication dans le codage, le renseignement et la technique financière. A l'opposé, WannaCry a été mal exécuté, avec de nombreuses erreurs de programmation qui ont ralenti sa progression et ont rendu difficiles les paiements en ligne. Cela a conduit certains commentateurs à suggérer que le but de l'attaque était d'embarrasser la NSA plutôt que de collecter de l'argent. Une autre possibilité est que des individus associés à Lazarus aient exécuté l'attaque sans le soutien de l'organisation. L'analyse linguistique suggère que les notes de rançon ont été écrites par des individus parlant une forme de Chinois méridional (et non le coréen) ; Macao est souvent décrit comme une base d'opérations majeure pour les services nord-coréens.

**Que pouvons-nous apprendre de WannaCry?**

Sur le plan technologique, WannaCry n'a pas introduit d'innovations dans le codage et la menace de rançongiciel était déjà connue. EternalBlue a déjà été utilisé comme vecteur de pénétration par d'autres logiciels malveillants mais ceux-ci avaient des objectifs plus ciblés. Cependant, nous pouvons faire deux observations.



Rédacteur : Gilles Hilary,
Chaired Professor, Houston Term Professor,
Department of Accounting and Control, Georgetown University,
chercheur associé du Centre de recherche
de l'École des officiers de la gendarmerie nationale

Premièrement, les ordinateurs infectés exécutaient des versions anciennes de Windows qui ne bénéficient plus du support technique de Microsoft. Par exemple, les médias ont indiqué qu'une étude menée par la société de cybersécurité Citrix a révélé que 90 % des hôpitaux britanniques du NHS utilisaient encore Windows XP en 2016. Il peut être tentant d'attribuer cette dépendance à une technologie obsolète à l'incompétence et à un financement inadéquat. Cependant, il est important de noter que de nombreux dispositifs médicaux utilisent des logiciels spécialisés qui ne peuvent pas migrer facilement vers des systèmes d'exploitation plus récents. Ce problème d'évolution va probablement croître avec le développement des objets connectés qui font partie de systèmes complexes. Beaucoup de ces périphériques ne seront pas conçus avec des fonctionnalités de sécurité robustes et perdront le support technique de leur fabricant après quelques années de service. L'identification rapide des composants défectueux du système et l'installation de correctifs de sécurité qui ne dégradent pas leur interopérabilité vont devenir de plus en plus critiques.

Deuxièmement, WannaCry a fait la une des médias internationaux avec des titres tels que « la catastrophe de rançongiciel de WannaCry expliquée » (un exemple pris sur le site du Washington Post). Les dommages réels ont été plus limités que ce que ces manchettes ne suggèrent. Les prix des actions des entreprises vendant des produits de cybersécurité sophistiqués ont augmenté de manière significative, bien que les solutions techniques (par exemple, l'installation des correctifs de sécurité, les sauvegardes de données) soient relativement faciles à mettre en œuvre. L'impact perçu de WannaCry a été probablement plus grand que son effet réel. Les problèmes de sécurité informatique sont souvent difficiles à expliquer et peuvent être source d'anxiété pour le grand public. Les entreprises qui vendent des solutions de cybersécurité exacerbent naturellement ceci avec des messages alarmistes. Cette anxiété peut être directement exploitée dans le futur par des adversaires. Les grands États ont la capacité d'infliger des dommages très significatifs sur les infrastructures critiques mais de telles attaques engendreraient probablement des ripostes toutes aussi dévastatrices. En revanche, il serait difficile pour des États démocratiques de répondre à une campagne cyber qui infligerait des dommages symboliques importants mais des dégâts physiques minimaux, en particulier si cette attaque se déroule sous une fausse signature. Les exemples incluent des attaques à grande échelle visant les médias (comme sur TV5, par exemple) ou sur des panneaux électroniques dans des gares ou des aéroports couplés à des attaques limitées sur des objectifs importants (par exemple, en ciblant un petit nombre de systèmes de contrôle industriel dans les usines chimiques). Dans des scénarios comme celui-ci, l'impact des événements rares mais graves créerait l'impression de conséquences catastrophiques tandis que les cas bénins mais à fort impact médiatique créeraient une caisse de résonance. Les auteurs de telles attaques pourraient estimer qu'elles resteraient sous le seuil d'escalade en dépit de leurs conséquences politiques importantes. Dans ce contexte, une communication efficace des autorités est cruciale pour prévenir les réactions irrationnelles du public et pour minimiser les conséquences psychologiques des attaques cyber.



Rédacteur : Gilles Hilary,
Chaired Professor, Houston Term Professor,
Department of Accounting and Control, Georgetown University,
chercheur associé du Centre de recherche
de l'École des officiers de la gendarmerie nationale