Peur de W@nn@Cry ? Séchez vos larmes ! IBM Watson veille sur vous.

- Paru le 15 mai 2017

Chris Hankins, CISSP, CFCE

Directeur technique Sécurité cognitive Amérique du Nord

Savez-vous quel est le point commun entre les rançongiciels, les menaces avancées persistantes (APT) et le service public de la santé ? Réponse : une cyberattaque massive. Baptisée WannaCry, WanaCrypt ou Wcry, la nouvelle campagne de rançongiciel qui a ébranlé la planète le week-end du 13-14 mai constitue l'une des plus grandes attaques de rançongiciels (si ce n'est la plus grande) jamais connues à ce jour. L'attaque qui a infecté plus de 70 000 ordinateurs dans près de 100 pays devrait encore prendre de l'ampleur dans les jours à venir.

Victime d'importantes perturbations, le secteur public de la santé est devenu la cible privilégiée des cybercriminels. En témoigne le Royaume-Uni, où 16 hôpitaux ont ainsi été paralysés toute la journée du samedi 13 mai, désorganisant sérieusement sinon totalement la plupart de leurs services. Le rançongiciel a également touché plusieurs grandes entreprises en Espagne, en Chine et en Russie, comme Telefonica, mais également de nombreuses universités ainsi que le Ministère russe de l'intérieur.

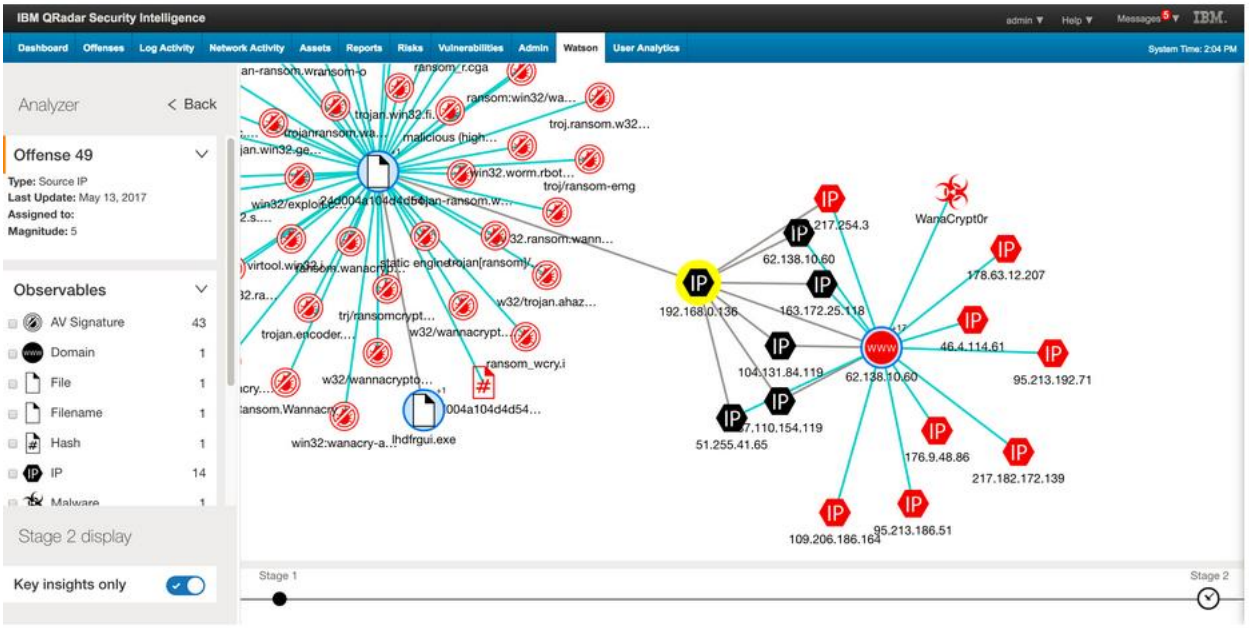
L'attaque exploite une faille de sécurité Microsoft Windows connue, appelée Eternal Blue (MS17-010 mars 2017) et récemment utilisée par le groupe de hackers Shadow Brokers pour dérober et dévoiler les outils et méthodes de chiffrement utilisés par l'Agence américaine du renseignement (la NSA). Même si aucune attribution n'a été associée aux attaques du rançongiciel WannaCry, cette cyberattaque mondiale montre à quel point les cyberattaques modernes standard deviennent de plus en plus sophistiquées grâce à l'exploitation des informations dérobées à des agences nationales. Je pense que nous commençons tout juste à constater l'impact de l'attaque de ce rançongiciel, et de nombreuses connaissances sur la menace ont été compilées et sont d'ores-et-déjà disponibles sur la Toile. À l'heure où la cyberattaque se propageait, nos équipes IBM Security et leurs téléphones portables (ainsi que le mien) sont restés sur le qui-vive tout au long du week-end et ont été vivement sollicités par de nombreux interlocuteurs qui s'interrogeaient sur nos capacités de détection et de protection face à cette menace grandissante. On ne pouvait pas rêver meilleur scénario pour tester les connaissances de Watson for Cyber Security en matière de détection des menaces en temps réel !

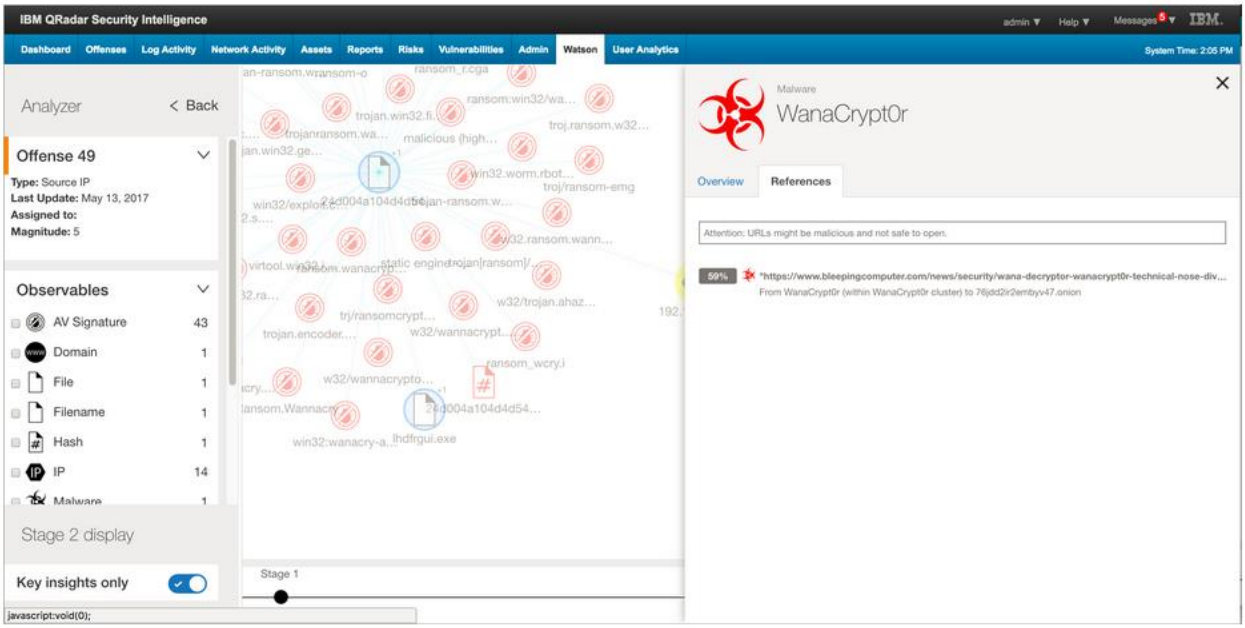
J'ai commencé à lire les différents articles publiés afin de déterminer si Watson était sur la bonne voie, mais également pour savoir comment la petite équipe d'IBMers dédiés et moi pouvions formuler une simulation d'attaque et obtenir les données observables appropriées pour démontrer le potentiel de Watson. IBM X-Force a posté un article très intéressant sur WannaCry, ainsi que son travail approfondi ici, par où j'ai commencé.

Le rançongiciel WCry (WanaCryptor et WannaCry) a au moins eu le mérite de sensibiliser le public sur l'importance des mises à jour de sécurité Microsoft. En effet, la vague de cyberattaques a permis de mettre en évidence deux problèmes majeurs qui ont été clairement identifiés dans tous les articles que j'ai lus à propos de cette menace : la mauvaise hygiène des systèmes (ou le défaut d'application des correctifs de sécurité adéquats) et l'utilisation de versions obsolètes et non sécurisées du système d'exploitation Windows. L'exposition d'un si grand nombre de systèmes à la faille de sécurité MS17-010 a ainsi permis au rançongiciel de se propager rapidement en utilisant les protocoles SMBv1. En fait, les systèmes auraient dû être patchés au moment même où Microsoft a publié son bulletin de sécurité en mars dernier et notamment lorsqu'on s'est rendu compte que l'exfiltration Shadow Brokers avait été atténuée par le patch. Malgré tout, la cyberattaque a fait son chemin et réussi à passer la seconde ligne de défense : les antivirus.

Ceux d'entre vous qui me connaissent bien ou qui m'ont déjà entendu parler de la sécurité générale savent ce que je pense des antivirus traditionnels basés sur les signatures : selon moi, ils sont tout bonnement inefficaces dans les environnements de sécurité modernes. Ils sont juste là pour contenter les auditeurs, et les attaques émergentes telles que celle que nous venons d'essuyer ne font que montrer leur impuissance. Par exemple, l'exécutable WCry n'a été détecté que par quelques antivirus le matin du 12 mai lorsque l'attaque a commencé à se propager. Vingt-quatre heures plus tard, tandis que centaines de données observables étaient partagées en temps réel, l'attaque n'était toujours pas détectée par de nombreux programmes antivirus.

Qu'en est-il de QRadar Advisor et de Watson for Cyber Security, et de leur approche cognitive en matière de détection et de réponse aux incidents ? Vous vous demandez sûrement comment Watson peut nous aider à lutter contre des logiciels jamais vus auparavant. L'apprentissage cognitif permet d'extrapoler d'importants volumes d'informations non structurées par rapport à l'être humain. Les connaissances sont extraites et à partir de blogues, de wikis ou encore de scripts de virus, puis sont publiées sur la Toile et s'enrichissent à mesure que nous en apprenons davantage sur la menace elle-même et sur ses morphes visant à détourner les logiciels de détection et à enrichir l'auteur de la menace. Or, les connaissances disponibles sont trop nombreuses pour qu'un consommateur humain puisse y accéder et les lire en temps réel ! Watson for Cyber Security explore le Web en continu, à la recherche de données de cybersécurité structurées et non structurées. Il est capable de mettre en évidence des relations distinctives imperceptibles parmi des millions de points de données et de reconnaître ces modèles de comportements pour fournir à l'analyste de sécurité le contexte et l'information dont il a besoin pour déterminer la menace identifiée et les aspects à prioriser pour les efforts d'investigation et de réponse aux incidents. Ainsi, notre équipe a travaillé jusqu'à tard dans la nuit le week-end du 13-14 mai pour recréer les différentes étapes de l'attaque. Comme le montre l'image ci-dessous, QRadar Advisor et Watson ont réussi à détecter WanaCryptor et à fournir rapidement les données observables nécessaires pour poursuivre l'investigation en se fondant sur des connaissances non structurées de la menace.





Grâce à des fonctionnalités, une rapidité et une précision sans égales, Watson constitue la solution idéale pour aider les analystes dans leurs investigations. En tant qu'analyste de sécurité, vous savez que Watson seul ne suffit pas et que vous devez mettre en œuvre d'autres outils. C'est pourquoi notre équipe IBM Security a travaillé d'arrache-pied tout au long du week-end du 13-

14 mai pour s'assurer que nos clients savent comment détecter et gérer wCry2 en leur prodiguant quelques conseils :

Comment IBM peut-il vous aider à vous protéger de wCry2 ?

Une nouvelle semaine de travail a commencé : toutes nos équipes internationales ont repris le chemin du bureau, se sont installées derrière leur écran et découvrent les derniers rebondissements concernant la cyberattaque qui a touché la planète ce week-end. Des centaines de nouveaux cyberblogues et rapports ont été publiés, et nous devrions être capables de mieux appréhender l'envergure et l'impact du rançongiciel wCry2. Néanmoins, il y a trois choses dont nous sommes certains. 1) La menace change au moment même, où nous apprenons à la connaître et à publier des informations à son sujet. 2) Les données et connaissances partagées vont continuer à être disséminées sous de nombreuses formes afin de nous aider à planifier nos plans de défense et de reprise. 3) La solution Watson for Cyber Security sera là pour nous aider et répondre à vos questions.