WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA

Mise à jour le 14/05 à 8h30 et le 15/05 à 17h50.

Il a semé la panique en Espagne, puis dans le monde entier. En quelques heures, le ransomware WannaCry, connu aussi sous le nom WanaCryptor ou WCry, s'est taillé un succès planétaire, multipliant les infections dans plus de 70 pays. Parmi ses victimes, l'opérateur Telefonica, les banques BBVA et Santander, le fournisseur d'électricité Iberdrola, le logisticien Fedex, la compagnie ferroviaire allemande Deutsche Bahn ainsi que l'opérateur de télécommunications Vodafone, mais aussi, en France, Renault. Le constructeur a admis avoir été pris dans la nasse de WannaCry, entraînant la mise à l'arrêt de certains sites de production afin « *d'éviter la propagation du virus* ». De source syndicale, l'usine de Sandouville (Seine-Maritime), qui emploie 3400 salariés, serait ainsi concernée, tout comme le site d'une filiale du groupe en Slovénie, à Novo Mesto. L'Anssi explique qu'aucune autre infection majeure ne serait à déplorer dans l'Hexagone.

Outre-Manche, c'est la NHS, l'organisme gérant la santé des Britanniques, qui a été durement frappé. Son système informatique a quasiment été paralysé par l'attaque entraînant des reports d'interventions jugées non urgentes dans un grand nombre d'hôpitaux. Au total, outre Manche, 48 entités de la NHS (un cinquième du total) ont été touchées, a reconnu l'organisation, qui n'écarte pas totalement d'éventuelles pertes de données. Samedi après-midi, l'activité de 6 entités de NHS demeurait perturbée. En somme, une cyberattaque d'un « *niveau sans précédent* » selon Europol. Dans la nuit de vendredi à samedi, un ingénieur de l'éditeur d'antivirus Avast, Jakub Kroustek, dénombrait plus de 100 000 systèmes Windows infectés en moins de 24 heures, 57 % d'entre eux étant situés en Russie.

Les failles SMB de Windows récupérées

Le mécanisme d'infection est pourtant des plus banals. WannaCry est un ransomware dont la première version a été détectée pour la première fois le 10 février dernier par un chercheur de Malwarebytes. La souche a fait ses premiers pas lors d'une brève campagne menée le 25 mars dernier. Sa deuxième version, qui a démarré ses ravages massifs le 12 mai, conserve les caractéristiques essentielles d'un ransomware : l'envoi par un e-mail piégé, une pièce jointe (Word ou PDF) qui déclenche l'infection, un chiffrement des données (documents, images, musique et autres) et une demande de rançon en bitcoins afin de

restaurer l'accès aux informations prises en otage (dans le cas présent, l'équivalent de 300 dollars).

Si WannaCry dépasse dans sa rapidité de diffusion tout autre ransomware connu à ce jour, y compris le tristement célèbre Locky, c'est qu'il s'appuie sur un second mécanisme amplifiant son potentiel de destruction. Un second effet Kiss-Cool reposant sur les failles du serveur SMB (Server Message Block) de Windows et Windows Server. Des vulnérabilités manifestement exploitées par la NSA, puisqu'elles servaient de socle à divers outils d'espionnage de l'agence américaine dévoilés par les Shadow Brokers, un mystérieux groupe de pirates qui a éventé de nombreux secrets de l'organisation de Fort Meade entre août 2016 et avril 2017.

Notons que cette infection en deux temps est en partie contestée. Quatre jours après l'attaque, des experts français estiment que les assaillants ont en réalité directement infectés les systèmes vulnérables, repérés sur Internet. Shuntant l'étape du phishing, habituellement incontournable dans tout campagne de ransomware (lire notre article sur ce sujet précis).

EternalBlue made in NSA

Tous basés sur les vulnérabilités de SMB et placés en accès libre sur la toile par les Shadow Brokers, les exploits EternalBlue, EternalChampion, EternalSynergy et EternalRomance, faisant partie du kit FuzzBunch, chargent DoublePulsar sur les systèmes compromis. Cette charge utile, qui se loge en mémoire, permet à un assaillant d'exécuter le shellcode de son choix sur le système Windows détourné et de charger d'autres malwares. C'est manifestement ce mécanisme qu'ont exploité les auteurs de WannaCry pour accélérer la diffusion de leur souche.

Dans son alerte, le CERT espagnol explique d'ailleurs que l'infection exploite EternalBlue et DoublePulsar, ce qui « *permet l'exécution de commandes à distance au travers de Samba (SMB) et une distribution (du ransomware, NDLR) aux autres machines Windows présentes sur le même réseau* ». Samba est le logiciel pour systèmes Unix permettant le partage d'imprimantes et de fichiers sur un réseau, en gérant l'interopérabilité avec le protocole SMB de Microsoft. Pour ce dernier, qui détaille le fonctionnement de la menace dans un billet de blog, on a affaire à « *un ransomware standard armé de fonctions de type ver informatique* ».

WannaCry surfe sur la persistance de Windows XP

Pour les spécialistes, ce scénario noir, qui voit des pratiques cybercriminelles s'emparer d'outils de hacking ultra-perfectionnés développés par des Etats, ne constitue pas une surprise. Dès la fin avril, un rapport de Recorded Future, une société américaine spécialisée dans l'intelligence sur les menaces, expliquait que les communautés de pirates chinois et russes avaient commencé à étudier les malwares dévoilés en avril par les Shadow Brokers. Avec un intérêt particulier pour les exploits ciblant les vulnérabilités SMB. « *On parle ici de techniques et outils très sophistiquées, généralement hors de portée de la communauté underground* », expliquait alors Levi Gundert, un des dirigeants de Recorded Future.

Si Microsoft a déjà patché les vulnérabilités qu'exploitent ces outils – de façon surprenante dès mars 2017, soit un mois avant la divulgation des malwares par les Shadow Brokers -, les pirates chinois échangeant sur les forums underground ne semblaient pas totalement persuadés de la

solidité de ces correctifs, selon Recorded Future. Par ailleurs, l'attaque reste valide contre les systèmes non patchés (pour une raison ou une autre) ou contre les versions d'OS qui ne sont plus supportées par Redmond. A Londres, la NHS est ainsi sous pression du fait des machines sous Windows XP qu'il exploite encore (près de 5 % du parc). Dans l'industrie, la santé, mais aussi dans les médias (comme l'avait montré l'affaire TV5 Monde), de nombreux systèmes tournent encore sous cet OS dépassé, en raison des applications très spécifiques qu'ils font tourner. Un OS qui ne reçoit plus de patchs de sécurité, Microsoft ayant cessé tout support sur ce produit.

WannaCry stoppé… par un coup de chance

Devant l'urgence de la situation, Microsoft a d'ailleurs sorti des correctifs pour les failles SMB sur Windows XP (y compris la version Embedded SP3), Windows Server 2003 et Windows 8. Une démarche « *inhabituelle* », explique Redmond dans un billet de blog en raison de l'urgence de la situation. L'éditeur précise que Windows 10 n'est pas touché. Mais s'attend à voir la menace évoluer afin de contourner les premières défenses mises en place. Redmond recommande ainsi de désactiver – si possible – le protocole SMB sur le réseau afin d'éviter de nouvelles mésaventures.

Pour l'instant, WannaCry est toutefois en décroissance rapide… suite à un coup de chance. Dans un billet de blog, le chercheur en sécurité connu sous le pseudo MalwareTech explique comment, en enregistrant un domaine apparaissant dans le code du malware, il a en réalité bloqué l'exécution de WannaCry et stoppé sa diffusion. D'après le chercheur, le domaine libre qu'il a enregistré correspondrait en réalité à une sécurité imaginée par les développeurs du malware, afin d'éviter les analyses par les systèmes de sécurité basée sur des sandbox. Mais, la sécurité offerte par ce coup de chance n'offre en réalité qu'un bref répit, les concepteurs de la souche pouvant très facilement modifier leur création pour contourner cet écueil. De facto, dès ce samedi, Costin Raiu, directeur de recherche et de l'équipe d'analyse du Kaspersky Lab, notait l'apparition de nouvelles versions dont la diffusion n'est plus entravée par les opérations de MalwareTech. La menace WannaCry est donc loin d'être totalement écartée.

A lire aussi :

Le ransomware WCry sème la pagaille en Espagne

Les cybercriminels s'emparent des outils de hacking de la NSA

Les Shadow Brokers publient les outils de hacking de serveurs de la NSA