Hacking de Moscou contre les Etats-Unis ? Les experts ne sont pas convaincus

Ni le rapport conjoint du FBI et du ministère de l'Intérieur américain (Department of Homeland Security ou DHS), ni la version déclassifiée du rapport remis au président des Etats-Unis Barack Obama par la communauté du renseignement n'auront rien changé à l'affaire : les spécialistes de la sécurité restent sur leur faim quant aux preuves de l'implication concrète de Moscou dans les différents piratages ayant émaillé la récente campagne présidentielle américaine.

Rappelons que l'administration américaine sortante ne s'embarrasse pas de périphrases pour accuser Vladimir Poutine d'avoir orchestré une campagne de déstabilisation de la candidate démocrate, Hillary Clinton, afin de favoriser son concurrent Donald Trump, réputé plus proche des positions de Moscou. Un Donald Trump qui prendra ses fonctions dans 10 jours et qui a, lui aussi, été briefé par les services de renseignement américains sur les conclusions de leur enquête. Après avoir dénigré sur Twitter les accusations des services de renseignement, le président élu a publié, vendredi dernier, un communiqué plus mesuré où il se contente d'indiquer que les cyber-attaques, d'où qu'elles viennent, n'ont eu aucun effet direct sur le processus électoral, comme l'indique d'ailleurs le rapport des services de renseignement.

Indicateurs techniques de mauvaise qualité

Si l'affaire a mis au jour des lignes de failles politiques, si elle engendre bien des questions sur la transition du pouvoir outre-Atlantique, elle n'a suscité, chez la plupart des spécialistes en cybersécurité, que scepticisme. En effet, si la version déclassifiée du rapport remis à Barack Obama ne comprend aucune information technique (afin de ne pas révéler « *des sources ou méthodes qui pourraient mettre en péril notre capacité à collecter des renseignements essentiels dans le futur* », explique le rapport), le document publié par le FBI et le DHS fin décembre 2016, lui, s'y aventure. Décrivant une cyber-opération menée par Moscou – baptisée Grizzly Steppe – avec, à l'appui de ses affirmations, des adresses IP et des signatures de malware censées pointer la responsabilité des services de renseignement russes (le FSB, héritier du KGB, et le GRU, les renseignements militaires). Des éléments qui ont évidemment suscité la curiosité des experts en cybersécurité. Et leur déception.

« *Les IoC (indicateurs de compromission, autrement dit les données techniques permettant de caractériser l'attaque, NDLR) dévoilés sont de très faible qualité, certaines adresses IP sont des adresses génériques liées à des services Internet classiques ou des nœuds de sortie Tor utilisés par de très nombreuses personnes*, résume Gérôme Billois, senior manager en gestion des risques et sécurité chez Wavestone. *On aurait pu penser que certains IoC de bonne qualité seraient révélés pour déstabiliser les équipes d'attaques concernées et les obliger à faire évoluer leur infrastructure, mais ce n'est à première vue pas le cas.* » Les conclusions sont similaires pour Loïc Guézo, expert cybersécurité de Trend Micro pour l'Europe du Sud, qui voit dans le rapport décrivant l'opération Grizzly Steppe une « *compilation d'éléments* » déjà en grande partie connus par les spécialistes. « *Sur l'analyse technique, beaucoup de points sont discutables* », ajoute-t-il.

Sony Pictures : la Corée du Nord, vraiment ?

Bref, s'il s'agissait de convaincre la communauté de la sécurité de l'implication des Russes dans le piratage des démocrates, le coup est raté. « *Je n'ai pas le sentiment que les Etats-Unis aient vraiment les moyens de nous démontrer, par des éléments techniques, l'implication russe*, résume Hervé Schauer, le fondateur de HSC et membre du conseil d'administration du Clusif. *Mais cette difficulté n'est pas spécifique à cette affaire en particulier. L'attribution reste un exercice complexe, car les possibilités de manipulation sont multiples* ». Et Hervé Schauer de remarquer par ailleurs que Barack Obama a déjà soutenu que la Corée du Nord était à l'origine du piratage de Sony Pictures : « *ce qui n'a aujourd'hui pas la moindre crédibilité auprès des experts de sécurité informatique* », tranche-t-il.

Pour Jeffrey Carr, un consultant en cybersécurité qui a décortiqué le rapport du FBI et du DHS dans un billet de blog, ce document se contente d'énumérer « *toutes les menaces signalées par une société privée en sécurité (une référence à Crowdstrike qui a été appelé à la rescousse par le comité national démocrate après son piratage, NDLR), menaces qui seraient fabriquées en Russie et rassemblées sous la bannière des services secrets russes, sans fournir aucune preuve qu'une telle connexion existe.* » Et de rappeler qu'une fois déployé, un malware échappe par définition à son créateur ou à son premier utilisateur. « *Il peut être disséqué par rétro-ingénierie, copié, modifié, partagé et redéployé encore et encore par n'importe qui* », écrit Jeffrey Carr. Ce dernier explique par exemple que la souche X-Agent, qui aurait été utilisée dans le piratage du comité du parti démocrate américain, a aussi été employée contre le Bundestag ou TV5 Monde et qu'elle a été récupérée par l'éditeur Eset. « *C'est à fois insensé et sans fondement d'affirmer, comme le fait Crowdstrike, que X-Agent est seulement utilisé par le gouvernement russe alors que le code source est disponible pour qui souhaite l'employer* », s'énerve Jeffrey Carr.

Outils typiques pour hackers typiques

D'autres analystes pointent d'autres faiblesses des indicateurs techniques publiés par le rapport sur l'opération Grizzly Steppe. Pour Marcus Ranum, un pionnier des firewalls et membre du IANS (un institut de recherche et de conseil de Boston spécialisé dans la cyber), le rapport censé montrer l'implication d'APT 28 et APT 29 (deux noms de code associés aux services secrets russes du FSB et du GRU) n'est en fait qu'une énumération « *d'outils typiques disponibles pour quiconque possèdent un PC connecté et des mauvaises intentions, des outils utilisés par des hackers typiques dans le cadre de hacking typiques.* » Et l'expert de railler : « *ainsi quelqu'un a envoyé à un membre d'un parti politique américain un malware, qui a été activé et un hacker quelconque a fait ce que tout autre hacker aurait fait. J'attends toujours de voir comment et pourquoi il s'agirait de Russes.* »

De son côté, Robert Graham, le Pdg de la société Errata Security, se penche sur la règle Yara dévoilée par le rapport JAR (Joint Analysis Report) du FBI et du DHS. Un indicateur prisé des chercheurs en sécurité pour analyser des attaques réussies, via l'identification d'indices sur les systèmes compromis. La signature livrée par le FBI et le DHS renvoie vers un web shell (des scripts permettant à des pirates d'interagir avec des serveurs) populaire au sein des communautés de hackers russe et ukrainienne. Sauf que le code source de ce shell (PAS TOOL WEB KIT) est librement disponible sur Github et que l'outil lui-même peut être téléchargé simplement par n'importe qui. « *Le problème, c'est que ce web shell PAS est [...] utilisé par des centaines voire des milliers de hackers, souvent*

associés à la Russie, mais aussi dispersés dans l'ensemble du monde (si j'en juge par les posts sur les forums de hackers), écrit Robert Graham. *Ce qui rend l'utilisation de la signature Yara problématique pour toute tentative d'attribution : ce n'est pas parce que vous trouvez des traces de PAS à deux endroits différents que vous aurez affaire au même hacker.* »

Provoquer des fausses alertes

Et c'est probablement là l'échec principal du rapport JAR : il ne fournit aucune indication réellement utile à des organisations tentant de se défendre des assaillants qui ont piraté le comité démocrate. Pour Aaron Turner, le vice-président de la sécurité de Verifone, l'une de ses plus grosses lacunes est de n'avoir pas établi de relations entre les différents indicateurs publiés, « *ce qui rend la majorité du rapport sans intérêt en matière d'intelligence sur les menaces* ». « *Les indicateurs ne sont pas très détaillés et vont générer un taux élevé de faux positifs pour les défenseurs qui vont les utiliser* », abonde Robert Lee, Pdg et fondateur de la société de cyber-sécurité Dragos.

Si Gérôme Billois reconnaît que le risque de faux positifs est bien présent, il estime malgré tout que la publication des IoC dans le JAR peut offrir aux organisations une opportunité d'alerter les autorités « *qui, elles, pourraient procéder à des analyses avec des indicateurs de compromission de bien meilleur qualité ; indicateurs que les services de renseignements doivent posséder étant donné les accusations proférées* ». Ce qui d'ailleurs s'est produit avec un fournisseur d'électricité du Vermont ; ce dernier a détecté sur son réseau une menace issue du rapport. Sauf qu'il s'agissait largement d'une fausse alerte, le malware en question ne touchant qu'un seul PC non raccordé aux infrastructures critiques de l'entreprise.

A lire aussi :

Comment la Russie crée des unités d'élite de pirates informatiques

Piratage des élections U.S. : tout a commencé par du spearphishing

L'élection de Trump brouillée par le piratage