Le ransomware GoldenEye infecte plusieurs entreprises, dont Saint-Gobain

Nouveau coup de chaud dans la cybersécurité. En milieu d'après-midi, des messages apparus sur Twitter laissent entrevoir une campagne d'infection par un ransomware aussi dévastatrice que WannaCry. A l'heure où nous écrivons ces lignes, la campagne apparaît en effet massive et a fait des victimes en Ukraine, en Russie, en Espagne, en Grande-Bretagne et aussi en France. Dans l'Hexagone, le groupe Saint-Gobain a confirmé avoir été touché aujourd'hui par un ransomware. Joint par la rédaction, un porte-parole du groupe industriel indique avoir « *isolé les systèmes informatiques par mesure de sécurité* », sans toutefois être à même de préciser comment cette mesure impacte l'activité de la société. « *L'incident est en cours de résolution* », indique le service communication de l'entreprise. Pour chaque PC compromis, les hackers réclament l'équivalent de 300 $ de rançon, payés en bitcoin.

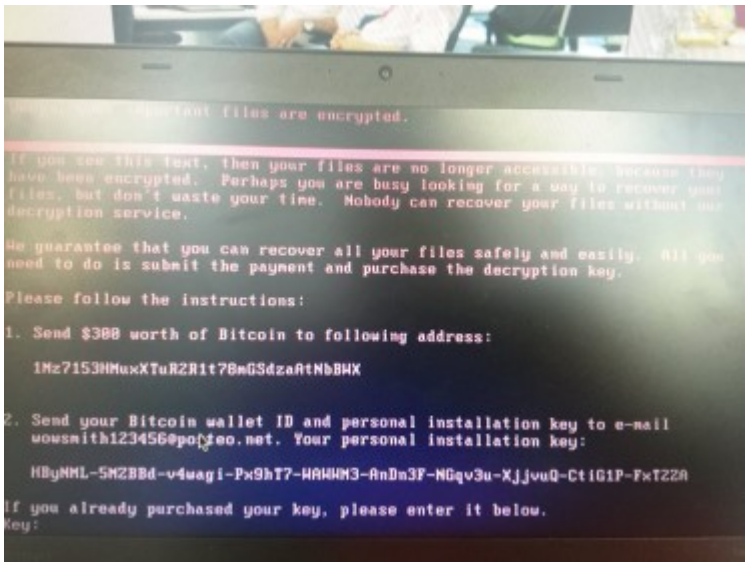
A l'heure actuelle, les autres entreprises françaises victimes de cette campagne infectieuse ne sont pas encore connues. Mais des entreprises globales comme le transporteur maritime Maersk ou le pétrolier russe Rosneft ont déjà confirmé être touchés.

« *L'alerte est venu des utilisateurs ce midi*, raconte Gérôme Billois, senior manager en gestion des risques et sécurité de Wavestone. *Nous sommes sur des niveaux de contamination similaires à ceux de WannaCry. Même si cette nouvelle infection cible plutôt des postes bureautiques. A l'instant t, des centaines de PC sont touchés chez nos clients, mais l'outil de production semble lui épargné.* » Rappelons que WannaCry avait de son côté fait de nombreux dégâts sur des applications métier ou industrielles, comme chez Renault ou à la Deutsche Bahn.

L'hypothèse Petya ou GoldenEye

L'alerte est venue un peu plus tôt d'Ukraine, où la banque centrale a indiqué que diverses banques et entreprises du pays (dont le métro de Kiev, les services postaux, l'opérateur télécoms principal et le distributeur national d'énergie Ukrenergo) ont été visées par une attaque qui a perturbé leur fonctionnement habituel. Rappelons que l'Ukraine a été la cible de plusieurs cyberattaques spectaculaires, dont deux sont parvenues à provoquer des pannes d'électricité (en décembre 2015 et décembre 2016). Cette fois, l'approvisionnement en électricité ne semble pas menacé.

Selon divers experts en cybersécurité, la campagne en cours serait orchestrée avec une variante de Petya, une souche connue depuis le début 2016 et qui a la particularité de chiffrer l'intégralité du disque dur afin de contrarier les efforts de récupération de données des victimes. « *Étant donné l'écran de demande de rançon qui s'affiche au redémarrage, et qui ne ressemble pas à un écran Windows, l'hypothèse Petya est pour l'instant la plus probable* », dit Gérôme Billois. Selon l'éditeur BitDefender, il s'agit plutôt d'une variante de GoldenEye, un ransomware ayant le même fonctionnement que Petya mais pour lequel il n'existe aucun outil permettant à une victime de retrouver les clefs avec lesquelles ses données ont été chiffrées.



BitDefender explique que GoldenEye renferme deux couches de chiffrement: une qui crypte individuellement les fichiers cibles sur l'ordinateur et une autre qui chiffre l'ensemble du système de fichiers NTFS. Ce qui empêche toute tentative de démarrage du disque dur pris en otage depuis un autre système.

L'hypothèse du ransomware dormant

Reste à connaître le mode de diffusion de cette nouvelle menace. Le caractère massif de l'infection laisse supposer que le ransomware se diffuse comme un ver, à l'instar de WannaCry, et non plus via des mails infectieux comme le faisaient Locky ou Cerber. Selon l'éditeur d'antivirus Avira, la nouvelle souche exploiterait, comme WannaCry, la faille EternalBlue, touchant le service SMB de Windows. Une vulnérabilité que Microsoft a corrigée, y compris pour des systèmes qui ne sont plus supportés comme Windows XP.

« *La principale question est de savoir comment ce malware a réussi à infecter autant de postes en si peu de temps*, analyse Gérôme Billois. *Soit la souche exploite EternalBlue pour se diffuser, mais ce serait une grosse surprise car, alertés par la crise WannaCry, les entreprises ont massivement corrigé cette faille. Soit la menace passe par une faille inconnue. Soit on a affaire à une bombe logique programmée pour se déclencher simultanément partout dans le monde.* » Bref, un malware dormant qui, d'ailleurs, a très bien pu exploiter EternalBlue pour se diffuser avant que cette vulnérabilité ne soit comblée…

A lire aussi :

Le ransomware Petya verrouille complétement le disque dur

WannaCry : le ransomware qui n'a plus besoin du phishing

Jean-Louis Lanet, Inria : « si le ransomware parfait existait… »

Photo : portalgda via VisualHunt / CC BY-NC-SA