COVID-19 – Plusieurs alertes cyber du CISA en collaboration avec le Royaume-Uni

Le 8 avril dernier, l'Agence pour la Sécurité des Infrastructures et la Cybersécurité (en anglais *CISA,* fait partie du Département de la Sécurité Intérieure) a publié conjointement avec le Centre National de Cybersécurité (NCSC) du Royaume-Uni une alerte [1] par rapport aux attaques d'acteurs malveillants profitant de la crise du COVID-19.

Parmi les types d'attaque, le communiqué liste l'hameçonnage (*phishing*) ou la distribution de logiciel malveillant qui dans les deux cas ont recours à des messages incitatifs liés au COVID-19. Les autorités ont également observé l'enregistrement d'un grand nombre de noms de domaine contenant des mots-clés associés au virus. Enfin, un autre type d'attaque fréquent vise les ordinateurs qui accèdent à distance aux réseaux de leurs entreprises et autres infrastructures déployées pour le télétravail (comme les *VPN*).

Des attaques qui visent les chercheurs

Outre la croissance du nombre d'attaques cyber en général, la CISA et le NCSC soulignent que les chercheurs mais également les entreprises pharmaceutiques sont des cibles privilégiées dans la période de crise actuelle.

Le 5 mai, les deux agences publient une nouvelle alerte commune appelant à la vigilance. Selon l'annonce, le but de ces attaques serait de collecter des données personnelles en masse, de la propriété intellectuelle ou du renseignement et autres informations sensibles en lien avec des intérêts nationaux (pour faire avancer la recherche de médicaments dans leur pays, par exemple).

Plusieurs procédés sont décrits. En premier lieu, les *hackers* peuvent identifier des cibles vulnérables parmi les différents sous-traitants en analysant les chaînes logistiques des entreprises et en misant sur le fait que les logiciels qu'ils utilisent ne soient pas mis à jour correctement. Une autre méthode appelée *password spraying* consiste à réutiliser une série de mots de passe communs (du type *password1234, bonjour2020, soleil123,* des dates de naissance etc.) sur un grand nombre de comptes. Cette dernière technique est moins facilement détectable car il y a moins de chance de verrouiller les comptes qu'en utilisant la méthode *brute force* (dans laquelle le *hacker* saisit un grand nombre de mots de passe sur un même compte).

Un autre document, publié le 13 mai (cette fois-ci par le FBI et la CISA [3]), pointe l'Etat chinois du doigt pour ce qui concerne les tentatives de vol de propriété intellectuelle et d'accès à des données de santé publique liées aux vaccins, traitements et tests de dépistage.

Parmi les recommandations faites, une vigilance accrue et du personnel dédié à la cybersécurité au sein des organisations sont préconisés. La mise à jour des systèmes informatiques et l'installation de patchs corrigeant les vulnérabilités connues est également recommandée ainsi qu'une veille active des applications Web pour des cas d'accès non-autorisés, de modification de fichiers ou d'autres activités suspectes.

L'association d'un établissement de recherche avec le COVID-19 par la presse doit également faire craindre un intérêt augmenté pour les *hackers* de s'en prendre à l'organisation.

[1] https://www.us-cert.gov/ncas/alerts/aa20-099a

[2] https://www.us-cert.gov/ncas/alerts/AA20126A

[3]
https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf

Rédacteur :

Kevin KOK HEANG, Attaché adjoint pour la Science et la Technologie, deputy-ntics@ambascience-usa.org