Zero day Microsoft Word : l'auberge espagnole pour hackers d'Etat et cybercriminels

Escrocs et espions se partageant la même gamelle. C'est un peu le tableau que décrit FireEye au sujet de la faille zero day de Microsoft Office, mise au jour par l'éditeur américain. Dévoilée en fin de semaine dernière par FireEye et McAfee et patchée depuis par Microsoft, cette vulnérabilité permet à des assaillants d'exécuter du code sur les machines cibles, via un fichier RTF piégé. Si cette faiblesse de la suite Office a été exploitée depuis sa divulgation publique le 7 avril (notamment via une campagne tentant d'installer le malware bancaire Dridex), elle l'a surtout été avant.

Pour FireEye, la faille – CVE-2017-0199 – a été mise à profit dès le début de l'année à la fois par un acteur étatique et par un groupe de cybercriminels, motivé par l'appât du gain. « *Et des similitudes dans leurs implémentations suggèrent qu'ils ont obtenu le code de l'exploit de la même source* », ajoute FireEye. L'éditeur n'est toutefois pas catégorique sur ces points. La société américaine écrit avoir une « *confiance modérée* » dans ses conclusions. Preuve que tout n'est pas encore totalement clair dans cette affaire.

Finspy pour l'espionnage, Latentbot pour les menus larcins

FireEye n'en décrit pas moins une campagne organisée d'infiltration basée sur la faille de Word. Dès le 25 janvier dernier, de faux documents, faisant référence à un décret du ministère de la Défense russe ou à un manuel prétendument publié par la République populaire du Donetsk (un Etat sécessionniste de l'Ukraine), s'y engouffrent pour tenter d'installer Finspy. Une veille connaissance puisqu'il s'agit là d'un développement de Gamma Group, une société germano-britannique vendant des technologies d'espionnage à des gouvernements. Un prestataire dont 40 Go de données ont été piratés en 2014, aboutissant à la publication notamment de ses codes source et de ses clients.

En mars 2017, FireEye observe une seconde campagne ciblant CVE-2017-0199, cette fois afin de distribuer le malware Latentbot. Une souche, découverte en décembre 2015, permettant de dérober des codes d'accès à ses victimes, d'effacer des données ou de désactiver des logiciels de sécurité. Ce malware est plutôt employé dans le cadre d'activités cybercriminelles. Par ailleurs, cette seconde campagne n'emploie pas des documents officiels piégés destinés à des cibles russophones, mais plutôt des sollicitations classiques utilisées par les cybercriminels dans leurs opérations de spearphishing.

Mais, pour FireEye, ces deux campagnes, aux motivations très différentes, auraient… une origine commune. « *Des artéfacts communs (en particulier l'heure de la dernière mise à jour, NDLR) dans les échantillons de Finspy et de Latentbot suggèrent que le même outil a été employé pour créer les deux, indiquant que l'exploit zero day a été fourni aux opérations de cyber-espionnage et aux opérations*

cybercriminelles par une source unique », écrivent Ben Read et Jonathan Leathery, deux chercheurs de FireEye, dans un billet de blog.

A lire aussi :

Une faille zero day de Microsoft Office exploitée depuis janvier

Adieu Patch Tuesday et bienvenue aux Security Updates

Photo : Mr. Cacahuate via Visual Hunt / CC BY