Sowbug : pourquoi ce groupe de cyberespionnage déroute Symantec

Quelle est la capacité de nuisance de **Sowbug** ?

Ce groupe pirate infiltre des institutions gouvernementales en Amérique du Sud et en Asie du Sud-Est par le biais de cyberattaques « très ciblées » de ministères ou d'organisations en charge de politique étrangère ou de relais diplomatiques pour mener des vols de documents sensibles.

Symantec, qui a repéré en premier ses méfaits, a détecté des assauts « en Argentine, au Brésil, en Equateur, au Pérou, au Brunei et en Malaisie ».

L'infographie en bas d'article présente les pays visés sur une carte du monde. Curieuse configuration d'assauts…

Felismus déclenche l'alerte

L'éditeur de solutions de sécurité IT d'origine américaine considère que Sowbug (« cloporte » en anglais) dispose de ressources suffisamment importantes pour affecter plusieurs cibles simultanément dans le monde.

Symantec considère que le groupe de cyberespionnage est actif depuis au moins à mai 2015 avec une opération visant un département d'un ministère des Affaires étrangères d'un pays en Amérique du Sud en charge de la zone Asie-Pacifique. Il tentait alors d'aspirer tous les documents Word d'un serveur de fichiers.

Les pirates ont pu manœuvrer incognito dans le système pendant cinq mois (mai-septembre 2015).

De manière camouflée, ils déposaient des fichiers leurres de mises à jour de Windows ou Adobe Reader. Tout en procédant à des veilles furtives sur les configurations des systèmes infectés (OS, hardware, réseau…).

Mais le véritable déclic de Symantec à propos des agissements de Sowbug est plus récent: en mars 2017, l'éditeur a repéré un dispositif malware complet baptisé Felismus visant une cible en Asie du Sud-est.

Le groupe pirate camoufle ses action en dehors des heures de travail des organisations pour se montrer le plus furtif possible.

Un travail sous les radars des dispositifs de sécurité IT qui lui a permis d'échapper à la vigilance pendant neuf mois. Symantec considérant que le système avait été infecté depuis septembre 2016.

En l'état actuel, Symantec déclare ignorer encore comment les systèmes étaient infiltrés.

Néanmoins, avec la découverte de Felismus, on sait que Sowbug exploitait un cheval de Troie dénommé Starloader aux multiples usages : déchiffrement de données, copie de codes d'accès,

enregistrement des frappes d'un clavier (keylogging).

L'éditeur de solutions de sécurité IT évoque aussi dans sa contribution blog en date du 7 novembre la piste de faux logiciels téléchargés lors de mises à jour des systèmes.

Ce n'est pas la première fois que Symantec détecte les méfaits du cyberespionnage dans le monde. D'autres éditeurs ont déterré des affaires de ce type comme « Octobre Rouge » par Kaspersky.

Mais l'éditeur américain s'étonne de la portée géographique de Sowbug avec son axe atypique entre l'Amérique du Sud et l'Asie du Sud-Est. De quoi perdre la boussole en matière de sécurité IT.

(Photo crédit image d'illustration à la une : mignon.jacques via Visual Hunt / CC BY)