Google, Microsoft et Cisco visés par la backdoor de CCleaner

Quels dégâts a fait la backdoor installée dans CCleaner (du nom d'un logiciel d'optimisation des PC) et repéré par son éditeur Piriform ?

La filiale d'Avast avait déclaré qu'elle a corrigé son logiciel et coupé les accès au serveur de commande et contrôle (C&C). Ce qui permettait aux attaquants d'injecter du code à distance depuis l'utilitaire de nettoyage de Windows sur les machines visées.

Mais les dégâts semblent plus importants. A travers la porte dérobée de CCleaner, une vingtaine de grandes entreprises informatiques dans le monde ont été malmenées.

En analysant le serveur C&C, les chercheurs en sécurité de Talos (groupe Cisco) ont découvert un deuxième fichier infectieux (le module de backdoor GeeSetup_x86.dll) qui était poussé vers une liste spécifique d'ordinateurs basée sur des noms de domaines locaux.

Google, Microsoft, VMware, HTC, Samsung, Linksys ou encore Cisco (maison mère de Talos), figurent dans la liste (consultable sur cette page).

700□000 machines infectées

Selon la base de données analysée par les experts, pas moins de 700□000 machines ont été infectées par le premier niveau de charge embarqué par la version infectée de CCleaner.

Le second niveau d'attaque qui visait la vingtaine de sociétés IT précédemment évoquées entendait probablement accentuer l'emprise des attaquants sur des systèmes stratégiques.

L'origine de l'attaque pourrait provenir de Chine. Les chercheurs de Kaspersky ont découvert des similitudes entre le code infectieux trouvé dans l'utilitaire Windows avec celui utilisé par le groupe de hackers chinois Axiom, aussi connu sous APT17, Group 72, DeputyDog, Tailgater Team, Hidden Lynx ou AuroraPanda.

« Le malware injecté dans CCleaner a du code commun avec plusieurs outils utilisé par l'un des groupes APT sous la couverture d'Axiom APT », déclare Costin Raiu, directeur de recherche monde chez l'éditeur de sécurité russe, via Twitter .

De leur côté, les experts de Talos mettent en avant que le fichier de configuration du serveur utilisé par les attaquants était à l'heure chinoise. Un constat mais pas une preuve en soi.

Réinitialisation conseillée des systèmes affectés

Quelle que soit la source de l'attaque, les entreprises touchées par la seconde charge infectieuses ont tout intérêt à réinitialiser leur système pour supprimer toute trace des malwares potentiellement introduit par CCleaner.

« Ces nouveaux résultats élève notre niveau de préoccupation alors que nos éléments de recherche pointent vers un éventuel acteur inconnu et sophistiqué », indiquent les chercheurs de Talos.

« *Ces résultats appuient et renforcent également notre recommandation précédente selon laquelle ceux qui ont été touchés par cette attaque ne devraient pas simplement supprimer la version affectée de CCleaner ou mettre à jour la dernière version, mais restaurer des sauvegardes ou des systèmes de restauration afin de supprimer complètement version avec backdoor de CCleaner mais aussi tout autre logiciel malveillant qui réside sur le système.* »

Rappelons que, affectées, les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud ont été mises à jour par Pirifom.

Mais il n'est pas certain que la seule mise à jour de la nouvelle version 5.34 garantisse l'innocuité aux utilisateurs concernés.

Lire également
Eugene Kaspersky craint pour les infrastructures nationales critiques
AVAST et CCleaner débarquent sur Mac OS X
Plus de la moitié des attaques SSH viennent de Chine

Crédit photo : Jne Valokuvaus-Shutterstock