L’utilitaire CCleaner compromis par une backdoor

Piriform, l’éditeur de l’utilitaire CCleaner de nettoyage et d’optimisation de Windows, vient de reconnaître qu’il a fait l’objet d’une attaque.

Les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud de sa solution ont été compromises.

« Une activité suspecte a été identifiée le 12 septembre 2017, où nous avons vu une adresse IP inconnue recevant des données du logiciel trouvé dans CCleaner et CCleaner Cloud sur les systèmes Windows 32 bits », alerte Paul Yung, Vice-Président Produit de Piriform.

Selon l’éditeur, le logiciel a été illégalement modifié avant sa livraison publique. Le pirate a réussi à installer une backdoor à deux niveaux afin d’exécuter du code envoyé à partir d’une adresse IP sur les systèmes affectés.

L’agent malveillant se cachait dans le CRT (Common Runtime), le code d’initialisation de l’application normalement intégré par le compilateur lors de l’opération de compilation en fichier CCleaner.exe.

Envoi de données personnelles

Résultat, l’application stockait certaines informations dans le registre de Windows afin de générer un identifiant unique potentiellement utilisé comme clé de chiffrement de communication, une valeur de synchronisation pour déclencher certaines actions, et une adresse IP pour un deuxième serveur de commande et contrôle (CnC).

Parallèlement, l’application envoyait au pirate un certains nombre de données personnelles comme le nom de l’ordinateur, la liste des logiciels installés, y compris les mises à jour Windows, celles des processus en cours, les adresses MAC des trois premiers adaptateurs réseau, et d’autres informations systèmes.

Piriform, qui déclare avoir alerté les autorités policières dès qu’il a eu connaissance de l’intrusion, ne donne pas de détails sur le mode opératoire des attaquants, ni depuis quand remonte l’attaque et quel volume d’informations a été dérobé.

« L’enquête est toujours en cours », justifie le porte-parole de la société.

Ampleur des dégâts inconnue

Aidé par Avast Threat Labs (sa maison mère depuis juillet dernier), l’éditeur britannique assure que le code étranger a été exclu du logiciel et que l’accès au serveur malveillant est désormais inexploitable par les auteurs de l’attaque.

Tous les utilisateurs des versions affectées devraient en outre voir leur application évoluer vers une

nouvelle version «clean». Ou, à défaut, le faire manuellement depuis cette page.

L'ampleur des dégâts, s'il y en a eu, reste donc inconnue. Ce qui pourrait poser problème aux utilisateurs victimes. Les pirates pourraient en effet exploiter les informations système recueillies pour lancer des attaques plus ciblées sur les postes affectées.

Et, selon Piriform, CCleaner est installé sur environ 130 millions de postes et terminaux mobiles dans le monde. Ceux qui exploitent la version Windows 32 bits de l'utilitaire vont devoir redoubler de vigilance.

Lire également
AVAST et CCleaner débarquent sur Mac OS X
La backdoor ShadowPad infecte les solutions serveurs de NetSarang
Backdoor et Zero Days pour plusieurs milliers de caméras IP

Crédit photo : BeeBright / Shutterstock