Forum: Sécurité

Topic: CCleaner : une backdoor dissimulée pendant un mois !

Subject: Re: CCleaner : une backdoor dissimulée pendant un mois !

Publié par: tignothe

Contribution le : 21/09/2017 09:07:06

Bonjour,

Plutôt que de nous mettre un article dans une langue qui est étrangère pour beaucoup sans aucune explication ni commentaire, il aurait été intéressant de nous faire la synthèse du sujet:

Citation :
Un nouveau rapport du groupe Talos de Cisco suggère que le piratage CCleaner était plus sophistiqué qu'on ne le pensait au départ. Les chercheurs ont trouvé des preuves d'une deuxième charge utile lors de leur analyse des logiciels malveillants qui ont ciblé des groupes très spécifiques en fonction des domaines.....

.....

Talos Group a suggéré de restaurer le système informatique à l'aide d'une sauvegarde créée avant l'infection. Les nouvelles preuves le confirment, et les chercheurs suggèrent fortement qu'il ne suffit peut-être pas de simplement mettre à jour CCleaner pour se débarrasser des logiciels malveillants.

Ces constatations appuient et renforcent également notre recommandation précédente selon laquelle les personnes touchées par cette attaque de la chaîne d'approvisionnement ne devraient pas simplement supprimer la version affectée de CCleaner ou mettre à jour la dernière version, mais devraient restaurer à partir de sauvegardes ou de systèmes de re-image pour s'assurer qu'elles suppriment complètement non seulement la version précédente de CCleaner, mais aussi tout autre logiciel malveillant qui pourrait être présent sur le système.

L'installateur de l'étape 2 est GeeSetup_x86. dll. Il vérifie la version du système d'exploitation, et implémente une version 32 bits ou 64 bits du cheval de Troie sur le système basé sur la vérification.

Lire aussi: Gestionnaire de mots de passe déterministe Problèmes

Le cheval de Troie 32 bits est TSMSISrv. dll, le cheval de Troie 64 bits est EFACli64. dll.

Identification des charges utiles de l'étape 2

Les informations suivantes aident à déterminer si une charge utile de l'étape 2 a été installée sur le système.

Clés de registre:

HKLMSoftwareMicrosoftWindows NTVersionCurrentVersionWbemPerf 01
HKLMSoftwareMicrosoftWindows NTVersionCurrentVersionWbemPerf 02
HKLMSoftwareMicrosoftWindows NTVersionCurrentVersionWbemPerf 03

HKLMSoftwareMicrosoftWindows NTVersionCurrentVersionWbemPerf 04
HKLMSoftwareMicrosoftWindows NTVersionCurrentVersionWbemPerfHBP

Fichiers:

GeeSetup_x86. dl (Hash:
dc9b5e8e8aa6ec86db86db8af0a7aaa897ca897ca61db3e5f3d2e0942e319074db1aaccfdc83)
EFACli64. dll (Hash:
128aca58be325174f0220bd7ca6030e4e206b4378796e82da46da460055733bb6f4f)
TSMSISrv. dll (Hash:
07fb252d2d2e853a9b1b32f30ede411f2efbb9f01e4a7782db5eacf3f55cf34902)
DLL dans le registre:
f0d1f88c59c59a005312faad902528d60acbf9cd5a7b36093db8ca811f763e1292a
Étape 2 Charge utile:
dc9b5e8aa6ec86db86db8af0a7aa7aa897ca61db3e5f3d2e0942e319074db1aaccfdc83

Ce qui tend à infirmer les précédentes déclarations et autres commentaires qu'il suffit simplement de modifier la version du logiciel incriminé.., et que seuls les heureux possesseurs de système 32 bits sont impactés. Quans à savoir s'il est réellement nécessaire de restaurer le système incriminé à une date antérieure ou carrément faire une «installation propre» c'est une autre histoire.

Comme quoi il ne faut jamais se contenter des premières conclusions hâtives suite à un événement,

Petite suggestion en passant, il serait peut être intéressant pour certain de partir à la découverte d'un autre nettoyeur de qualité open source Bleachbit qui lui, n'est pas pollué.