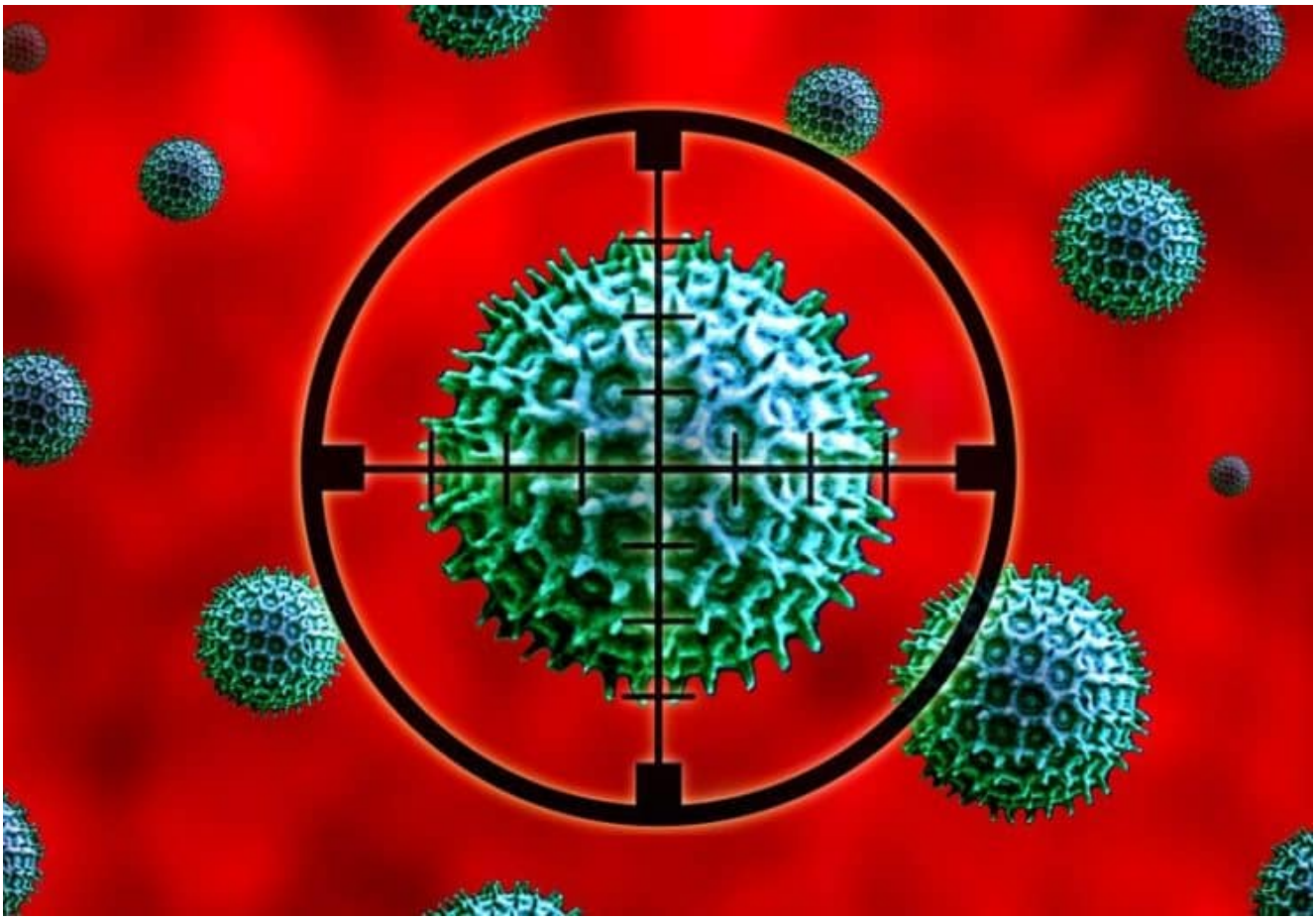
Alerte PC Asus: risque de malware via le live update !

27/03/2019



Bonjour le Monde !

Un hacker est parvenu à infecter le système de Live Update de Asus !

Asus a corrigé le problème et **Kaspersky** fournit un outil de vérification ici: **https://shadowhammer.kaspersky.com/**

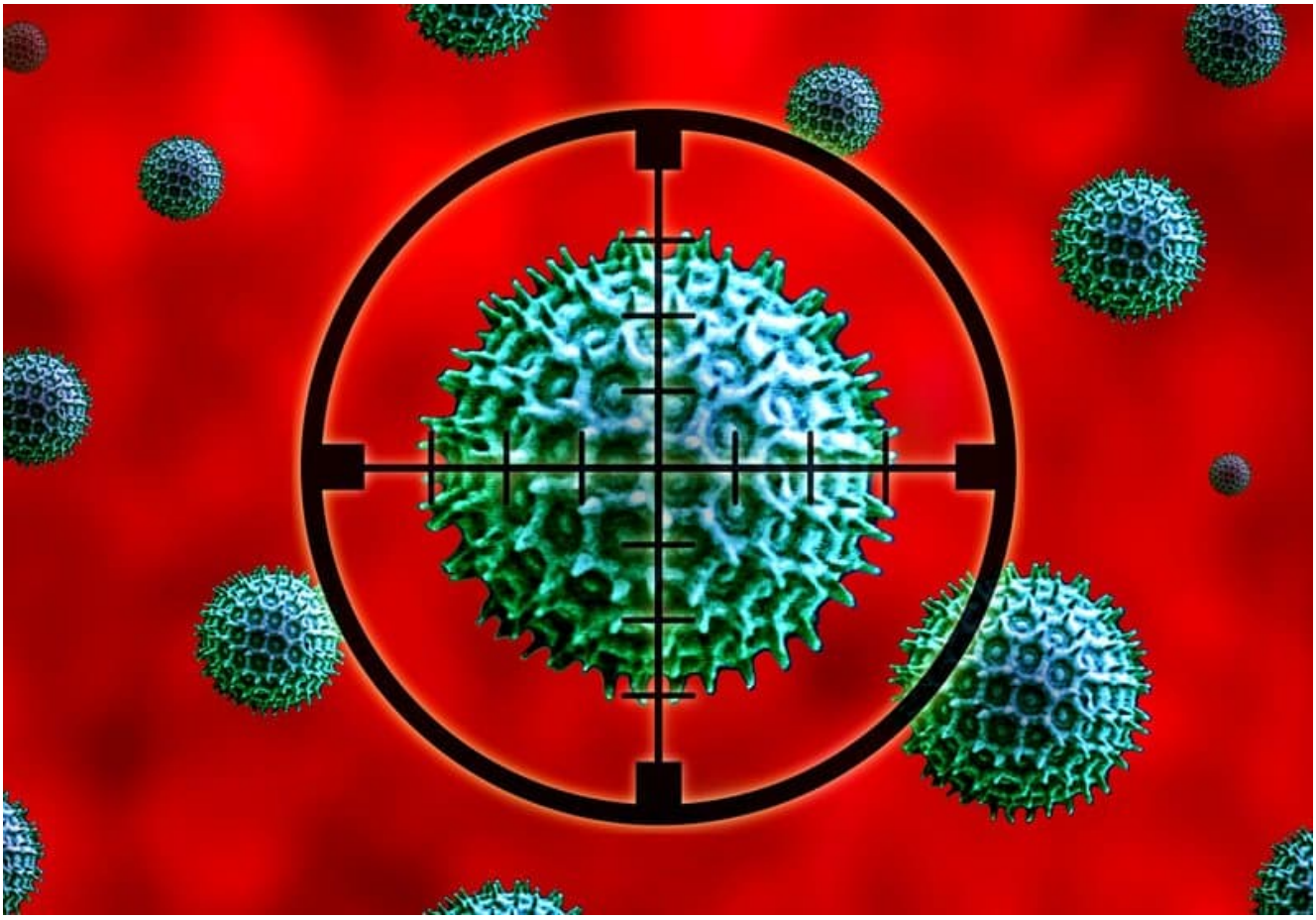
Asus dit avoir prévenu les personnes concernées mais cela ne concerne que ceux qui se sont enregistrés et qui ont fourni des coordonnées exactes, évidemment.

Près d'**un million d'utilisateurs sont concernés** mais le malware ne ciblait « que » 600 PC via leur adresse MAC (adresse matérielle unique d'une connexion réseau); il s'agit de cette suite de chiffes hexadécimaux normalement affiché sur tout appareil avec une connexion réseau cablée et/ou WIFI et/ou Bluetooth.

L’attaque a commencé dans la 2e moitié de 2018, le malware a été découvert par Kaspersky en janvier 2019 et signalé à Asus le 31 janvier 2019.

Asus n’a pas prévenu ses utilisateurs tant que Kaspersky n’avait pas une solution qui est arrivée ce lundi 25 mars en même temps que l’annonce publique du problème.

Je conseille donc à tous les possesseur de PC, laptop, tablette et smartphone Asus de tester leur appareil via le lien ci-dessus.



Une deuxième raison pour laquelle j’écris cet article est de vous montrer que **la détection et la résolution d’une attaque peut prendre beaucoup de temps**; dans le cas présent, la détection est intervenue plusieurs mois après le début de l’attaque et il a encore fallu 3 mois supplémentaires pour fournir une solution définitive avec un outil de détection/nettoyage.

Il aura fallu longtemps ici car le hacker a utilisé un véritable certificat de Asus dérobé par d’autres moyens, certificat qui sert justement a identifier une « source sûre » !
Un certificat est par exemple utilisé pour sécuriser un site web et faire apparaître le fameux cadenas et l’utilisation du protocole de communication **https** (encrypté)

plutôt que **http** entre le site web et votre navigateur internet. Il y a plusieurs sortes de certificats suivant l'usage et le degré de sécurité souhaités.

CCleaner a aussi subi une attaque du même genre en mars 2017 avec plus de 2,2 millions d'utilisateurs ayant téléchargé le programme infecté. Il aura fallu attendre septembre pour avoir une solution définitive. En Juin de cette même année 2017, CCleaner a été racheté par Avast (il appartenait à Piriform auparavant).
De ces 2.2 millions, 1.65 millions ont installé la version infectée de CCleaner qui a donc contacté le hacker (ou plutôt le groupe de hackers) via Internet mais seulement 40 ont été utilisés en août 2017 pour attaquer 11 sociétés (les particuliers comme nous n'intéressant pas ce groupe de hackers).
C'est un outil que je conseille et utilise toujours aujourd'hui mais je me souviens très bien de cette période où il était difficile de télécharger une nouvelle version de CCleaner. Le site actuel est, propriétaire actuel Avast oblige, plein de pub, essayant de vous faire acheter la version payante et il faut savoir comment faire pour télécharger la version gratuite sans passer par l'infâme site de téléchargement Download.com ! Enfin, il faut explorer et comprendre les réglages avancés pour désactiver la surveillance de l'espace disque en temps réel qui ne sert pas à grand-chose puisque Windows le fait déjà…
C'est la raison pour laquelle je n'utilise plus Avast ! Leurs produits gratuits sont bons mais trop « chiants » ! C'est aussi une des raisons de la disparition progressive des programmes gratuits…
Bla-Bla avait raison: la pub ? Beuuuuurk !

La leçon a retenir est que si une mise à jour ne veut pas se faire, il ne faut pas insister et attendre (parfois très patiemment) que cela refonctionne …

Li P'ti Fouineu vous salue bien !

Source: article WIRED du 25 mars 2019