Des sites Web administratifs exploités en mode cryptomining à leur insu

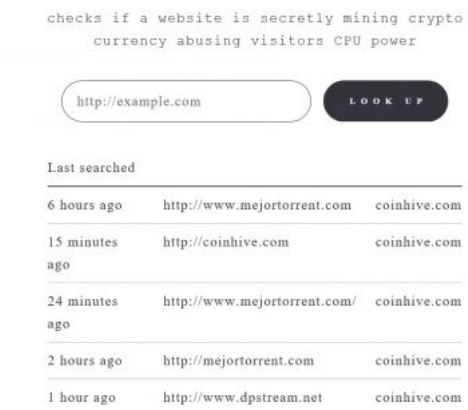
Après les ransomware, une nouvelle menace fait son apparition : le **cryptojacking**.

Toujours opportunistes, les cybercriminels se sont intéressés à la folie spéculative autour des monnaies virtuelles telles que le Bitcoin ou l'Ether, le Ripple et autres Litcoin.

L'extraction de ces crypto-devises est devenue un business légal en soi mais s'est aussi transformée en une forme de déviance exploitée sous forme de malware.

Les « mineurs » qui valident les transactions en résolvant des problèmes mathématiques complexes sont, en effet, rémunérés via cet argent virtuel mais bien réel.

Ce travail de minage nécessite une puissance de calcul toujours plus grande. Plutôt que de consister des fermes de serveurs comme les mineurs légaux, les hackers font appel à des botnets.



Ces derniers jours, quelque 4 300 sites Web administratifs ont été infectés par un code malveillant puisant dans les ressources informatiques de leurs visiteurs.

Selon un article de The Guardian du 11 février, le système de santé publique britannique (National Health Service) ou l'organisme de financement des étudiants anglais (Student Loans Company) ont été touchés.

Si l'attaque a majoritairement concerné les pays anglo-saxons, 16 sites Internet français seraient concernés dont celui de la commune d'Asnières-sur-Seine (Hauts-de-Seine).

Un site recense leurs URL et un autre, baptisé Whoismining, précise si un site Web a été contaminé en entrant son URL.

Pour Shay Nahari, responsable de « Red Team Services » chez CyberArk, les sites administratifs sont une cible de choix pour ce type d'attaques compte tenu de leur trafic et de la diversité de leurs utilisateurs.

« Les pirates n'ont pas besoin d'implémenter un logiciel malveillant sur le terminal utilisé, et les internautes peuvent ne jamais s'apercevoir que la puissance de calcul de leur appareil était utilisée à des fins malveillantes. »

Un JavaScript malicieux

Baptisé Coinhive, le programme malveillant en question participe au minage de la crypto-devise Monero. Il se présente sous le forme d'un JavaScript. Pour l'insérer dans une page Web, les hackers ont corrompu Browsealoud du nom d'un plug-in pour navigateur édité par Texthelp et conçu pour aider les personnes malvoyantes à lire des textes sur le Web.

L'éditeur a reconnu les faits sur son site et un expert en sécurité informatique – Scott Helme – explique les modalités de l'attaque sur son blog.

De son côté, Malwarebytes avait révélé dès novembre la menace Coinhive. Le fournisseur de solutions de cybersécurité a aussi identifié une campagne de cryptomining à destination des mobiles sous Android.

Si le bruit du ventilateur d'un ordinateur fortement sollicité peut mettre la puce à l'oreille à un utilisateur, l'attaque est plus difficile à détecter sur un smartphone ou une tablette.

Malwarebytes conseille d'installer sur leurs appareils mobiles, les mêmes outils qu'ils auraient sur leur PC car « *les 'cryptomines 'non désirées ne sont pas seulement une nuisance ponctuelle mais peuvent causer des dommages permanents.* »

En complément : YouTube : quand la publicité devient un vecteur de cryptojacking (Itespresso.fr, 30 janvier 2018)