Nodersok et Divergent : des malware garantis sans fichiers malveillants

L'un l'appelle Nodersok ; l'autre, Divergent. Mais Microsoft et Cisco Talos semblent avoir mis le doigt sur le même phénomène.

En l'occurrence, une campagne de diffusion de *malware* qui a la particularité de n'exploiter que des outils « légitimes », dont certains déjà présents sur les systèmes ciblés.

Microsoft et Cisco Talos en ont observé deux formes différentes, avec cependant le même point d'entrée : une application HTML.

Celle-ci peut se télécharger lorsque l'utilisateur clique sur un élément dans son navigateur internet. Ou bien se cacher dans une bannière publicitaire.
Microsoft souligne le recours à des CDN de confiance pour augmenter les chances de passer sous les radars.

Node.js détourné

Cette application HTML n'est que le premier maillon de la chaîne.

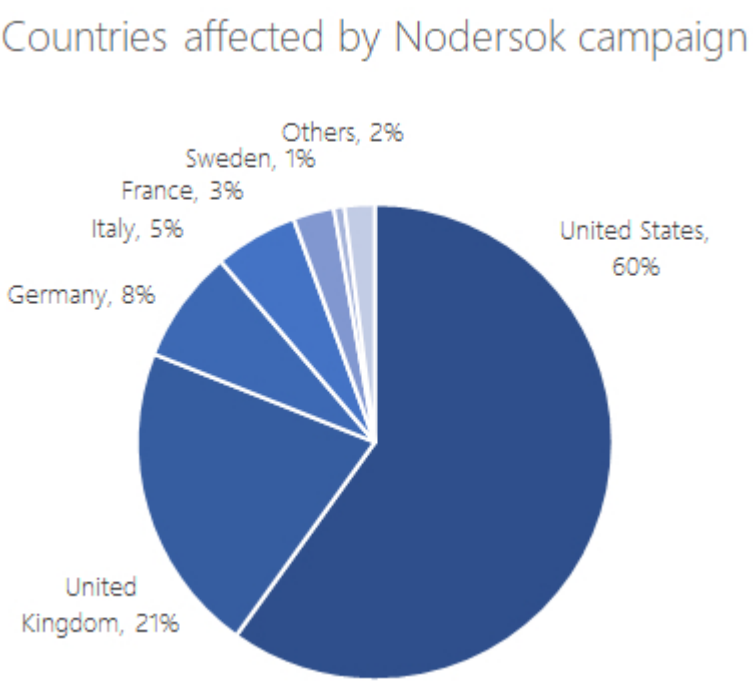
Dans le scénario que présente Cisco Talos, elle ouvre la voie à l'installation de plusieurs composantes destinées à alimenter une activité de fraude au clic.

À ces fins, elle crée plusieurs entrées au registre Windows et y intègre ses différentes fonctionnalités.

La version la plus ancienne que Cisco Talos ait détectée remonte à février 2019. Au fil du temps, Divergent est devenu plus discret, que ce soit en maximisant l'usage des scripts PowerShell* ou en privilégiant l'exécution en mémoire.

Une fois la charge initiale en place, elle réalise quelques vérifications, dont la présence d'un CPU à au moins deux cœurs. Et cherche, en particulier, à désactiver certaines fonctionnalités de Windows Defender tout en empêchant sa mise à jour.

La fraude au clic est réalisée à travers Node.exe, implémentation du *framework* Node.js.
Divergent tire son nom de l'outil WinDivert, dont il fait usage pour manipuler certains paquets réseau et se faire passer pour d'autres appareils (Android et iOS notamment).



Microsoft a observé un pic d'activité début septembre. Il est question de « milliers de machines » visées ces dernières semaines, essentiellement aux États-Unis (60 %) et en Europe (21 % au Royaume-Uni, 3 % en France).

La firme de Redmond note la courte durée de vie (1 à 2 jours) des domaines depuis lesquels l'application HTML télécharge les autres composantes.
Elle constate la possibilité qu'offre Nodersok de faire des machines compromises des proxys. Autrement dit, des relais de diffusion de *malware*.

** À travers des commandes dissimulées dans des variables d'environnement.*

Photo d'illustration © Eugène Sergueev – Shutterstock.com