Les publicités piégées au ransomware se multiplient

Une nouvelle campagne de «*malvertizing*» sévit sur Internet. Weather.com, Drudgereport.com, wunderground.com, des sites qui génèrent plusieurs millions de visites mensuelles, en seraient victimes. L'infection serait en train de **s'étendre à Ebay.com et AOL.com**, indique Stu Sjouwerman, le CEO de KnowBe4, une société spécialisée dans le conseil en sécurité qu'il a créée avec Kevin Mitnick, l'un des hackers les plus médiatiques des années 90. Rappelons que ce dernier avait accédé aux systèmes de grandes entreprises américaines, ce qui lui a valu 5 ans d'emprisonnement en 1995.

Selon KnowBe4 la campagne infectieuse diffuserait des **ransomware de type CryptoWall**. Une fois installée dans le système, généralement des PC sous Windows, cette bestiole crypte les fichiers locaux. Pour pouvoir les déchiffrer et y accéder de nouveau, ses auteurs réclament une **rançon de 500 dollars** (montant généralement constaté aujourd'hui), généralement en Bitcoin, à la victime. Un récent rapport de Proopoint estimait que les attaques par CryptoWall généraient jusqu'à 25 000 dollars par jour de revenus pour les pirates. Selon des chercheurs de Dell SecureWorks, plus de 830 000 personnes dans le monde avaient été victimes d'un ransomware fin 2014.

Adspirit.de, le propagateur

Ce ne pas les sites eux-mêmes qui sont infectés, mais la plate-forme de diffusion des annonces publicitaires qui, indirectement, contribue à la propagation infectieuse en distribuant les fichiers publicitaires malveillants. Dans le cas présent, le réseau Adspirit.de serait à l'origine de la contamination. L'entreprise sert en effet d'intermédiaire entre les annonceurs et les sites «afficheurs». Quand les annonceurs sont des pirates, les choses se compliquent. Les publicités infectieuses ne se distinguant pas en apparence des réclames légitimes, il est facile de tomber dans le panneau. Un simple clic sur ces pubs déclenche le processus d'infection.

Pire : dans de nombreux cas, leur simple affichage suffit à enclencher le mécanisme de contamination par exploitation d'une faille système (particulièrement celle du player Flash, ou encore de Java, d'où l'importance d'appliquer régulièrement ses mises à jour de sécurité) sans aucune intervention de l'utilisateur. Pour s'en prémunir, KnowBe4 préconise d'utiliser le mode « clic-to-play » qui impose une intervention manuelle pour dérouler un contenu publicitaire en Flash, voire de supprimer le plugin d'Adobe de son navigateur. Ou encore d'installer un bloqueur de publicités comme Ad-Blocker, utilisé par 200 millions de personnes dans le monde et honni par la presse en ligne qui l'accuse d'un manque à gagner de 45 millions de dollars rien qu'aux Etats-Unis.

Si KnowBe4 nomme bien Adspirit.de comme étant la source de cette campagne infectieuse dans son communiqué, le nom du diffuseur n'apparaît pas dans le billet de blog de la société de conseils en sécurité. Aucune alerte n'a cependant été émise du côté du réseau allemand. Quelques semaines auparavant, c'est Yahoo qui avait exposé ses visiteurs à une campagne d'attaques par publicités déguisées.

Lire également

Sécurité : le ransomware Cryptowall 2.0 contourne les antivirus
Google protège Chrome contre le téléchargement de logiciels indésirables
Ransomware : un retour sur investissement très lucratif

crédit photo @ GlebStock – Shutterstock