Le blog du journal The Independent victime de malvertising, la faute à Flash

Le blog du journal The Independent victime de malvertising, la faute à Flash

L'un des blogs du quotidien britannique The Independent a été victime d'un piratage et l'un de ses encarts publicitaires redirigeait les utilisateurs vers un logiciel malveillant. La meilleure parade pour l'internaute lambda ? Tenir Adobe Flash à jour.

La société Trend Micro alerte sur son blog d'une attaque visant l'un des blogs du quotidien britannique The Independent. Dans un post daté de mercredi, la société de cybersécurité fait état d'une cyberattaque ayant visé le blog du quotidien américain britannique The Independent. La source de l'infection provient selon Trend Micro de l'un des blogs WordPress du quotidien : les chercheurs de Trend Micro ont ainsi remarqué que celui-ci redirigeait les utilisateurs vers une page de l'Angler Exploit Kit. Celui-ci tentait par la suite d'exploiter une vulnérabilité au sein d'Adobe Flash afin d'installer un logiciel de type rançongiciel sur la machine des utilisateurs affectés.
Selon un porte-parole de The Independent interrogé par la BBC, l'infection était causée par une opération de malvertising : en conséquence, les administrateurs du site ont donc bloqué l'affichage de publicité sur la page incriminée en attendant que le problème soit résolu. Le quotidien britannique précise que rien ne laisse entendre que des utilisateurs du site ont pu être affectés par l'attaque.

Adobe Flash : usual suspect

L'attaque n'a rien d'inhabituel : au contraire, on a plutôt affaire à un cas d'école assez représentatif des nouveaux moyens d'infections utilisés par les cybercriminels. D'une part, la technique du malvertising se démocratise : cette méthode consiste pour les cybercriminels à se faire passer pour des régies d'annonceurs publicitaires afin de pouvoir exploiter les outils de marketing programmatique pour faire apparaître leurs pages web malveillantes sur des sites à forte audience.
Dailymotion a ainsi été récemment victime de ce type d'attaque, qui gagne en popularité ces derniers mois. Les attaquants ont également eu recours à l'Angler Exploit Kit, le kit d'exploit le plus populaire actuellement parmi les cybercriminels. Véritables couteaux suisses des pirates, ces outils se présentent sous la forme de plateformes mises à jour afin d'exploiter facilement les vulnérabilités récemment découvertes dans les programmes populaires, Adobe Flash étant l'une des cibles favorites.
Enfin, le malware distribué appartient à la catégorie des ransomware, ou rançongiciel en français : le bien connu Cryptolocker. Celui-ci permet à l'attaquant de chiffrer l'ensemble des données sur le disque de la victime, données qui ne seront déchiffrées qu'en l'échange d'une rançon de 499$.
Pour l'utilisateur, la meilleure protection possible reste de veiller à conserver son navigateur et ses différents programmes à jour. Tout particulièrement Flash : on en profite pour signaler qu'une nouvelle mise à jour a été publiée par Adobe et corrige un peu plus de 70 failles de sécurités affectant le logiciel d'Adobe. Celui-ci étant la cible de choix des cybercriminels, on peut également envisager la suppression pure et simple du logiciel pour les plus paranoïaques.
Adobe annonçait d'ailleurs récemment amorcer la mise à la retraite de sa technologie, qui semble de moins en moins pertinente à l'heure de HTML5. Pour les victimes de ransomwares tels que cryptolocker, certaines sociétés de cybersécurité proposent des utilitaires permettant de decrypter les fichiers chiffrés par le logiciel malveillant, mais le fonctionnement n'est pas garanti.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/le-blog-du-journal
-the-independent-vi
ctime-de-malvertising-la-faute-a-flash-39829632.htm