Le HTML5 pas plus sûr que le Flash pour les navigateurs

Feu Steve Jobs avait sonné le signal de départ, en 2010, en bannissant le Flash des iPhone (voire même des MacBook). La technologie d'Adobe qui, depuis un plugin, permet d'exécuter des applications au sein d'un navigateur, au premier rang desquelles la lecture de vidéos, n'était pas assez stable et sécurisée pour continuer à être supportée. Même son éditeur s'en accordait en cessant les développements de son player pour terminaux mobiles. Rien qu'en 2015, plus de 300 vulnérabilités ont été constatées sur les lecteurs Flash. Autant de failles systèmes dont s'emparent régulièrement les cybercriminels pour lancer leurs attaques. Surtout, l'alternative HTML5, avec sa capacité à lire nativement les contenus multimédia, s'inscrivait comme l'acteur qui allait donner le dernier coup de pelle pour enterrer la technologie d'Adobe.

Il n'en reste pas moins que, 6 ans après le choix stratégique du fondateur d'Apple, Flash perdure dans nombre de sites. Qui plus est, une étude vient mettre en cause la sécurité de l'alternative HTML5 plus moderne. *« L'utilisation de HTML5 n'empêchera finalement pas les attaques de malvertising »*, déclare GeoEdge. Etude à l'appui, cette société spécialisée dans la vérification de l'intégrité des publicités en ligne assure constater l'existence de campagnes d'infection par détournement d'affichage publicitaire dans les pages web qui ne recourent pas au Flash. *« Même avec les annonces vidéo HTML5, le code malveillant peut être inséré dans l'annonce elle-même ou les paramètres VAST »* (video ad serving template), la norme industrielle de réponse XML d'un serveur publicitaire.

JavaScript en cause

GeoEdge focalise principalement les risques sur l'usage du JavaScript dans le langage HTML5. *« L'une des principales caractéristiques des attaques de logiciels malveillants est l'insertion d'un code JavaScript*, indique le prestataire. *JavaScript est le langage de base pour HTML5, donc le code malveillant peut être embarqué dans HTML5 sans grande difficulté. »* Et les pirates ne s'en priveraient guère pour insérer du code malveillant dans des publicités détournées. C'est d'autant plus inquiétant qu'il *« n'y a rien à faire pour empêcher un attaquant d'injecter une URL malveillante utilisant le code tiers dans l'injection directe VAST ou XML, ou à partir d'un bloc d'annonces malveillant dans le lecteur vidéo conçu pour le site »*.

Sans négliger les risques que les publicités en ligne vérolées peuvent constituer comme vecteurs d'attaques, il appartient aux régies chargées de diffuser ces annonces d'en vérifier l'intégrité (au risque de perdre ses clients si ces derniers infectent, indirectement, les utilisateurs finaux). De son côté, GeoEdge a tout intérêt à gonfler un peu l'aspect anxiogène autour des «défauts» du HTML5 (défauts intrinsèques au langage de code qui se veut, par nature, ouvert) pour vendre ses services. Le prestataire ne s'en cache d'ailleurs pas. *« Les cyber-criminels vont continuer à construire des campagnes de malvertising parce que les gains sont élevés et le risque faible*, déclare Sagi Elgavi, vice président de la R&D de GeoEdge. *Il est de notre mission de protéger les entreprises et leurs utilisateurs en bloquant les attaques, quelle qu'en soit la source – Flash, HTML5 ou injections JavaScript. »*

Lire également

Les publicités piégées au ransomware se multiplient
Chrome prêt à embaumer Flash avec du HTML5
Adobe Flash : c'est fini (dans Creative Cloud)
Adobe Flash n'est plus le bienvenu chez Amazon

Crédit Photo : Welcomia-Shutterstock