Attaques massives à cause de à la faille «zero day» d'Internet Explorer

La faille «zero day» qui frappe Internet Explorer et découverte il y a deux mois fait de nouveau parler d'elle. Microsoft vient de mettre à jour son alerte de sécurité pour informer de l'existence d'attaques en cours. *« Microsoft est conscient de l'existence de preuves de faisabilité publiques concept utilisé dans des attaques limitées et ciblées »*, déclare l'éditeur sans préciser la teneur de ces attaques.

Liée à la façon dont le MHTML du navigateur interprète les requêtes en format MIME pour les blocs de documents, la vulnérabilité permet à un attaquant de provoquer l'exécution d'un code malveillant sur l'ordinateur de la victime par la simple visite d'une page web spécialement codée. *« Ces conséquences sont similaires à celles d'une vulnérabilité de type cross site scripting (XSS) »*, prévient Microsoft. Toutes les versions de Windows, y compris serveur (sauf celles installées avec l'option Server Core), sont concernées.

Se protéger en désactivant le protocole MHTML

Selon l'éditeur, il est néanmoins possible de se prémunir contre ce risque en désactivant le protocole MHTML dans les paramètres du navigateur (voir les explications sur cette page du support de Microsoft). L'application de cette alternative est, en attendant le correctif adéquate, fortement conseillée. *« Nous collaborons avec des fournisseurs de services pour enquêter sur des solutions côté serveur, mais nous recommandons d'appliquer une ou plusieurs des solutions de contournement côté client dans la section des mesures proposées (suggested action) de cette alerte afin d'aider à bloquer certains vecteurs d'attaque potentiels quel que soit le service »*, précise Redmond.

Parmi les partenaires en question, un certain Google apporte son expertise pour limiter les dégâts. Dans un billet du 11 mars, la firme de Mountain View confirme qu'elle a *« constaté quelques attaques très ciblées et apparemment politiquement motivées contre nos utilisateurs. Nous croyons que des activistes peuvent avoir représenté une cible spécifique. Nous avons également vu des attaques contre les utilisateurs d'un autre site de réseau social populaire. »* Attaques toutes issues de l'exploitation de la faille qui frappe le protocole MHTML d'Internet Explorer.

« Pour renforcer la protection de nos utilisateurs de nos services, nous avons déployé plusieurs systèmes de défense côté serveur pour rendre la vulnérabilité MHTML plus difficile à exploiter, souligne Google qui ajoute que*ce ne sont cependant pas des solutions à long terme et nous ne pouvons garantir à 100 % leur fiabilité. »*

Microsoft sous pression

Google ne précise pas qui sont les pirates à l'origine des attaques ni même quels sont les principaux sites visés, notemment le « populaire site de réseau social ». Néanmoins, ces derniers temps, la Chine a été au centre de l'origine de nombre d'attaques ciblées. La dernière étant celle du ministère des Finances en France. Les militants activistes auxquels Mountain View fait référence pourraient être des défenseurs de la cause tibétaine.

Google recommande à son tour aux utilisateurs d'IE d'appliquer la solution alternative de

désactivation du MHTML pour se prémunir de ce type d'attaques. L'entreprise a même la délicatesse de ne pas évoquer son propre navigateur Chrome pour éviter les attaques. Il n'en reste pas moins que Microsoft subit aujourd'hui une pression de plus en plus intense pour corriger la vulnérabilité à la source. On peut donc espérer une solution pour le prochain *« patch tuesday »* prévu le 12 avril.