Le français Snecma fait les frais d'une vulnérabilité d'Internet Explorer

Comme le syndicat professionnel Gifas (Lire : *Une faille d'Internet Explorer exploitée pour cibler l'aéronautique française*), le motoriste français **Snecma** aurait été victime de hackers ayant tiré profit d'**une faille du navigateur Internet Explorer**, d'après un spécialiste de la sécurité informatique cité anonymement par Reuters. L'information n'a pas été confirmée par l'industriel.

Faille zero day sur IE 9 et 10

Le 11 février dernier, l'éditeur américain de solutions de sécurité IT FireEye a annoncé que **la faille zero day découverte sur IE 10**, mais touchant également **la version 9** du navigateur de Microsoft, avait été utilisée par des pirates informatiques pour attaquer le site d'anciens combattants américains VFW (Veterans of Foreign Wars).

La société de sécurité Websense a ensuite indiqué avoir repéré la vulnérabilité dès le 20 janvier, soit trois semaines avant la première annonce de l'exploitation de la faille. Depuis, Microsoft **recommande à ses clients d'utiliser IE 11**.

Un serveur hébergé aux États-Unis

Mardi, Seculert a indiqué dans un billet que la vulnérabilité aurait été exploitée dès le 17 janvier et que cette exploitation pourrait encore se poursuivre. L'entreprise israélienne spécialisée dans la cybersécurité assure que cette faille a été utilisée pour mener une attaque sophistiquée (Advanced Persistent Threat) contre un fabricant français de moteurs pour l'aérospatiale, sans toutefois le nommer…

Mais cette attaque implique, d'après Seculert, un autre logiciel malveillant que celui (ZXShell) utilisé dans la campagne ciblant l'organisation de vétérans américains (compromission du site). Malgré tout, une fois installé, le *malware* communiquerait avec **un système de commande et contrôle** hébergé sur le même serveur que celui utilisé pour mener l'opération contre le site de vétérans de l'armée américaine.

Pour l'industriel français, les hackers auraient utilisé le logiciel en question pour dérober les identifiants que des salariés, partenaires et revendeurs utilisent pour **accéder à distance au réseau de l'entreprise française**. Les pirates auraient également cherché à voler des informations de sessions de navigation. Le groupe Safran, maison mère de Snecma, n'a pas commenté l'incident présumé.

Voir aussi

Une faille d'Internet Explorer exploitée pour cibler l'aéronautique française