Forum: Sécurité

Topic: Attention aux fausses mises à jour Meltdown et Spectre sous Windows

Subject: Attention aux fausses mises à jour Meltdown et Spectre sous Windows

Publié par: Wullfk

Contribution le : 20/01/2018 00:43:17

Bonsoir,

Meltdown et Spectre sous Windows, attention aux fausses mises à jour

Citation :
Les utilisateurs Windows sont la cible d'une fausse mise à jour contre les failles Meltdown et Spectre. Elle permet de déployer des logiciels malveillants.

L'alerte est lancée par la firme Malwarebytes. Dans un communiqué, elle tire la sonnette d'alarme concernant un faux patch. Il est actuellement proposé aux utilisateurs allemands. Il est cependant précisé qu'il peut facilement subir de petites modifications pour s'attaquer à un public plus large (français, américain, anglais…).

Ce faux patch est un fichier exécutable nommé « **Intel-AMD-SecurityPatch-10-1-v1** ». Son exécution permet l'installation d'un « Smoke Loader », une forme de malware capable d'ouvrir une porte au téléchargement d'autres outils. Les pirates peuvent alors accéder à des informations d'identification et d'autres données sensibles. Une fois qu'il a infecté le PC, de multiples connexions à plusieurs domaines russes sont tentées avec des transferts de données chiffrées.

Malwarebytes explique:

"*Nous avons identifié un domaine récemment enregistré qui offre une page d'informations avec différents liens vers des ressources externes sur Meltdown et Spectre et son impact sur les processeurs. Bien qu'il semble provenir de l'Office fédéral allemand de la sécurité de l'information (BSI), ce site d'hameçonnage SSL n'est affilié à aucune entité gouvernementale légitime ou officielle* ".
Source : https://www.ginjfo.com/actualites/secu ... usses-mises-jour-20180116