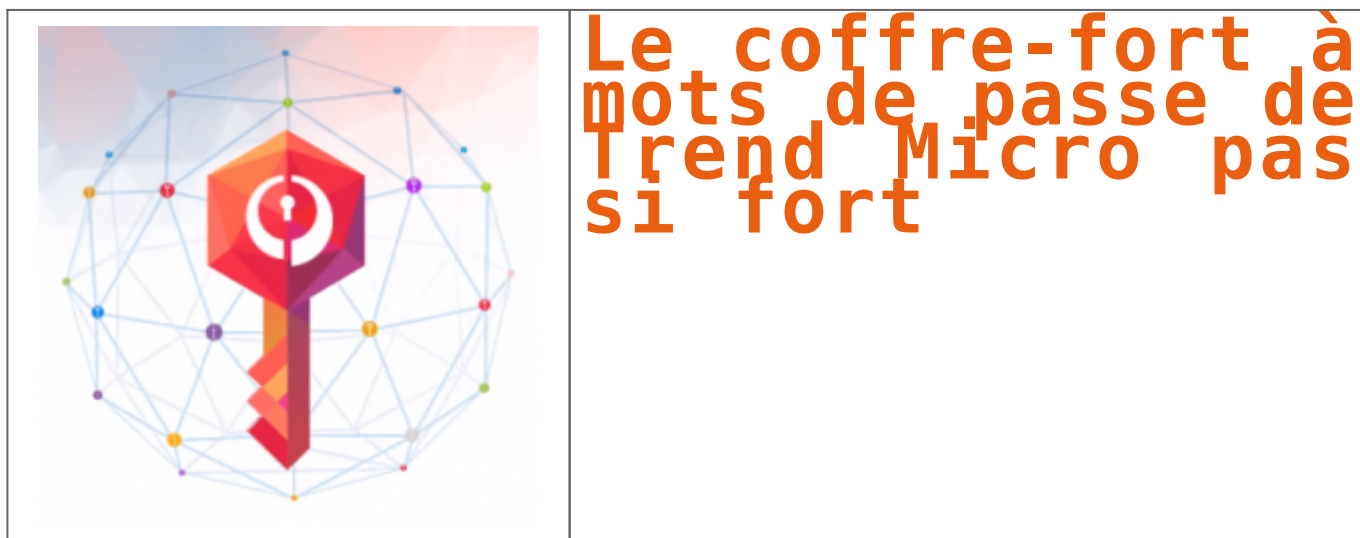
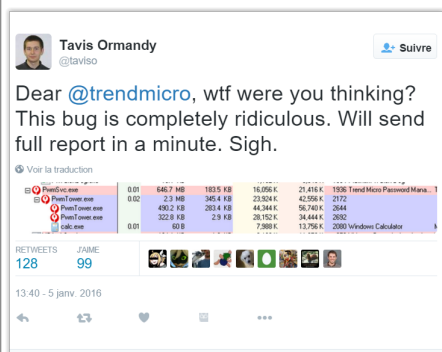


Le coffre-fort à mots de passe de Trend Micro pas si fort



L'éditeur de solutions de sécurité Trend Micro a lancé un correctif pour patcher une faille dans son logiciel Password Manager permettant à un attaquant distant de voler les mots de passe utilisateur.

Un chercheur en sécurité de Google, Tavis Ormandy, a tiré la sonnette d'alarme après avoir trouvé plusieurs failles dans le gestionnaire de mots de passe de Trend Micro, Password Manager. Ces dernières peuvent permettre à un personne malintentionnée d'exécuter du code à distance et de voler les mots de passe des utilisateurs stockés dans ce logiciel. L'éditeur japonais a confirmé ces problèmes et propose une mise à jour automatique pour les résoudre.



Ce n'est pas la première fois que Tavis Ormandy alerte l'éditeur sur l'existence de telles failles de sécurité. Se sentant frustré par un temps de réaction trop long de Trend Micro, le chercheur de Google a d'ailleurs pris la décision de poster les derniers échanges qu'il a eus avec la société. « Alors cela signifie que n'importe quel internaute peut voler tous les mots de passe en silence, autant qu'exécuter du code arbitraire sans aucune interaction utilisateur », s'est indigné Tavis Ormandy. « J'espère vraiment que vous prenez conscience de la gravité de la situation car je suis très étonné de tout cela. »

Des mots de passe utilisateurs trouvés en 30 secondes

Les utilisateurs des solutions antivirus de Trend Micro peuvent choisir d'utiliser le gestionnaire de mots de passe Password Manager afin pour exporter dedans l'ensemble de leurs mots de passe et de n'avoir plus qu'un mot de passe maître à retenir et utiliser. Les concurrents Dashlane ou LastPass proposent des services similaires. Ce gestionnaire est écrit en Javascript avec node.js et ouvre de multiples ports HTTP RPC pour des requêtes API, a précisé Tavis Ormandy. En 30 secondes, le chercheur indique avoir trouvé une requête API permettant d'accepter du code distant et également qu'une autre lui a permis d'accéder aux mots de passe stockés dans le gestionnaire. Cerise sur le gâteau, M. Ormandy a trouvé plus de 70 API de Trend Micro étaient exposées et a recommandé – non sans humour – à l'éditeur de recruter un consultant externe pour auditer son code.

Les logiciels antivirus tournent avec un haut niveau de privilège sur les systèmes d'exploitation, ce qui signifie que l'exploitation d'une vulnérabilité peut donner à un attaquant un accès profond à un ordinateur. Des dizaines de sévères vulnérabilités ont été trouvés sur les 7 derniers mois dans les logiciels antivirus incluant ceux de Kaspersky Lab, Eset, Avast, AVG Technologies, Intel Security et Malwarebytes.



Réagissez à cet article

Source : *Le coffre-fort à mots de passe de Trend Micro transformé en passoire – Le Monde Informatique*