Le Ransomware Dharma enfin décrypté

	Le Ransomware Dharma enfin décrypté

Les clés de déchiffrement du ransomware Dharma ainsi que toutes ses variantes ont été mises en ligne par un utilisateur. Kaspersky et Eset ont mis à jour leurs outils de lutte contre les ransomwares pour permettre à toute personne ou entreprise de déchiffrer gratuitement leurs fichiers chiffrés.

Les fournisseurs de sécurité dont Kaspersky et Eset ont mis à jour leurs outils pour permettre de déchiffrer les fichiers piégés par le ransomware Dharma. (crédit : D.R.)

C'est une belle victoire qui vient d'être remportée contre le diabolique ransomware Dharma. Les personnes ayant des fichiers chiffrés par ce programme peuvent en effet souffler car ils peuvent désormais avoir accès à des clés de déchiffrement pour pouvoir les retrouver. Apparu pour la première fois en novembre, Dharma est basé sur l'ancien programme de ransomware Crysis. Il est facile de le reconnaitre par l'ajout aux fichiers chiffrés de l'extension .[email_address].dharma. , l'adresse mail correspondant à celle utilisée par le pirate pour tenter d'extorquer sa victime.

Mercredi, un utilisateur sous le pseudonyme de gektar a publié un lien vers un post Pastbin sur le forum du support technique de BleepingComputer.com. Un post indiquant contenir les clés de déchiffrement du ransomware Dharma et de toutes ses variantes. Etrangement, la même chose s'est produite en novembre avec les clés de son prédécesseur, Crysis ce qui a permis à des chercheurs de créer des outils de déchiffrement. Aucune autre motivation que celle de mettre à disposition ces clés n'a été enregistrée concernant gektar. La bonne nouvelle est que ce leak a permis aux chercheurs de Kaspersky et d'Eset de vérifier son travail. Bingo : les deux sociétés ont mis à jour leurs outils de déchiffrement respectifs à savoir RakniDecryptor et CrysisDecryptor.

Une guerre des gangs dans les ransomwares

Cette situation devrait résonner à l'oreille des personnes touchées par des ransomwares qui ne devraient pas oublier de conserver une copie de leurs fichiers chiffrés à leur insu. Les chercheurs trouvent en effet parfois des failles dans les implémentations du chiffrement des ransomwares leur permettant de casser le chiffrement des clés. Dans d'autres cas, les autorités judiciaires et de police saisissent les serveurs de commande et de contrôle utilisés par les gangs de ransomware et publient ces clés.

Dans d'autres cas comme ici, les clés arrivent à la surface par d'autres moyens inexpliqués. Peut être parce que le développeur du ransomware a décidé de fermer boutique et décide de lâcher les clés, ou alors a-t-on à faire à une rivalité entre deux gangs de hackers qui se mettent des bâtons dans les roues pour court-circuiter l'activité des uns et des autres. Dans tous les cas, il est également recommandé de jeter un oeil sur le site NoMoreRansom.org, régulièrement mis à jour et proposant aussi bien des outils que des conseils pour lutter contre ces fichus ransomwares.

Article rédigé par Lucian Constantin / IDG News Service

Réagissez à cet article

Source : *Un ransomware piège les Mac*