

Victime du ransomware Bart ? Bitdefender publie un outil gratuit de déchiffrement

Victime du
ransomware
Bart ? Bitdefender publie
un outil gratuit de
déchiffrement

L'outil proposé par Bitdefender fonctionne avec tous les échantillons connus. Le ransomware Bart, qui chiffre les appareils sans avoir besoin de connexion Internet, a été analysé par les chercheurs des Bitdefender Labs. Les victimes de ce malware peuvent désormais télécharger l'outil gratuit de déchiffrement afin de récupérer leurs données perdues.

Communiqué de presse – Alors que ce ransomware a été détecté en circulation pour la première fois en juillet 2016, Bitdefender est le seul éditeur de solutions de sécurité à proposer un outil de déchiffrement pour toutes les versions de Bart. L'outil de déchiffrement du ransomware Bart permet de déchiffrer les fichiers avec des extensions « .bart.zip », « .bart » et « .perl » et est également téléchargeable sur le site Internet « No More Ransom » depuis le 4 avril 2017.

Cet outil est le fruit d'une collaboration entre Bitdefender, Europol et la police roumaine en soutien à l'initiative « *No More Ransom* » lancée par le Centre européen de lutte contre la cybercriminalité d'Europol.

Le fonctionnement du ransomware Bart

Contrairement à d'autres familles de ransomwares, Bart chiffre les fichiers des victimes sans avoir besoin de recourir à une connexion Internet. Cependant, le processus de déchiffrement nécessite pour sa part une connexion Internet afin d'accéder au serveur de commande et contrôle (C&C) de l'attaquant, de pouvoir transférer des bitcoins et recevoir la clé de déchiffrement.

Alors que les premières versions de Bart se limitaient à un chiffrement plutôt rudimentaire, tel que la création d'archives .zip protégées par mot de passe, les nouvelles versions vont bien au-delà cette méthode.

Voici comment fonctionne Bart :

- Il supprime les points de restauration du système
- Il génère une clé de chiffrement en se basant sur les informations de la machine de la victime
- Il comptabilise tous les fichiers et les chiffre à l'aide de la clé générée
- Il utilise une master key pour chiffrer la clé utilisée pour chiffrer les fichiers (qui devient l'identifiant unique de la victime, l'UID)
- Il affiche l'avis de rançon et redirige vers un site Internet .onion (l'URL contient l'UID de la victime)...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Bitdefender publie un outil gratuit de déchiffrement du ransomware Bart | UnderNews*