Bitdefender : Un ransomware crypte les fichiers dâ□□internautes et leur demande 50 euros

SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/4/2012 15:00:00

Ce scareware, dÃ©tectÃ© par **Bitdefender** et identifiÃ© sous le nom de **Trojan.Ransom.HM**, a Ã©tÃ© dÃ©tectÃ© sur les rÃ©seaux de partage de fichiers qui hÃ©bergent souvent des versions piratÃ©es de musiques, films et autres. AprÃ¨s avoir chiffrÃ© certains fichiers non exÃ©cutables sur le PC des victimes, il prÃ©tend avoir dÃ©tectÃ© des programmes illÃ©gaux sur leur ordinateur et leur demande une somme dâ□□argent qui doit Ãªtre envoyÃ©e via une adresse Gmail.

Ces scammeurs accusent des internautes dâ□□utiliser des programmes illÃ©gaux et modifient ensuite leurs extensions et icÃ´nes. Un nouveau scareware sâ□□en prend aux personnes qui tÃ©lÃ©chargent des films, de la musique et dâ□□autres fichiers sur des services de partage. Selon une Ã©tude rÃ©alisÃ©e par les chercheurs de Bitdefender, le scareware chiffre les fichiers de lâ□□ordinateur des victimes et leur demande 50 euros en Ã©change dâ□□un code pour les rÃ©cupÃ©rer.

Une fois installÃ© sur un nouveau systÃ¨me hÃ´te, il chiffre toutes les extensions de films, musiques, photos, raccourcis, fichiers PDF, textes et html en ajoutant Â« .EnCiPhErEd Â» aux extensions de fichiers valides. Il remplace Ã©galement les icÃ´nes par dÃ©faut de tous les fichiers dont les extensions ont Ã©tÃ© remplacÃ©es, par une icÃ´ne rose.

Dans chaque dossier quâ□□il trouve sur les systÃ¨mes infectÃ©s, le scareware ajoute un fichier nommÃ© Â« HOW TO DECRYPT FILES.txt Â» et le message dâ□□avertissement suivant :

Â« *Attention ! Tous vos fichiers sont chiffrÃ©s ! Vous utilisez des programmes sans licence ! Pour restaurer vos fichiers et y accÃ©der, envoyez le code Ukash ou Paysafecard dâ□□une valeur de 50 â□¬ Ã lâ□□e-mail Koeserg @ gmail .com. Vous recevrez le jour-mÃªme une rÃ©ponse avec le code. Vous avez droit Ã 5 essais pour saisir le code. Si vous dÃ©passez cette limite, toutes vos donnÃ©es resteront dÃ©finitivement endommagÃ©es.Faites bien attention lorsque vous saisissez le code !* Â»

Les utilisateurs doivent apporter la preuve du versement effectif de 50 euros Ã lâ□□adresse Gmail indiquÃ©e. Le jour mÃªme, les victimes reÃ§oivent une rÃ©ponse avec un code Ã taper dans la case Â« dÃ©chiffrement Â». Si les utilisateurs saisissent mal le code, leurs donnÃ©es seront dÃ©finitivement perdues.

Le scammeur justifie le chiffrement non autorisÃ© par lâ□□avertissement concernant lâ□□utilisation de programmes sans licence. Il suit la tendance de ces derniers mois au cours desquels certaines personnes ont endossÃ© lâ□□identitÃ© dâ□□autoritÃ©s policiÃ¨res Ã la recherche dâ□□utilisateurs tÃ©lÃ©chargeant et utilisant des logiciels piratÃ©s.

La confusion concernant les icÃ´nes et les extensions de fichier est destinÃ©e Ã faire paniquer les utilisateurs et Ã leur extorquer 50 euros. Les expressions comme Â« programmes sans licence Â», Â« chiffrement Â» et Â« attention Â» visent Ã inciter les gens Ã agir sans prendre le temps de se renseigner. Leur PC fonctionne encore parfaitement mais la plupart des utilisateurs sont trop occupÃ©s Ã rechercher leurs donnÃ©es personnelles pour y attacher la moindre importance.

Une fonction du scareware semble permettre aux victimes de dÃ©chiffrer les fichiers si celles-ci saisissent un code transmis par lâ□□escroc par e-mail.

Attitude Ã adopter : Pour Ã©viter ce type de problÃ¨me, soyez attentif aux fichiers que vous choisissez de tÃ©lÃ©charger sur les rÃ©seaux peer-to-peer.

Pour retrouver Bitdefender en ligne