

Popcorn Time, un rançongiciel bien vicieux

 Popcorn Time, un rançongiciel bien vicieux

Depuis peu, les rançongiciels (ou ransomware) constituent de véritables fléaux dans l'univers de l'informatique et du web. Ils touchent les données personnelles de millions de gens de par le monde. Les experts en sécurité se sont même mis à taxer 2016 comme étant « l'année des rançongiciels ».

Payez ou infectez vos amis

Sur cette année, il se peut que Popcorn Time soit le rançongiciel qui vienne clore la propagation de ces logiciels de chantage. Ce nouveau ransomware pose un gros dilemme à sa victime en lui imposant de payer une rançon ou d'infecter ses amis.

Pour commencer, il emprunte le nom d'une application de streaming vidéo ayant défrayé la chronique en 2015, ce qui incite au téléchargement de celle-ci. Ensuite, il infecte l'ordinateur de la victime par le biais d'un courriel piégé ou d'un lien malveillant, puis crypte ses données personnelles en usant d'un algorithme de chiffrement AES 256 bits.

Après que les données ont été cryptées, il impose à la victime de donner la valeur de 1 bitcoin (soit environ 700 €) ou de le transmettre sur l'ordinateur d'un ami. C'est une méthode toute nouvelle avec en plus une limite du nombre d'introductions de clé de déchiffrement. Entrer quatre fois la mauvaise clé ferait perdre définitivement ses données.

Les dossiers Windows sont les premières cibles

D'après la conclusion des enquêtes réalisées par le site Bleeping Computer sur ce rançongiciel, il ciblerait en premier les fichiers présents dans les dossiers Windows : Mes Documents, Images, Musiques et toutes les données sur le Bureau.

Afin de faire face à ce logiciel de rançon, la meilleure façon pour un utilisateur lambda est de prendre des précautions préventives basées sur les mesures de sécurité les plus basiques :

- faire des copies de ses données personnelles vers un support externe qui se débranche de l'ordinateur après chaque usage de ce dernier et sur les Clouds comme Dropbox, OneDrive, Google Drive, Mediafire, Mega, pCloud, Flipdrive... ;
- éviter d'ouvrir les mails aux destinataires inconnus et contenant des liens ou des pièces jointes. Il est aussi possible que Popcorn Time provienne d'une personne de votre liste de contact. Prenez les mêmes réserves tant que le contenu n'a pas été formellement reconnu ;
- mettre à jour son système d'exploitation et son antimalware.

...[lire la suite]

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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

Original de l'article mis en page : Popcorn Time : le plus vicieux rançongiciel de cette année – @Sekurigi