Vos média sociaux personnalisent ce ransomware pour mieux vous piéger

	Un Ransomware utilise vos média sociaux pour mieux vous piéger

Ransoc utilise les médias sociaux pour personnifier la menace et tenter d'attendrir ses victimes. Car rien ne vaut les détails personnels pour faire peur.

Une nouvelle forme de ransomware utilise les comptes des médias sociaux et les fichiers locaux des victimes afin de créer des demandes personnalisées, et menacer d'une action en justice si la rançon n'est pas payée.

Nommé Ransoc par les chercheurs en cybersécurité de Proofpoint en raison de son lien avec les médias sociaux, y compris Facebook, LinkedIn et Skype, ce ransomware est une nouvelle évolution du logiciel malveillant qui s'est répandu cette année sur le Web. Ce n'est pas la première variante de ransomware à utiliser l'ingénierie sociale pour forcer les victimes à payer, mais Ransoc est unique par sa façon de retourner les fichiers des utilisateurs contre eux – surtout si ces fichiers sont téléchargés.

Pas de chiffrage, de la menace directe

Peut-être parce qu'il se concentre sur l'exploitation de cette peur, Ransoc ne chiffre pas les fichiers des victimes de la même manière qu'un ransomware comme Locky. Ransoc livre tout simplement ses exigences via le navigateur après avoir infecté le système via Internet Explorer sur Windows et Safari sur OS X.

Ce procédé pourrait paraître basique ou daté par rapport à des formes plus sophistiquées de ransomware – les ransomwares qui verrouillent les ordinateurs ont vu leur apogée entre 2012 et 2014 – mais Ransoc est construit de manière à pouvoir rechercher sur les disques durs de la victime et sur les médias sociaux les données qu'il va pouvoir ensuite utiliser. Ces données seront ensuite façonnées pour réaliser une demande de rançon sur mesure, en y incluant des images issues de comptes Facebook et LinkedIn.

Détection de matériel illégal

Les chercheurs de Proofpoint ont découvert qu'une variante de la demande de rançon n'est affichée que lorsque Ransoc soupçonne la victime de posséder des fichiers contenant des images illégales ou des fichiers multimédias téléchargés via un protocole torrent. Dans ce cas, Ransoc menace la victime d'une amende et de divulguer ces informations dans le cadre d'une action en justice.

Contrairement à la plupart des systèmes utilisés dans les ransomware, qui exigent des paiements intraçables en Bitcoin, les auteurs de Ransoc ont choisi de faire payer les victimes avec leur carte de crédit.

…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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 : Ce ransomware utilise vos profils de médias sociaux pour personnaliser ses demandes – ZDNet