

Vos médias sociaux personnalisent ce ransomware pour mieux vous piéger

Balliffs Service
Department of pre-trial settlement
Date of issue: Oct 26, 2016
Ref. #: 10/26/2016-200

PENALTY NOTICE

PENALTIES DETAILS
Amount: **\$100**
Due date: **Oct 27, 2016**
Remaining:

WE HEREBY INFORM YOU THAT ON YOUR PC FOUND

ALL ACTIVITY OF THIS PC IS BEING RECORDED USING AUDIO, VIDEO AND OTHER DEVICES

1. CHILD SEXUAL ABUSE MATERIALS
We would like to inform you that pursuant to the provisions of 18 U.S.Code § 1466A and 18 U.S.Code § 2252A any person shall be fined up to \$200,000 and imprisoned for not less than 15 years not more than 40 years. **\$200,000**
40 years in prison

2. MATERIALS THAT VIOLATE THE INTELLECTUAL PROPERTY RIGHTS
We would like to inform you that pursuant to the provisions of 17 U.S. Code § 504 willful copyright infringement carries a penalty up to \$150,000 per instance. **\$150,000**
per instance

3. SUSPICIOUS ACTIVITY
We would like to inform you that pursuant to the provisions of 18 U.S.Code § 1030 any person shall be fined up to \$100,000, imprisoned for not more than 10 years, or both **\$100,000**
10 years in prison

In the course of pre-trial settlement, in case of removal of all detected violations, and payment of the fine within 3 hours since the receipt of this notice,
ALL ACTIONS WILL BE STOPPED AND THE PROCEEDINGS WILL BE CEASED!
(ALL MONEY WILL BE REFUNDED TO YOU IF YOU ARE NOT CAUGHT AGAIN WITHIN 180 DAYS)

You must pay penalty within 3 hours to settle the case out of court. In case of failure to comply claims
ALL COLLECTED DATA WILL BE MADE PUBLIC AND THE CASE GOES TO TRIAL!

Please note:
You must pay penalty within 3 hours to settle the case out of court!

PAY A PENALTY OF \$100 TO SETTLE THE CASE OUT OF COURT

CRIMINAL CASE HAS BEEN INITIATED!
ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

Un Ransomware utilise vos médias sociaux pour mieux vous piéger



Ransoc utilise les médias sociaux pour personnaliser 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 chiffrement, de la menace directe

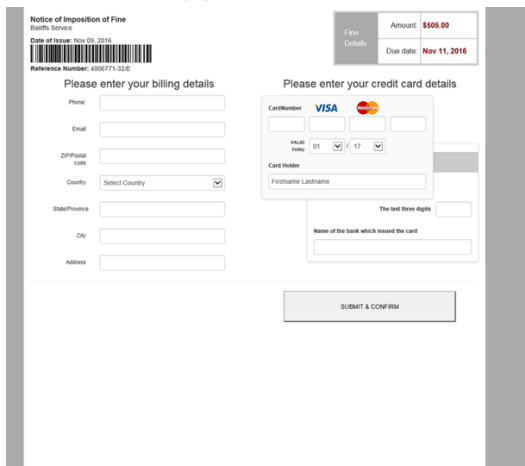
Peut-être parce qu'il se concentre sur l'exploitation de cette peur, Ransoc ne chiffre pas les fichiers des victimes de la même manière qu'un ransomware comme Locky. Ransoc livre tout simplement ses exigences via le navigateur après avoir infecté le système via Internet Explorer sur Windows et Safari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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ce ransomware utilise vos profils de médias sociaux pour personnaliser ses demandes – ZDNet