Détection d’une grande famille de malware et découverte de son mode opératoire

	Détection d’une grande famille de malware et découverte de son mode opératoire

La nouvelle variante de ransomware TorrentLocker atteint en 2014 plus de 40 000 systèmes informatiques européens.

Quelles sont les caractéristiques de cette nouvelle variante ?

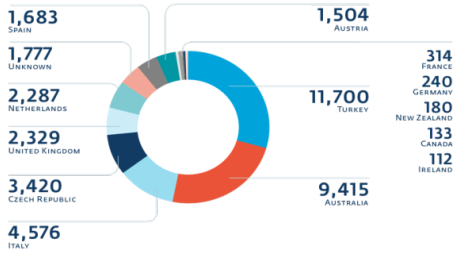
L'équipe de chercheurs canadienne ESET, spécialisée en menaces cybercriminelles, a découvert que depuis le début de l'année 2014, des attaques de ransomware du nom de TorrentLocker se propageaient partout en Europe. Cette variante identifiée par ESET comme Win32/Filecoder.Dl, appartient à la famille des ransomware. Il paraîtrait que les acteurs cachés derrière ce malware seraient de la même famille que le cheval de Troie bancaire : Hesperbot. Sa méthode change en revanche, puisque qu'il passe de la norme AES (Advanced Ecryption Standards) du chiffrement basé sur un compteur (CTR) au chiffrement d'enchaînement des blocs (Cipher Block Chaining, CBC)..

Le logiciel malveillant s'introduit malicieusement dans le système d'exploitation de sa victime, via des liens infiltrés eux-mêmes dans des e-mails frauduleux. Le logiciel crypte ensuite les données de l'ordinateur. Les documents, photographies et autres fichiers sont alors inutilisables pour le propriétaire. Le hacker peut aussitôt demander à la victime de payer une rançon si elle ne veut pas que ses données soient détruites. Les sommes demandées sont considérables, pouvant atteindre les 1200€. Pour déverrouiller ces données, la victime a besoin d'un code de déchiffrement que seul le pirate peut lui fournir et sans garantie.

Des techniques de persuasion toujours plus performantes

Les propriétaires de ces logiciels malveillants savent être de plus en plus convaincants en ciblant le message en fonction des pays qu'ils convoitent. Ils savent de mieux en mieux personnaliser et adapter leur message sur leurs cibles. Par conséquent, ils sont de plus en plus dangereux, car ces « faux » e-mails sont de plus en plus difficile à détecter pour les victimes.

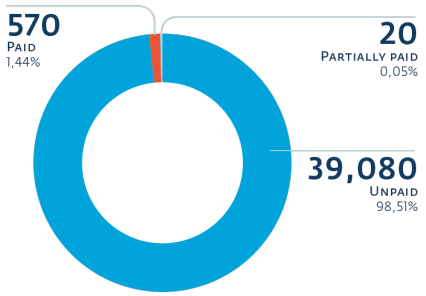
Les acteurs de ce logiciel malveillant utilisent de nombreuses ruses pour convaincre les internautes. Ils envoient des messages personnalisés, en mimant la provenance d'un organisme certifié. Ils en profitent ensuite pour réclamer le paiement d'une fausse facture. Ils arrivent même à troubler les internautes en allant jusqu'à insérer des images de CAPTCHA.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

Des conséquences irrémédiables, attention à ne pas les encourager !

La dernière vague de TorrentLocker a atteint 40 000 ordinateurs, représentant 280 millions de documents chiffrés en Europe, Canada, Australie et Nouvelle-Zélande. Près de 600 victimes ont payé la rançon, ce qui a fait gagner 481 578€ aux malfaiteurs en Bitcoins! En France, Torrentlocker a intercepté 2 170 247 fichiers avec une demande de rançon d'au minimum 830€.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

L'équipe de chercheurs canadiens ESET a su démanteler TorrentLocker en localisant le malware grâce aux serveurs C&C qui généraient des URL pour les pages d'échanges d'argent avec les victimes.

La première règle à prendre en considération est qu'il faut d'une part protéger ses appareils que ce soit un PC, un Mac, un smartphone ou une tablette sous Android. Ensuite il faut veiller à ne pas ouvrir des e-mails inconnus ou paraissant suspects et surtout ne pas cliquer sur un lien trop rapidement ni ouvrir la pièce jointe. Le conseil à retenir est de ne pas payer les rançons demandées, ce qui encourage les pirates et les entraîne à développer leurs logiciels malveillants.

Les actualités sur Torrentlocker

Le logiciel malveillant est en constante évolution, l'équipe de sécurité ESET a mis en place un livre blanc, où elle publie régulièrement leurs analyses et informe sur les nouvelles apparences que prend le logiciel au fil du temps, disponible sur www.welivesecurity.com.

Pour plus d'informations sur TorrentLocker, vous pouvez consulter le livre blanc sur
http://presse.marketing-land.com/r/?F=23e5g9n2ctsdr5hy9tpgyh7gqgazh6hj3y38q6ds3xp5zm8q23sfj4q-5686679

Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a6329542c28f29