Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web | Le Net Expert Informatique

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web

Un nouveau rançongiciel s’attaque aux machines Linux et cible en particulier les dossiers contenant les pages web. Le procédé du logiciel malveillant appelé Linux.Encoder est simple. Le rançongiciel crypte les répertoires de MySQL, Apache ainsi que le répertoire home/root. Le système demande alors de payer un seul bitcoin pour déverrouiller les fichiers.

Une fois que la rançon est payée, le système reçoit une instruction lui faisant parcourir les répertoires pour déchiffrer leurs contenus. Pour s’exécuter, la ransomware a besoin des privilèges d’administrateur et éventuellement d’une autorisation de la part d’un administrateur système pour qu’un tel programme puisse s’exécuter sans restriction. Selon le site drweb.com, une fois que le rançongiciel est lancé avec les privilèges d’administrateur, le logiciel télécharge le contenu des dossiers ciblés et crée un ficher contenant le lien vers une clé RSA publique. Le rançongiciel commence alors à supprimer les fichiers originaux et la clé RSA est utilisée pour générer une clé AES qui sera utilisée pour chiffrer les fichiers sur l’ordinateur infecté.

Source : Dr.WEB

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.developpez.com/actu/92220/Un-rancongiciel-Linux-s-attaque-aux-webmasters-en-chiffrant-les-donnees-des-repertoires-contenant-les-pages-web/