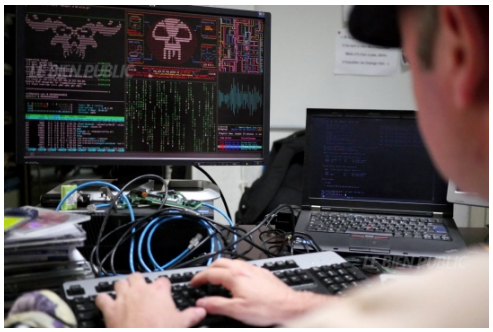
Alerte à partager : Vigilance face au logiciel malveillant Didrex | Le Net Expert Informatique

	Alerte à partager : Vigilance face au logiciel malveillant Didrex

Vols d'identifiants et d'informations personnelles, transferts de fonds non autorisés… devant la multiplication du nombre d'ordinateurs infectés par le logiciel malveillant Dridex, la gendarmerie nationale lance une mise en garde à tous les utilisateurs d'Internet et distille quelques conseils pour se prémunir de la menace.

Depuis le début du mois de juin 2015, la France fait face à une campagne massive de dissémination de logiciel malveillant (malware) par le biais de courriers électroniques non sollicités (Spam). Ce logiciel connu sous le nom de «Dridex» a pour vocation d'infecter les postes informatiques utilisant le système d'exploitation Microsoft Windows (toutes versions allant de Windows XP à Windows 8.1). Actuellement, 28 000 postes sont infectés en France.

Un mail trompeur sous forme de facture

Le but de ce logiciel est de prendre le contrôle de la machine à des fins crapuleuses. En effet, après avoir été infecté, le poste informatique compromis va servir, à la fois, à la collecte de données personnelles (numéro de compte, identifiants et mot de passe de connexion, numéro de carte bancaire, historique de navigation, etc.) ainsi qu'à la réalisation de manœuvres frauduleuses (transfert d'argent, connexion à des sites Internet, envoi de message, relais mandataire, etc.) et ce, à l'insu du légitime propriétaire de la machine. La victime, particulier ou entreprise, est destinataire d'un message électronique contenant une pièce jointe, le plus souvent, un document au format Microsoft Word/Excel, voire dans certains cas, au format portable Document File (.pdf). Cette pièce jointe est souvent intitulée «Invoice» ou «facture» et l'objet du message est souvent en lien avec un paiement ou une facture.

Tous vos codes et données collectés

L'ouverture de cette pièce jointe entraîne, lorsque l'activation des macros est autorisée, le téléchargement d'un logiciel malveillant qui va permettre la prise de contrôle à distance de la machine. Par la suite, lorsque la victime se connecte au site de sa banque en ligne, le malware, va récupérer toutes les informations intéressantes (identifiant, mot de passe, nom, prénom, numéro de téléphone, numéro de compte, numéro de carte bancaire, solde du compte, etc.). Muni de l'ensemble de ces données, l'escroc va alors réaliser des transferts de fonds depuis le compte de la victime vers celui d'une tierce personne pouvant se trouver en France, mais plus généralement à l'étranger.

Comment se prémunir de Didrex

-> Observez une grande vigilance vis-à-vis de la messagerie électronique et ayez un esprit critique sur l'origine des messages qui vous parviennent
– Supprimez tous les e-mails suspects prospectifs (spam) reçus dans la boîte de messagerie, surtout s'ils contiennent des pièces jointes.
– N'ouvrez surtout pas les documents en pièce jointe contenus dans un spam; il suffit de les supprimer.
– Si vous avez des suspicions sur un courriel prétendant provenir d'organisations légitimes (banques, administrations, sites de ventes, etc…), il vaut mieux avant, vérifier auprès de ces organisations en question, la véracité de l'envoi du message et l'authenticité de la pièce jointe.
– Installez une solution antimalware qui protège également des spams. En premier lieu, cela devrait du moins réduire ou au mieux éliminer le risque d'ouvrir accidentellement un de ces pourriels et pièces jointes malveillantes
– Désactivez les macros exécutables automatiquement dans Microsoft Word et Excel
– S'il y a soupçon d'infection, changez immédiatement le mot de passe d'accès au compte bancaire en ligne, pour ce faire veuillez contacter rapidement votre établissement bancaire et l'alerter d'un risque potentiel de fraude. DRIDEX étant capable de dérober d'autres types d'identifiants de connexion, il est vivement recommandé pour tous autres accès à des services en ligne, de modifier les « logins et mots de passe ». ATTENTION : faites ceci en utilisant un autre moyen de connexion que l'ordinateur suspecté d'infection
– Procédez à la même mesure concernant tous autres comptes de services internet dont vous êtes titulaires (fournisseur d'accès internet, vente en ligne, réseaux sociaux, etc…). Dridex vole aussi ce genre d'information
– Surveillez l'activité de vos comptes bancaires et vérifiez la légitimité de vos transactions.

Source : http://www.bienpublic.com/actualite/2015/08/06/la-gendarmerie-appelle-a-la-vigilance-face-a-didrex