Bulletin d'information
PREVENTION ET REMEDIATION
MALWARE DRIDEX

Qu'est-ce que Dridex ?

Dridex est un logiciel malveillant (cheval de Troie). Il cible en particuliers les données bancaires notamment les identifiants, mots de passe et codes secrets (claviers virtuels ou code sms) permettant d'accéder aux comptes bancaires en ligne. Le but recherché par les pirates qui pilotent Dridex, est de réaliser des virements bancaires frauduleux à l'aide des données dérobées.

Ce « malware » est très actif depuis juin et juillet 2015 sur le réseau français. Une grande vigilance doit donc être observée, et il est recommandé de porter attention particulière aux messages emails que vous recevez. Une bonne hygiène informatique et de bonnes conduites sont vivement conseillées notamment au regard des « Spams » (pourriels).

Dridex n'affecte que les ordinateurs qui fonctionnent sous système d'exploitation Microsoft Windows (XP, Vista, Windows 7 et Windows 8).

Dridex se contracte via des messages « spams » (pourriels) qui renferment des pièces jointes aux formats de fichiers principalement de types : Word (.doc ; .docx), Excel (.xls ; .xlsx) et PDF. Les fichiers joints contiennent des routines (macros microsoft) qui s'exécutent automatiquement à l'ouverture desdits documents. Les routines alors vont télécharger le cheval de Troie. Celui-ci s'installera à l'insu des utilisateurs. Les antivirus installés sur l'ordinateur ne le détecteront pas.

Une fois que l'ordinateur a été infecté, Dridex vole des données bancaires ainsi que d'autres informations personnelles. Les pirates peuvent prendre le contrôle à distance de l'ordinateur.

Chaque jour, les spams de diffusion de Dridex varient tant dans leurs origines que dans leurs objets. Les noms des fichiers joints changent également fréquemment. Les pirates qui pilotent Dridex, incitent à ouvrir les documents en pièces jointes. Pour cela, ils usent de stratagèmes attisant la curiosité des destinataires des spams. En effet, ces pourriels se font passer pour des banques, des administrations, des organisations ou des sites commerçants. Ces pourriels font souvent référence à une facture vous concernant, ceci pour vous piéger.

Que faire pour se prémunir de Dridex ? 10 recommandations simples…

Les utilisateurs peuvent se protéger de Dridex en respectant les bonnes conduites d'hygiène informatique suivantes:

1. Observez une grande vigilance vis-à-vis de la messagerie électronique et ayez un esprit critique sur l'origine des messages qui vous parviennent.
2. Supprimez tous les e-mails suspects prospectifs (spam) reçus dans la boite de messagerie, surtout s'ils contiennent des pièces jointes.
3. N'ouvrez surtout pas les documents en pièce jointes contenus dans un spam ; il suffit de les supprimer.
4. Si vous avez des suspicions sur un courriel prétendant provenir d'organisations légitime (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.

5. 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.
6. Désactivez les macros exécutables automatiquement dans Microsoft Word et Excel. Pour aider, consulter le ticket Microsoft suivant : https://support.office.com/fr-be/article/Activer-ou-désactiver-les-macros-dans-les-documents-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12?ui=fr-FR&rs=fr-BE&ad=BE
7. 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.*
8. 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.
9. Surveillez l'activité de vos comptes bancaires et vérifiez la légitimité de vos transactions.
10. Testez votre ordinateur avec « dridexdetector », ci-après.

Diagnostiquer et se débarrasser de la présence de Dridex ?

La méthode suivante permet de mettre en évidence la présence de Dridex sur un ordinateur et de couper le malware de ses communications avec les pirates, le rendant ainsi inefficace (pour autant la charge virale est toujours résidente mais inopérante) :

Utiliser **Dridexdetector.** Il s'agit d'un programme exécutable développé par la Société LEXSI, spécialisée dans la sécurité des systèmes d'information. Ce programme est gratuit et téléchargeable à l'adresse suivante : https://extranet.lexsi.com/resources/files/Lexsi_DridexDetector_v2.zip (mot de passe pour ouvrir le fichier : **DridexDetectorByL3x$1**)

Vous pouvez lire et appliquer les recommandations de LEXSI disponibles sur la page : https://www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

A noter qu'un fichier d'activité « DridexDetector.log » est créé. Ce fichier contient un résumé de ce qui a été découvert par l'outil. Ce fichier d'évènement conserve la trace de la présence effective de Dridex sur la machine diagnostiquée.

Que faire si vous avez détecté Dridex ?

Les personnes qui ont pu mettre à jour la présence du malware Dridex sur leur ordinateur doivent observer les recommandations suivantes :

1. Si n’êtes pas encore victime d’un virement frauduleux, signalez l’infection à votre banque. Vos données ont pu être déjà captées et transmises aux pirates. Il faut surveiller les virements. Editez quand même et conservez-le, au besoin.
2. Si vous êtes victime d’un virement frauduleux et que vous avez détecté Dridex avec l’outil de la société LEXSI, il est recommandé de déposer plainte dans un service de police ou de gendarmerie le plus proche. Il est vivement conseillé, dans la mesure du possible, de fournir l’impression le rapport du détecteur « dridexdetector » (fichier journal), ceci comme élément de preuve rattachant le cas de fraude à l’activité de ce malware.
3. Prévenez la banque de toutes fraudes sur vos comptes dans tous les cas.