Comment se protéger du virus Dridex contenu dans les e-mails piégés | Denis JACOPINI

Comment se protéger du virus Dridex contenu dans les e-mails piégés

Après un mois d'interruption seulement, l'un des logiciels malveillants les plus virulents de 2015 fait son retour en France : plusieurs vagues d'envois massifs de courriels contenant le virus Dridex ont été constatées ces derniers jours. Ce malware de type « cheval de Troie » s'installe sur les ordinateurs Windows par le biais de pièces jointes piégées, dans le but de voler des coordonnées bancaires.

D'où vient ce virus ?

Identifié dès juillet 2014 et repéré dans au moins 26 pays, Dridex n'a jamais vraiment disparu. Pourtant, fin août, une opération internationale coordonnée par le FBI et Europol (E3C), les agences de sécurité américaine et européenne, aboutissait à l'arrestation du Moldave Andreï Ghinkul, dit « Smilex », principal administrateur du virus. Les envois des courriels non-sollicités avaient été stoppés presque totalement le 2 septembre.

Mais le soulagement a été de courte durée : le 1er octobre, Palo Alto Networks détecte une nouvelle activité de Dridex au Royaume-Uni, puis le 14 octobre, c'est au tour de l'éditeur d'antivirus Avira d'émettre des doutes sur l'arrêt réel du botnet (réseau de serveurs et programmes destinés à propager le virus). Ce dernier paraît en effet toujours actif, selon Ayoub Faouzi, l'un des experts d'Avira.

Et effectivement, en France, le CERT-FR avertit le 23 octobre qu'une soixantaine de vagues d'envois massifs d'e-mails piégés visant la France ont eu lieu en moins de quinze jours.

Une nouvelle technique d'assemblage du code dite « just-in-time » (ou à la volée) permet aux pirates d'éviter les détections, mais aussi d'adapter plus rapidement le malware – une technique utilisée par d'autres logiciels malveillants comme GameOver Zeus.

Comment fonctionne t-il ?

Le mail reçu se présente de façon anodine : la plupart du temps, une relance de facture, incluant une pièce jointe au format. doc de Microsoft Office. À l'heure actuelle, peu d'antivirus détectent la nouvelle variante de ce logiciel (qui est signé avec un certificat officiel paraissant émaner de l'entreprise de sécurité Comodo), et la plupart ne suppriment donc pas la pièce jointe.

Si le destinataire tente d'ouvrir le document Word joint, une page vierge va s'afficher, mais le logiciel de Microsoft va tout de même demander à l'utilisateur s'il veut activer les macros (permettant d'interpréter les codes éventuellement contenus dans les documents Office). Une réponse positive active le virus et va lancer le téléchargement discret d'un premier code malicieux.

D'autres fichiers sont ensuite téléchargés afin d'installer divers programmes-espions. Il ne reste plus au pirate qu'à décider quand et quel programme utiliser et installer pour récupérer les données personnelles et bancaires puis effectuer des opérations frauduleuses.

A quoi ressemblent ces e-mails piégés ?

Les premières vagues de mails, le plus souvent intitulés « Relance Facture urgent » ou de « AR CDE + Facture Proforma », ont touché des messageries personnelles ou d'entreprises dès le mois de juin. Ecrits dans un français très correct et sans fautes d'orthographe, ces textes courts, et suffisamment sibyllins pour inquiéter ceux qui les reçoivent, ont déjà fait l'objet d'une première alerte officielle émanant du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. La nouvelle vague de mails reçus ces deux dernières semaines sont du même tonneau.

Exemples :

« Objet : PIXOLUTIONS – FACTURE N°03480830-260615

Bonsoir,

Veuillez trouver en pièce jointe la facture n°03480830-260615 correspondant à la réalisation et pose du logo végétalisé à Perpignan. Vous en souhaitant bonne réception, bien cordialement, ».

« Objet : DUPLICATA FAC N°87878241

Salut,

Il parait que tu recherches la facture avec les Rimauresq Rosé et Blanc ? La voici en pièce jointe. Veux-tu que je te la remette au courrier également ? »

« Objet : Comptabilité de PACAR : facture n° 94352132 du 26/10 de 439,99 euros

Bonjour,

Pouvez-vous nous envoyer un chèque de 439,99 euros en paiement de la facture n° 94352132 dont vous trouverez la copie ci-jointe. En vous remerciant, Bien cordialement, »

Comment s'en protéger ?

En plus d'un antivirus à jour, il est recommandé d'observer une grande vigilance à la réception de tout message contenant une pièce jointe, et ce quel que soit son format (.doc, .odt, .xls, .pdf, etc.).

Si le courriel semble émaner d'un organisme officiel (administrations, banques, boutiques en ligne, etc.), il est préférable de tenter de les contacter soit par téléphone, soit par mail pour vérifier l'objet de la correspondance et la légitimité de l'envoi.

Enfin, l'étape de sécurité optimale consiste à désactiver l'exécution automatique des macros dans les suites bureautiques de type Microsoft Office (aller dans Fichiers/Options/Centre de gestion de la confidentialité/Paramètre du Centre de gestion de la confidentialité/Paramètres des macros/Désactiver toutes les macros avec notifications).

Comment vérifier sa présence et s'en débarrasser ?

La société française de sécurité Lexsi propose un simple outil de détection permettant tout à la fois de vérifier sa présence sur un ordinateur puis de l'éradiquer complètement. Il est également possible, comme l'explique Lexsi, de nettoyer manuellement son ordinateur.

Téléchargez l'outil sur :
https://www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

Source : http://www.lemonde.fr/pixels/article/2015/10/29/e-mails-pieges-nouvelle-alerte-au-virus-dridex-en-france_4799355_4408996.html