Les logiciels de paiement hors ligne ciblés par des pirates: des PME touchées

(25.07.2016) Ces derniers jours, MELANI a observé plusieurs cas dans lesquels le maliciel Dridex est dirigé contre des logiciels de paiement hors ligne. Ce type de logiciel est utilisé par les entreprises, afin de transmettre un grand nombre d'ordre de paiements à une ou plusieurs banques. Si la machine sur laquelle un tel logiciel est installé est compromise, les dommages potentiels sont très importants. MELANI recommande fortement de protéger les ordinateurs utilisés pour le trafic de paiement en conséquence.

Ces derniers jours, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a reçu plusieurs informations concernant des cas dans lesquels des attaquants ont essayé de procéder à des versements frauduleux à travers des logiciels de paiement hors ligne en utilisant le maliciel Dridex. Dans plusieurs cas, les auteurs ont essayé de diriger plusieurs paiements vers des destinataires à l'étranger dans un court laps de temps. Le dommage potentiel est ainsi élevé.

Dridex est un cheval de Troie bancaire connu, se propageant généralement à travers des documents Office malicieux, contenus dans des e-mails provenant d'expéditeurs en apparence légitimes. MELANI a déjà informé le public début juillet à ce sujet.

Vagues de courriels contenant des documents Office malicieux
https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/malicious_office_documents.html

Après l'infection, Dridex recherche d'éventuels logiciels de paiement hors ligne présents sur la machine. Ce type de logiciel est utilisé par les entreprises, afin de transmettre un grand nombre d'ordre de paiements à une ou plusieurs banques. Actuellement, Dridex recherche les logiciels de paiement hors ligne suivants, respectivement les logiciels des fournisseurs figurant ci-dessous. Si Dridex trouve un logiciel de ce type sur l'ordinateur infecté, du code malveillant supplémentaire pourra être téléchargé depuis Internet, dans le but d'effectuer des paiements frauduleux.

Fournisseurs de logiciel
Abacus
Abrantix
Alphasys
Argo-Office
Bellin
Cashcomm
CoCoNet
Crealogix
Epsitec
financesuite
Financesuite
Macrogram
Mammut

Mmulticash
Moneta
Multiversa
Myaccessweb
Omikron
Quatersoft
Softcash
Softcrew
Starmoney
Trinity
Extrait original du fichier de configuration de Dridex (liste de fournisseurs de logiciels de paiement)

Afin de se prémunir contre de telles attaques, MELANI recommande de protéger les ordinateurs utilisés pour ces trafics de paiements de cette manière :

- Utilisez pour votre logiciel de paiement hors ligne et le eBanking un ordinateur dédié uniquement à cette activité, qui ne sera pas utilisé pour naviguer sur Internet ou recevoir des e-mails.
- Pour la validation des paiements, utilisez une signature collective à travers un deuxième canal (par exemple eBanking). Votre banque pourra vous informer des possibilités existantes.
- Si vous utilisez un jeton d'authentification physique (Hardware Token), tel que Smart Card ou USB Dongle, retirez le après utilisation du logiciel de paiement.
- N'enregistrez pas les données d'accès (numéro de contrat, mot de passe, etc.) pour le eBanking ou le logiciel de paiement sur l'ordinateur ou dans le logiciel.
- Informez-vous des possibilités supplémentaires de sécurité auprès du fournisseur du logiciel de paiement et activez les mises à jour automatiques.
- Annoncez d'éventuels paiements suspects à votre banque immédiatement

Pour éviter une infection par Dridex ou un autre logiciel malveillant, MELANI recommande par ailleurs les mesures suivantes

- Veillez à bloquer ou filtrer la réception de courriels contenant des fichiers potentiellement dangereux sur votre passerelle de messagerie ou filtre antispam. Sont dangereux notamment les fichiers:

.js (JavaScript)
.jar (Java)
.bat (Batch file)
.exe (Windows executable)
.cpl (Control Panel)
.scr (Screensaver)
.com (COM file)
.pif (Program Information File)
.vbs (Visual Basic Script)
.ps1 (Windows PowerShell)
.wsf (Windows Script File)
.docm (Microsoft Word avec macro)

.xlsm (Microsoft Excel avec macro)
.pptm (Microsoft PowerPoint avec macro)

- Veillez à ce que ces fichiers soient également bloqués lorsqu'ils sont envoyés dans un fichier d'archive tel qu'un fichier ZIP ou RAR ou dans un fichier d'archive protégé (par exemple un ZIP protégé par un mot de passe.
- Par ailleurs, il est recommandé de bloquer tous les fichiers joints contenant des macros (par exemple les fichiers joints Word, Excel ou PowerPoint contenant une macro).

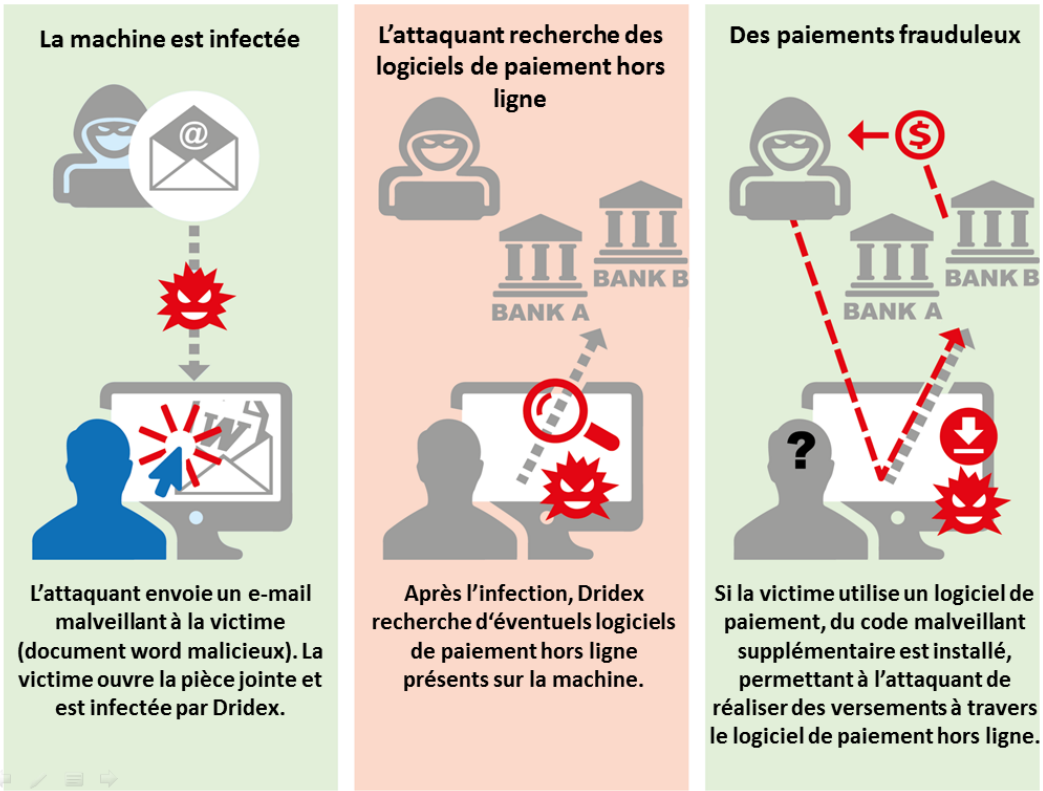
Des mesures et recommandations supplémentaires pour améliorer la sécurité des PME sont disponibles dans notre aide-mémoire.

Sécurité informatique: aide-mémoire pour les PME:
https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

Programme en 10 points pour améliorer la sécurité informatique:
https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/infrastructure-ti/infrastructure-technologie-information-ti/infrastructure-securite-ti.html

Avis important de sécurité pour mammut soft ag:
https://www.mammut-soft.ch/images/Doku/Avis_important_de_sécurité.pdf

Modus Operandi:



Source: MELANI, 25.07.2016,
https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/offline-payment-software.html