POLICE CANTONALE

COMMUNIQUE DE PRESSE

Cybercriminalité: plusieurs sociétés vaudoises infectées par le virus RETEFE

Ces dernières semaines, plusieurs sociétés vaudoises ont annoncé avoir subi une attaque de leur système informatique par le biais de leur boîte de messagerie électronique, engendrant une augmentation significative des infections par le virus RETEFE. Ce dernier a pour effet de détecter les connexions des victimes sur leurs sites de paiements en ligne et de rediriger automatiquement la victime, vers un faux site e-banking. La police cantonale vaudoise conseille aux entreprises et aux personnes se reconnaissant dans ce modus d'être extrêmement vigilantes lors de la réception des messages électroniques contenant des fichiers attachés.

Plusieurs sociétés vaudoises nous annoncent avoir subi une attaque de leur système informatique avec la prise de contrôle par des pirates de leur boîte de messagerie électronique (e-mails). Les pirates envoient ensuite des e-mails, directement depuis la messagerie des lésés en utilisant les carnets d'adresses à disposition. Ce faisant, les destinataires de ces e-mails frauduleux reçoivent un courriel d'un expéditeur connu et ouvrent une pièce jointe (document Word, Excel, PDF) infectée par le virus RETEFE, ayant pour conséquence d'infecter l'ordinateur.

Ce virus a pour effet de détecter les connexions des victimes sur leurs sites de paiements en ligne et de rediriger automatiquement la victime vers un faux site e-banking. Lorsque le plaignant insère ses identifiants (nom utilisateur et mot de passe), le virus les enregistre et les transmet au pirate qui peut aisément effectuer des virements frauduleux depuis le compte bancaire de la victime.

Nous conseillons aux entreprises et aux personnes se reconnaissant dans ce modus d'être extrêmement vigilantes lors de la réception des messages électroniques contenant des fichiers attachés. N'ouvrez pas les fichiers attachés sauf si ceux-ci sont attendus. De plus, si après l'avoir ouvert, un message vous demande d'exécuter des macros, ne le faites pas et supprimez le message en avisant l'expéditeur.

Mesures à prendre en prévention:

- en cas de doute n'ouvrez pas les fichiers attachés et contactez l'entreprise par téléphone
- contrôlez toujours l'expéditeur de l'e-mail
- désactivez les macros dans les programmes Office (Excel, Word, etc.) en consultant la partie «Modifier les paramètres des macros dans le Centre de gestion de la Confidentialité» accessible ici: https://support.office.com/fr-fr/article/activer-ou-d%C3%A9sactiver-les-macros-dans-les-fichiers-office-12b036fd-d140-4e74-b45e-16fed1a7e5c6
- assurez-vous que votre logiciel antivirus est à jour
- contrôlez vos paiements en attente d'exécution ou exécutés
- contrôlez votre ordinateur en le testant ici: http://retefe-check.ch/

Police cantonale vaudoise — Direction communication et relations avec les citoyens
Centre de la Blécherette, 1014 Lausanne
tél. + 41 21 644 81 90
E-mail: communication.police@vd.ch — web: www.police.vd.ch

POLICE CANTONALE

COMMUNIQUE DE PRESSE

Mesures à prendre en cas d'infection:

- avisez votre hébergeur web sans tarder
- avisez votre responsable informatique
- avisez vos clients sans tarder
- avisez votre banque que vous avez été victime du virus RETEFE
- activez les protections maximales sur vos transactions financières en activant des doubles validations de paiements auprès de votre partenaire bancaire
- prenez toutes les mesures nécessaires pour vous assurer que vos ordinateurs et votre réseau est protégé
- mettez de côté tous les éléments qui seront utiles à l'enquête (copie d'e-mails, en-tête d'e-mails, dates et heures des événements)
- déplacez-vous pour déposer une plainte pénale dans le Poste de police le plus proche de chez vous après avoir procédé aux deux conseils précédents (localiser le poste de police le plus proche (https://www.vd.ch/toutes-les-autorites/departements/departement-des-institutions-et-de-la-securite-dis/police-cantonale-vaudoise-polcant/ou-nous-trouver/)

Le site internet du MELANI peut vous apporter des conseils complémentaires:
https://www.melani.admin.ch/melani/fr/home.html

En cas d'attaque avérée, il est important de déposer plainte dans le poste de police le plus proche. Il est également recommandé d'annoncer les cas et/ou les tentatives d'attaques auprès du service dédié de la Confédération:
https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Lausanne, le 14 juin 2018

Olivia Cutruzzolà, Of sp.
Police cantonale vaudoise
Direction communication et relations avec les citoyens

Renseignements: 021 644 80 27 / 079 808 50 13