Quand la recherche d'un chef de clinique en psychiatrie mène à un cheval de Troie

Tout a commencé par un message alarmant de notre confrère Jürg Unger du Comité central. Les cliniques psychiatriques ont beaucoup de peine à pourvoir les postes de cadres avec des médecins qualifiés. Les candidatures spontanées par courriel sont donc intéressantes. Le problème est que cet été, une candidature spontanée a pratiquement paralysé le système d'exploitation de la clinique. Le document attaché n'était pas le CV annoncé, mais un cheval de Troie. A la pénurie de personnel est donc venu s'ajouter un grave problème informatique.

Les logiciels malveillants, ou maliciels, ne sont pas un phénomène nouveau. Les chevaux de Troie dissimulés dans un fichier joint à un courriel font partie des classiques. En revanche, avec la forte progression de l'informatique dans les cabinets et cliniques, les systèmes d'exploitation des institutions de santé font désormais de plus en plus souvent l'objet d'attaques ciblées, ce qui est nouveau. Or ces institutions gèrent presque exclusivement des données sensibles. Ici, la protection et la sécurité des données ne sont pas seulement une question de temps et d'argent; c'est aussi la condition essentielle pour préserver la confiance des patients et garantir la qualité élevée des traitements.

Suite à l'inquiétude – justifiée – exprimée par Jürg Unger, nous avons souhaité publier une série d'articles sur ce domaine en pleine évolution qu'est le monde numérique et la cybersanté ainsi que sur les possibilités et les risques qu'il présente. Lorsque cela est possible, nous céderons la parole à des experts, à l'instar de Pascal Lamia de MELANI, qui ouvre cette série d'articles.

Yvonne Gilli

Dr méd., membre du Comité central de la FMH, responsable du département Numérisation / eHealth

Les rançongiciels dans la santé aussi

eHealth actuel

Pascal Lamia

Chef de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)

Les logiciels de rançon (chevaux de Troie verrouillant les données), appelés aussi rançongiciels, appartiennent à une famille particulière de logiciels malveillants (maliciels). Ils se propagent typiquement par le biais de fichiers infectés joints à des courriels (p. ex. dossier de candidature, rappels de paiement, livraison d'un colis UPS, etc.) ou de sites Internet piratés.

Suite à l'infection, le logiciel chiffre les données présentes sur l'ordinateur de la victime ainsi que sur les éventuels lecteurs réseau et supports d'enregistrement (p. ex. disques durs externes, sticks USB) auxquels cet ordinateur est relié, ce qui les rend inutilisables pour la victime. Une fois les données chiffrées, le logiciel fait alors afficher un écran verrouillé demandant à la victime de payer une certaine somme d'argent sous la forme d'une monnaie virtuelle (p. ex. bitcoin) pour déverrouiller les données (chantage).

Paiements le plus souvent en bitcoins

L'utilisation d'une monnaie virtuelle comme le bitcoin rend difficile l'identification de l'auteur de l'attaque. De plus, même si la victime paye, il n'existe aucune garantie qu'elle puisse récupérer ses données. En payant la rançon, la victime participe en outre au financement de l'activité des criminels et leur permet d'améliorer l'efficacité de leurs prochaines attaques.

Les logiciels de chantage ne sont pas un phénomène nouveau: le premier rançongiciel est apparu en Suisse en 2011 déjà.

Forte augmentation du nombre de victimes

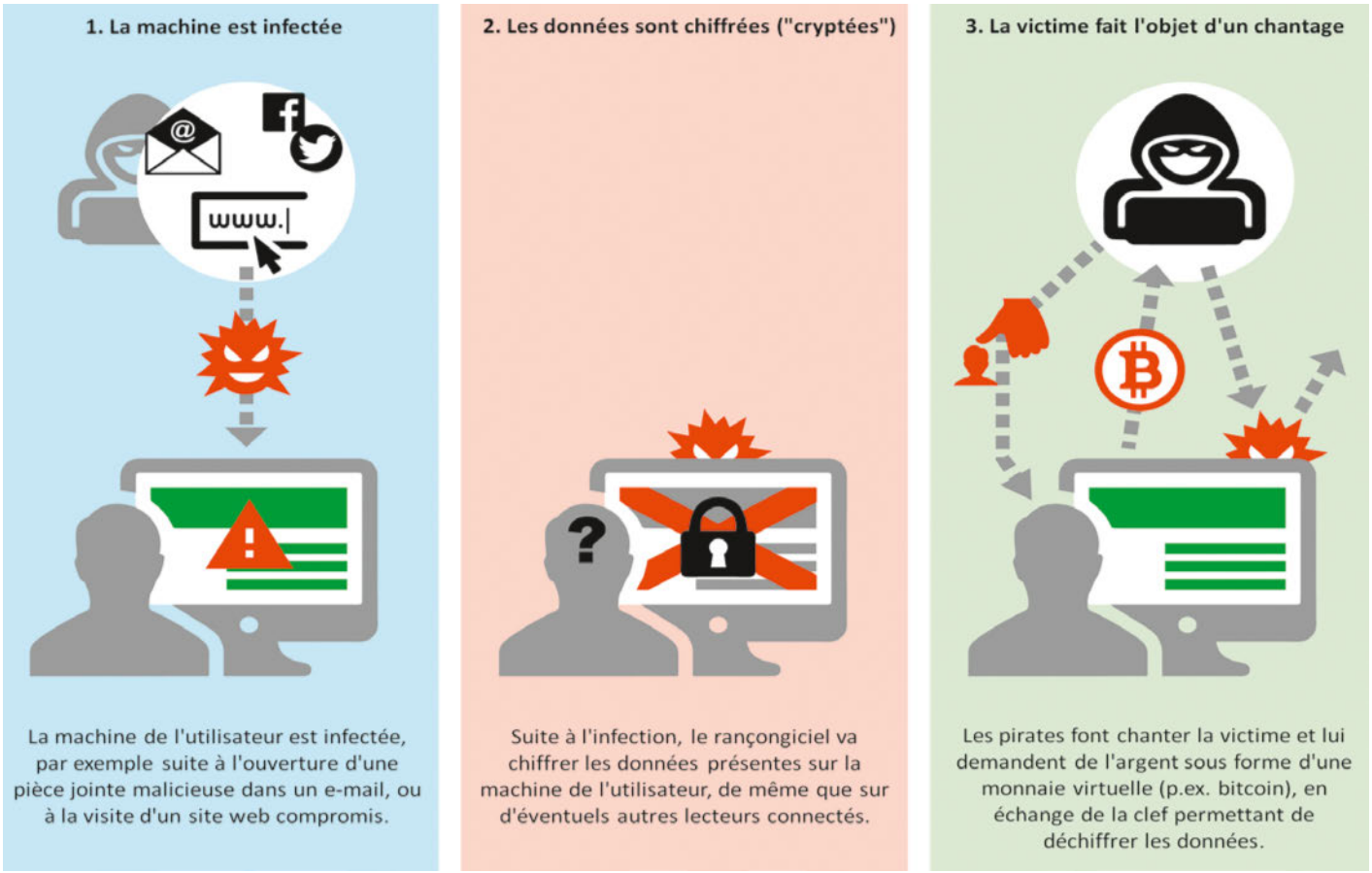
Au cours des derniers mois cependant, le nombre de victimes des logiciels de chantage en Suisse a fortement augmenté. Ce ne sont désormais plus seulement les utilisateurs privés qui sont visés par ces attaques, mais de plus en plus de petites et moyennes entreprises (PME) principalement dans le secteur de la santé (hôpitaux).

Alors qu'en cas d'incident, les utilisateurs privés n'ont plus accès à leurs données personnelles, les conséquences sont bien plus graves pour les entreprises et en particulier les hôpitaux ou les cabinets médicaux.

Crédits photo
Mise à disposition par l'auteur

Pascal Lamia

Pascal Lamia dirige la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de la Confédération. MELANI est un modèle de coopération entre l'Unité de pilotage informatique (UPIC) et le Service de renseignement (SRC), rattachés respectivement au Département des finances et au Département fédéral de la défense, de la protection de la population et des sports.



Les données chiffrées et rendues ainsi inutilisables sont souvent des données critiques comme les contrats, données de clients et de comptabilité, données de patients. Un hôpital ou un cabinet peut rapidement se retrouver dans une situation d'urgence l'incitant d'autant plus à payer la rançon pour pouvoir accéder de nouveau à ses données.

Cela ne doit pas arriver. Les trois mesures suivantes doivent permettre aux citoyens mais aussi aux PME de se protéger efficacement contre les rançongiciels:

Conseils de sécurité

Veillez à effectuer des sauvegardes régulières de vos données. Les données devraient être sauvegardées sur un lecteur externe (hors ligne), p. ex. sur un disque dur externe. Après la sauvegarde, veillez à déconnecter de l'ordinateur le support contenant les données sauvegardées, sans quoi ces données pourront également être verrouillées et rendues inutilisables en cas d'infection de l'ordinateur par un rançongiciel.

Faites preuve d'une grande prudence avec les courriels. N'ouvrez jamais les fichiers joints à un courriel inattendu ou provenant d'un expéditeur inconnu et ne cliquez sur aucun lien.

Il convient de toujours maintenir à jour les logiciels et modules d'extension installés sur son ordinateur. Veillez à ce que tous les logiciels, applications et modules d'extension de navigateur web (p. ex. Flash Player, Java) installés soient toujours à jour. Lorsque cela est possible, activez toujours la mise à jour automatique.

Vous trouverez des informations détaillées sur les rançongiciels et les mesures de protection sur le site Internet de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI: https://www.melani.admin.ch/ransomware

Les règles de comportement lors de l'utilisation d'ordinateurs et d'Internet ainsi que d'autres mesures permettant d'améliorer la sécurité informatique dans les PME peuvent être consultées sur les sites Internet suivants:

- **Règles de comportement:** https://www.melani.admin.ch/verhaltensregeln
- **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

Correspondance:
Fédération des médecins suisses (FMH)
Divisions Numérisation / eHealth
Elfenstrasse 18
Cas postale 300
CH-3000 Berne 15
Tél. 031 359 11 11
ehealth[at]fmh.ch