PIRATAGE DE SITES INTERNET DE COLLECTIVITÉS PAR DES PHARMACIES ILLICITES

Les sites de pharmacies illicites sont extrêmement répandus sur l'Internet. Ces sites tentent d'attirer leurs clients potentiels en leur faisant miroiter l'achat facile de médicaments acheminés par correspondance. Ces médicaments sont souvent des produits érectiles dont la vente est réglementée. Les produits commandés sur ces sites ne sont pas toujours livrés et quand ils le sont, ils s'avèrent en général être des contre-façons qui peuvent être dangereuses pour la santé de leurs consommateurs.

Une forte recrudescence de présence de pages de pharmacies illicites sur des sites Internet officiels de collectivités (principalement de mairies) a été constatée ces derniers temps.

Les acteurs de ce type de cybermalveillance profitent généralement de défauts de sécurisation des sites Internet des collectivités sur lesquels ils arrivent à s'installer. Les collectivités concernées ont souvent des difficultés à identifier ce forfait, car leur site continue de fonctionner normalement. Les pages de pharmacies illicites présentes sur les sites des collectivités ne permettent pas toujours de passer commande directement et donnent alors les renseignements permettant de finaliser l'achat : numéros de téléphones, références vers d'autres sites ou adresse de messagerie…

La présence de ce type de commerces illicites sur des sites officiels de collectivités est de nature à nuire gravement à la réputation et à la crédibilité des collectivités concernées auprès de ses publics.

BUT RECHERCHÉ

En installant leur officines illégales sur des sites de collectivités insuffisamment sécurisés, les cybercriminels ont pour objectif principal de dissimuler leur activité, tout en augmentant la visibilité de leur commerce en stimulant le système de référencement des moteurs de recherche.

MESURES PRÉVENTIVES

- A l'instar de n'importe quel système, une application Web doit faire l'objet d'un réglage de ses paramètres de sécurité avant sa mise en service au risque de laisser des « portes » inutilement ouvertes. Cette étape est primordiale.
- Appliquez de manière systématique et sans délai les correctifs de sécurité des serveurs de publication, des outils de gestion de contenu du site Web et de l'ensemble de leurs extensions (*plugins* en anglais).
- Appliquez également de manière systématique et sans délai les correctifs de sécurité du système d'exploitation et des logiciels tiers qui pourraient être présents sur le serveur du site Web.
- Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement, et que ceux qui existent par défaut sont supprimés ou correctement remplacés. (voir le guide de l'ANSSI: www.ssi.gouv.fr/guide/mot-de-passe/)
- Ayez un pare-feu correctement paramétré : fermez tous les ports et tous les services inutilisés ; ne laissez que les adresses des machines indispensables accéder aux fonctionnalités d'administration du site.
- Faites des sauvegardes régulières hors ligne du site et du système et avec une rétention suffisante pour pouvoir revenir en arrière en cas de besoin.
- Procédez à un examen régulier des fichiers de journalisation du système et de votre pare-feu afin de pouvoir identifier toute anomalie dans le fonctionnement et l'utilisation normale du site.
- Faites vous assister au besoin dans l'application de ces mesures par des professionnels qualifiés.

SI VOUS ÊTES VICTIME

- A la constatation d'une compromission, mettez de préférence immédiatement le site hors ligne et a minima les pages de vente illicite après en avoir fait une copie pour les services enquêteurs.
- Identifiez ou faites identifier le vecteur qui a permis de prendre le contrôle du serveur.
- Vérifiez qu'une fuite de données n'a pas également eu lieu en analysant notamment les différents fichiers de journalisation. A compter du 25 mai 2018 et en application du règlement général européen sur la protection des données, en cas de fuite de données personnelles, il conviendra de déclarer l'incident à la CNIL et d'informer les personnes concernées.
- Essayez de récupérer ou de faire récupérer les fichiers de journalisation (log) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.
- Réalisez ou faites réaliser une copie complète de la machine attaquée et de sa mémoire.
- Déposez plainte au commissariat de police ou à la brigade de gendarmerie à laquelle vous êtes

- rattaché et tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.
- Sollicitez les moteurs de recherche pour faire supprimer le référencement des pages illicites.
- Lorsque vous aurez repris le contrôle de la machine touchée, toutes les vulnérabilités identifiées doivent être corrigées et tous les mots de passe changés avant de la remettre en ligne.
- Faites vous assister au besoin dans l'application de ces mesures par des professionnels qualifiés. Vous trouverez sur www.cybermalveillance.gouv.fr des prestataires de proximité spécialisés susceptibles de pouvoir vous apporter leur expertise.

Les infractions

L'incrimination principale qui peut être retenue ici est celle de l'**atteinte à un système de traitement automatisé de données** (STAD).

Les articles 323-1 à 323-7 du code pénal disposent :

- « le fait d'accéder ou de se maintenir, frauduleusement » dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité);
- « le fait d'introduire frauduleusement des données » dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site. La défiguration désigne la modification non sollicitée de la présentation d'un site web, à la suite d'un piratage du site ;
- le fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données » d'un système de traitement automatisé de données. La copie frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement ;
- « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » ;
- les tentatives de ces infractions sont punies des mêmes peines.

En fonction du cas d'espèce, les peines encourues sont de 2 à 7 ans d'emprisonnement et de 60 000 € à 300 000 € d'amende.

Par ailleurs, les articles L5125-33 et suivants du code de la santé publique disposent **:**
« On entend par commerce électronique de médicaments l'activité économique par laquelle le pharmacien propose ou assure à distance et par voie électronique la vente au détail et la dispensation au public des médicaments à usage humain et, à cet effet, fournit des informations de santé en ligne. »

« Seuls peuvent faire l'objet de l'activité de commerce électronique les médicaments qui ne sont pas soumis à prescription obligatoire. »

« La création du site internet de commerce électronique de médicaments de l'officine de pharmacie est soumise à autorisation du directeur général de l'agence régionale de santé territorialement compétente. Le pharmacien informe de la création du site le conseil compétent de l'ordre des pharmaciens dont il relève. »

Au titre de l'article L4223-1 du code de la santé publique, le fait de se livrer à des opérations réservées aux pharmaciens, sans réunir les conditions exigées, constitue un **exercice illégal de la profession de pharmacien,** qui est un **délit passible de deux ans d'emprisonnement et de 30 000 euros d'amende.**