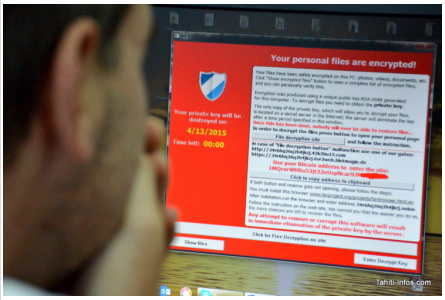
Attaque informatique importante contre les administrations et entreprises de Polynésie

Attaque informatique importante contre les administrations et entreprises de Polynésie

Depuis jeudi dernier, une attaque informatique de grande ampleur touche les services du Pays, de l'Etat et des entreprises de la Polynésie française. Le virus s'introduit sur les postes de travail par les mails, jeux flash et sites contaminés…



Les services informatiques du Territoire, de l'Etat et des entreprises sont en alerte rouge depuis bientôt une semaine : un virus s'est introduit sur de nombreux postes de travail et contamine même des serveurs au cœur de l'infrastructure des administrations et sociétés.

Un message de ce type peut accueillir les internautes imprudents

Ce virus est particulièrement vicieux, pour deux raisons. La première est qu'il est très évolué. Ce logiciel malveillant de dernière génération (une évolution de TeslaCrypt-2.0, détecté pour la première fois en juillet dernier) n'était pas encore identifié par les éditeurs d'anti-virus la semaine dernière. Kaspersky, la solution de sécurité du Pays et l'un des meilleurs du domaine, n'a mis à jour sa base de données virale contre cette nouvelle version qu'il y a deux jours.

La deuxième raison est le type d'attaques que commet ce virus : c'est un crypto-locker, aussi appelé « ransomware » pour « logiciel de rançon ». Une fois introduit sur les ordinateurs des victimes, il encrypte tous les fichiers du disque-dur puis demande une rançon pour rendre ses données à son propriétaire. Mais payer ne garantirait même pas le retour de toutes les données intactes…

NE PAS PAYER MAIS DEMANDER DE L'AIDE

Le conseil est de ne pas payer : « on ne peut pas décrypter les fichiers, mais des solutions existent pour récupérer les données. On peut essayer de revenir à des versions antérieures du fichier, sauvegardées automatiquement par Windows… Il y a aussi des façons de récupérer les fichiers originaux supprimés par le virus » nous explique un expert du CLUSIR (une association d'experts en informatique du Pays), qui assure qu'il ne faut pas céder à la panique. Il explique qu'en cas de contamination, il faut immédiatement éteindre le poste et le déconnecter du réseau, puis contacter son service informatique ou son prestataire informatique.

La situation semble désormais maitrisée dans les administrations après une sacrée frayeur. Nous avons ainsi appris que la direction de la Santé, l'Aviation civile, la direction des Ressources Marines et Minières, le palais de justice ou encore la clinique Paofai ont été attaqués. Certains serveurs auraient été contaminés et des bases de données rendues inaccessibles, par exemple celles de localisation des pêcheurs… Qui aurait été récupérée.

DES POSTES CONTAMINÉS VIA LES JEUX EN LIGNE

Les pirates utilisent des logiciels spéciaux pour infecter des sites web très populaires mais mal protégés. Ensuite, le « toolkit » essaiera de pénétrer les ordinateurs de tous les internautes qui visiteront ce site en testant les failles de sécurité connues. Pour vous protéger, gardez votre version de Windows, Flash, Javascript, votre navigateur etc. à jour.

On ne sait pas encore si c'est une attaque délibérée d'un groupe de pirates informatique – les mafias du monde entier se sont mises à ce nouveau modèle d'extorsion très juteux – ou s'il s'agit justes d'attaques aléatoires qui touchent particulièrement la Polynésie à cause de simples effets réseaux (un seul poste qui tombe et tout le réseau est contaminé ; un chef de service qui se fait avoir et tout son carnet d'adresses reçoit le virus par mail…). Les experts penchent pour la deuxième hypothèse, d'autant que le malware fait parler de lui dans le monde entier depuis quelques jours.

Les services informatiques qui luttent contre l'attaque en ce moment même nous confient que le principal point d'entrée du virus dans les réseaux était… Les sites de jeux en ligne contaminés par les pirates. Ensuite le virus a réussi à se répandre sur les réseaux des administrations puis des entreprises, jusqu'aux serveurs de fichiers du Pays par exemple, qui ont tous été passés en mode « lecture seule » ce mercredi pour essayer d'achever le virus.

L'autre mode de contamination : les fichiers attachés (particulièrement ceux ayant les extensions .js, .zip et .exe) et… les sites porno. Le meilleur conseil reste celui d'un informaticien contacté pour cet article : « Cette attaque c'est pour tout le monde, il est vraiment temps de faire vos sauvegarde. »

Les conseils de prudence du service informatique du Pays

Depuis le début de l'attaque contre les services du Pays, les informaticiens du Territoire sont sur le pied de guerre contre ce virus particulièrement sophistiqué. Plusieurs sources nous ont transmis les mails reçus dans toute l'administration territoriale, dont voici un extrait du dernier en date :

« Suite aux précédents courriels que nous vous avons envoyés, nous souhaitons vous tenir informés de l'évolution de l'infection virale. Elle touche aussi désormais d'autres sociétés de Polynésie française. La situation est inquiétante. (…)

Mise à jour de la définition virale

Nous vous demandons de vérifier que votre anti-virus Kaspersky est à jour. Pour cela, placer la souris sur l'icône « K » en bas à droite de votre bureau : la date d'édition des bases ne doit pas être antérieure à deux jours. Dans le cas contraire, merci de bien vouloir contacter le support du service informatique.

Sauvegarde de vos données personnelles

Nous vous rappelons aussi que vous devez faire des sauvegardes de vos données professionnelles se trouvant sur votre poste de travail. Les serveurs de fichiers étant en lecture seule, sauvegardez vos données professionnelles sur un support externe (disque USB, clé USB), ne pas oublier de le déconnecter à la fin de la sauvegarde.

Rappels sur des règles de sécurité

Afin de vous protéger des virus qui sévissent actuellement, nous vous demandons de suivre scrupuleusement les consignes de sécurité suivantes :

– ne pas ouvrir des courriels suspects (expéditeur inconnu, objet du courriel rédigé en anglais…)

– ne pas ouvrir les pièces jointes à un courriel suspect, en particulier, ne surtout pas ouvrir les fichiers se terminant par l'extension .js. »

Réagissez à cet article

Source : http://www.tahiti-infos.com/Attaque-informatique-importante-contre-les-administrations-et-entreprises-de-Polynesie_a141657.html