Flash n°9 – 10 mars 2014

Flash
ingérence économique

Ce « flash » de l'ingérence économique relate un fait dont une entreprise française a récemment été victime. Ayant vocation à illustrer la diversité des comportements offensifs susceptibles de viser les sociétés, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité au sein de votre entreprise. Aussi, nous vous invitons à le faire suivre le plus largement possible.

Vous comprendrez que par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier l'entreprise visée.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de nous écrire à l'adresse :
securite-economique@interieur.gouv.fr

Mise en garde sur les attaques informatiques de type

« ransomware » ou « crypto-virus »

Récemment, une société francilienne a été victime d'une attaque informatique ayant eu pour effet le cryptage malicieux de ses répertoires de fichiers. En l'espèce, le poste de travail d'un salarié était bloqué par l'ouverture d'une fenêtre exigeant le paiement d'une somme de 400 euros en échange de la clé de chiffrement permettant la récupération des fichiers compromis.

Un « ransomware » (littéralement, logiciel de rançon) ou **« crypto-virus »** est un logiciel malicieux qui bloque les fichiers d'un ordinateur ou d'un réseau et exige le versement d'une somme d'argent en échange du moyen de déblocage des données.

La société ne disposait pas de sauvegarde centralisée sur un serveur commun à tous les salariés et a vainement tenté de récupérer les fichiers compromis.

Une plainte a été déposée. Les premières constatations ont révélé que le logiciel utilisé dans le cas d'espèce faisait appel à des moyens de chiffrement suffisamment sophistiqués pour mettre en échec leur neutralisation par une société privée de sécurité informatique.

Commentaire :

Ces logiciels malveillants transitent par le biais de clés USB infectées, de mails nantis de pièces jointes piégées ou de sites web dont la page d'accueil est compromise au moyen de virus exploitant les failles des systèmes Java, Flash ou du navigateur Internet.

Il existe deux variantes de **« ransomwares »** :

- Les fichiers ne sont pas chiffrés bien que votre PC soit bloqué et assorti d'une demande de rançon. Il est alors possible de supprimer le virus en démarrant l'ordinateur sur un antivirus au boot, figurant sur un CD ou une clé USB. L'ordinateur est ensuite paramétré pour redémarrer sur ce support extérieur en lieu et place du disque dur ;
- votre PC est bloqué, une rançon exigée et vos fichiers cryptés. Un scan antivirus au démarrage de l'ordinateur est susceptible de neutraliser le virus mais vos fichiers restent chiffrés.

Les **« ransomwares »** peuvent emprunter l'apparence d'un logiciel antivirus qui affiche le message suivant : « *Un virus a été trouvé et par sécurité nous avons bloqué votre PC ; veuillez acheter notre antivirus pour supprimer le malware trouvé* ».

Ils peuvent aussi prendre la forme de messages qui semblent provenir d'institutions publiques ou privées (police, gendarmerie, ANSSI, SACEM…). Il vous est reproché le téléchargement d'œuvres protégées par le droit d'auteur ou la détention de fichiers pédopornographiques et il vous est demandé de payer une amende par Internet pour débloquer votre PC. L'apparition d'une fenêtre sur l'écran exigeant le versement d'une « rançon » assortie d'un compte à rebours accordant un délai de paiement de 48 ou 72 heures est caractéristique de ce type d'escroquerie « virtuelle ».

Le versement de la « rançon » par la victime se fait généralement par le biais de monnaies électroniques « bitcoins » ou via des services de paiement en ligne de type « U Kash », rendant quasiment impossible le « traçage » de la transaction.

* * *

Les attaques informatiques de type **« ransomware »** illustrent l'urgente nécessité pour toute entité, publique ou privée, détentrice d'informations numériques stratégiques, d'effectuer une sauvegarde de son système informatique et de sanctuariser l'archivage de ses données.

Afin de garantir la future sécurité informatique des entreprises ayant subi une attaque de ce type, il est vivement conseillé de procéder à la réinstallation des systèmes d'exploitation, d'autres logiciels malicieux ayant pu être installés lors de l'intrusion initiale.