Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 34 - Juin 2017

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°34 Juin 2017

Les risques cyber liés aux rançongiciels

Un rançongiciel est une forme d'attaque informatique visant à extorquer une somme d'argent à un utilisateur *via* l'infection de son périphérique. L'outil malveillant bloque le matériel ou chiffre les données afin de rendre impossible tout travail sur ce dernier. Une rançon est demandée en contrepartie du rétablissement de l'accès au périphérique ou de la fourniture d'une clé de déchiffrement. En pratique, le périphérique touché affichera le plus souvent une fenêtre *pop-up* avec les instructions permettant le déverrouillage. La pression psychologique de l'attaque sur l'utilisateur peut être renforcée par la présence d'un chronomètre qui affiche le temps restant jusqu'à l'augmentation de la rançon, la destruction des données ou leur diffusion en clair sur les réseaux.

Le paiement de la rançon est régulièrement demandé en crypto-monnaie – *Bitcoin* la plupart du temps – ce qui permet de masquer l'identité de l'attaquant et d'entraver les actions de suivi (pas de trace liée à l'existence d'un compte bancaire nominatif, pas de rencontre physique pour paiement en liquide, etc.). Les rançongiciels sont le plus souvent utilisés par le milieu cybercriminel, mais la facilité d'accès à de tels outils sur le *Dark Web* les rendent utilisables par des attaquants disposant d'un plus faible niveau de technicité.

Si les modes de propagation sont variés, la diffusion de pièces jointes par courrier électronique reste le mode d'infection le plus courant avec la mise à disposition d'un lien vers un site Internet ayant une apparence authentique. Le facteur humain est déterminant dans la réussite d'une tentative d'infection, celle-ci dépendant fortement de l'inattention de l'utilisateur.

1er exemple : *WannaCry*, plus de 250 000 victimes dans le monde en mai 2017

WannaCry est un rançongiciel tirant profit d'une vulnérabilité de certains systèmes d'exploitation Windows, dévoilée par une entité connue sous le nom de *ShadowBrokers*, qui l'attribue à la NSA. L'outil malveillant a permis d'infecter des cibles telles que *Téléfonica* en Espagne, le *National Health Service* au Royaume-Uni ou encore certaines usines de Renault en France. L'impossibilité d'accéder aux postes touchés a obligé l'arrêt de la production au sein de certaines entreprises, impliquant des pertes financières non négligeables.

2ème exemple : *Locky*, plus d'un million de victimes en 2016

Découvert pour la première fois en février 2016, *Locky* a touché des cibles dans la plupart des pays. Une pièce jointe malveillante prenant la forme d'une facture reste le principal mode de propagation de ce rançongiciel. L'utilisateur ayant ouvert le fichier Word et activé les macros voit l'intégralité de ses fichiers chiffrés. Une fenêtre *pop-up* explique le fonctionnement et guide l'utilisateur jusqu'au paiement de la rançon, allant de 200 à 1000€. *Locky* a connu plusieurs versions. Il serait l'œuvre d'un groupe ayant déjà conçu un rançongiciel du nom de *Dridex* en 2015.

Préconisations de la DGSI

La DGSI recommande quelques actions visant à se prémunir au mieux des risques inhérents aux rançongiciels :

En amont de l'infection :

- Sensibiliser son personnel : l'infection s'effectue souvent par une pièce jointe frauduleuse reçue par courriel électronique sous une forme légitime (facture, bon de livraison, etc.). L'ouverture d'une seule de ces pièces jointes peut suffire à propager l'infection sur l'ensemble des systèmes d'information de l'entreprise. Il est donc essentiel de sensibiliser son personnel quant aux risques inhérents à l'ouverture des documents provenant d'émetteurs inconnus et/ou douteux ;
- Utiliser un outil de filtrage de courriers électroniques en plus d'une solution anti-virus efficace ;
- Effectuer fréquemment les mises à jour des systèmes d'exploitation et programmes ;
- Avoir une politique de sauvegarde de ses données afin de pouvoir les restaurer en cas de problème.

Pendant l'infection :

- Éviter de payer la rançon afin de limiter l'attrait de ces pratiques et de ne pas risquer une nouvelle attaque. Le paiement de la rançon ne garantit pas la récupération des données ou le déverrouillage des postes touchés ;

- Prendre les mesures nécessaires pour circonscrire l'infection sur les systèmes d'information placés sous votre responsabilité et, le cas échant, conserver les preuves relatives à l'attaque ;

- Informer le correspondant de la DGSI ;

- Consulter le site CERT-FR afin de vérifier l'existence d'un bulletin d'alerte, d'une campagne en cours ou de moyens de remédiation contre le rançongiciel qui vous a ciblé.

Après l'infection :

- Déposer plainte auprès des services de police (OCLTIC ou BEFTI) ou de gendarmerie compétents ;

- Effectuer un retour d'expérience sur la gestion de la crise afin de limiter les impacts d'une éventuelle future cyberattaque ;

- Evaluer les solutions de cybersécurité disponibles dans l'hypothèse où l'entreprise ne dispose pas au moment de l'incident des outils d'entrave nécessaires;

- Restaurer le système à l'aide de sauvegardes ou à défaut reformater le disque.

Nota : Il est parfois utile de conserver les supports de stockage infectés, des chercheurs en cybersécurité mettant régulièrement en ligne quelques jours plus tard des méthodes ou des outils de déchiffrement.