INGERENCE ECONOMIQUE

Flash n° 62 – Avril 2020

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°62 avril 2020

Les risques cyber liés aux rançongiciels dans le cadre de l'épidémie du COVID-19

Depuis le début de l'épidémie de Covid-19, une recrudescence des cyberattaques à l'encontre des entreprises et organismes publics a été relevée en France et dans le monde. Les cybercriminels profitent particulièrement de l'inquiétude liée à la propagation du virus pour envoyer de faux courriels d'alerte piégés contenant des 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. La DGSI estime aujourd'hui qu'il s'agit de la menace informatique la plus sérieuse pour les entreprises et les institutions. 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.

PREMIER EXEMPLE

Au Japon, plusieurs préfectures ont reçu des courriels malveillants incluant en pièces jointes de la documentation officielle autour de l'épidémie du Covid-19. Les courriels prétendaient indiquer la localisation de la propagation du virus dans plusieurs villes japonaises, encourageant la victime à ouvrir le document. A l'ouverture, la pièce-jointe démarrait alors l'installation d'Emotet, cheval de Troie principalement utilisé pour la diffusion de rançongiciels ou d'autres campagnes malveillantes. Emotet permet en effet de faire rentrer d'autres logiciels espions sur l'ordinateur.

Outre cette campagne au Japon, des chercheurs en cybersécurité font état d'une campagne de *phishing* aux Etats-Unis où les pirates se font passer pour le *Center for Disease Control and Prevention* (CDC), l'agence fédérale américaine chargée de la prévention des épidémies et de la gestion des crises sanitaires.

DEUXIEME EXEMPLE

Un laboratoire médical anglais chargé de tester d'éventuels vaccins contre le coronavirus a été victime d'un rançongiciel. Une fois identifiée, l'attaque a pu être stoppée rapidement sans avoir à verser de rançon.
Profitant de la surcharge d'activité liée à l'épidémie de Covid-19 et de la baisse de vigilance d'utilisateurs amenés à travailler dans l'urgence et souvent à distance, certains rançongiciels ciblent en particulier les organismes évoluant dans le secteur médical et hospitalier.

TROISIEME EXEMPLE

Une administration locale française a été victime d'une attaque par rançongiciel ayant entrainé le chiffrement des données personnelles de tous les agents de l'institution, de ses fournisseurs et de ses partenaires. Le rançongiciel a été activé par un code malveillant caché dans la pièce-jointe d'un courriel envoyé à un service de l'administration. En dépit des recommandations officielles, l'administration locale a choisi de payer la rançon, et a reçu en retour une clé de déchiffrement qui s'est avérée inefficace.

Commentaires

Les courriels proposant des liens ou des pièces jointes doivent provenir de **sources** connues et identifiées. Une vigilance accrue doit être accordée aux **messages alarmants** dans le cadre de la pandémie de Covid-19.
L'**inquiétude** liée à la pandémie et la **modification de l'environnement de travail** des employés peuvent occasionner un relâchement de l'attention qui constitue l'un des principaux facteurs de réussite des cyberattaques.

PRECONISATIONS DE LA DGSI

En amont de l'attaque par rançongiciel :

→ Sensibiliser son personnel et lui rappeler les gestes de cyber-hygiène : l'infection s'effectue souvent par une pièce jointe frauduleuse reçue par courriel 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, mettre en place une politique de sauvegarde des données afin de pouvoir les restaurer en cas de problème et les tester de manière régulière ;

→ L'Agence nationale de la sécurité des systèmes d'information (ANSSI) publie régulièrement des recommandations qu'il convient de consulter et d'appliquer, disponibles sur le site web de l'agence : www.ssi.gouv.fr.

Lors de la découverte du rançongiciel :

→ Ne pas 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 la découverte du rançongiciel :

→ 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 disposerait 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.