GROUPEMENT DE GENDARMERIE DEPARTEMENTALE DE LA GIRONDE

ALERTE AUX RANSOMWARE

La cellule des enquêteurs nouvelles technologies (Ntech) du Groupement de Gendarmerie de la Gironde vous alerte sur une recrudescence des attaques informatiques de type « RANSOMWARE » auprès des entreprises de la Gironde, tous secteurs d'activités confondus. Les informations ci-dessous visent à attirer votre attention sur le phénomène et à vous guider dans une démarche de prévention.

Définition : Un « ransomware » est un logiciel malveillant qui infecte les ordinateurs et les serveurs des entreprises afin de chiffrer (*dans le sens de crypter*) l'ensemble des données du système attaqué.

Vulnérabilité : Sa propagation se fait généralement au travers des pièces jointes transmises par émail ou des clés USB polluées. Une variante plus furtive (dénommée CRYSIS) à récemment fait son apparition et infecte directement le serveur de l'entreprise par le réseau, sans recours à une quelconque intervention humaine.

Menace : Une fois que le « malware » a chiffré les données vitales au bon fonctionnement de l'entreprise, une rançon par Bitcoin est demandée afin d'obtenir la clé numérique nécessaire au déchiffrage.

Risque : Les impacts sont multiples, (*financier, réglementaire, ...*) et peuvent mettre l'entreprise ciblée en difficulté, voire la conduire au dépôt de bilan. Aucune entité publique ou privée n'est encore en mesure de parer le déchiffrage des données.

Préconisations techniques et organisationnelles : Si le risque zéro n'existe pas, il n'en demeure pas moins que quelques préconisations peuvent être adoptées, sans délai, pour déjouer ou réduire les risques encourus. Ces conseils sont à mettre en œuvre selon le degré de vos exigences en sécurité évaluées aux regards de la sensibilité de votre patrimoine informationnel:

- Déployer une solution antivirale de nouvelle génération dite « Endpoint » (*analyse comportementale des postes, détection du trafic et flux réseau - parefeu -, gestion centralisée avec contrôle des composants et déploiements correctifs, filtrage émail,...*). Augmenter la fréquence de mise à jour de cette solution avec récupération de la base virale le plus fréquemment possible (*ex 10 minutes*).

- Mettre en place un serveur émail (SMTP) avec solution anti-spam.

- Recourir à des logiciels « anti-malware » et procéder à leur utilisation régulièrement. Disposer sur les postes informatiques des logiciels de la famille « Sandbox » qui permettent de procéder à des inspections des exécutables (*bac à sable qui permet de tester les exécutables en milieu fermé et sécurisé avant de les déployer sur votre système d'information)*

- Mettre en œuvre un plan de sauvegarde et de restauration efficace. La sauvegarde doit être effectuée selon vos exigences quant à la Durée Maximale d'Interruption d'Activité -DMIA- et doit être externalisée. Elle ne doit être en aucun cas sur le réseau mais ranger en lieu sûr et hors connexion. Il convient de la tester régulièrement pour s'assurer qu'elle pourra être utilisée en cas de sinistre.

- Mettre en place de Plan de Reprise d'Activité (PRA) ou Plan de Continuité d'Activité (PCA).

- Sensibiliser et former les collaborateurs sur le phénomène (*pas d'ouverture des pièces jointes aux extensions exotiques et /ou aux destinataires inconnus, bonne utilisation des logiciels de sécurité fournis et surtout savoir qui alerter immédiatement en cas d'infection ou de suspicion d'infection*)

- Mettre en œuvre des contrôles *(audits internes, campagnes d'ingénierie sociales*)

- La variante CRYSIS infecte directement le serveur de l'entreprise par le port 3389 (*Remote Desktop Protocol*) qui permet initialement aux collaborateurs de l'entreprise d'avoir accès au serveur depuis l'extérieur. Il convient de contrôler ou de fermer ce port (*solution Parefeu et/ou antivirus Endpoint paramétré*) et adopter un VPN pour les collaborateurs.

<u>En cas d'infection :</u>

Le temps de réaction est primordial pour préserver les fonctions vitales du logiciel.

- Identifier et isoler immédiatement du réseau le ou les PC infectés. Isoler la sauvegarde et tester sa virginité à l'aide d'un ordinateur sain et des solutions antivirales efficaces.

- Procéder à un audit technique et complet de tout le système d'information avec recherche des signatures de « malwares » à l'aide des logiciels dédiés sur tous les postes informatiques.

- Alerter la gendarmerie ou la police après avoir préservé les preuves numériques (*entête d'émail du pirate, identification du wallet pour le paiement de la rançon, estimation impact et préjudice subi*)

- En cas d'infection avec une variante « Ransomware » d'ancienne génération, tester l'outil gratuit suivant : https://noransom.kaspersky.com

- Réinstaller le système d'information à l'aide de la dernière sauvegarde saine.