Attaques de ransomware : ce que DarkSide révèle

Groupe de cybercriminels qui crée des ransomwares, DarkSide s'est organisé professionnellement pour lancer des attaques à grande échelle sur de nombreuses organisations, dans le but de gagner de l'argent en demandant une rançon aux entreprises victimes de leurs attaques.

Si ce type d'attaque n'a rien de nouveau, le récent piratage de la société Colonial Pipeline, aux États-Unis, est un rappel brutal que tout excès de confiance a un prix, des enseignements sont à tirer.

Les cyberattaques de DarkSide ont généralement pour effet de crypter les données d'organisations ou de leur en voler, puis de les supprimer des différents devices ou de leur système. Une fois l'attaque réussie, DarkSide demande une rançon à ses victimes en échange du décryptage des données ou de la restitution des données supprimées.

Les cyberattaques sont fréquentes en raison des lacunes présentes dans les mécanismes de défense de cybersécurité des organisations, d'un niveau accru de sophistication des outils et des méthodes utilisées par les acteurs malveillants, ou bien d'une combinaison de ces deux facteurs.

En raison du dynamisme dont les organisations font preuve dans leur déploiement de la technologie, et parce que les politiques et contrôles de sécurité ne suivent pas le rythme de ces évolutions, les organisations finissent par avoir des surfaces d'attaque exposées aux cyberattaques.

Se préparer aux attaques par ransomware

Devenues plus fréquentes ces deux dernières années, les attaques par ransomware peuvent être évitées ; il est aujourd'hui essentiel que les entreprises renforcent leur protection et celle de leurs réseaux.

Bien qu'il soit inévitable pour une entreprise de contrôler chaque aspect des systèmes informatiques, une sauvegarde régulière de tous les fichiers importants permettrait de ne pas perdre des données précieuses en cas d'incident. Il convient de noter que DarkSide a les capacités de crypter ou supprimer également les données sauvegardées. Les entreprises doivent donc envisager d'améliorer la sécurité des systèmes de sauvegarde concernés.

Les attaques de phishing permettent de prendre le contrôle des courriers électroniques. L'objet de l'e-mail ainsi que son contenu peuvent donner des informations sur l'expéditeur du courriel. Une formation à la sécurité dispensée aux employés peut contribuer à limiter les incidents de sécurité. En outre, le filtrage des e-mails peut aider à identifier les menaces avant qu'elles n'atteignent les employés.

Même s'il peut être pertinent d'utiliser le meilleur produit de sa catégorie pour garantir la sécurité du système global, il est judicieux d'utiliser les bons produits à chaque niveau pour détecter les menaces au cas où l'un des produits échouerait.

Une étude récente a conclu que l'utilisation de plusieurs produits, et donc une certaine diversification de la protection, facilite la sécurité de l'entreprise par rapport à l'utilisation d'un seul type de produit. La classification du réseau en couches peut aider à organiser la réponse de sécurité de manière appropriée et à réduire la surface d'attaque.

L'entreprise doit mettre en place une politique de mot de passe et un zonage interne des fichiers destiné à empêcher l'accès des personnes aux fichiers et dossiers non désirés. Le principe est d'utiliser la détection des mouvements latéraux pour le trafic est-ouest.

D'un point de vue plus technique, il est indispensable de renforcer la sécurité du contrôleur de domaine :

– Créer des répliques du contrôleur de domaine, autoriser les utilisateurs à accéder uniquement aux répliques.
– Appliquer les politiques de pare-feu pour le contrôleur de domaine
– Déploiement de l'EDR sur le contrôleur de domaine
– Appliquer la détection des mouvements latéraux pour le trafic entrant et sortant du contrôleur de domaine.

Pour qu'une entreprise optimise sa protection contre la prise de contrôle, il faut qu'elle bloque l'accès aux Anonymiseurs, Proxies TOR mais aussi qu'elle permette aux IPS de détecter et bloquer d'autres types de C&C. La sécurité des partages de fichiers doit aussi être renforcée et des politiques de pare-feu pour ces partages doivent être mises en place.

Il serait judicieux d'appliquer des correctifs aux applications lorsque des mises à jour de sécurité sont disponibles. En effet, les applications peuvent introduire des failles de sécurité et constituer un problème pour les organisations.