Rançongiciel 3.0 : le scénario de cyberattaque le plus redouté des RSSI

La majorité des responsables des systèmes d'information se rejoignent pour admettre que le rançongiciel est le pire scénario de cyberattaque qui puisse affecter leur organisation. Certains RSSI préfèrent même encore être victime d'une fuite de données confidentielles à celle du rançongiciel. Lors des récentes attaques ciblant le secteur public, le attaques par rançongiciel ont démontré à quel point elles pouvaient être lucratives pour les cybercriminels et avoir des effets dévastateurs sur toute organisation. Elles peuvent en effet, anéantir les systèmes opérationnels de base, coûter des millions de dollars pour permettre à l'entreprise de se rétablir ou entraîner une baisse des cours et des pertes d'emploi. Alors comment faire pour éviter ce type d'incident dévastateur ?

Naissance du rançongiciel à l'ère des crypto-monnaies

Les tout premier rançongiciel sont apparus avec l'arrivée des crypto-monnaie, ils permettaient aux cybercriminels de monnayer anonymement leurs cyberattaques. Dans un premier temps, les logiciels malveillants étaient distribués en masse par des emails exigeants un paiement de la part de la machine qu'ils infectaient. Ce type d'attaque a atteint son apogée lorsqu'en mai 2017, WannaCry a utilisé un mécanisme d'attaque automatisé pour infecter des centaines de milliers de machines.

Cette cyberattaque mondiale avait contribué à semer la panique dans le secteur de la sécurité et a fini par affecter à un niveau critique des infrastructures du monde entier ainsi que des établissements de santé. Cette frappe d'une ampleur sans précédent démontre à quel point une attaque par rançongiciel a pu créer des opportunités d'extorsion massive de fonds auprès d'organisations à la fois publiques et privées.

Aujourd'hui, les attaques par rançongiciels favorisent ce qu'on appelle la pêche aux gros poissons. Il s'agit en réalité du rançongiciel 2.0, une attaque plus ciblée et plus méthodique. En effet, les criminels compromettent un point d'entrée individuel (soit par l'email, soit par le protocole de bureau à distance, soit par un dispositif vulnérable tourné vers l'Internet comme un VPN), et pénètrent dans le réseau.

Au fil du temps, les cybercriminels ont su augmenter leurs privilèges d'accès, avec notamment l'identification de données sensibles, l'exfiltration d'informations, ou encore la contamination des systèmes de sauvegardes.

Lorsque le logiciel malveillant implose, la victime a peu de recours. L'option de ne pas payer est difficilement envisageable car les sauvegardes sont compromises et, même si la victime se rétablit par ses propres moyens, l'attaquant détient toujours le pouvoir de divulguer les données sensibles dérobées au préalable. C'est bien face à cette situation critique et peu réjouissante que les RSSI du monde entier craignent le plus d'être confrontés.

L’émergence du rançongiciel 3.0 : une menace pour les infrastructures cloud

Depuis quelques années, la gestion des données est devenue un enjeu stratégique pour les entreprises. Avec la migration vers le cloud qui s’est accélérée, en partie sous l’impulsion de la pandémie de COVID 19, les entreprises dépendent davantage des systèmes et du stockage de données de tiers. Une dépendance qui n’est pas sans risque.

En effet, les RSSI doivent plus que jamais s’attendre cette année à ce que les rançongiciels ciblent plus agressivement l’infrastructure du cloud. Les cybercriminels peuvent l’exploiter comme une passerelle d’accès aux identités de l’entreprise ou alors en attaquant directement les données de l’entreprises stockées sur le cloud.

Aujourd’hui, le rançongiciel 3.0 représente une nouvelle forme de menace, avec la possibilité d’étendre les répercussions et de créer un flux de revenus à plus long terme à la faveur de l’attaquant. Les rançongiciels augmentent ainsi en sophistication dans la mesure où les cyberattaquants peuvent également s’en prendre à l’intégrité des personnes. En effet, avec l’expérience qu’ils détiennent, il est devenu très facile pour les attaquants de s’emparer de certaines données confidentielles.

Aujourd’hui, force est de reconnaitre que les cybercriminels disposent d’un levier de menace supplémentaire qui peut être activé de deux manières. Soit l’entreprise refuse de payer la rançon, et souhaite récupérer ses données sans « l’aide » de l’attaquant, elle peut être alors informée de divergences importantes dans les données clés qui pourraient compromettre son activité.

Ou alors, si l’attaquant a pu infiltrer les sauvegardes, l’entreprise ne pourra pas se fier à ses systèmes de sauvegarde et devra très certainement payer pour être informée des erreurs de données introduites. Si l’entreprise paie la rançon et récupère ses données, l’attaquant peut revenir à la charge et exiger une nouvelle rançon pour faciliter la résolution.

Une entreprise confrontée à une simple fuite de données peut se rétablir, il est de même pour une entreprise confrontée à une panne de service temporaire. Cependant, une fois les modèles économiques d’organisations fragilisés par des cyberattaques, il devient difficile d’établir un rapport de confiance avec les clients.

C’est pourquoi, un préjudice de réputation d’une grande ampleur causé par ce genre de menace est tout simplement irréversible. Le climat de confiance reste une condition sine qua non pour le succès commercial qu’une organisation peut espérer avoir vis-à-vis de ses utilisateurs finaux.

Face à une menace redoutable : une prise de conscience et des actes

Parmi les actes de cybercriminalité recensés, les rançongiciels représentent aujourd’hui la menace la plus sérieuse. Ils augmentent en nombre, en fréquence et peuvent être lourds de conséquences sur la continuité d’activité voire la survie de l’entité victime.

Pour lutter contre ces nouvelles formes de cybercriminalité, il est crucial que les professionnels de la sécurité œuvrent main dans la main avec les acteurs publics afin de prévenir, sensibiliser et renforcer les différentes parties prenantes des organisations.

En effet, le rançongiciel est une menace qui peut littéralement mettre des organisations puissantes devant le fait accompli avec à la clé des pertes de revenus considérables. Il est donc plus que jamais essentiel que les RSSI prennent toutes les mesures nécessaires pouvant permettre d'éviter une telle attaque.

– Protégez les passerelles évidentes – Laisser les passerelles VPN non corrigées est une véritable brèche pour les cyberattaquants ; il en va de même pour les connexions RDP ou toute passerelle tournée vers Internet. Il est important de s'assurer que les correctifs et le contrôle du périmètre sont complets et surveillés quotidiennement.

– Concentrer les contrôles sur les principaux facteurs d'attaque, qui sont en réalité les courriels et les personnes – Pour prévenir les attaques de logiciels malveillants, il est fortement recommandé de s'assurer d'avoir une bonne hygiène des courriels, et cela passe aussi par de la formation et de la sensibilisation aux bonnes pratiques de sécurité informatique, car la grande majorité des cyberattaques visent en priorité les personnes.

– Détecter et prévenir la violation des informations d'identification – Le vol et l'utilisation abusive des informations d'identification sont des points de départ universels pour les attaquants. À partir de là, ils peuvent lancer des attaques de type « Business Email Compromise » (BEC) et « Email Account Compromise » (EAC), mais aussi voler des données, altérer des documents et installer des rançongiciels. La dégradation des justificatifs d'identité est le premier signe d'une attaque à l'encontre d'une organisation ; il est donc crucial d'apporter une attention particulière à ce vecteur d'attaque.

– Rétablir les sauvegardes hors ligne – L'attrait des sauvegardes instantanées et en ligne a conduit de nombreuses entreprises à supprimer les versions hors ligne, ce qui signifie que les attaquants disposant d'informations d'identification volées peuvent être en mesure d'altérer ou d'empoisonner les systèmes de sauvegarde. D'où l'importance d'envisager des alternatives hors ligne.

– Investir dans un logiciel d'analyse de sauvegarde – Les grandes entreprises technologiques traitent désormais des analyses sur les mouvements de données, ce qui leur permet d'identifier les changements subtils des données au fil du temps. Cela peut passer inaperçu lors d'une attaque, mais cela est primordial pour identifier un chemin de retour vers une intégrité totale des données.

Face à l'émergence des attaques de l'infrastructure du cloud, il est important de noter que la sécurité des systèmes critiques peut nécessiter d'investir dans une infrastructure informatique entièrement parallèle, mais déconnectée, qui fournit une sauvegarde en cas de défaillance du système principal.

Cette solution n'est pas bon marché, mais elle peut constituer une barrière ultime pour assurer la continuité du service en cas d'attaque. Anticiper les attaques par rançongiciel et en faire une priorité semblent constituer la meilleure stratégie que les organisations peuvent envisager si elles souhaitent à minima limiter les dégâts économiques, de confiance et humains.