Le ransomware : plus spécialisé et plus virulent en 2020

Le ransomware (rançongiciel) est aujourd'hui un business florissant puisqu'il génère environ 1 milliard de dollars de revenus annuels pour les acteurs malveillants. Les victimes de ransomware sont de plus en plus nombreuses à mesure que les criminels développent de nouveaux moyens d'infiltrer les environnements informatiques, de voler les données et de forcer les entreprises à payer les rançons.

Secteur public, prestataires de santé et industriels : cibles privilégiées des pirates

Le ransomware n'a pas encore atteint son apogée. Cependant, il va se spécialiser et cibler des secteurs spécifiques au cours de l'année à venir.

Jusqu'à récemment, les pirates avaient une approche plutôt diffuse. Les attaques Ryuk et WannaCry en 2017 sont typiques d'une approche basée sur de grands volumes d'attaques ciblant de nombreuses victimes pour accroître les chances de résultat. A partir de maintenant, les pirates vont devenir plus sélectifs et se concentrer sur les secteurs qui peuvent leur apporter le meilleur retour sur investissement.

Les secteurs publics, de la santé et industriels, deviennent des cibles privilégiées pour les pirates. S'ils sont particulièrement visés c'est parce qu'ils s'appuient sur des données critiques et essentielles au bon déroulé de leurs opérations quotidiennes. Les cybercriminels savent bien que si les attaques perturbent les services critiques, les organisations auront moins de temps pour prendre une décision et seront plus disposées à payer la rançon. Plus les enjeux sont importants, plus les chances qu'une victime paye sont grandes.

À mesure que les pirates deviennent plus sélectifs en termes de cibles, les acteurs de la santé, de l'industrie et du secteur public doivent prendre conscience que les menaces auxquelles ils font face vont s'accentuer et se renforcer. Pour assurer une bonne préparation, il est primordial d'améliorer sa propre visibilité des données et de s'engager vers une meilleure automatisation des processus : le but étant de garantir la sauvegarde et la récupération rapides de données souvent réparties sur un nombre croissant d'emplacements et d'environnements informatiques différents.

Le ransomware à l'attaque de la propriété intellectuelle

Que font les entreprises prospères une fois qu'elles se sont établies sur un marché ? Elles se diversifient. Il en va de même pour le ransomware. Alors que les entreprises recherchent aujourd'hui de nouvelles sources de revenus, les pirates cherchent, de leur côté, à augmenter leurs gains grâce à de nouvelles techniques d'exfiltration de données.

De nouvelles variantes de ransomware, mêlant verrouillage de données standard et capacités d'exfiltration, vont voir le jour en 2020. Ce type d'attaque visera notamment les données les plus lucratives - celles relatives à la propriété intellectuelle. Là où l'objectif consistait à contourner les défenses et à obtenir le plus de données possibles, il s'agira bientôt de récupérer les informations critiques telles que des prototypes de produits, schémas ou encore des modèles de conception.

Si une attaque par ransomware peut empêcher une entreprise d'accéder aux prototypes d'une nouvelle voiture ou d'un nouveau téléphone, elle permet également de récupérer ces informations pour les revendre aux concurrents sur le marché noir. Les entreprises doivent rester agiles pour conserver leur avance sur leurs concurrents. Si elles ne peuvent plus accéder à leurs données critiques, comme celles relatives à la propriété industrielle, alors c'est toute la chaine de développement produits et l'avancée d'autres projets essentiels qui seront considérablement entravées. Les pirates vont donc adapter leur ransomware afin d'obtenir spécifiquement ce type d'information. C'est pourquoi il est si important pour les entreprises de disposer de mesures appropriées pour la protection de leurs données les plus sensibles.

Les méthodes d'attaque utilisant l'ingénierie sociale évolueront pour cibler la supply chain dans son ensemble

Au regard de son efficacité, les cybercriminels ont longtemps utilisé l'ingénierie sociale comme l'une de leur méthode d'attaque privilégiée. En incitant les employés à partager des informations ou à télécharger des programmes malveillants, les pirates récupèrent les identifiants leur permettant d'accéder aux ressources clés de l'entreprise. Cependant, avec l'évolution et le renforcement des politiques de sécurité d'entreprise, leurs techniques seront elles aussi amenées à évoluer.

Un marché parallèle illégal des identifiants volés commence à apparaître. Sur le dark web, les ransomwares alimentent un marché en plein essor qui permet aux cybercriminels d'avoir accès plus rapidement et plus facilement aux systèmes des entreprises. Cette expansion est soutenue par des stratégies d'attaque variables qui vont encore se développer en 2020. Les cybercriminels concentreront de plus en plus leurs efforts non pas sur les employés en interne, mais sur des cibles tierces et d'autres comptes leur permettant d'avoir accès au système de l'entité ciblée. Cela inclut notamment les sous-traitants, les freelances, les partenaires ou encore les vendeurs agréés.

En réponse aux attaques indirectes (sur les cibles tierces), les équipes de cybersécurité pourraient avoir un rôle plus important dans les processus d'achat afin de garantir l'intégrité d'un fournisseur. Avant d'intégrer un nouveau fournisseur, l'entreprise doit s'assurer que ce dernier dispose et applique des mesures de protection comparables aux siennes. Assez rapidement, la responsabilité autour des données ne concernera plus seulement les acteurs en interne mais sera liée à la façon dont les organisations voudront mener leurs business et choisiront leurs partenaires.

Toujours avoir un plan de sauvegarde

Pour se défendre en 2020, il sera essentiel d'adopter une démarche proactive en matière de prévention contre les ransomwares reposant notamment sur des politiques et systèmes de protection de données répartis sur plusieurs niveaux. Cela doit inclure des solutions résistantes aux attaques par ransomware et offrant une protection améliorée des données critiques. Il sera nécessaire d'y associer un programme de formation à la protection des données destiné aux employés de tous niveaux. Toute faille qui pourrait exister dans le système de défense pourra être utilisée par les cybercriminels. Une protection complète est donc indispensable.

Une protection à long terme doit également s'appuyer sur une bonne stratégie de sauvegarde. Aucune stratégie de défense n'est parfaite et la question n'est plus de savoir si une attaque va se produire mais bien quand ? Les entreprises doivent créer des copies de sauvegarde de leurs données et les stocker offline afin de les préserver. Il est également nécessaire d'établir une surveillance proactive et de limiter l'accès aux sauvegardes, tout en en effectuant régulièrement afin de limiter la perte d'éventuelles données.

Enfin, les entreprises doivent mettre leur système de défense contre le ransomware à l'épreuve en les testant régulièrement. Ces logiciels et autres méthodes d'attaques sont destinés à évoluer au

cours des prochaines années et les tests de résistance seront essentiels pour garantir une stratégie de sauvegarde solide et efficace.