Encryption-less Ransomware: A New Era of Cyber Threats and How CISOs Can Defend Their Organizations - ITsMine Beyond DLP

Rançongiciels sans chiffrement : une nouvelle ère de cybermenaces et comment les RSSI peuvent défendre leurs organisations

En ce qui concerne les cyberattaques, la sagesse dominante veut que la menace #1 dont les RSSI doivent être conscients est le ransomware. Bien que cela soit toujours vrai, c'est la *nature* des ransomwares qui a changé, sous l'impulsion d'une nouvelle génération de ransomwares, et il est impératif pour les RSSI de comprendre cette nouvelle menace.
L'essor des rançongiciels sans chiffrement signifie que les outils et tactiques traditionnels utilisés pour défendre les organisations ne sont plus pertinents dans une large mesure.

Une attaque par rançongiciel sans chiffrement se produit lorsque les attaquants n'essaient pas de chiffrer les données. Ils exigeront une rançon pour ne pas publier les informations volées.

La double extorsion se produit lorsque les attaquants volent les fichiers *et* cryptent les fichiers dans le stockage de fichiers de l'entreprise, mais les fichiers qu'il prennent ne sont pas cryptés.
Les entreprises *peuvent* effectuer une restauration à partir d'un cloud de sauvegarde pour surmonter l'élément de chiffrement, mais ne peuvent rien faire pour les données qui se trouvent actuellement chez les attaquants.

Par exemple, si des attaquants volent les données sensibles d'une entreprise et menacent de les publier sur le dark web, il n'est pas pertinent de disposer d'une sauvegarde de ces données.

Cette forme de ransomware sans chiffrement représente un passage des attaques traditionnelles, où la principale menace était le chiffrement des données, à un scénario où les informations sensibles sont exfiltrées et détenues contre rançon. Ce changement nécessite une réévaluation des stratégies de défense pour protéger efficacement les données de l'organisation.

Nous aidons les RSSI à s'assurer que :

1. Ils sont préparés à ces attaques
2. Ils ont cela dans leur stratégie et le testeront comme ils le font pour les solutions de sauvegarde et de restauration

Tout d'abord, commençons par une compréhension plus approfondie du problème :

Le problème

1. L'essor des rançongiciels sans chiffrement

Le piratage du logiciel MOVEit Transfer, révélé par Progress en mai 2023, est rapidement devenu l'événement de cybersécurité le plus important de l'année dernière, marquant un exemple notable de ransomware sans chiffrement. Contrairement aux attaques de ransomware traditionnelles qui cryptent les données de la victime pour demander une rançon, cet incident impliquait le ransomware **Clop** et le gang d'extorsion qui ont volé des données sensibles sur les serveurs de MOVEit Transfer. Les attaquants ont ensuite menacé de publier les données volées s'ils ne recevaient pas de paiement, en utilisant la menace d'exposition comme principale arme d'extorsion.

Les chiffres de cette attaque mettent en évidence le danger auquel sont confrontés les RSSI modernes :

- **Plus de 1 000 victimes connues** de la violation de MOVEit, ce qui en fait l'un des plus grands piratages de l'histoire récente.
- **Plus de 60 millions de personnes ont été touchées**, un nombre qui continue d'augmenter à mesure que de plus en plus d'organisations confirment des violations de données connexes.
- **83,9 % des entreprises victimes connues sont basées aux États-Unis**, l'Allemagne, le Canada et le Royaume-Uni étant également très touchés.
- **Maximus**, un sous-traitant de services gouvernementaux américains, est devenu la plus grande victime connue, avec jusqu'à 11 millions d'informations sensibles consultées.
- **Le coût total estimé** des piratages de masse de MOVEit jusqu'à présent est d'environ 9,92 milliards de dollars, avec un potentiel d'au moins 65 milliards de dollars.
- **Prime de 10 millions de dollars** offerte par le département d'État américain pour des informations sur le groupe de rançongiciels **Clop**.
- **Clop pourrait gagner jusqu'à 100 millions de dollars** grâce à la campagne de piratage de masse MOVEit, mettant en évidence la nature lucrative des ransomwares et de l'extorsion de données.

Un incident similaire est arrivé à Deloitte. L'entreprise mondiale de services professionnels a connu un incident de cybersécurité important où, contrairement aux attaques de ransomware traditionnelles qui chiffrent les données, cette attaque impliquait l'accès non autorisé et le vol de données sensibles à partir de la plateforme de messagerie de Deloitte. Les attaquants ont ensuite menacé de libérer les données volées à moins qu'une rançon ne soit payée, incarnant les caractéristiques d'une attaque par ransomware sans chiffrement.

Cet incident n'a pas suivi le modèle de ransomware le plus courant consistant à chiffrer les données des victimes et à exiger le paiement des clés de déchiffrement. Au lieu de cela, il a utilisé la menace de divulgation publique d'informations sensibles comme levier d'extorsion.

Ces dernières années, on a assisté à une **augmentation de 40 % des attaques sans chiffrement**, ce qui met en évidence un changement significatif dans les tactiques des cybercriminels. Ces attaquants ne s'appuient plus uniquement sur le chiffrement pour paralyser leurs victimes, mais menacent plutôt de divulguer des données sensibles à moins qu'une rançon ne soit payée. Cette forme d'attaque met non seulement les informations confidentielles en danger, mais expose également les organisations à des amendes réglementaires, à des atteintes à leur réputation et à la perte potentielle d'activité.

Les recherches de CrowdStrike montrent que **75 % des attaques étaient exemptes de logiciels malveillants**. Il y a également eu une augmentation de 76 % du nombre de victimes de vol de données nommées sur le dark web.

Ces statistiques montrent à quel point cette question est urgente et répandue.

De plus, les rançongiciels sans chiffrement posent un problème à multiples facettes qui va au-delà de la menace immédiate de l'exposition des données. On ne saurait trop insister sur l'impact psychologique sur les organisations, sachant que leurs données sensibles peuvent être exposées à tout moment. Cette forme de cyber-extorsion crée un état perpétuel d'insécurité et de peur, ce qui en fait une arme puissante dans l'arsenal des cybercriminels.

Les conséquences d'un ransomware sans chiffrement sont graves :

- **Atteinte à la réputation** : l'exposition publique de données sensibles peut gravement ternir la réputation d'une organisation, érodant la confiance des clients, des partenaires et du marché dans son ensemble. Le rétablissement de cette confiance peut prendre des années et nécessiter des investissements importants.
- **Sanctions réglementaires** : De nombreux secteurs sont soumis à des réglementations strictes en matière de protection des données. La divulgation non autorisée d'informations sensibles peut entraîner des amendes et des pénalités substantielles, ce qui aggrave encore l'impact financier d'une attaque.
- **Perturbation opérationnelle** : Le vol d'informations exclusives ou de données opérationnelles sensibles peut perturber les opérations de l'entreprise, entraînant une perte de revenus et donnant potentiellement un avantage indu aux concurrents.
- **Vulnérabilités stratégiques** : L'exposition de plans stratégiques, d'informations financières ou de propriété intellectuelle peut avoir des répercussions à long terme sur la position concurrentielle et la valeur marchande d'une organisation.

De plus, l'essor des rançongiciels sans chiffrement représente une évolution sophistiquée des stratégies cybercriminelles, exploitant la nature interconnectée des opérations commerciales modernes. Les cybercriminels sont de plus en plus conscients que les données ne sont pas seulement un actif numérique, mais aussi une pierre angulaire de la confiance, de l'intégrité opérationnelle et de l'avantage concurrentiel. La menace de publier des données volées dans le domaine public ou de les vendre au plus offrant sur les places de marché du dark web introduit un paysage de risques complexe que les mesures de cybersécurité traditionnelles ne sont pas en mesure de gérer.

L'ère des rançongiciels sans chiffrement appelle à un changement de paradigme dans la façon dont les entreprises abordent la cybersécurité. Il souligne l'inadéquation de s'appuyer uniquement sur des défenses périmétriques ou des stratégies traditionnelles de protection des données, qui peuvent être efficaces contre les ransomwares qui chiffrent les données, mais sont inefficaces contre les menaces qui exfiltrent les données.

2. Pourquoi les défenses traditionnelles ne suffisent plus

L'évolution vers des rançongiciels sans chiffrement a rendu les mesures de sécurité traditionnelles, telles que les sauvegardes et les systèmes de détection et de réponse aux points de terminaison (EDR), moins efficaces. Ces solutions sont conçues pour contrer les effets du chiffrement, mais elles offrent peu de protection contre le vol et l'extorsion de données sensibles.

Par exemple :

- **Exfiltration de données avant la détection :** les rançongiciels sans chiffrement fonctionnent en exfiltrant furtivement les données sensibles avant que toute demande ne soit faite. Au moment où la violation est détectée, les données peuvent déjà être entre les mains de cybercriminels, ce qui rend

les défenses préventives telles que les pare-feu et les antivirus insuffisantes en tant que solutions autonomes.

- **Inefficacité des sauvegardes :** Les sauvegardes sont essentielles pour récupérer des données cryptées sans payer de rançon. Cependant, dans le cas d'un ransomware sans chiffrement, la menace n'est pas l'impossibilité d'accéder aux données, mais plutôt la publication non autorisée de données volées. Les sauvegardes n'atténuent pas le risque d'exposition des données et les atteintes à la réputation qui en résultent, les pénalités réglementaires et les perturbations opérationnelles potentielles.
- **Limites de la détection et de la réponse aux points de terminaison (EDR) :** Les systèmes EDR sont conçus pour détecter et répondre aux activités malveillantes sur les terminaux. Bien qu'ils jouent un rôle crucial dans l'identification et l'atténuation des attaques par ransomware, leur efficacité est diminuée dans les scénarios où les données sont exfiltrées silencieusement. En l'absence d'indicateurs clairs de l'activité de chiffrement des rançongiciels, ces systèmes risquent de ne pas déclencher d'alertes ou de réponses à temps pour empêcher le vol de données.
- **Surveillance des menaces internes :** Les mesures de sécurité traditionnelles se concentrent souvent sur les menaces externes, négligeant le potentiel de menaces internes. Les rançongiciels sans chiffrement peuvent exploiter cette vulnérabilité, soit par collusion directe entre initiés, soit en manipulant les informations d'identification des initiés, en contournant de nombreuses mesures de sécurité conventionnelles qui ne parviennent pas à surveiller les activités internes inhabituelles.
- **Manque de protection et de contrôle lorsque les données résident chez des tiers :** Par exemple, Blackbaud, l'un des plus grands fournisseurs mondiaux de logiciels de collecte de fonds, de gestion financière et d'éducation, a subi une cyberattaque au cours de laquelle des cybercriminels ont réussi à accéder aux données des systèmes de Blackbaud et à les exfiltrer. Les données volées comprenaient des informations sensibles relatives aux donateurs, aux anciens élèves et aux autres parties prenantes des institutions qui comptent sur les services de Blackbaud. Cela a permis aux attaquants d'extorquer non seulement Blackbaud, mais aussi ses clients et partenaires en menaçant de divulguer les données volées à moins qu'une rançon ne soit payée. Une fois que les entreprises partagent des données, celles-ci leur échappent.

Quelle *devrait* être la solution ?

Pour contrer efficacement la menace nuancée et évolutive des ransomwares sans chiffrement, les entreprises doivent adopter une attitude de cybersécurité à la fois complète et flexible, capable de faire face non seulement au paysage actuel des menaces, mais aussi aux menaces futures. Cela doit inclure les fonctionnalités suivantes :

- **Surveillance proactive des données et détection des anomalies :** En tirant parti de l'apprentissage automatique et de l'IA, le système devrait détecter et alerter automatiquement sur les comportements anormaux qui s'écartent des modèles établis, indiquant un accès potentiel non autorisé aux données ou des tentatives d'exfiltration. Cela devrait inclure les personnes non autorisées qui accèdent à des données sensibles.
- **Rendre les données exfiltrées inutilisables :** En cas d'exfiltration de données sensibles, il devrait être possible de les rendre instantanément illisibles, neutralisant ainsi la menace posée par le vol de données.
- **Capacités d'investigation complètes :** En cas d'attaque sans chiffrement, les équipes de sécurité doivent être en mesure de savoir instantanément quelles données ont été affectées.
- **Capacité à protéger les données :** Les organisations devraient avoir la capacité de protéger spécifiquement les données sensibles, un « Fort Knox » virtuel.
- **Solution pour l'environnement collaboratif :** Les employés partageant des données sensibles avec des tiers, une solution gagnante devrait permettre aux organisations de garder le contrôle de leurs données même lorsqu'elles sont avec ce tiers, ce qui signifie que si le tiers est victime d'une violation, les données de l'organisation d'origine sont toujours en sécurité.
- **Éducation et autonomisation de la main-d'œuvre :** Une solution idéale devrait promouvoir une culture de sensibilisation à la sécurité par le biais d'une formation régulière et continue, y compris les meilleures pratiques en matière d'accès, de stockage et de partage des données.

Ce que ITsMine peut faire pour vous

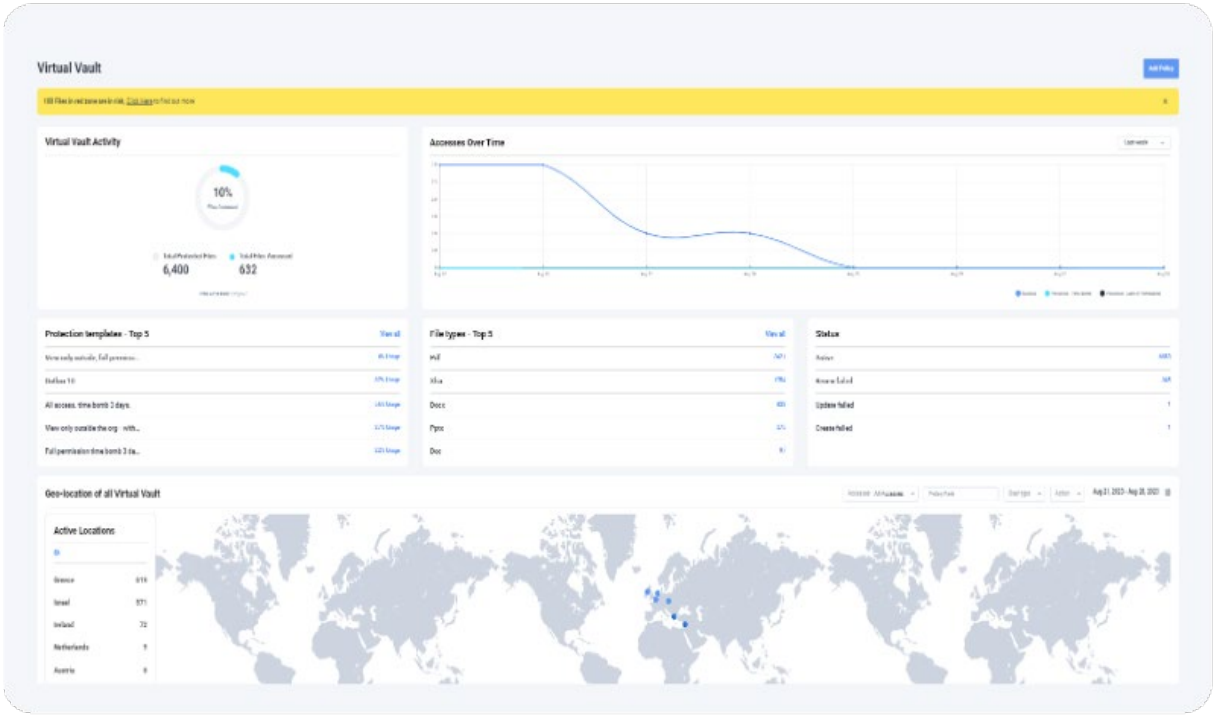
En réponse à cette menace en constante évolution, ITsMine a développé une solution complète conçue pour permettre aux RSSI et à leurs équipes de se défendre contre les attaques de ransomware sans chiffrement. Cette solution de protection des ransomwares sans chiffrement d'ITsMine offre aux RSSI :

- Des **alertes** lorsque les données ont été utilisées à l'extérieur de l'organisation
- La **liste des fichiers** que l'attaquant a pris (pour limiter l'exposition potentielle)
- La capacité de **rendre illisibles les données les plus importantes**, même si l'attaquant les conserve sur un système externe hors ligne
- La capacité de **présenter aux organismes de réglementation la preuve que des** données importantes n'ont pas été utilisées et ne peuvent pas être utilisées après qu'elles ont été détruites.

Pour ce faire, elle utilise les technologies innovantes suivantes :

ITsMine SoftwareMines™ : alerte immédiatement lorsqu'une violation de données se produit et fournit des informations judiciaires complètes sur l'événement d'exfiltration.

ITsMine Virtual Vault™ & File-GPS™ : offre la possibilité de rendre illisibles des fichiers même si l'attaquant les détient dans un environnement externe isolé.



Les coffres-forts virtuels d'ITsMine en action

En résumé, ITsMine offre une solution complète de protection des données et de réponse qui comprend :

- des **alertes** en cas d'utilisation externe non autorisée de données
- un **suivi de l'inventaire** des fichiers compromis pour minimiser l'exposition
- des **capacités d'assainissement** pour neutraliser les données critiques, même sur des systèmes externes hors ligne
- Des **outils d'assurance** pour prouver aux régulateurs que les données vitales n'ont pas été utilisées à mauvais escient et qu'elles sont hors de portée après l'incident

Un appel à l’action pour les RSSI

Alors que les ransomwares sans chiffrement deviennent une menace de plus en plus courante, les RSSI doivent adapter leurs stratégies de cybersécurité pour protéger leurs organisations. Il s’agit non seulement de déployer les bonnes technologies, telles que la solution complète d’ITsMine, mais aussi de sensibiliser à la nature changeante des attaques par ransomware.

Plus précisément, il devrait maintenant être clair que les RSSI doivent s’assurer qu’ils sont préparés à ces attaques sans chiffrement, et que leur stratégie comprend une réponse robuste, y compris des tests et des simulations, comme cela se fait pour d’autres menaces courantes.

En comprenant les nuances des ransomwares sans chiffrement et en mettant en œuvre des mécanismes de défense robustes, les RSSI peuvent protéger leurs organisations contre cette menace en constante évolution.

ITsMine offre une solution qui permet aux RSSI d’être alertés, de garder le contrôle et de se défendre contre ces attaques sophistiquées, garantissant ainsi la sécurité des informations sensibles.

ITsMine est représentée en France par AMC SOFT
https://amcsoft.fr contact@amcsoft.fr Tel : +33680741316