La prévention des rançongiciels et des logiciels malveillants commence par une bonne cyberhygiène

Andrew Kramer :

L'adage « mieux vaut prévenir que guérir » est particulièrement vrai en ce qui concerne les infections par logiciels malveillants et les attaques de rançongiciels, qui sont devenues l'une des cybermenaces les plus importantes auxquelles les individus et les organisations sont confrontés aujourd'hui.

Les attaques de ransomware ne sont pas un problème nouveau, mais elles gagnent en popularité et attirent l'attention des experts en cybersécurité en raison de leurs effets néfastes.
Selon un rapport de Verizon, les attaques de ransomware ont considérablement augmenté en 2022 et représentaient 25% des violations signalées.
En outre, un rapport Sophos 2022 a montré que les ransomwares ont touché 66 % des organisations en 2021, soit une augmentation de 66 % par rapport à l'année précédente. Notamment, ces statistiques sont seulement aussi bonnes que les données, et de nombreux compromis peuvent ne pas être signalés.

VirusTotal a publié un rapport indiquant que depuis 2020, plus de 130 souches de ransomware ont été détectées, y compris des variantes familières telles que Wannacry, TeslaCrypt, CryptoWall et autres.
Les cybercriminels utilisent diverses techniques pour lancer des attaques de ransomware, telles que les courriels de phishing, l'exploitation des vulnérabilités et l'ingénierie sociale avec succès.

Alors que le nombre de variantes et de compromis continue d'augmenter, les individus et les organisations doivent se tenir au courant des dernières tendances et tactiques en matière de ransomware, suivre de saines pratiques de cybersécurité et comprendre les bases des logiciels malveillants et des ransomwares.

Logiciels malveillants et rançongiciels 101

À un niveau élevé, les rançongiciels peuvent chiffrer des fichiers sur les systèmes d'un utilisateur ou d'une organisation et fournir les clés cryptographiques à un acteur de la menace.
Les auteurs de logiciels malveillants mettent souvent en œuvre des algorithmes de chiffrement robustes qui sont mathématiquement insolubles dans un délai réaliste.
En conséquence, une fois que les fichiers sont cryptés, ils sont rendus inaccessibles sans accès à la clé de déchiffrement, que l'attaquant détient contre rançon.

Les retombées des attaques de ransomware peuvent avoir des impacts durables, y compris la perte de propriété intellectuelle et des dommages financiers ou opérationnels pour les victimes.
En outre, ces attaques peuvent également entraîner des temps d'arrêt importants tout au long du processus de récupération, entraînant une perte de productivité, de revenus et de réputation.
Certaines attaques de rançongiciels ont même entraîné la publication d'informations sensibles, entraînant des conséquences juridiques et réglementaires supplémentaires. Bien que le coût du paiement d'une rançon soit facilement mesurable, ces autres dommages sont plus difficiles à comptabiliser, surtout si l'on considère les impacts à long terme.

Conseils de prévention des attaques

Pour prévenir les attaques de rançongiciels et de logiciels malveillants, le FBI recommande plusieurs bonnes pratiques.
Tout d'abord, les utilisateurs finaux doivent être très attentifs aux courriels, aux téléphones et autres tentatives de phishing.
Des pratiques exemplaires simples, telles que ne pas ouvrir les pièces jointes/liens dans les courriels non sollicités, peuvent contribuer grandement à atténuer les tentatives d'hameçonnage.
Il est tout aussi important de maintenir à jour tous les logiciels, systèmes d'exploitation, applications et solutions anti-malware.
Si un attaquant envoie un fichier malveillant à un point de terminaison, le taux de réussite d'une compromission supplémentaire diminue considérablement par rapport à un fichier qui n'exécute pas les dernières versions.

Des sauvegardes régulières hors site ou dans le cloud sont une stratégie efficace pour minimiser les impacts d'une infection par ransomware.
Les administrateurs système peuvent récupérer des fichiers et des données cruciaux avec des sauvegardes à jour et précises, bien que cela puisse prendre beaucoup de temps.
En outre, la planification d'urgence pour la continuité des activités et les tests réguliers des plans de reprise après sinistre peuvent être utiles pour estimer le coût de la récupération après une attaque de ransomware.
Cependant, les sauvegardes ne sont pas infaillibles, car certains attaquants ont recours à des approches multi-extorsion.
Dans ces scénarios, les attaquants menacent de divulguer des données sensibles sur l'individu ou l'organisation si la rançon n'est pas payée.

En plus de suivre les meilleures pratiques et la diligence raisonnable, le signalement de toute cyberattaque peut aider les forces de l'ordre à suivre et à perturber les réseaux criminels et à ralentir la propagation d'incidents similaires.

Les attaques de ransomware constituent une menace importante pour les individus et les organisations.
Les gains monétaires et intellectuels alimentent les criminels de cybersécurité dans leurs efforts, et le paysage des menaces continuera d'évoluer en conséquence.
Il est impératif de prendre des mesures proactives pour prévenir les attaques de ransomware, telles que maintenir les systèmes à jour, rechercher régulièrement les logiciels malveillants et sauvegarder les données.
En suivant ces meilleures pratiques, les individus et les organisations peuvent réduire considérablement leur risque d'être victimes d'attaques de ransomware.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231010
"C'est ensemble qu'on avance"