Confinement des rançongiciels

Présenté par BullWall Ransomcare (RC)

RICOH
imagine. change.
imaginer. changer.

Une solution automatisée pour arrêter une éclosion de rançongiciels au sein de votre entreprise

Les rançongiciels sont devenus des maliciels de niveau professionnel qui prennent des ordinateurs et les fichiers de données en otage, verrouillent rapidement des systèmes en entier et paralysent des entreprises pendant des jours, voire des mois. Dans le cas où un rançongiciel aurait déjà contourné vos solutions de sécurité existantes, ce dernier est maintenant « autorisé » à attaquer votre entreprise, causant autant de perturbations que possible en chiffrant le plus de fichiers qu'il le peut dans les plus courts délais. Ainsi, soit vous payerez le malfaiteur ou l'attaquant pour récupérer les fichiers, sans garantie qu'il vous les rendra, soit vous perdrez les données pour toujours.

RansomCare est une nouvelle technologie innovatrice qui détecte les attaques de rançongiciels à partir de l'installation du serveur central (sans agent) en examinant par euristique vos fichiers de données réels (p. ex., Word, Excel et PDF) stockés sur votre réseau et dans le nuage.

RansomCare détecte et arrête les attaques de rançongiciels, même s'ils ont contourné tous les dispositifs de protection de vos terminaux et les autres outils de prévention ou de sécurité comportementale existants. Il est un élément essentiel de votre stratégie de défense globale, fournissant des défenses de sécurité essentielles pour une fraction du budget dont vous disposez pour la sécurité.

Pouvez-vous répondre à ces questions dans un cas d'éclosion de rançongiciel?

- Comment savez-vous quels fichiers sont chiffrés et quels sont leurs emplacements?
- Comment déterminez-vous quel utilisateur et quel appareil ont initié l'attaque?
- Comment arrêtez-vous immédiatement le chiffrement en cours avant que des dommages importants surviennent?
- Combien de temps vous faudra-t-il pour récupérer des centaines de milliers de fichiers et quel est le coût total de ce temps d'arrêt?
- Combien de temps est nécessaire pour signaler une attaque avec exactitude conformément au règlement général sur la protection des données (RGPD) si des milliers de fichiers contenant des renseignements personnels ont été perdus en raison d'un chiffrement illégal?

Pourquoi faut-il se préoccuper des rançongiciels?

Aujourd'hui plus que jamais, la haute direction (directeur des systèmes d'information, responsable de la sécurité de l'information, directeur financier et chef de la direction) a tout intérêt à sécuriser les données et le capital intellectuel afin de protéger les données d'identification personnelle (PII) et les revenus, de maintenir la loyauté des clients et de sécuriser la valeur actionnariale. Les cybercriminels inventent continuellement de nouvelles techniques inconnues pour combattre les méthodes traditionnelles de détection basées sur les signatures.

Il est essentiel que les entreprises ne comptent pas seulement sur une réponse réactive aux menaces des maliciels modernes. Chaque jour, nous entendons parler de l'échec de cette stratégie. Votre future stratégie de défense doit inclure la continuité des opérations et la reprise après sinistre grâce à une solution de dernière ligne de défense qui offre des alertes automatiques, une réponse d'arrêt et une récupération rapide sans les coûts énormes fréquemment associés aux attaques de rançongiciels.

Le fonctionnement

À cause d'une surface d'attaque en expansion rapide à défendre et de multiples points d'entrée des maliciels dans les entreprises d'aujourd'hui, RansomCare offre une solution de confinement automatique 24 heures sur 24, sept jours sur sept, contre les éclosions de rançongiciels avec des rapports intégrés, conformément aux réglementations comme le RGPD. L'utilisateur ou l'appareil ayant déclenché l'attaque n'a pas d'importance. Tout comme cela n'importe pas s'il s'agit d'une attaque de rançongiciels connus ou inconnus, si elle a commencé d'un terminal, d'un téléphone cellulaire, d'un appareil connecté, d'un courriel, d'une attaque par téléchargement furtif sur un site Web, d'une application de clavardage instantané, d'une clé USB ou d'un téléchargement, ou si elle a été déployée par quelqu'un dans votre entreprise.

Lorsque RansomCare détecte une attaque de rançongiciels, une alerte est émise instantanément, et une réponse peut être déclenchée pour fermer le terminal subissant l'attaque (Windows, Mac et Linux) afin que le chiffrement soit immédiatement arrêté. RansomCare s'occupe également des environnements virtuels comme les serveurs et les sessions de Citrix, les serveurs et les sessions de Terminal, Hyper-V et VMware, et du nuage, y compris Azure, Amazon AWS/EC2, SharePoint, Google Drive et Microsoft 365. RansomCare met hors service et arrête l'appareil qui chiffre vos données, y compris les appareils mobiles.

Installation à distance facile et sans tracas

RansomCare est une solution sans agent qui n'est PAS installée sur vos terminaux ni sur vos serveurs existants ou vos serveurs de fichiers. Il n'a aucun impact sur vos terminaux et n'entraîne aucun problème de performance de réseau. La surveillance sans agent du comportement des fichiers et les techniques d'apprentissage automatiques sont facilement déployées en quatre à six heures, et RansomCare est automatiquement configuré. Une intégration complète à d'autres solutions de sécurité – telles que Cisco ISE et Windows Defender ATP – ou à un système de gestion de l'information et des événements de sécurité (GIES) est offerte par l'intermédiaire de l'API RESTful, permettant à votre équipe de sécurité d'unifier la gestion de la sécurité à travers une quantité de terminaux de plus en plus complexe.

- **Pas d'installation dans le nuage**
- **Pas d'installation sur les terminaux (sans agent)**
- **Pas d'installation sur le serveur de fichiers**
- **Pas d'installation sur la plateforme d'entreposage**

Alertes et intégrations

Services d'alertes intégrés à RansomCare
- Avis par courriel
- Avis par WhatsApp
- Alerte par message texte
- Centre des opérations mobile
- API vers un autre système

Interface bidirectionnelle avec RESTful API
(scripts préconfigurés)
- Splunk
- Cisco ISE
- Windows Defender
- Aruba
- IBM Radar
- McAfee
- Symantec
- TrendMicro
- ForeScout

Test d'évaluation de rançongiciels
Ricoh peut effectuer un test d'évaluation de rançongiciel pour vérifier si vos solutions de sécurité existantes peuvent arrêter un chiffrement illégal en utilisant un outil de simulation de rançongiciel sécuritaire. Nous testerons ensuite RansomCare pour vous démontrer comment votre solution devrait répondre à une éclosion. Demandez à un représentant des ventes pour plus d'informations.

RICOH
imagine. change
imaginer. changer

Ricoh Canada Inc., 100-5560 Explorer Drive, Mississauga, ON L4W 5M3, 1 888 742-6417