ARRÊTER LES RANSOMWARES AVANT QU'ILS NE SE PROPAGENT

Une solution automatisée pour stopper une attaque ransomwares au sein de votre organisation

Faisons face aux faits: Même les organisations les mieux protégées sont victimes de ransomware. Les cybercriminels développent en permanence des moyens nouveaux et innovants pour déjouer les méthodes de détection traditionnelles, basées sur la prévention. Pour rester à l'abri des ransomwares, une entreprise doit faire évoluer ses défenses de sécurité et adopter une approche à plusieurs niveaux. Une fois que le ransomware a déclenché son action de cryptage, il est peut être dèjà trop tard pour que la sécurité existante réagisse. À ce stade, ce qui compte, c'est la vitesse à laquelle vous pouvez arrêter le cryptage illégitime pouvant aller jusqu'à 10000 fichiers par minute.

Une approche par couche, intégre une solution complémentaire pour détecter et arrêter le cryptage illégitime une fois qu'il est en cours. Elle peut surveiller l'activité des fichiers sur les partages de fichiers et dans le cloud. Dès que la solution identifie un cryptage criminel et une corruption de fichiers en cours, elle réagit et isole l'utilisateur qui en est à l'origine.

Voici la solution de confinement des ransomwares de Ricoh, RICOH RansomCare créé par BullWall, une défense unique et éprouvée. Plus de 20 capteurs de détection évaluent chaque changement de fichier sur les partages surveillés. Si les signes indicateurs d'un ransomware (cryptage illégitime) sont initiés et que des fichiers sont activement cryptés sur les partages de fichiers et dans le cloud surveillés, RICOH RansomCare réagit en isolant l'appareil et l'utilisateur compromis pour arrêter le processus de cryptage criminel. La solution est un élément vital de votre stratégie de défense globale qui offre une protection de sécurité essentielle pour une petite partie de votre budget sécurité actuel.

Pouvez-vous répondre à ces questions en cas d'attaque de ransomware ?

- Comment pouvez-vous voir quels fichiers sont cryptés et où ils se trouvent ?
- Comment identifiez-vous l'utilisateur et l'appareil qui crypte les fichiers ?
- Comment arrêtez-vous rapidement le cryptage en cours avant que des dommages importants ne se produisent ?
- Combien de temps faut-il pour restaurer des centaines de milliers de fichiers, et quel est le coût total de l'interruption de votre activité ?
- Quel délai est nécessaire pour signaler avec précision aux autorités responsables des données si des milliers de fichiers contenant des informations personnelles ont été cryptées illégalement ?

RICOH
imagine. change.

Pourquoi les Ransomwares sont importants

Aujourd'hui plus que jamais, la direction de l'entreprise (DSI, RSSI, directeur financier et PDG) a tout intérêt à sécuriser ses données et sa propriété intellectuelle afin de protéger les informations personnelles identifiables (IPI), ses revenus, maintenir la confiance et l'image auprés de ses clients et de ses actionnaires. Les dispositifs de sécurité traditionnels se concentrent sur la prévention de l'exécution des logiciels malveillants alors que les périphériques finaux en sont la cible. Mais que se passe-t-il si ils échouent ? Les ransomwares, c'est une toute autre réalité. Ils ont paralysé des organisations malgré la mise en place des meilleures solutions de sécurité. Aujourd'hui, les organisations devraient envisager de déployer une ligne de défense supplémentaire pour agir comme un "système de pulvérisation" en cas d'échec des solutions de sécurité basées sur la prévention.

Il est essentiel que les organisations ne se limitent pas à une approche réactive face aux menaces modernes que représentent les logiciels malveillants. Nous voyons quotidiennement des rapports sur l'échec de cette stratégie. La stratégie de défense du futur doit inclure la continuité des activités et la reprise après sinistre, afin de permettre des alertes automatiques, une réponse d'arrêt et une récupération rapide sans que cela n'entraîne les coûts énormes souvent liés aux attaques par ransomwares

Comment cela fonctionne

Face à l'expansion rapide de la surface d'attaque à défendre et aux multiples points d'entrée des logiciels malveillants dans les entreprises, RICOH RansomCare offre une réponse automatisée de confinement 24 heures sur 24, 7 jours sur 7, face aux attaques de ransomware, avec une réactivité immédiate et des rapports intégrés. Peu importe l'utilisateur ou l'appareil qui a déclenché le cryptage. Il n'est pas non plus important de savoir si l'attaque est une variante de ransomware connue ou inconnue ou si l'épidémie a démarré sur un point de terminaison, un téléphone mobile, un appareil IoT, par e-mail, USB, ou a été déployée par quelqu'un au sein de votre organisation. RICOH RansomCare enquête sur l'heuristique de chaque fichier auquel un utilisateur a accédé que ce soit sur les partages de fichiers surveillés, sur site ou dans le cloud, sans provoquer de surcharge du réseau. Lorsque RICOH RansomCare détecte un cryptage et une corruption de fichiers en cours sur les partages surveillés, une alerte est déclenchée instantanément et une réponse est mise en place pour désactiver et isoler le périphérique et l'utilisateur qui cryptent vos données.

RICOH RansomCare fonctionne également dans les environnements virtuels tels que les serveurs/sessions Citrix, les serveurs/sessions Terminal, Hyper-V, VMware et le Cloud, notamment Azure et Amazon AWS/EC2, SharePoint, Google Drive et Microsoft 365. Un large éventail de méthodes d'isolation personnalisables peut être utilisé, comme l'arrêt forcé, la désactivation du VPN, la désactivation de l'utilisateur AD, la désactivation de l'accès au réseau, la révocation des autorisations du cloud, et bien d'autres. L'intégration à d'autres solutions de sécurité par le biais d'une API RESTful permet à vos équipes de sécurité d'unifier la gestion de la sécurité dans une multitude de terminaux de plus en plus complexes.

Installation à distance sans encombre

RICOH RansomCare est une solution sans agent et n'est pas installé sur les terminaux, les serveurs existants ou les serveurs de fichiers. Il n'y a aucun impact sur les performances du réseau. La surveillance du comportement des fichiers sans agent et les techniques d'apprentissage automatique sont déployées facilement en quatre à six heures, et RICOH RansomCare sera configuré en fonction de votre environnement. RICOH RansomCare dispose de connecteurs Cloud pour les organisations qui utilisent Microsoft O365 (SharePoint, Teams, OneDrive) et Google Drive. Une intégration complète à d'autres solutions de sécurité comme Cisco ISE et Windows Defender ATP ou un système SIEM est disponible via une API RESTful permettant à vos équipes de sécurité d'unifier la gestion de la sécurité sur une multitude de périphériques finaux de plus en plus complexes.

- Pas d'installation dans le cloud
- Pas d'installation d'agent sur les points d'extrémités
- Pas d'installation de stockage/serveur de fichier

Alertes et intégrations

Services d'alerte intégrés à RICOH RansomCare

Notifications par email
Alerte par SMS
« SOC » mobile
API vers d'autres systèmes

Interface bidirectionnelle avec Restful

Splunk
Cisco ISE
Windows Defender
Aruba
IBM Radar
McAfee
Symantec
TrendMicro
ForeScout
etc.

Test d'évaluation du ransomware

Nous pouvons effectuer un test d'évaluation de ransomware dans lequel le simulateur RICOH RansomCare, sûr et sous contrôle, est utilisé pour simuler un cryptage de fichiers et des modifications rapides de fichiers. Nous testerons ensuite RICOH RansomCare dans votre environnement pour démontrer comment la solution réagit à une attaque de cryptage de fichiers. Demandez à votre correspondant commercial RICOH de vous fournir de plus amples informations.

RICOH
imagine. change.