CryptoSpike

Protection contre les Ransomwares et transparence des accès

Les Ransomwares, également connu sous le nom cryptotrojans, se compose de programmes malveillants qui chiffrent les données sur l'ordinateur. L'entreprise touchée est sommée de payer une rançon pour débloquer les fichiers, souvent via bitcoin, et même si elle est payée, il n'y a pas de garantie que le criminel fournira une clé de décryptage.

Des exemples bien connus de logiciels malveillants incluent WannaCry et Petya. Ils entrent dans les entreprises via des liens modifiés ou des pièces jointes par e-mail, déguisés en publicité par phishing ou spam.

Faits et chiffres sur les Ransomware

Selon le rapport que vous lisez, la croissance de Ransomware est astronomique estimée à plus de 50% chaque année. Une nouvelle organisation est victime de Ransomware toutes les 14 secondes, et aucune organisation n'est épargnée - les attaques sont fréquentes dans le secteur public, les grandes entreprises, et même les équipes sportives de premier plan.

Le coût financier se chiffre en milliards de dollars et peut avoir également un effet domino avec des arrêts de production et la perte de clients.

Le pire de tout :

Un simple clic d'un employé suffit à infecter l'ensemble du réseau

Ce ne sont pas seulement les fichiers sur l'ordinateur local de l'employé qui sont endommagés, mais aussi les fichiers sur les lecteurs réseau. Comme tout virus, le cryptage se propage rapidement et attaque généralement le stockage central - ainsi tout client qui utilise (licence CIFS / NFS) ONTAP comme NAS (Network Attached Storage) devrait avoir une protection contre les ransomwares mis en œuvre.

Avec la montée des menaces internes, certaines organisations ne remarquent l'attaque que lorsqu'il est trop tard

Les menaces internes sont d'autant plus préoccupantes que les utilisateurs ont l'autorisation d'accéder aux systèmes - de sorte qu'un problème n'est souvent remarqué qu'une fois que l'infection s'est produite.

Certaines d'entre eux sont le fait de négligence ou par des employés mécontents, mais le problème beaucoup plus important est la compromission d'employés - car ils ne savent pas qu'ils ont été piratés.

La solution est CryptoSpike qui combat le chantage numérique en temps réel

Aucun système d'exploitation n'est à l'abri des attaques de ransomwares. Beaucoup d'entreprises ne savent même pas si des fichiers individuels ont été cryptés, étant donné les millions de fichiers qu'elles ont stockés. Avec CryptoSpike, vous pouvez détecter rapidement les logiciels malveillants et les empêcher de se propager. CryptoSpike a été spécialement conçu pour les systèmes de stockage ONTAP. Les attaques des utilisateurs du CIFS et du NFS sont enregistrées par l'API FPolicy. En temps réel, la solution surveille chaque opération dans le système ONTAP pour des anomalies liées aux extensions de fichiers ou au comportement de l'utilisateur.

Points Clé

L'utilisateur Infecté
Est bloqué et les fichiers encryptés sont localisés. Cela empêche la poursuite de l'encryptions et, par conséquent, l'échec des processus critiques

CryptoSpike
Scanne les accès aux fichiers en temps réels en utilisant une stratégie en trois étapes pour identifier les attaques de ransomware et bloquer l'attaque et la propagation immédiatement.

L'attaque
Est littéralement tué dans l'œuf, de fait les tentatives de chantage aussi!!

Ransomware
Les attaques sont de plus en plus importante et une entreprise est infectée toutes **les 14 secondes**

Un simple clic
Sur une pièce jointe ou un lien malveillant est suffisant pour que malware commence à chiffrer les fichiers. Pas seulement sur le PC local mais sur chaque lecteurs réseau accessible.

Comment cela fonctionne:

L'architecture permet d'utiliser l'image logicielle pour faciliter Installation

Les images CryptoSpike et FPolicy Server sont fournies prêts à l'emploi en tant que machine virtuelle qui peut être simplement déployée sur n'importe quel hyperviseur disponible. La configuration, la gestion de configuration et la définition des règles et des valeurs de seuil se font à l'aide des règles intuitives du gestionnaire CryptoSpike.

Trois stratégies alignées pour détecter les attaques

Passlist: sur la base d'une liste d'extensions de fichiers autorisées, telles que .doc .xls .pdf. Si une nouvelle extension inconnue est détectée, CryptoSpike bloque l'utilisateur. S'il s'agit d'une nouvelle application autorisée, l'administrateur peut l'ajouter à la liste.

La première liste est vide et doit être configuré manuellement - CryptoSpike scanne de manière autonome l'ensemble du stockage de l'entreprise.

Block list: sur la base d'une liste d'environ 5000 (nombre en hausse rapide!) extensions connues de ransomware mise à jour tous les jours. Chaque fois qu'une nouvelle liste de blocage est disponible, CryptoSpike appliquera automatiquement ces nouvelles entrées.

Comportements: Surveille les habitudes comportementales des utilisateurs relatives aux opérations de lecture/ écriture/ d'ouverture/ fermeture de fichiers.

CryptoSpike utilise aussi des listes de blocage de comportements: celle-ci ont été créés en suivant le comportement de WannaCry et d'autres modèles ransomware pendant une infection surveillée - l'algorithme analyse les modèle d'opérations ouvertures/ cryptages/ Fermeture. Cette liste peut être complétée par d'autres modèles d'attaques auxquelles le client a été exposé.

Pourquoi les comportements sont l'élément essentiel

Les attaques de ransomwares sont de plus en plus problématiques, parce que de nombreux codes malveillants ne changent plus les extensions de fichier à des valeurs telles que. crypto ou .locky. Par conséquent, vous ne pouvez plus dire si un fichier .xls est indemne ou non.

Pour détecter une attaque dans de tels cas, les modélisations agissent comme un deuxième filet de sécurité plus precis. Par exemple, si un fichier est accédé plus souvent que le seuil défini dans un modèle, l'algorithme l'identifie en temps réel comme un comportement non autorisé, bloque l'utilisateur et sonne l'alarme.

Choix sur mesure d'une stratégie adaptée

Les politiques (blocklist/passlist), peuvent être réglés au besoin, individuellement pour les niveaux: Cluster/ SVM/Volume/Part.

Dans le même temps, vous pouvez également utiliser la hiérarchie parent- enfant, ce qui signifie que vous pouvez simplement définir une stratégie au niveau SVM, qui sera ensuite héritée à la fois par le volume ainsi que par le partage.

Alarmes: Blocage en temps réel et restauration rapide

• CryptoSpike suit chaque opération en temps réel. Si une anomalie est détectée, le système tire la sonnette d'alarme et bloque l'attaque de l'employé afin d'éviter toute nouvelle contagion sur le stockage ONTAP.

• L'employé bloqué n'a plus qu'accès en lecture seule ou aucun accès en fonction de la stratégie configurée.

• CryptoSpike fournit d'abord les informations clés: quels fichiers sont affectés? L'administrateur reçoit automatiquement les détails du chemin et du nombre de fichiers concernés et examine les opérations récentes.

• Si l'utilisateur a été bloqué à tort, s'il s'agit par exemple d'un développeur testant une nouvelle application, l'administrateur peut immédiatement les débloquer à nouveau et, si nécessaire, adapter les modèles.

• S'il s'agit d'une attaque de ransomware, l'administrateur analyse quels programmes malveillants sont en cours d'exécution en arrière-plan. Lorsque l'utilisateur est débloqué après le nettoyage, CryptoSpike prend en charge le processus de récupération avec la liste des fichiers affectés, de sorte qu'un Snapshot peut être utilisé pour les restaurer rapidement.

Modèle de tarification

CryptoSpike suit un modèle de tarification à plusieurs niveaux, selon le nombre et la taille des contrôleurs de stockage ONTAP.

Avantages

• Facile à installer via images systèmes dédiées.

• Extension de fichiers, noms de fichiers et comportements utilisateurs sont tous vérifié pour détecter des Anomalies

• Informations immédiates sur l'emplacement de l'attaque et aide à la restauration des fichiers endommagés

• Chaque opération dans le système de stockage est surveillée en temps réel et les utilisateurs infectés sont immédiatement bloqués.

• Politiques de surveillance sur mesure pour répondre aux besoins de chaque service.