Fonctions de détection des ransomwares Cisco WSA et vérification de l'intégration AMP

Table des matières

Problème

Une enquête a été effectuée pour savoir si Cisco Secure Web Appliance (WSA) fournit des fonctionnalités de signature ou de détection spécifiques pour Triple X Ransomware. Cette question comprenait également une demande de clarification sur la façon de vérifier si une intégration entre Advanced Malware Protection (AMP) et Cisco Talos Threat Intelligence fonctionnait correctement sur la plate-forme WSA.

Environnement

- Appareil Web sécurisé Cisco (WSA)
- Intégration d'AMP (Advanced Malware Protection)
- Intégration de Cisco Talos Threat Intelligence
- Réputation Web et filtrage des URL (WBRS)
- Moteurs d'analyse anti-programme malveillant (Webroot, McAfee, Sophos)
- Visibilité et contrôle des applications (AVC)

Résolution

Cisco Secure Web Appliance ne repose pas sur une seule signature dédiée spécifiquement nommée pour Triple X Ransomware. Au lieu de cela, WSA utilise une architecture de sécurité multicouche complète qui utilise diverses techniques de détection pour identifier et bloquer les menaces de ransomware, y compris les variantes Triple X Ransomware.

Méthodes de détection WSA

La plate-forme WSA utilise les techniques de détection suivantes pour la protection contre les ransomwares :

- Algorithmes de correspondance des modèles
- Analyse heuristique
- Techniques d'émulation
- Advanced Malware Protection (AMP) intégré à Cisco Talos Threat Intelligence
- Réputation Web et filtrage des URL (WBRS)
- Plusieurs moteurs d'analyse anti-programme malveillant, notamment Webroot, McAfee et Sophos
- Visibilité et contrôle des applications (AVC)

Ces fonctionnalités de détection sont continuellement mises à jour avec de nouvelles règles déployées toutes les quelques minutes pour assurer une protection contre les menaces émergentes.

Vérification de l'intégration AMP et Talos

Pour vérifier que l'intégration entre Advanced Malware Protection (AMP) et Cisco Talos Threat Intelligence fonctionne correctement sur WSA, les administrateurs peuvent consulter les journaux suivants :

Étape 1: Consulter les journaux d'accès WSA

Examinez les journaux d'accès sur l'appliance WSA pour vérifier que les verdicts AMP sont appliqués aux fichiers téléchargés et aux requêtes Web.

Étape 2: Vérifier les journaux AMP

Consultez les journaux AMP pour vérifier que les résultats de l'analyse des programmes malveillants et les données de renseignements sur les menaces sont traités.

Étape 3: Vérification des scores WBRS

Assurez-vous que les scores de réputation Web (WBRS) sont remplis et qu'ils sont associés aux requêtes Web dans les journaux.

Si les verdicts AMP et les scores WBRS sont remplis et appliqués dans les journaux, cela indique que l'intégration d'AMP et de Talos fonctionne comme prévu et fournit des décisions basées sur des informations en temps réel sur les menaces.

Motif

Il s'agissait d'une demande d'information concernant les fonctionnalités de détection des ransomwares WSA plutôt que d'un problème technique nécessitant un dépannage. L'enquête a été lancée pour comprendre comment WSA protège contre des variantes de ransomware spécifiques et pour vérifier que les intégrations d'informations sur les menaces fonctionnent correctement.

Autres informations utiles

- Fonctionnalités et avantages de l'appliance Web sécurisé Cisco
- Services Cisco Talos Threat Intelligence
- Fiche technique sur Cisco Secure Web Appliance
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.