Cisco WSA Ransomware-Erkennungsfunktionen und Überprüfung der AMP-Integration

Inhalt

Problem

Es wurde angefragt, ob die Cisco Secure Web Appliance (WSA) spezifische Signatur- oder Erkennungsfunktionen für Triple X Ransomware bereitstellt. Bei dieser Frage ging es auch darum, zu klären, wie überprüft werden kann, ob eine Integration zwischen Advanced Malware Protection (AMP) und Cisco Talos Threat Intelligence auf der WSA-Plattform ordnungsgemäß funktioniert.

Umwelt

- Cisco Secure Web Appliance (WSA)
- Integration von Advanced Malware Protection (AMP)
- Cisco Talos Threat Intelligence-Integration
- Webreputation und URL-Filterung (WBRS)
- Anti-Malware-Scan-Engines (Webroot, McAfee, Sophos)
- Application Visibility and Control (AVC)

Auflösung

Cisco Secure Web Appliance verwendet keine dedizierte Signatur, die speziell für Triple X Ransomware benannt wurde. Stattdessen setzt die WSA eine umfassende, mehrschichtige Sicherheitsarchitektur ein, die verschiedene Erkennungstechniken nutzt, um Ransomware-Bedrohungen zu identifizieren und zu blockieren, einschließlich Triple X Ransomware-Varianten.

WSA-Erkennungsmethoden

Die WSA-Plattform nutzt diese Erkennungstechniken zum Schutz vor Ransomware:

- Algorithmen zum Mustervergleich
- Heuristikanalyse
- Emulation Techniken
- Advanced Malware Protection (AMP) integriert mit Cisco Talos Threat Intelligence
- Webreputation und URL-Filterung (WBRS)
- Mehrere Anti-Malware-Scan-Engines, darunter Webroot, McAfee und Sophos
- Application Visibility and Control (AVC)

Diese Erkennungsfunktionen werden alle paar Minuten durch neue Regeln aktualisiert, um einen effektiven Schutz vor neuen Bedrohungen zu gewährleisten.

Überprüfen der AMP- und Talos-Integration

Um sicherzustellen, dass die Integration zwischen Advanced Malware Protection (AMP) und Cisco Talos Threat Intelligence auf der WSA ordnungsgemäß funktioniert, können Administratoren die folgenden Protokolle überprüfen:

Schritt 1: WSA-Zugriffsprotokolle überprüfen

Überprüfen Sie die Zugriffsprotokolle auf der WSA-Appliance, um zu überprüfen, ob AMP-Verdicts auf heruntergeladene Dateien und Webanfragen angewendet werden.

Phase 2: AMP-Protokolle überprüfen

Überprüfen Sie die AMP-Protokolle, um sicherzustellen, dass die Ergebnisse der Malware-Analyse und die Bedrohungsinformationen verarbeitet werden.

Schritt 3: WBRS-Bewertungen überprüfen

Stellen Sie sicher, dass die Webreputations-(WBRS)-Bewertungen ausgefüllt und mit Webanfragen in den Protokollen verknüpft werden.

Wenn AMP-Verdicts und WBRS-Bewertungen in die Protokolle aufgenommen und durchgesetzt werden, weist dies darauf hin, dass die Integration von AMP und Talos wie erwartet funktioniert und auf Echtzeitinformationen zu Bedrohungen basierende Entscheidungen ermöglicht.

Ursache

Dies war eher eine Informationsanfrage bezüglich der Ransomware-Erkennungsfunktionen von WSAs als ein technisches Problem, das eine Fehlerbehebung erfordert. Die Untersuchung ergab sich aus der Notwendigkeit, zu verstehen, wie WSA gegen bestimmte Ransomware-Varianten schützt, und zu überprüfen, ob Threat-Intelligence-Integrationen ordnungsgemäß funktionieren.

Verwandte Inhalte

- Funktionen und Vorteile der Cisco Secure Web Appliance
- Cisco Talos Threat Intelligence Services
- Cisco Secure Web Appliance - Datenblatt
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.