Cisco WSA Ransomware Detection Capabilities en AMP Integration Verification

Inhoud

uitgifte

Er is gevraagd of Cisco Secure Web Appliance (WSA) specifieke handtekening- of detectiemogelijkheden biedt voor Triple X Ransomware. Deze vraag bevatte ook een verzoek om verduidelijking over hoe te verifiëren of een integratie tussen Advanced Malware Protection (AMP) en Cisco Talos Threat Intelligence correct functioneerde op het WSA-platform.

milieu

- Cisco Secure Web Appliance (WSA)
- Advanced Malware Protection (AMP)-integratie
- Integratie van Cisco Talos Threat Intelligence
- Webreputatie en URL-filtering (WBRS)
- Anti-malware scanning engines (Webroot, McAfee, Sophos)
- Application Visibility and Control (AVC)

resolutie

Cisco Secure Web Appliance vertrouwt niet op een enkele, speciale handtekening die specifiek is genoemd voor Triple X Ransomware. In plaats daarvan maakt WSA gebruik van een uitgebreide meerlaagse beveiligingsarchitectuur die verschillende detectietechnieken gebruikt om ransomware-bedreigingen te identificeren en te blokkeren, waaronder Triple X Ransomware-varianten.

WSA-detectiemethoden

Het WSA-platform gebruikt deze detectietechnieken voor ransomwarebescherming:

- Patroonovereenkomende algoritmen
- Heuristische analyse
- Emulatietechnieken
- Advanced Malware Protection (AMP) geïntegreerd met Cisco Talos Threat Intelligence
- Webreputatie en URL-filtering (WBRS)
- Meerdere anti-malware scanning engines, waaronder Webroot, McAfee en Sophos
- Application Visibility and Control (AVC)

Deze detectiemogelijkheden worden voortdurend bijgewerkt met nieuwe regels die om de paar minuten worden geïmplementeerd om bescherming te bieden tegen opkomende bedreigingen.

Integratie van AMP en Talos verifiëren

Om te bevestigen dat de integratie tussen Advanced Malware Protection (AMP) en Cisco Talos Threat Intelligence correct werkt op WSA, kunnen beheerders deze logbestanden bekijken:

Stap 1: WSA-toegangslogboeken bekijken

Controleer de toegangslogboeken op het WSA-toestel om te controleren of AMP-vonnissen worden toegepast op gedownloade bestanden en webverzoeken.

Stap 2: Controleer AMP-logboeken

Controleer de AMP-logboeken om te bevestigen dat de resultaten van de malwareanalyse en de gegevens van de bedreigingsinformatie worden verwerkt.

Stap 3: WBRS-scores verifiëren

Zorg ervoor dat de Web Reputation (WBRS) scores worden ingevuld en dat ze worden

geassocieerd met webverzoeken in de logs.

Als AMP-vonnissen en WBRS-scores worden ingevuld en gehandhaafd in de logboeken, geeft dit aan dat de AMP- en Talos-integratie werkt zoals verwacht en realtime op dreigingsinformatie gebaseerde beslissingen biedt.

Oorzaak

Dit was een informatieverzoek met betrekking tot WSA's ransomware detectie mogelijkheden in plaats van een technisch probleem dat het oplossen van problemen. Het onderzoek kwam voort uit de noodzaak om te begrijpen hoe WSA beschermt tegen specifieke ransomware-varianten en om te verifiëren dat integratie van bedreigingsinformatie goed functioneert.

Gerelateerde inhoud

- Functies en voordelen van Cisco Secure Web Appliance
- Cisco Talos Threat Intelligence Services
- Gegevensoverzicht van Cisco Secure Web Appliance
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.