Inzicht in Secure Web Applicatie Malware en Spyware Protection

Inhoud

Inleiding

Dit document beschrijft de uitgebreide functies voor de bescherming van malware en spyware van de Cisco Secure Web Applicatie (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Cisco SWA is ontworpen om robuuste en uitgebreide gateway-beschermingsmechanismen te bieden tegen een breed spectrum van spyware en webgebaseerde malware. Het effectief tegengaat bedreigingen uiteenlopend van adware, die berucht is voor het veroorzaken van aanzienlijke netwerk resource drain en ondersteunende uitdagingen, tot ernstigere bedreigingen zoals trojans, browser hijackers, browser helper objecten, phishing, pharming, systeem monitors, keyloggers, en wormen.

Belangrijkste onderscheidende factoren van SWA

Geïntegreerde Layer 4 Traffic Monitor (L4TM)

De L4 Traffic Monitor is in staat om alle netwerkpoorten (65.535 in totaal) op draadsnelheid te scannen, waardoor uitgebreide detectie en blokkering van malware en ongeoorloofde communicatiepogingen mogelijk is. Deze functionaliteit belemmert effectief malware die probeert om algemene poorten zoals poorten 80 en 443 te omzeilen, en het onderdrukt ook schurken peer-to-peer (P2P) en Internet Relay Chat (IRC) activiteiten.

Proxy-laagverwerking

De SWA bevat een krachtige webproxy met geïntegreerde caching en contentversnellingsfuncties. Aangedreven door Cisco bedrijfseigen AsyncOS, kan deze webproxy tot tien keer meer verbindingen beheren dan conventionele UNIX-gebaseerde proxyservers. Als webproxy faciliteert het uitgebreide inhoudsinspectie op de applicatielaag, wat essentieel is voor een precieze verdediging tegen webgebaseerde malware.

Filters voor webreputatie

Als de industrie baanbrekende web reputatie filters, deze bieden een extra laag van defensie. Met behulp van SenderBase® evalueren deze filters meer dan 50 webverkeer en netwerkgerelateerde parameters om de betrouwbaarheid van een URL te bepalen. Geavanceerde security modelleringstechnieken worden gebruikt om individuele gewichten toe te wijzen aan elke parameter, culminerend in een reputatiescore variërend van -10 tot +10. Beheerder geconfigureerd beleid past dynamisch aan op basis van deze scores.

Dynamic Vectoring and Streaming (DVS) Engine

De DVS Engine introduceert versnelde handtekeningscanning binnen de SWA, die zich onderscheidt van oudere architecturen die afhankelijk zijn van Internet Content Adaptation Protocol (ICAP) en multibox implementaties voor het scannen van malware. Dit hypermoderne platform maakt gebruik van geavanceerde objectparsing, vectortechnieken, stream scanning en verdict caching, waarmee tot een tienvoudige toename in scandoorvoersnelheid wordt bereikt in vergelijking met oplossingen van de eerste generatie op basis van ICAP.

Cisco-systeem tegen malware

Dit systeem maakt gebruik van de DVS Engine naast meerdere handtekeningtypes die afkomstig zijn van Webroot, en biedt ongeëvenaarde bescherming tegen een diverse reeks webgebaseerde bedreigingen. Het spectrum van bedreigingen omvat adware, browser hijackers, phishing, pharming aanvallen, en meer kwaadaardige entiteiten zoals trojans, systeemmonitors, en keyloggers. SWA beschikt over de grootste malware-handtekeningsdatabase van de branche bij de gateway, die uitgebreide bescherming biedt.

De Cisco Web Security Applicatie is dus gepositioneerd als marktleider bij het beveiligen van netwerkgateways tegen een uitgebreide reeks op internet gebaseerde bedreigingen, waardoor zowel robuuste bescherming als hoogwaardige netwerkdoorvoersnelheid worden gegarandeerd.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web applicatie

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.