Informazioni sulla protezione da malware e spyware di Secure Web Appliance

Sommario

Introduzione

Questo documento descrive le funzionalità complete di protezione da malware e spyware di Cisco Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Cisco SWA è progettato per fornire meccanismi di difesa gateway affidabili e completi contro un'ampia gamma di spyware e malware basato sul Web. È in grado di contrastare efficacemente minacce che vanno dall'adware, noto per la causa di problemi significativi di esaurimento delle risorse di rete e di supportabilità, a minacce più gravi, tra cui trojan, dirottatori di browser, oggetti browser helper, phishing, pharming, monitor di sistema, keylogger e worm.

Principali fattori di differenziazione della SWA

L4TM (Layer 4 Traffic Monitor) integrato

L'L4 Traffic Monitor è in grado di analizzare tutte le porte di rete (65.535 in totale) alla velocità wire-speed, garantendo il rilevamento completo e il blocco di malware e tentativi di comunicazione non autorizzati. Questa funzionalità impedisce in modo efficace il malware che tenta di ignorare le porte comuni, ad esempio le porte 80 e 443, e sopprime inoltre le attività peer-to-peer (P2P) e IRC (Internet Relay Chat) non autorizzate.

Elaborazione livello proxy

Lo SWA incorpora un proxy Web ad alte prestazioni con funzionalità integrate di caching e accelerazione dei contenuti. Basato su AsyncOS, un proxy Web proprietario di Cisco, può gestire fino a dieci volte più connessioni rispetto ai tradizionali server proxy basati su UNIX. In qualità di proxy Web, facilita l'ispezione esaustiva dei contenuti a livello di applicazione, che è essenziale per una difesa precisa dal malware basato sul Web.

Filtri reputazione Web

In quanto filtri di reputazione Web all'avanguardia nel settore, questi forniscono un ulteriore livello di difesa. Utilizzando SenderBase®, questi filtri valutano oltre 50 traffico Web e parametri relativi alla rete per determinare l'attendibilità degli URL. Per assegnare pesi individuali a ciascun parametro vengono utilizzate tecniche avanzate di modellazione della sicurezza, che culminano con un punteggio di reputazione compreso tra -10 e +10. I criteri configurati dall'amministratore vengono adattati in modo dinamico in base a questi punteggi.

Motore DVS (Dynamic Vectoring and Streaming)

Il motore DVS introduce una scansione accelerata delle firme nell'ambito dell'SWA, distinguendosi dalle architetture legacy che dipendono dal protocollo ICAP (Internet Content Adaptation Protocol) e dalle installazioni multi-box per la scansione dei malware. Questa piattaforma all'avanguardia utilizza sofisticate tecniche di analisi degli oggetti, vettorizzazione, scansione dei flussi e memorizzazione dei verdetti nella cache, ottenendo un incremento fino a dieci volte superiore della velocità di scansione rispetto alle soluzioni basate su ICAP di prima generazione.

Sistema antimalware Cisco

Questo sistema sfrutta il motore DVS insieme a diversi tipi di firma provenienti da Webroot, offrendo una protezione senza pari contro una vasta gamma di minacce basate sul Web. Lo spettro di minacce include adware, dirottatori di browser, phishing, attacchi pharming, e altre entità più dannose come trojan, monitor di sistema e keylogger. SWA vanta il più grande database di firme malware del settore presso il gateway, garantendo una protezione completa.

Cisco Web Security Appliance è quindi leader nella protezione dei gateway di rete da un'ampia gamma di minacce basate sul Web, garantendo una protezione efficace e un throughput di rete ad alte prestazioni.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).