Entender a proteção segura contra malware e spyware do dispositivo da Web

Contents

Introdução

Este documento descreve os recursos abrangentes de proteção contra malware e spyware do Cisco Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

O Cisco SWA foi projetado para fornecer mecanismos de defesa de gateway robustos e abrangentes contra um amplo espectro de spyware e malware baseado na Web. Ele combate com eficiência ameaças que variam de adware, que é conhecido por causar um consumo significativo de recursos de rede e desafios de capacidade de suporte, a ameaças mais graves, incluindo cavalos de Troia, sequestradores de navegador, objetos auxiliares do navegador, phishing, pharming, monitores de sistema, keyloggers e worms.

Principais diferenciais do SWA

Monitor de tráfego de camada 4 integrado (L4TM)

O L4 Traffic Monitor é capaz de examinar todas as portas de rede (65.535 no total) em velocidade de cabo, garantindo detecção e bloqueio abrangentes de malware e tentativas de comunicação não autorizadas. Essa funcionalidade impede com eficiência o malware que tenta contornar portas comuns, como as portas 80 e 443, e também suprime atividades invasoras Peer-to-Peer (P2P) e Internet Relay Chat (IRC).

Processamento de Camada Proxy

O SWA incorpora um proxy da Web de alto desempenho com recursos integrados de cache e aceleração de conteúdo. Baseado na tecnologia AsyncOS proprietária da Cisco, esse proxy da Web pode gerenciar até dez vezes mais conexões do que os servidores proxy baseados em UNIX convencionais. Como um proxy da Web, ele facilita a inspeção completa de conteúdo na camada de aplicação, o que é essencial para uma defesa precisa contra malware baseado na Web.

Filtros do Web Reputation

Como os filtros de reputação da Web pioneiros do setor, eles fornecem uma camada adicional de defesa. Utilizando o SenderBase®, esses filtros avaliam mais de 50 tráfego da Web e parâmetros relacionados à rede para determinar a confiabilidade de uma URL. As técnicas avançadas de modelagem de segurança são empregadas para atribuir pesos individuais a cada parâmetro, culminando em uma pontuação de reputação que varia de -10 a +10. As políticas configuradas pelo administrador se adaptam dinamicamente com base nessas pontuações.

Mecanismo DVS (Dynamic Vetoring and Streaming)

O DVS Engine introduz a varredura acelerada de assinaturas no SWA, destacando-se das arquiteturas antigas que dependem do Internet Content Adaptation Protocol (ICAP) e de implantações em várias caixas para a varredura de malware. Essa plataforma de última geração utiliza análise sofisticada de objetos, técnicas de vetorização, varredura de fluxo e cache de veredito, obtendo um aumento de até dez vezes na taxa de transferência de varredura em

comparação com as soluções de primeira geração baseadas em ICAP.

Sistema antimalware da Cisco

Este sistema aproveita o DVS Engine junto com vários tipos de assinatura originados do Webroot, oferecendo proteção inigualável contra uma ampla gama de ameaças baseadas na Web. O espectro de ameaças inclui adware, sequestradores de navegador, phishing, ataques de pharming e mais entidades mal-intencionadas, como cavalos de Troia, monitores de sistema e keyloggers. O SWA apresenta o maior banco de dados de assinaturas de malware do setor no gateway, garantindo uma proteção abrangente.

O Cisco Web Security Appliance é, portanto, líder na proteção de gateways de rede contra uma ampla gama de ameaças baseadas na Web, garantindo proteção robusta e throughput de rede de alto desempenho.

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.