Visão geral do WSA Cisco Web Reputation

Contents

Introduction

Este documento fornece uma visão geral do Cisco Web Reputation (WBRS) para o Cisco Web Security Appliance (WSA).

Contribuído por Josh Wolfer e Stephan Fiebrandt, engenheiros do Cisco TAC.

Visão geral do WBRS

O WBRS é um método inovador que analisa o comportamento e as características de um servidor Web e oferece a mais recente defesa na luta contra spam, vírus, phishing e ameaças de spyware.

O WBRS usa análise em tempo real em um vasto, diversificado e global conjunto de dados para detectar URLs que contêm alguma forma de malware. O WBRS é uma parte essencial do banco de dados de segurança da Cisco, que protege os clientes contra ameaças combinadas de e-mail ou tráfego da Web.

Uso WBRS de SenderBase

O WBRS aproveita os dados do Common Security Database (SenderBase ® Network) da Cisco, que é a maior rede de monitoramento de e-mail e tráfego da Web do mundo. Ele rastreia mais de 50 parâmetros distintos que são excelentes indicadores da reputação de um URL. Com sofisticados agentes de modelagem de segurança e detecção de malware, a Cisco avalia essas URLs com base nessas informações.

Alguns dos parâmetros incluem:

- Dados de categorização de URL
- Presença de código para download
- Presença de contratos de licença de usuário final (EULAs) longos e obscuros
- Volume global e alterações no volume
- Informações do proprietário da rede

- Histórico de um URL
- Idade de um URL
- Presença de vírus / spam / spyware / phishing / pharming blacklist(s)
- Tipos de URL de domínios populares
- Informações do agente de registro
- informação de endereço IP

Granularidade de WBRS

O WBRS difere de uma lista negra ou whitelist de URL tradicional porque analisa um amplo conjunto de dados e produz uma pontuação altamente granular de -10 a +10, em vez das categorizações binárias **boas** ou **ruins** da maioria dos aplicativos de detecção de malware. Essa pontuação granular oferece aos administradores maior flexibilidade; diferentes políticas de segurança podem ser implementadas com base em diferentes intervalos de pontuação do WBRS.