

Vista geral da reputação da Web WSA Cisco

Índice

[Introdução](#)

[Vista geral WBRS](#)

[Uso WBRS de SenderBase](#)

[Granularidade WBRS](#)

Introdução

Este documento fornece uma vista geral da reputação da Web de Cisco (WBRS) para a ferramenta de segurança da Web de Cisco (WSA).

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

Vista geral WBRS

WBRS é um método inovativo que analisa o comportamento e as características de um servidor de Web e fornece a defesa a mais atrasada na luta contra o Spam, os vírus, o phishing, e as ameaças do spyware.

WBRS usa a análise em tempo real em um conjunto de dados vasto, diverso, e global a fim detectar as URL que contêm algum formulário do malware. WBRS é uma parte crítica da base de dados de segurança de Cisco, que protege clientes das ameaças misturadas do email ou do tráfego de web.

Uso WBRS de SenderBase

WBRS leverages dados do base de dados da segurança comum de Cisco (rede do [®] de SenderBase), que é rede o email do mundo e da monitoração de tráfego de web os maiores. Segue sobre os parâmetros distintos dos 50 pés que são indicadores excelentes da reputação de uma URL. Com os agentes sofisticados da detecção da modelagem e do malware de Segurança, Cisco avalia estas URL baseadas nestas entradas.

Alguns dos parâmetros incluem:

- Dados da categorização URL
- Presença de código carregável
- Presença de por muito tempo, contratos de licença confundidos do utilizador final (EULAs)
- Volume e mudanças globais no volume

- Informação do proprietário da rede
- História de uma URL
- Idade de uma URL
- Presença de vírus/Spam/spyware/phishing/listas negras pharming
- Erros tipográficos URL de domínios populares
- Informação do escrivão do domínio
- Informação do endereço IP de Um ou Mais Servidores Cisco ICM NT

Granularidade WBRS

WBRS difere de uma lista negra tradicional ou do whitelist URL porque analisa um conjunto de dados largo e produz uma contagem altamente granulada de -10 a +10, em vez das **boas** ou categorizações **ruins** binárias da maioria de aplicativos da detecção do malware. Esta contagem granulada oferece a administradores o aumento de flexibilidade; as políticas de segurança diferentes podem ser executadas com base em WBRS diferente que marca escalas.