

WSA Cisco Web Reputation - Overzicht

Inhoud

[Inleiding](#)

[WBS - Overzicht](#)

[WBRS Gebruik van SenderBase](#)

[WBRS-granulariteit](#)

Inleiding

Dit document geeft een overzicht van Cisco Web Reputation (WBRS) voor Cisco Web Security Appliance (WSA).

Bijgedragen door Josh Wolfer en Stephan Fiebrandt, Cisco TAC Engineers.

WBS - Overzicht

WBRS is een innovatieve methode die het gedrag en de kenmerken van een webserver analyseert en de meest recente verdediging biedt in de strijd tegen spam, virussen, phishing en spyware-bedreigingen.

WBRS gebruikt real-time analyse op een uitgebreide, diverse en mondiale dataset om URL's te detecteren die een of andere vorm van malware bevatten. WBRS is een cruciaal deel van de Cisco security database, die klanten tegen gemengde bedreigingen tegen e-mail of internetverkeer beschermt.

WBRS Gebruik van SenderBase

WBRS maakt gebruik van gegevens van Cisco's Common Security Database (SenderBase[®] Network), 's werelds grootste e-mail en Web traffic monitoring netwerk. Het volgt meer dan 50 verschillende parameters die uitstekende indicatoren van de reputatie van een URL zijn. Met geavanceerde security modellering en malware detectie agenten, evalueert Cisco deze URLs op basis van deze input.

Enkele van de parameters zijn:

- URL-categorisatiegegevens
- Aanwezigheid van de downloadbare code
- Aanwezigheid van lange, verduisterde Gebruiksrechtovereenkomst (EULA's)
- Totale omvang en volumemutaties

- Informatie over de netwerkeigenaar
- Historie van een URL
- Leeftijd van een URL
- Aanwezigheid van virussen / spam / spyware / phishing / farming zwarte lijst(en)
- URL-typen van populaire domeinen
- Domain Registrar-informatie
- IP-adresinformatie

WBRS-granulariteit

WBRS verschilt van een traditionele URL-zwarte lijst of witte lijst omdat hij een brede reeks gegevens analyseert en een zeer granulaire score van -10 tot +10 produceert, in plaats van de binaire **goede** of **slechte** categorisaties van de meeste malware detectietoepassingen. Dit granulaire score biedt beheerders meer flexibiliteit; verschillende beveiligingsbeleidsmaatregelen kunnen worden uitgevoerd op basis van verschillende scoringmarges van de WBRS.