Содержание

Введение

Этот документ предоставляет обзор веб-Репутации Cisco (WBRS) для Cisco Web Security Appliance (WSA).

Внесенный Джошем Уолфером и Штефаном Фибрандтом, специалистами службы технической поддержки Cisco.

Обзор WBRS

WBRS является передовым методом, который анализирует поведение и характеристики Web-сервера и предоставляет последнюю защиту в борьбе со спамом, вирусами, фишингом и угрозами шпионского ПО.

WBRS использует анализ в режиме реального времени обширного, разнообразного, и глобального набора данных для обнаружения URL, которые содержат некоторую форму вредоносного ПО. WBRS является критической частью базы данных Безопасности Cisco, которая защищает клиентов от смешанных угроз от электронной почты или Веба - трафика.

Использование WBRS SenderBase

WBRS усиливает данные от Базы данных Стандартной безопасности Cisco (Сеть SenderBase®), который является самой большой электронной почтой в мире и сетью мониторинга Веба - трафика. Это отслеживает более чем 50 отдельных параметров, которые являются превосходными индикаторами репутации URL. Со сложным моделированием безопасности и вредоносными агентами обнаружения, Cisco оценивает эти URL на основе этих вводов.

Некоторые параметры включают:

- Данные классификации URL
- Присутствие загружаемого кода
- Присутствие длинных, запутываемых Лицензионных соглашений Конечного пользователя (EULAs)
- Глобальная громкость и изменения в громкости
- Сетевые сведения о владельце

- История URL
- Возраст URL
- Присутствие вируса / спам / шпионское ПО / фишинг / pharming черный список (списки)
- Опечатки URL популярных доменов
- Доменная информация о регистраторе
- Информация о IP-адресе

Глубина детализации WBRS

WBRS отличается от традиционного черного списка URL или белого списка, потому что это анализирует широкий набор данных и производит очень гранулированный счет-10 к +10 вместо двоичных **хороших** или **плохих** классификаций большинства вредоносных приложений обнаружения. Этот гранулированный счет предлагает увеличение гибкости администраторов; другая политика безопасности может быть внедрена на основе другого WBRS выигрывающие диапазоны.