Aperçu de réputation de Web WSA Cisco

Contenu

Introduction

Ce document fournit un aperçu de la réputation de Web de Cisco (WBRS) pour l'appliance de sécurité Web de Cisco (WSA).

Contribué par Josh Wolfer et Stephan Fiebrandt, ingénieurs TAC Cisco.

Aperçu WBRS

WBRS est une méthode innovatrice qui analyse le comportement et les caractéristiques d'un serveur Web et assure la dernière défense dans le combat contre le Spam, les virus, le phishing, et les menaces de logiciel espion.

WBRS emploie l'analyse en temps réel sur un vaste, divers, et global ensemble de données afin de détecter l'URLs qui contiennent une certaine forme de malware. WBRS est un élément essentiel de la base de données de sécurité Cisco, qui protège des clients contre des menaces mélangées d'email ou de trafic web.

Utilisation WBRS de SenderBase

WBRS accroît des données de la base de données de la Sécurité commune de Cisco (réseau de ® de SenderBase), qui est le plus grands email du monde et réseau surveillance de trafic web. Il dépiste plus de 50 paramètres distincts qui sont d'excellents indicateurs de la réputation d'un URL. Avec les agents sophistiqués de détection de modélisation et de malware de Sécurité, Cisco évalue ces l'URLs basé sur ces entrées.

Certains des paramètres incluent :

- Données de catégorisation URL
- Présence de code téléchargeable
- Présence des longs, assombris contrats de licence utilisateurs finaux (CLUF)
- Volume et changements globaux de volume

- Les informations de propriétaire de réseau
- Historique d'un URL
- Âge d'un URL
- Présence de virus/de Spam/de logiciel espion/de phishing/de listes noires pharming
- Typos URL des domaines populaires
- Les informations de registrar de domaine
- Les informations d'adresse IP

Finesse WBRS

WBRS diffère d'une liste noire traditionnelle ou du whitelist URL parce qu'il analyse une large gamme de données et produit une vingtaine fortement granulaire de -10 à +10, au lieu des **bonnes** ou **mauvaises** catégorisations binaires de la plupart des applications de détection de malware. Ce score granulaire offre à des administrateurs le gain de souplesse ; différentes stratégies de sécurité peuvent être mises en application ont basé sur différentes plages de marquage WBRS.