Contenu

Question

L'appliance de sécurité Web de Cisco (WSA) assure-t-elle la protection de malware/logiciel espion ?

L'appliance de sécurité Web de Cisco (WSA) assure la défense la plus complète de la passerelle du secteur contre le logiciel espion et le malware basé sur le WEB. Ceci inclut tout du logiciel publicitaire (qui entraîne les la plupart des questions de prise en charge et consomme les ressources de réseau importantes) à des menaces plus malveillantes telles que chevaux de Troie, des objets d'aide de pirates de l'air de navigateur, de navigateur, le phishing, le Pharming, des moniteurs système, des enregistreurs de frappe, des vers, etc.

Les différentiateurs principaux de la solution de sécurité Web de Cisco incluent :

1. Un moniteur intégré du trafic de la couche 4 (L4) balaye tous les ports à la vitesse du câble, détectant et bloquant l'activité de malware et de téléphone-maison. En dépistant chacun des 65,535 ports de réseau, le moniteur du trafic L4 arrête efficacement le malware que les tentatives de sauter le port 80 et empêche également le P2P escroc et l'IRC activité relative.
2. Traitement de Proxy-couche : L'appliance de sécurité Web de Cisco inclut également extrêmement un proxy de Web de hautes performances, avec la mise en cache intégrée et les capacités satisfaites d'accélération. Construit sur le système d'exploitation propriétaire de Cisco, AsyncOS, l'appliance de proxy de Web de Cisco peut prendre en charge jusqu'à 100,000 connexions simultanées autant que les serveurs proxys basés sur Unix plus que traditionnels 10x. Être un proxy de Web tient compte de l'inspection satisfaite complète à la couche application - une condition requise essentielle vers assurer la précision contre le malware basé sur le WEB.
3. Les premiers filtres de réputation du Web du secteur assurent une couche externe puissante de la défense. Accroissant le ® de SenderBase, les filtres de réputation de Web de Cisco analysent au-dessus du trafic web 50+ différent et des paramètres liés au réseau pour évaluer exactement la fiabilité d'un URL. La Sécurité sophistiquée modelant des techniques sont utilisées pour peser individuellement chaque paramètre et pour générer un score simple sur une échelle de -10 à +10. Les stratégies configurées par administrateur sont dynamiquement appliquées, basé sur des scores de réputation.
4. Lecture accélérée de signature utilisant l'engine dirigeante et coulante dynamique (engine DVS). À la différence des solutions existantes d'architecture qui se fondent sur l'ICAP et un déploiement de multi-case pour assurer la lecture de malware, le WSA de Cisco a introduit l'engine DVS pour une solution intégrée de lecture de sur-case. Cette plate-forme innovatrice utilise l'objet sophistiqué analysant et dirigeant des techniques, avec la mise en cache de lecture de flot et de verdict, ayant pour résultat jusqu'à une augmentation de débit de la lecture 10x au-dessus des solutions ICAP basées sur de première génération.
5. Le système du l'Anti-malware de Cisco de leader accroît l'engine DVS et la signature de

multiple tape de Webroot pour assurer la protection de meilleur contre la plus grande variété de menaces basées sur le WEB. Ces menaces peuvent s'étendre du logiciel publicitaire, des pirates de l'air de navigateur, du phishing et des attaques pharming à des menaces plus malveillantes telles que chevaux de Troie, des moniteurs système et des enregistreurs de frappe. WSA offre la plus grande base de données de signature du malware du secteur à la passerelle.