Sécurité du courrier électronique de Cisco : Compréhension de l'engine adaptative de lecture de contexte (CAS)

Contenu

Introduction

L'augmentation du volume de menaces mélangées a été excessive. Plusieurs des attaques de virus les plus significatives pendant les dernières deux années ont été associées avec la livraison de Spam – la signification de la charge utile de virus crée une armée des ordinateurs de « zombie » – qui sont utilisés pour envoyer le Spam, le phishing, le logiciel espion, et bien plus de virus. le logiciel espion Email-soutenu avait doublé tous les six mois, et il n'est pas rare que l'URLs spammed installe les « enregistreurs de frappe » qui dérobent des noms d'utilisateur et mot de passe. Des virus peuvent même être utilisés pour créer un réseau des zombies pour lancer une attaque massive de déni de service distribué, comme quand la variante Mydoom.B a pris le site Web du SCO off-line avec un assaut coordonné.

Que pilote l'augmentation soudaine des menaces mélangées ? En bref, c'est l'argent. Pendant que des techniques de première génération d'anti-Spam (comme des listes noires et des filtres de contenu) plus largement ont été déployées, les méthodes traditionnelles (comme envoyer le Spam d'une banque fixe des serveurs contenant une « offre » dans le texte du message) sont devenues moins rentables. Avec plus de réseaux utilisant la technique anti-spam, moins messages spam « simples » lui transforment des filtres de Spam de passé et en boîte de réception du destinataire. Ceci blesse les marges plus élevées des spammers et les a forcées pour s'adapter à ces modifications.

Les spammers ont manipulé cette situation de deux manières distinctes :

1. Ils envoient bien plus de Spam avec l'espoir que ce qu'ils perdent en débits de la livraison, ils composeront en volume.
2. Ils se tournent vers des attaques mélangées pour déguiser leurs messages et pour augmenter leur profit par message.

La deuxième technique devient souvent une activité criminelle. Des réseaux de criminalité organisée ont été établis pour exécuter des attaques et pour profiter des virus, du phishing, et d'autres menaces. En 2004, une personne nommée John Douvres a été arrêtée après le

commerce plus de deux millions de numéros de carte de crédit, qui ont été dérobés par des attaques par phishing.

Les techniques utilisées dans des attaques mélangées sont également devenues de plus en plus sophistiquées. L'email Sober.N, les téléchargements de Web, les chevaux de Troie, et les zombies employés par virus. Les filtres traditionnels d'analyse du contenu ne sont aucune correspondance pour ces menaces intelligentes. Beaucoup d'utilisateurs des filtres de première génération d'anti-Spam ont constaté qu'ils doivent passer des heures croissantes « formant » leurs filtres ou écrivant de nouvelles règles. Cependant, en dépit de ces efforts, leur taux de capture et débit sont tous deux qui refusent. Le résultat est que les coûts font suivre pendant que plus de systèmes sont exigés pour suivre le chargement, alors que plus de temps de gestion est utilisé de gérer chaque système.

La sécurité du courrier électronique de Cisco a adressé ces menaces avec une seule technologie mélangée de défense contre des menaces connue sous le nom d'engine adaptative de lecture de contexte (CAS). La technologie du CAS de la sécurité du courrier électronique de Cisco est utilisée pour arrêter le Spam traditionnel et les attaques basées sur zombie sophistiquées. Cette même technologie de lecture est également utilisée pour empêcher des virus et le malware pas moins de 42 heures en avant de Disponibilité de signature – avec un balayage unifié simple pour l'efficacité.

Compréhension du CAS, détectant des menaces mélangées dans le contexte

Des filtres de première génération ont été conçus pour regarder le contenu d'un message et pour faire une détermination. Par exemple, si le mot « libre » apparaissait dans un message plus de deux fois, avec le mot « de fines herbes, » c'était probablement Spam. Il est relativement facile pour des spammers défaire cette approche à l'aide des caractères ou des nombres masqués au lieu des lettres, telles que « f0r y0u » au lieu de « pour vous. » Techniques de la seconde génération, comme les filtres bayésiens, tentés pour adresser cette limite en apprenant pour différencier les caractéristiques du Spam et pour légitimer l'email automatiquement. Mais ces techniques ont prouvé trop la remise en question à s'exercer, à réagir trop tard, et à ralentir trop pour balayer.

Etant donné les techniques avancées d'obscurcissement utilisées avec le Spam d'aujourd'hui, les filtres de pointe doivent examiner la messagerie entrante dans le plein contexte. Le CAS utilise les techniques d'apprentissage automatique avancées qui émulent la logique utilisée par un humain qui évalue la légitimité d'un message. Un lecteur humain, aussi bien que la technologie du CAS de la sécurité du courrier électronique de Cisco, pose quatre questions fondamentales :

1. Qui m'a envoyé le message ?
2. Où les liens dans le message me prennent ?
3. Comment le message a-t-il été construit ?
4. Que le message contient-il ?

Pour suivre est un examen de chaque zone logique évaluée.

Qui ?

En tant que filtres plus tôt et de première génération indiqués de Spam a compté principalement sur des recherches par mot clé pour identifier le Spam. En 2003, Cisco (IronPort) a révolutionné le

secteur de sécurité du courrier électronique en introduisant le concept du filtrage de réputation. Tandis que le filtrage selon le contenu posait la question, « qu'est dans le message ? », le filtrage de réputation pose la question, « qui a envoyé le message ? ». Ce concept simple mais puissant a élargi le contexte par lequel des menaces sont évaluées. D'ici 2005, presque chaque principal constructeur commercial de Sécurité avait adopté un certain type de système de réputation.

La détermination de la réputation implique d'examiner une large gamme de données au sujet du comportement d'un expéditeur donné (un expéditeur est défini comme adresse IP envoyant la messagerie). Cisco considère plus de 120 paramètres différents, y compris le volume d'email au fil du temps, le nombre de « Spam emprisonne » le hit par cet IP, pays d'origine, si l'hôte est compromis, et beaucoup plus. Cisco a une équipe de statisticiens qui développent et mettent à jour les algorithmes, qui traitent ces données pour générer un score de réputation. Ce score de réputation est alors rendu disponible à l'appliance de réception de sécurité du courrier électronique de Cisco (ESA), qui peut alors étrangler un expéditeur basé sur leur fiabilité. En bref – le « spammy » un expéditeur apparaît, plus il va lentement. La réputation filtrant également aborde les problèmes associés avec les volumes de augmentation d'email par les connexions de rejet ou de étranglement avant que le message soit reçu, de ce fait améliorant spectaculairement la performance et la Disponibilité du système de messagerie. Les filtres de réputation de Cisco ESA arrêtent plus de 80 pour cent de Spam entrant, approximativement deux fois le taux de capture de systèmes de concurrence.

Où ?

Tandis que la combinaison de l'analyse du contenu et de la réputation d'email était de pointe en 2003, la complexité de la tactique de l'auteur du spammer et du virus continue à se développer. Dans la réponse, Cisco (IronPort) a introduit la notion de la réputation de Web – un nouveau vecteur essentiel pour élargir le contexte dans lequel un message est évalué. Semblable à l'approche utilisée en calculant la réputation d'un email, la réputation de Web de Cisco regarde plus de 45 paramètres associés par serveur pour évaluer la réputation de n'importe quel URL donné. Les paramètres incluent le volume de demandes de HTTP à l'URL au fil du temps, si l'URL est hébergé sur une adresse IP avec un score pauvre de réputation, si cet URL est associé avec une « zombie » connue ou hôte infecté PC, et l'âge du domaine utilisé par l'URL. Comme avec la réputation d'email, cette réputation de Web est mesurée utilisant un score granulaire, qui permet au système pour traiter les ambiguïtés des menaces sophistiquées.

Comment ?

Une autre approche nouvelle à l'analyse contextuelle de la sécurité du courrier électronique de Cisco est d'examiner la construction d'un message. Les clients mail légitimes, tels que Microsoft Outlook, construisent des messages des façons uniques – utilisant le codage MIME, le HTML, ou d'autres moyens semblables. Un examen de la construction d'un message peut indiquer beaucoup au sujet de sa légitimité. Dire l'exemple de ceci se produit quand des essais d'un serveur de Spam pour émuler la construction d'un client mail légitime. Il est difficile faire ce, et une émulation imparfaite est un indicateur fiable d'un message illégitime.

Ce qui ?

Une analyse contextuelle complète doit considérer le contenu d'un message, mais, en tant que première, analyse du contenu remarquable seule n'est pas une approche suffisante à identifier la messagerie illégitime. La technologie du CAS de la sécurité du courrier électronique de Cisco exécute l'analyse du contenu complète, utilisant des techniques d'apprentissage automatique de

pointe. Ces techniques examinent le contenu du message et le marquent dans diverses catégories – est-ce financier, pornographique, ou contient-il le contenu qui est connu pour le corréler avec l'autre Spam ? Cette analyse du contenu est factorisée dans le CAS avec les autres attributs – qui, où, comment, et ce qui – pour évaluer le plein contexte du message.

CAS dans l'action

En raison de la largeur des données analysées par CAS, la technologie est utilisée dans un grand choix d'applications sécurité – comprenant l'anti-Spam d'IronPort (IPAS), le Graymail, et les filtres d'attaque de virus (VOF). L'exemple au-dessous des points culminants comment le CAS est utilisé pour arrêter le Spam. Le contenu de message est presque identique à obtenir d'organisation phished, ainsi l'analyse du contenu du message n'identifierait aucune menace. Aux filtres basés sur contenu, ce message semble être une transmission légitime. Pour déterminer si ce message est Spam, filtres qui se fondent principalement sur « ce que » pourrait facilement être dupé dans identifier le message comme légitime. Cependant, une analyse du plein contexte du message peint un tableau différent.

- L'adresse IP du serveur de messagerie de envoi est méfiante – elle a eu une surtension soudaine dans le volume, et le domaine, en échange, ne reçoit pas la messagerie.
- L'URL de l'email indique un serveur qui semble être dans un réseau haut débit du consommateur.
- L'URL annoncé dans le message est différent de l'URL de « effectif » que l'utilisateur est navigué vers en cliquant sur sur le lien.

Quand chacun des trois de ces facteurs est considéré dans le contexte, il apparaît clairement que ce n'est pas un message légitime, mais est, en fait, une attaque de Spam.

Traditionnels « filtres satisfaits »
Quels FILTRES SATISFAITS les trouvent

Ce qui ? Contenu du message légitime.

Verdict : UNKNOWN

Lecture adaptative de contexte
Quel CAS le trouve

Ce qui ? Contenu du message légitime.
Comment ? La construction de message émule le client de Microsoft Outlook.
Qui ?
1) une surtension soudaine en volume d'email éta envoyé.
2) En échange, le serveur de messagerie ne reçc la messagerie.
3) Serveur de messagerie situé dans l'Ukraine.

Où ?
1) l'ismatch heure du matin entre l'affichage et le domaine de site Web URL de cible s'est enregistr a un jour.
2) site Web hébergé sur le réseau haut débit du consommateur.
3) Les données « WHOIS » affichent le propriétai domaine comme spammer connu.

Verdict : BLOC

Quand le CAS est utilisé dans des filtres d'attaque de virus, les mêmes capacités de marquage et

d'apprentissage automatique sont appliquées – quoiqu'à un poste de données séparément accordé. Les filtres d'attaque de virus sont une solution préventive d'antivirus offerte par Cisco et actionnée par la technologie de CAS. L'épidémie filtre des messages de balayages de solution contre des règles « en temps réel » d'épidémie (émises par des épidémies spécifiques de Cisco Talos) et des règles adaptatives « illimitées » (que résidez sur le CAS à tout moment), protégeant des utilisateurs contre des épidémies avant qu'ils aient eu une occasion de former entièrement. ENFERMEZ les filtres d'attaque de virus d'enables pour le détecter et se protéger contre des attaques de virus de plusieurs manières exactement. D'abord, le CAS peut rapidement balayer des messages basés sur des paramètres tels que l'extension de fichier de la connexion, de la taille de fichier, du nom du fichier, des mots clé de nom du fichier, du Magic de fichier (l'extension réelle d'un fichier), et de l'URLs encastré. Puisque la technologie de CAS analyse des messages à ce niveau de précision, Cisco Talos peut émettre les règles extrêmement granulaires d'épidémie, qui se protègent exactement contre une épidémie avec les faux positifs minimaux. Le CAS peut dynamiquement recevoir des règles mises à jour d'épidémie, qui s'assure qu'il se protège contre les dernières épidémies.

En plus de l'analyse des messages basés sur des règles d'épidémie, la technologie de CAS balaye également des messages basés sur des règles adaptatives. Les règles adaptatives sont heuristique et algorithmes finement accordés qui examinent des messages entrant pour des caractéristiques de malformation et de mystification indicatives des virus. En plus de ces paramètres, l'adaptatif ordonne des messages de score basés sur leur score de virus de SenderBase (SBVS). SBVS est un score semblable à un score de réputation de SenderBase (SBRS), mais avec un classement basé sur la probabilité que l'interlocuteur de envoi envoie aux emails viraux, plutôt que le Spam. Une majorité d'email viral est envoyée par les ordinateurs précédemment infectés de « zombie », ainsi identifier et marquer ces interlocuteurs de envoi est un facteur essentiel dans les virus contagieux.

La technologie du CAS de la sécurité du courrier électronique de Cisco permet à des filtres d'attaque de virus d'arrêter des attaques de virus bien avant les solutions traditionnelles d'antivirus parce que le CAS examine des messages de plusieurs manières. Il a la capacité d'analyser de nombreuses caractéristiques des connexions de message, le contenu du message, et la construction de message, aussi bien que la capacité d'analyser des messages basés sur leur réputation d'expéditeur. Et, parce que le CAS agit également en tant qu'anti-Spam d'IronPort et engine de filtres de réputation, les besoins d'un message seulement d'être balayé une fois pour toutes de ces applications.

Hautes performances, coût réduit

La logique derrière la technologie de CAS peut être très sophistiquée, et donc très CPU intensive traiter. Pour maximiser l'efficacité, le CAS utilise une seule technologie de « première sortie ». La première sortie donne la priorité à l'efficacité des règles innombrables traitée par CAS. La technologie de CAS exécute les règles avec la première le plus à haute impression et le plus peu coûteux. Si un verdict statistique est atteint (si positif ou négatif), aucune règle supplémentaire n'est exécutée, enregistrant des ressources système. L'élégance dans cette approche a une bonne compréhension de l'efficacité de chaque règle. ENFERMEZ automatiquement les moniteurs et adaptez la commande de l'exécution de règle comme l'efficacité change.

Le résultat de la première sortie est que la technologie de CAS traite des messages approximativement 100 pour cent de plus rapide qu'un filtre basé sur les règles traditionnel. Ceci a des avantages distincts pour de grands ISP et entreprises. Mais il a également des avantages pour des PMEs. L'efficacité du CAS, ajoutée à l'efficacité du système d'exploitation d'AsyncOS de la sécurité du courrier électronique de Cisco, signifie qu'ESAs avec AsyncOS et technologie de

CAS peut être mis en application sur le matériel très bon marché – entraînant une réduction des frais financiers.

Une autre manière que la technologie de CAS se traduit au coût réduit est en éliminant des frais d'administration. La CAISSE est accordée et mise à jour automatiquement, des milliers de périodes chaque jour. Cisco Talos fournit les ingénieurs qui sont formés, les techniciens multilingues, et les statisticiens. Les analystes de Cisco Talos ont des outils spéciaux qui mettent en valeur des anomalies dans le flux de courrier détecté dans le réseau de n'importe quel de Cisco client de sécurité du courrier électronique, ou des structures de trafic globales d'email. Cisco Talos génère les nouvelles règles qui sont automatiquement poussées au système en temps réel. Cisco Talos met à jour également un corpus massif de « Spam et de jambon, » qui est utilisé pour former de diverses règles utilisées par CAS. Les règles automatiquement à jour de CAS signifient que les administrateurs ne doivent pas être accordants et tordants le filtre ou passants le temps pataugeant par des quarantaines de Spam.

Résumé

Le Spam, les virus, le malware, le logiciel espion, les attaques par déni de service, et les attaques tous de récolte de répertoire sont pilotés par le même motif sous-jacent – des profits. Ces profits sont atteints par la vente ou la publicité de l'article ou le vol des informations. Les profits de ces ventes pilotent des attaques de plus en plus sophistiquées, développées par les ingénieurs professionnels. Les systèmes de sécurité du courrier électronique avancés doivent analyser un message dans le plus large possible contexte pour parer ces menaces. La technologie adaptative d'engine de lecture du contexte de la sécurité du courrier électronique de Cisco pose les quatre questions fondamentales : Qui, où, ce qui, et comment – pour sarcler les messages légitimes des menaces mélangées.

- « Qui » est la réputation d'email de l'expéditeur – qui a envoyé le message.
- « Où » est la réputation de la source accueillant le site Web – analysant où le lien vous prendrait.
- « Ce que » est une analyse du contenu du message – ce que le message contient (les systèmes de première génération souvent comptez seulement sur » ce qui » type d'analyse).
- En conclusion, « comment » est une analyse de la façon dont le message est construit.

Ce cadre de base d'analyser qui, où, ce qui, et comment travaux aussi bien pour arrêter le Spam comme il fait pour empêcher des attaques de virus, des attaques par phishing, logiciel espion email-soutenu, ou autre menaces d'email. Les postes de données et les ensembles de règles d'analyse sont accordés spécifiquement pour chaque menace. La technologie de CAS permet à Cisco ESA pour arrêter la plus large plage des menaces avec l'efficacité plus élevée possible en traitant ces menaces sur une engine performante simple.