# Sécurité de la messagerie Cisco : Présentation de Context Adaptive Scanning Engine (CASE)

## Table des matières


Introduction

Présentation de CASE, détection des menaces mixtes dans leur contexte

- Qui ?
- Where?
- Comment ?
- Quoi ?

AFFAIRE en instance

Hautes performances, faible coût

Résumé


## Introduction

L'augmentation du volume des menaces combinées a été spectaculaire. La plupart des attaques virales les plus importantes des deux dernières années ont été associées à l'envoi de spams (ce qui signifie que la charge utile du virus crée une armée d'ordinateurs « zombies ») qui sont utilisés pour envoyer du spam, du phishing, des logiciels espions et bien d'autres virus. Les logiciels espions véhiculés par les e-mails doublent tous les six mois et il n'est pas rare que les URL de spam installent des « enregistreurs de frappe » qui volent des noms d'utilisateur et des mots de passe. Les virus peuvent même être utilisés pour créer un réseau de zombies pour lancer une attaque massive par déni de service distribué, comme lorsque la variante Mydoom.B a déconnecté le site Web de SCO avec une attaque coordonnée.

Quelle est la cause de l'augmentation soudaine des menaces combinées ? En bref, c'est l'argent qui compte. Alors que les techniques antispam de première génération (comme les listes noires et les filtres de contenu) ont été plus largement déployées, les méthodes traditionnelles (comme l'envoi de spam à partir d'une banque fixe de serveurs contenant une « offre » dans le texte du message) sont devenues moins rentables. Avec un plus grand nombre de réseaux utilisant la technologie antispam, un nombre moins important de messages de spam « simples » passent les filtres antispam et arrivent dans la boîte de réception du destinataire. Cela nuit aux marges bénéficiaires des spammeurs et les oblige à s'adapter à ces changements.

Les spammeurs ont géré cette situation de deux manières différentes :

1. Ils envoient encore plus de spam avec l'espoir que ce qu'ils perdent dans les taux de livraison, ils rattraperont en volume.
2. Ils se tournent vers des attaques mixtes pour masquer leurs messages et augmenter leur profit par message.

La seconde technique devient souvent une activité criminelle. Des réseaux criminels organisés ont été mis en place pour lancer des attaques et tirer profit des virus, du phishing et d'autres menaces. En 2004, un individu nommé John Dover a été arrêté après avoir échangé plus de deux millions de numéros de carte de crédit, qui ont été volés par des attaques de phishing.

Les techniques utilisées dans les attaques combinées sont également devenues de plus en plus sophistiquées. Le virus Sober.N utilisait la messagerie électronique, les téléchargements Web, les chevaux de Troie et les zombies. Les filtres d'analyse de contenu traditionnels ne correspondent pas à ces menaces intelligentes. De nombreux utilisateurs de filtres antispam de première génération ont constaté qu'ils devaient passer de plus en plus d'heures à « former » leurs filtres ou à rédiger de nouvelles règles. Cependant, malgré ces efforts, leur taux de capture et leur débit sont tous deux en baisse. Il en résulte que les coûts augmentent à mesure que davantage de systèmes sont nécessaires pour faire face à la charge, tandis que plus de temps d'administration est nécessaire pour gérer chaque système.

La solution de sécurisation de la messagerie Cisco a permis de contrer ces menaces grâce à une technologie unique de protection contre les menaces, appelée CASE (Context Adaptive Scanning Engine). La technologie CASE de Cisco Email Security est utilisée pour stopper à la fois le spam traditionnel et les attaques sophistiquées basées sur les zombies. Cette même technologie d'analyse est également utilisée pour empêcher les virus et les programmes malveillants jusqu'à 42 heures avant la disponibilité des signatures, avec une seule analyse unifiée pour une meilleure efficacité.

## Présentation de CASE, détection des menaces mixtes dans leur contexte

Les filtres de première génération ont été conçus pour examiner le contenu d'un message et prendre une décision. Par exemple, si le mot « gratuit » apparaît plus de deux fois dans un message, avec le mot « à base de plantes », il s'agit probablement d'un spam. Cette approche est relativement facile pour les spammeurs à vaincre en utilisant des caractères cachés ou des chiffres au lieu de lettres, comme «f0r y0u» à la place de «pour vous.» Les techniques de deuxième génération, telles que les filtres bayésiens, ont tenté de remédier à cette limitation en apprenant à différencier automatiquement les caractéristiques du spam et des e-mails légitimes. Mais ces techniques se sont avérées trop difficiles à former, trop tardives pour réagir et trop lentes à analyser.

Étant donné les techniques d'obscurcissement avancées utilisées avec le spam actuel, les filtres de pointe doivent examiner le courrier entrant dans son intégralité. CASE utilise des techniques avancées d'apprentissage automatique qui émulent la logique utilisée par un humain qui évalue la légitimité d'un message. Un lecteur humain, ainsi que la technologie CASE de Cisco Email Security, pose quatre questions de base :

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

Pour suivre est un examen de chaque domaine logique évalué.

## Qui ?

Comme indiqué précédemment, les filtres antispam de première génération s'appuyaient principalement sur des recherches par mot-clé pour identifier le spam. En 2003, Cisco (IronPort) a révolutionné le secteur de la sécurité de la messagerie en introduisant le concept de filtrage par réputation. Alors que le filtrage du contenu posait la question « Qu'est-ce que contient le message ? », le filtrage par réputation posait la question « Qui a envoyé le message ? ». Ce concept simple mais puissant élargit le contexte d'évaluation des menaces. En 2005, presque tous les grands fournisseurs de solutions de sécurité avaient adopté un système de réputation.

La détermination de la réputation implique l'examen d'un large ensemble de données relatives au comportement d'un expéditeur donné (un expéditeur est défini comme une adresse IP qui envoie un courrier). Cisco prend en compte plus de 120 paramètres différents, notamment le volume d'e-mails au fil du temps, le nombre de « pièges à spam » détectés par cette adresse IP, le pays d'origine, l'éventuelle compromission de l'hôte, etc. Cisco dispose d'une équipe de statisticiens qui développent et gèrent des algorithmes qui traitent ces données pour générer un score de réputation. Ce score de réputation est ensuite mis à la disposition de l'appliance de sécurité de la messagerie électronique (ESA) qui peut alors contrôler un expéditeur en fonction de sa fiabilité. En bref, plus un expéditeur apparaît comme un spammeur, plus il ralentit. Le filtrage par réputation résout également les problèmes associés à l'augmentation des volumes de courriers électroniques en rejetant ou en limitant les connexions avant que le message ne soit accepté, ce qui améliore considérablement les performances et la disponibilité du système de messagerie. Les filtres de réputation Cisco ESA bloquent plus de 80 % du spam entrant, soit environ deux fois le taux de capture des systèmes concurrents.

## Where?

Alors que l'association de l'analyse du contenu des e-mails et de la réputation était à la pointe de la technologie en 2003, la sophistication des tactiques des spammeurs et des développeurs de virus ne cesse de croître. En réponse, Cisco (IronPort) a introduit la notion de réputation Web, un nouveau vecteur essentiel pour élargir le contexte dans lequel un message est évalué. À l'instar de l'approche utilisée pour calculer la réputation d'un e-mail, Cisco Web Reputation examine plus de 45 paramètres liés au serveur pour évaluer la réputation d'une URL donnée. Les paramètres incluent le volume de requêtes HTTP vers l'URL au fil du temps, si l'URL est hébergée sur une adresse IP avec un score de réputation médiocre, si cette URL est associée à un hôte PC « zombie » ou infecté connu, et l'âge du domaine utilisé par l'URL. Comme pour la réputation des e-mails, cette réputation Web est mesurée à l'aide d'un score granulaire, qui permet au système de gérer les ambiguïtés des menaces sophistiquées.

## Comment ?

Une autre approche innovante de l'analyse contextuelle de Cisco Email Security consiste à examiner la construction d'un message. Les clients de messagerie légitimes, tels que Microsoft Outlook, créent des messages de manière unique, en utilisant le codage MIME, HTML ou d'autres

moyens similaires. L'examen de la construction d'un message peut révéler beaucoup de choses sur sa légitimité. Un exemple très révélateur de cela se produit quand un serveur de spam essaie d'émuler la construction d'un client de messagerie légitime. C'est difficile à faire, et une émulation imparfaite est un indicateur fiable d'un message illégitime.

### Quoi ?

Une analyse contextuelle complète doit tenir compte du contenu d'un message, mais, comme nous l'avons déjà mentionné, l'analyse du contenu ne suffit pas à elle seule à identifier le courrier illégitime. La technologie CASE de Cisco Email Security effectue une analyse complète du contenu, à l'aide de techniques d'apprentissage automatique de pointe. Ces techniques examinent le contenu du message et le classent dans différentes catégories : est-il financier, pornographique ou contient-il du contenu connu pour être en corrélation avec d'autres courriers indésirables ? Cette analyse de contenu est prise en compte dans CASE avec les autres attributs - Qui, Où, Comment et Quoi - pour évaluer le contexte complet du message.

## AFFAIRE en instance

En raison de l'étendue des données analysées par CASE, la technologie est utilisée dans diverses applications de sécurité, notamment IronPort Anti-Spam (IPAS), Graymail et Virus Outbreak Filters (VOF). L'exemple ci-dessous illustre l'utilisation de CASE pour bloquer le spam. Le contenu du message est presque identique à celui de l'entreprise qui a été victime d'un hameçonnage, de sorte que l'analyse du contenu du message n'identifie aucune menace. Pour les filtres basés sur le contenu, ce message semble être une communication légitime. Pour déterminer si ce message est du spam ou non, les filtres qui s'appuient principalement sur le « Quoi » peuvent facilement être trompés et faire reconnaître le message comme légitime. Cependant, une analyse du contexte complet du message donne une image différente.

- L'adresse IP du serveur de messagerie expéditeur est suspecte : il a connu une augmentation soudaine du volume et le domaine, en retour, n'accepte pas le courrier.
- L'URL de l'e-mail pointe vers un serveur qui semble se trouver dans un réseau haut débit grand public.
- L'URL annoncée dans le message est différente de l'URL « réelle » vers laquelle l'utilisateur est dirigé lorsqu'il clique sur le lien.

Lorsque ces trois facteurs sont pris en compte dans le contexte, il apparaît clairement qu'il ne s'agit pas d'un message légitime, mais bien d'une attaque de spam.

| « Filtres de contenu » traditionnels<br><br>Que recherchent les FILTRES DE CONTENU | Analyse contextuelle adaptative<br><br>Ce que CASE trouve |
|---|---|
| Quoi ? Contenu du message légitime. | Quoi ? Contenu du message légitime. |

<table>
<tr>
<td>
</td>
<td>Comment ? La construction du message émule le client Microsoft Outlook.<br><br>Qui ?<br><br>1) Une soudaine augmentation du volume d'e-mails envoyés.<br><br>2) En retour, le serveur de messagerie n'accepte pas les messages.<br><br>3) Serveur de messagerie situé en Ukraine.<br><br>Where?<br><br>1) Une incohérence entre le domaine du site Web d'affichage et d'URL cible enregistré il y a un jour.<br><br>2) Site Web hébergé sur un réseau haut débit grand public.<br><br>3) Les données « Whois » indiquent que le propriétaire du domaine est un spammeur connu.</td>
</tr>
<tr>
<td>Verdict : INCONNU</td>
<td>Verdict : BLOCK</td>
</tr>
</table>

Lorsque CASE est utilisé dans les filtres contre les attaques de virus, les mêmes fonctions de notation et d'apprentissage automatique sont appliquées, mais à un ensemble de données réglé séparément. Les filtres contre les attaques de virus sont une solution antivirus préventive proposée par Cisco et optimisée par la technologie CASE. La solution Outbreak Filters analyse les messages en fonction des règles d'attaque « en temps réel » (émises par les attaques spécifiques de Cisco Talos) et des règles adaptatives « toujours actives » (qui résident sur CASE à tout moment), protégeant ainsi les utilisateurs contre les attaques avant qu'ils n'aient pu se former complètement. CASE permet aux filtres contre les attaques de virus de détecter les attaques de virus et de les protéger de plusieurs façons précises. Tout d'abord, CASE peut analyser rapidement les messages en fonction de paramètres tels que l'extension de la pièce jointe, la taille du fichier, le nom du fichier, les mots-clés du nom du fichier, la magie du fichier (l'extension réelle d'un fichier) et les URL intégrées. Comme la technologie CASE analyse les messages avec ce niveau de détail, Cisco Talos peut émettre des règles d'attaque extrêmement précises, qui protègent précisément contre une attaque avec un minimum de faux positifs. CASE peut recevoir

des règles d'attaque mises à jour de manière dynamique, ce qui garantit une protection contre les dernières attaques.

Outre l'analyse des messages basée sur les règles d'attaque, la technologie CASE analyse également les messages basés sur les règles adaptatives. Les règles adaptatives sont des heuristiques et des algorithmes finement paramétrés qui examinent les messages entrants à la recherche de caractéristiques de malformation et d'usurpation indiquant la présence de virus. En plus de ces paramètres, les règles adaptatives notent les messages en fonction de leur score de virus SenderBase (SBVS). SBVS est un score similaire à SenderBase Reputation Score (SBRS), mais avec un classement basé sur la probabilité que l'expéditeur envoie des e-mails viraux, plutôt que du spam. La majorité des e-mails viraux sont envoyés par des machines « zombies » précédemment infectées. Par conséquent, l'identification et la notation de ces expéditeurs constituent un facteur essentiel dans la détection des virus.

La technologie CASE de Cisco Email Security permet aux filtres contre les attaques de virus d'arrêter les attaques de virus bien avant les solutions antivirus traditionnelles, car le filtre CASE examine les messages de plusieurs manières. Il est capable d'analyser de nombreuses caractéristiques des pièces jointes, du contenu et de la construction des messages, ainsi que d'analyser les messages en fonction de leur réputation. Et, comme CASE agit également comme moteur antispam et filtres de réputation IronPort, un message ne doit être analysé qu'une seule fois pour toutes ces applications.

## Hautes performances, faible coût

La logique sous-jacente à la technologie CASE peut être très sophistiquée et donc très gourmande en CPU à traiter. Pour optimiser l'efficacité, CASE utilise une technologie unique de « sortie anticipée ». La sortie anticipée donne la priorité à l'efficacité de la multitude de règles traitées par CASE. La technologie CASE exécute les règles avec le plus grand impact et le coût le plus faible en premier. Si un verdict statistique est atteint (qu'il soit positif ou négatif), aucune règle supplémentaire n'est exécutée, ce qui permet d'économiser des ressources système. L'élégance de cette approche est d'avoir une bonne compréhension de l'efficacité de chaque règle. CASE surveille et adapte automatiquement l'ordre d'exécution des règles à mesure que l'efficacité change.

La technologie CASE traite les messages environ 100 % plus rapidement qu'un filtre traditionnel basé sur des règles. Cela présente des avantages distincts pour les grands FAI et les grandes entreprises. Mais elle présente également des avantages pour les petites et moyennes entreprises. L'efficacité de CASE, associée à l'efficacité du système d'exploitation AsyncOS de Cisco Email Security, permet de mettre en oeuvre des ESA avec AsyncOS et la technologie CASE sur du matériel très économique, ce qui réduit les coûts d'investissement.

La technologie CASE permet également de réduire les coûts en éliminant les frais d'administration. CASE est réglé et mis à jour automatiquement, des milliers de fois par jour. Cisco Talos met à votre disposition des ingénieurs formés, des techniciens multilingues et des statisticiens. Les analystes de Cisco Talos disposent d'outils spéciaux qui mettent en évidence les anomalies dans le flux de messages détectées sur le réseau de tout client de Cisco Email Security, ou les modèles de trafic de messagerie mondial. Cisco Talos génère de nouvelles règles

qui sont automatiquement envoyées au système en temps réel. Cisco Talos dispose également d'un vaste corpus de « spam and ham », qui sert à former diverses règles utilisées par CASE. Grâce aux règles CASE mises à jour automatiquement, les administrateurs n'ont plus à ajuster et à peaufiner le filtre ni à passer du temps à se faufiler dans les quarantaines de spam.

## Résumé

Le spam, les virus, les programmes malveillants, les logiciels espions, les attaques par déni de service et les attaques par extraction de répertoire sont tous motivés par le même motif sous-jacent : les bénéfices. Ces bénéfices sont obtenus soit par la vente ou la publicité de marchandises, soit par le vol d'informations. Les bénéfices de ces ventes entraînent des attaques de plus en plus sophistiquées, développées par des ingénieurs professionnels. Les systèmes avancés de sécurité de la messagerie électronique doivent analyser un message dans le contexte le plus large possible pour contrer ces menaces. La technologie Context Adaptive Scanning Engine de Cisco Email Security pose les quatre questions de base suivantes : Qui, où, quoi et comment - pour éliminer les messages légitimes des menaces combinées.

- « Qui » est la réputation de l'expéditeur du message par e-mail.
- « Où » correspond à la réputation de la source qui héberge le site Web, c'est-à-dire qu'elle analyse où le lien vous mènerait.
- « Quoi » est une analyse du contenu du message - ce que le message contient (les systèmes de première génération se basent souvent uniquement sur le type d'analyse « Quoi »).
- Enfin, « Comment » est une analyse de la façon dont le message est construit.

Ce cadre de base d'analyse de qui, où, quoi et comment fonctionne aussi bien pour stopper le spam que pour prévenir les attaques de virus, les attaques par phishing, les logiciels espions véhiculés par e-mail ou d'autres menaces. Les ensembles de données et les ensembles de règles d'analyse sont réglés spécifiquement pour chaque menace. La technologie CASE permet à Cisco ESA d'arrêter le plus grand nombre de menaces avec la plus grande efficacité possible en traitant ces menaces sur un seul moteur hautes performances.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.