WHITE PAPER

Pourquoi vous avez besoin d'un moteur de détection d'exploit

Les sociétés doivent renforcer leur protection antivirale pour une sécurité optimale

Ce document explique ce que sont les exploits d'email, fournit des exemples d'exploits d'emails courants, et pourquoi une approche non basée sur une signature (par ex., qui n'est pas basée sur un moteur anti-viral) est nécessaire pour se protéger contre les exploits d'emails.

Introduction

Les auteurs de virus emploient des techniques de plus en plus complexes et sophistiquées pour contourner la protection antivirus et diffuser leurs virus. Nimda, par exemple, virus d'une triste notoriété, a employé de multiples méthodes de diffusion et était basé sur un exploit et non sur un code malveillant. Les utilitaires de sécurisation de messagerie doivent évoluer dans ce sens afin de bloquer les menaces avant qu'elles ne puissent nuire. L'antivirus classique, bien qu'il reste un élément essentiel, ne peut combattre efficacement de telles menaces ; c'est pourquoi un outil de détection d'exploit via email est nécessaire.

Qu'est-ce qu'un exploit?

C'est l'exploitation des vulnérabilités connues au sein des applications ou des systèmes d'exploitation pour exécuter un programme. Il « exploite » la particularité d'un programme ou d'un système d'exploitation à ses propres fins, comme exécuter des programmes bien précis, lire/écrire des fichiers sur le disque dur, ou pénétrer illicitement un réseau.

Qu'est-ce qu'un exploit via email?

C'est une intrusion via la messagerie. Un exploit d'email peut être contenu dans un email et exécuté sur la machine du destinataire une fois que l'utilisateur ouvre ou reçoit le message. Cela permet au pirate informatique de contourner les pare-feux et les antivirus.

Différences entre un logiciel antivirus et un logiciel de détection d'exploit

Les logiciels antivirus sont conçus pour détecter du code malicieux connu. Un moteur anti-exploit de messagerie adopte une approche différente : il analyse le code à la recherche d'exploits POTENTIELLEMENT malicieux. Cela signifie qu'il protège contre les nouveaux virus, et principalement contre les virus/codes malicieux INCONNUS. Ceci est crucial car un virus inconnu peut tout aussi bien être un morceau de code unique, développé tout particulièrement pour pénétrer dans votre réseau.

Le logiciel de détection d'exploits de messagerie recherche les exploits dans les messages email - c'est-à-dire qu'il recherche les méthodes utilisées pour exploiter le système d'exploitation, le client email ou Internet Explorer - qui peuvent permettre l'exécution de code ou d'un programme sur le système de l'utilisateur. Il ne vérifie pas si le programme est malicieux ou non. Il suppose simplement qu'il existe un risque de sécurité si un email utilise un exploit destiné à exécuter un programme ou une portion de code.

De cette manière, un moteur anti-exploit de messagerie fonctionne comme un système de détection d'intrusion (SDI) pour la messagerie. Le moteur anti-exploit de messagerie peut créer plus de faux positifs, mais il ajoute une nouvelle couche de protection qui n'est pas disponible sur un progiciel antivirus normal, simplement parce qu'il utilise une façon totalement différente de sécuriser la messagerie.

Les moteurs d'antivirus protègent contre certains exploits mais ils ne procèdent pas à une vérification de tous les exploits ou de toutes les attaques. Un moteur de détection d'exploit vérifie tous les exploits connus. Du fait que le moteur d'exploits d'emails est optimisé pour rechercher et trouver tous les exploits dans les emails, il peut donc être plus efficace dans son travail qu'un moteur antivirus général.

Moins de mises à jour pour les moteurs d'anti-exploits

Un moteur anti-exploit ne doit pas être mis à jour aussi souvent qu'un moteur antivirus, parce qu'il recherche des méthodes plutôt que des virus spécifiques. Bien que les mises à jour des moteurs anti-exploits et antivirus soient très semblables, les résultats sont différents. Une fois qu'un exploit a été reconnu et incorporé dans le moteur anti-exploits, ce moteur peut vous protéger contre tout nouveau virus basé sur un exploit connu. Cela signifie que le moteur anti-exploit arrêtera le virus avant même que le fournisseur d'anti-virus soit au courant de son arrivée, et certainement avant que les fichiers de spécification antivirus aient été mis à jour pour contrer l'attaque. Cela est un avantage crucial, comme le montrent les exemples suivants qui se sont passés en 2001.

Les leçons tirées de Nimda, BadTrans.B, Yaha et Bugbear

Nimda et BadTrans.B, virus mondialement connus de l'année 2001, ont infecté un nombre colossal d'ordinateurs Windows connectés à l'Internet. Nimda a, à lui seul, infecté 8,3 millions d'ordinateurs à l'échelle mondiale, selon les estimations de la société américaine Computer Economics en Novembre 2001

Nimda est un ver qui emploie de multiples méthodes pour infecter automatiquement d'autres ordinateurs. Il peut se reproduire par email en exploitant une faille publiée plusieurs mois avant que Nimda ne frappe ; l'exploit d'en-tête MIME BadTrans.B est un ver de publipostage qui se diffuse en utilisant également l'exploit d'en-tête MIME. Il est apparu pour la première fois après

la percée de Nimda.

La rapidité de diffusion de Nimda et BadTrans.B a pris les éditeurs d'antivirus par surprise. Bien qu'ils aient essayé de publier des mises à jour de fichier de définition dès leur découverte, les virus avaient déjà contaminé un grand nombre de PC.

Et bien que les deux virus aient employé le même exploit, les éditeurs d'antivirus ont dû publier une mise à jour de fichier de définition séparée pour chacun. Au contraire, un moteur de détection d'exploit aurait reconnu l'exploit employé, identifié la tentative de lancer automatiquement un fichier exécutable en exploitant la faille d'entête MIME et aurait bloqué les deux vers empêchant l'infection.

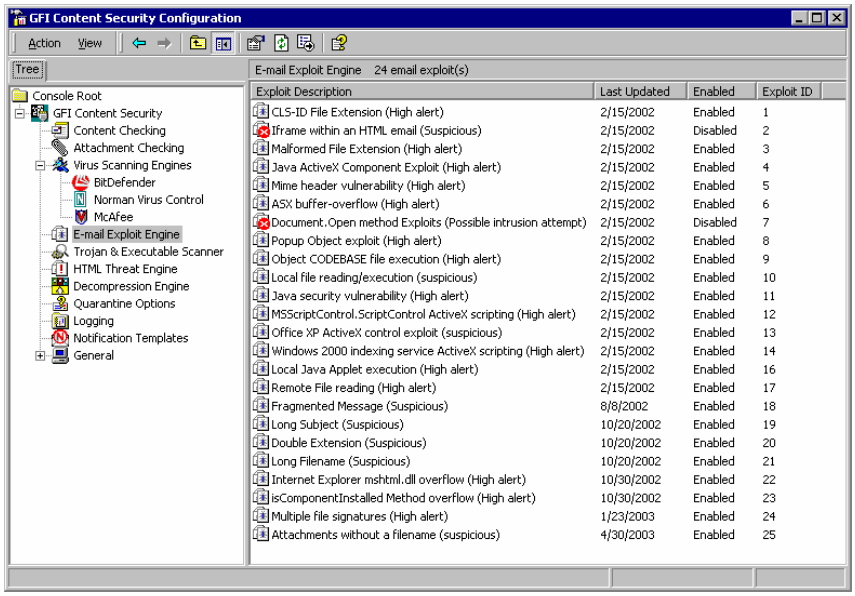
Autres exemples d'exploits

Vulnérabilité à double extension
Virus : Klez, Netsky et Lovegate.
Ce qu'il fait : Les fichiers malicieux reçoivent une double extension tel que nomfichier.txt.exe pour persuader l'utilisateur d'appliquer l'exécutable.

Exploit falsifié d'URL
Virus : Aucun virus/ver qui utiliserait cette méthode, n'a encore été trouvé. Cependant, elle a été utilisée pour insérer des backdoors sur les ordinateurs Windows.
Ce qu'il fait : Permet aux spammers et aux phishers (personnes tentant de frustrer les utilisateurs d'un ordinateur) de tromper les utilisateurs et de les entraîner vers un site Internet malicieux au lieu d'un site légitime.

Exécution de fichier de données d'objet
Virus : Bagle.Q.
Ce qu'il fait : Permet aux attaqueurs d'infecter automatiquement les versions sans patch d'Internet Explorer/Outlook (Express) en téléchargeant et en appliquant les codes à partir d'un site HTTP.

Le moteur anti-exploit GFI MailSecurity



Configuration du moteur d'anti-exploits dans GFI MailSecurity

GFI MailSecurity for Exchange/SMTP, un pack qui comprend un moteur de détection anti-exploit de messagerie parmi plusieurs autres composants clés conçus pour fournir une protection complète contre les menaces email. C'est le premier produit de sécurité de messagerie à vous protéger contre les exploits d'emails, S'inspirant des recherches avancées de GFI Software sur les exploits d'emails, ce moteur détecte les signatures des exploits d'emails actuellement connues et bloque tout message contenant ces signatures. La plupart des problèmes identifiés par le moteur d'anti-exploits de GFI MailSecurity ne sont détectés par aucun autre programme sur le marché. GFI MailSecurity contient les vérifications d'importants exploits d'emails et peut aussi télécharger automatiquement de nouvelles vérifications d'exploits dès qu'elles deviennent disponibles.

GFI MailSecurity a aussi d'autres fonctionnalités telles que de multiples moteurs antivirus, afin de garantir un taux de détection supérieur et une réponse plus rapide aux nouveaux virus ; vérification du contenu et des attachements, afin de mettre en quarantaine des attachements et contenus dangereux ; un moteur de menaces HTLM, pour désactiver les scripts HTML ; un scanner de chevaux de Troie et d'exécutables, pour détecter les exécutables malicieux ; et plus encore. Pour plus d'informations et pour télécharger un essai complet, allez sur http://www.gfi.com/fr/mailsecurity/.

A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grace à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site http://www.gfsfrance.com/.