Cisco Email Security: Grundlagen der Context Adaptive Scanning Engine (CASE)

Inhalt

Einführung

Das Volumen an kombinierten Bedrohungen ist dramatisch angestiegen. Viele der bedeutendsten Virenausbrüche der letzten zwei Jahre wurden mit Spam-Nachrichten in Verbindung gebracht - was bedeutet, dass der Virus-Payload eine Armee von "Zombie"-Computern schafft - die zum Senden von Spam, Phishing, Spyware und noch mehr Viren verwendet werden. E-Mail-basierte Spyware hat sich alle sechs Monate verdoppelt, und es ist nicht ungewöhnlich, dass Spam-E-Mails "Keylogger" installieren, die Benutzernamen und Passwörter stehlen. Viren können sogar dazu verwendet werden, ein Zombies-Netzwerk zu schaffen, um einen massiven verteilten Denial-of-Service-Angriff einzuleiten, z. B. wenn die Variante Mydoom.B die Website von SCO mit einem koordinierten Angriff offline nahm.

Was ist die Ursache für die plötzliche Zunahme kombinierter Bedrohungen? Kurz gesagt, es ist das Geld. Da immer häufiger Antispam-Techniken der ersten Generation (wie Blacklists und Content-Filter) eingesetzt werden, sind herkömmliche Methoden (wie das Senden von Spam von einer festen Bank von Servern, die im Text der Nachricht ein "Angebot" enthalten) weniger profitabel geworden. Da immer mehr Netzwerke mit Anti-Spam-Technologie arbeiten, werden Spam-Nachrichten durch weniger "einfache" Nachrichten über Spam-Filter und in den Posteingang des Empfängers geleitet. Dies schadet den Gewinnmargen der Spammer und hat sie gezwungen, sich an diese Veränderungen anzupassen.

Spammer haben diese Situation auf zwei verschiedene Arten behandelt:

1. Sie senden sogar noch mehr Spam, in der Hoffnung, dass das, was sie in der Zustellungsrate verlieren, sie in der Menge ausgleichen wird.
2. Durch kombinierte Angriffe verschleiern sie ihre Botschaften und steigern ihren Gewinn pro Nachricht.

Die zweite Technik wird oft zu einer kriminellen Aktivität. Netzwerke der organisierten Kriminalität wurden eingerichtet, um Angriffe auszuführen und von Viren, Phishing und anderen Bedrohungen zu profitieren. 2004 wurde eine Person namens John Dover verhaftet, nachdem sie mehr als zwei Millionen Kreditkartennummern in Zahlung gegeben hatte, die durch Phishing-Angriffe gestohlen wurden.

Auch die Techniken, die bei kombinierten Angriffen zum Einsatz kommen, werden immer raffinierter. Der Sober.N-Virus verwendete E-Mails, Web-Downloads, Trojaner und Zombies. Herkömmliche Content-Analyse-Filter sind für diese intelligenten Bedrohungen nicht geeignet. Viele Benutzer von Anti-Spam-Filtern der ersten Generation haben festgestellt, dass sie mehr Stunden damit verbringen müssen, ihre Filter zu "trainieren" oder neue Regeln zu schreiben. Trotz dieser Bemühungen sinken jedoch sowohl die Abfangrate als auch der Durchsatz. Dies führt zu einer Kosteneskalierung, da mehr Systeme erforderlich sind, um mit der Last Schritt zu halten, während für das Management jedes Systems mehr Administrationszeit erforderlich ist.

Cisco Email Security hat diese Bedrohungen mit einer einzigartigen kombinierten Technologie zur Abwehr von Bedrohungen bekämpft, die als Context Adaptive Scanning Engine (CASE) bekannt ist. Die CASE-Technologie von Cisco Email Security dient sowohl der Abwehr von klassischem Spam als auch von komplexen zombie-basierten Angriffen. Dieselbe Scan-Technologie wird auch eingesetzt, um Viren und Malware bereits 42 Stunden vor der Verfügbarkeit der Signatur zu verhindern - mit einem einzigen vereinheitlichten Scan für mehr Effizienz.

FALLerkennung, kombinierte Bedrohungen im Kontext

Filter der ersten Generation wurden entwickelt, um den Inhalt einer Nachricht zu überprüfen und eine Entscheidung zu treffen. Wenn beispielsweise das Wort "frei" zusammen mit dem Wort "pflanzlich" mehr als zweimal in einer Nachricht auftauchte, war es wahrscheinlich Spam. Dieser Ansatz ist für Spammer relativ einfach zu besiegen, indem sie anstelle von Buchstaben "f0r y0u" anstelle von "für Sie" versteckte Zeichen oder Zahlen verwenden. Techniken der zweiten Generation, wie Bayes-Filter, versuchten, diese Einschränkung zu beseitigen, indem sie lernten, die Eigenschaften von Spam und legitimen E-Mails automatisch zu unterscheiden. Doch erwiesen sich diese Techniken als zu schwierig, um zu trainieren, zu spät, um darauf zu reagieren, und zu langsam, um zu scannen.

Angesichts der fortschrittlichen Verschleierungstechniken, die heute bei Spam zum Einsatz kommen, müssen moderne Filter eingehende E-Mails im vollständigen Kontext prüfen. CASE verwendet fortschrittliche maschinelle Lerntechniken, die die Logik eines Menschen nachahmen, der die Legitimität einer Nachricht bewertet. Ein menschlicher Leser sowie die CASE-Technologie von Cisco Email Security stellen vier grundlegende Fragen:

1. Wer hat mir die Nachricht geschickt?
2. Wo finde ich die Links in der Nachricht?
3. Wie wurde die Nachricht erstellt?
4. Was enthält die Nachricht?

Es folgt eine Untersuchung jedes bewerteten logischen Bereichs.

Wer?

Wie bereits erwähnt, basierten die Spamfilter der ersten Generation hauptsächlich auf Schlüsselwortsuche, um Spam zu identifizieren. 2003 revolutionierte Cisco (IronPort) die E-Mail-Security-Branche mit dem Konzept der Reputationsfilterung. Während die Inhaltsfilterung die Frage stellte: "Was ist in der Nachricht?", stellt die Reputationsfilterung die Frage "Wer hat die Nachricht gesendet?". Dieses einfache, aber leistungsstarke Konzept erweiterte den Kontext, in dem Bedrohungen bewertet werden. Bis 2005 hatten fast alle wichtigen Anbieter von kommerziellen Sicherheitslösungen Reputationssysteme eingeführt.

Die Reputation wird ermittelt, indem eine Vielzahl von Daten über das Verhalten eines bestimmten

Absenders geprüft wird (ein Absender wird als IP-Adresse definiert, die E-Mail sendet). Cisco berücksichtigt mehr als 120 verschiedene Parameter, darunter E-Mail-Volumen im Laufe der Zeit, die Anzahl der von dieser IP erfassten "Spam-Traps", das Ursprungsland, die Frage, ob der Host kompromittiert ist und vieles mehr. Cisco verfügt über ein Team von Statistikern, die Algorithmen entwickeln und verwalten, die diese Daten verarbeiten, um eine Reputationsbewertung zu erstellen. Diese Reputationsbewertung wird dann der empfangenden Cisco E-Mail Security Appliance (ESA) zur Verfügung gestellt, die dann einen Absender aufgrund seiner Vertrauenswürdigkeit drosseln kann. Kurz gesagt: Je mehr "Spam" ein Absender erscheint, desto langsamer wird er. Die Reputationsfilterung behebt auch die Probleme im Zusammenhang mit steigender E-Mail-Volumes, indem Verbindungen entweder zurückgewiesen oder gedrosselt werden, bevor die Nachricht akzeptiert wird, wodurch die Leistung und Verfügbarkeit des Mailsystems erheblich verbessert wird. Die Reputationsfilter der Cisco ESA halten mehr als 80 Prozent der eingehenden Spam-E-Mails an, was etwa der doppelten Abfangrate von Systemen anderer Anbieter entspricht.

Wo?

Die Kombination aus Analyse und Reputation von E-Mail-Inhalten war 2003 zwar auf dem neuesten Stand, die Taktik von Spammer und Virenschreibern entwickelt sich jedoch immer weiter. Als Reaktion darauf führte Cisco (IronPort) das Konzept der Web-Reputation ein - ein wichtiger neuer Vektor zur Erweiterung des Kontexts, in dem eine Nachricht evaluiert wird. Ähnlich wie bei der Berechnung der Reputation einer E-Mail-Nachricht werden bei der Cisco Web-Reputation mehr als 45 serverbezogene Parameter berücksichtigt, um die Reputation einer beliebigen URL zu bewerten. Zu den Parametern gehören das Volumen der HTTP-Anfragen an die URL im Laufe der Zeit, ob die URL auf einer IP-Adresse mit schlechter Reputationsbewertung gehostet wird, ob diese URL einem bekannten "Zombie"- oder infizierten PC-Host zugeordnet ist, und das Alter der von der URL verwendeten Domäne. Wie bei E-Mail-Reputation wird auch diese Web-Reputation anhand einer präzisen Punktzahl gemessen, sodass das System die Mehrdeutigkeiten komplexer Bedrohungen bewältigen kann.

Wie?

Ein weiterer Novum bei der kontextbezogenen Analyse von Cisco Email Security besteht darin, die Erstellung einer Nachricht zu untersuchen. Legitime E-Mail-Clients wie Microsoft Outlook erstellen Nachrichten auf einzigartige Weise - mit MIME-Codierung, HTML oder anderen ähnlichen Mitteln. Eine Untersuchung der Gestaltung einer Botschaft kann viel über ihre Legitimität enthüllen. Ein aufschlussreiches Beispiel hierfür ist der Versuch eines Spam-Servers, die Konstruktion eines legitimen Mail-Clients zu emulieren. Dies ist schwierig zu tun, und eine unvollkommene Emulation ist ein verlässlicher Indikator für eine unrechtmäßige Botschaft.

Was?

Eine vollständige Kontextanalyse muss den Inhalt einer Nachricht berücksichtigen, aber wie bereits erwähnt, reicht die Inhaltsanalyse allein nicht aus, um unzulässige E-Mails zu identifizieren. Die CASE-Technologie von Cisco Email Security führt mithilfe modernster maschineller Lernverfahren eine vollständige Inhaltsanalyse durch. Diese Techniken untersuchen den Inhalt der Nachricht und bewerten sie in verschiedenen Kategorien: Ist sie finanziell, pornografisch oder enthält sie Inhalte, die bekanntermaßen mit anderen Spam korrelieren? Diese Inhaltsanalyse wird zusammen mit den anderen Attributen - "Who, Where, How, and What" (Wer, Wo, Wie und Was) in CASE berücksichtigt, um den vollständigen Kontext der Nachricht zu bewerten.

Fall in Aktion

Aufgrund der Breite der von CASE analysierten Daten wird die Technologie in einer Vielzahl von Sicherheitsanwendungen eingesetzt, darunter IronPort Anti-Spam (IPAS), Graymail und Virus-Outbreak-Filter (VOF). Im folgenden Beispiel wird veranschaulicht, wie Spam mithilfe von CASE gestoppt wird. Die Inhalte der Nachricht sind nahezu identisch mit denen der Organisation, die Phishing-Angriffe auslöst, sodass die Content-Analyse der Nachricht keine Bedrohungen identifizieren würde. Für inhaltsbasierte Filter scheint diese Nachricht eine legitime Kommunikation zu sein. Um festzustellen, ob es sich bei dieser Nachricht um Spam handelt, können Filter, die primär auf das "Was" setzen, leicht dazu verleitet werden, die Nachricht als legitim zu erkennen. Eine Analyse des vollständigen Kontexts der Nachricht zeichnet jedoch ein anderes Bild.

- Die IP-Adresse des sendenden Mail-Servers ist verdächtig - sie hat einen plötzlichen Anstieg der Lautstärke, und die Domäne akzeptiert im Gegenzug keine E-Mails.
- Die URL der E-Mail verweist auf einen Server, der sich scheinbar in einem Breitbandnetzwerk für Privatnutzer befindet.
- Die in der Nachricht angegebene URL unterscheidet sich von der URL, zu der der Benutzer beim Klicken auf den Link navigiert wird.

Wenn alle drei Faktoren im Kontext betrachtet werden, wird deutlich, dass es sich hierbei nicht um eine legitime Nachricht handelt, sondern um einen Spam-Angriff.

Herkömmliche "Content-Filter"
Suchen nach Content-FILTERN

Was? Der Nachrichteninhalt ist legitim.

Verdict: UNBEKANNT

Kontextadaptives Scannen
Was FALLS FÄLLT?

Was? Nachrichteninhalt legitim.
Wie? Message-Konstruktion emuliert Microsoft Outlook-Client.
Wer?
1) Ein plötzlicher Anstieg des E-Mail-Volumens.
2) Im Gegenzug akzeptiert der Mail-Server keine Mail.
3) Mailserver in der Ukraine.

Wo?
1) Eine Diskrepanz zwischen der vor einem Tag registrierten Anzeige- und Ziel-URL-Website-Dom
2) Website wird im Breitbandnetz für Privatnutzer gehostet.
3) "Whois"-Daten zeigen dem Domäneninhaber, e er ein bekannter Spammer ist.

Verdict: BLOCKIEREN

Wird CASE in Virus-Outbreak-Filtern verwendet, werden die gleichen Bewertungs- und maschinellen Lernfunktionen angewendet, wenn auch auf einen separat angepassten Datensatz. Virus-Outbreak-Filter sind eine von Cisco angebotene präventive Virenschutzlösung, die durch die CASE-Technologie unterstützt wird. Die Outbreak-Filterlösung scannt Nachrichten sowohl nach "Echtzeit"-Outbreak-Regeln (die von Cisco Talos-spezifischen Outbreaks ausgegeben werden) als auch nach "Always-On"-adaptiven Regeln (die jederzeit im CASE enthalten sind), um Benutzer

vor Outbreaks zu schützen, bevor sie sich vollständig bilden konnten. CASE ermöglicht Virus-Outbreak-Filtern, Virus-Outbreaks auf verschiedene Weise genau zu erkennen und zu schützen. Zunächst kann CASE Nachrichten schnell anhand von Parametern wie Dateierweiterung, Dateigröße, Dateiname, Dateinamen, Schlüsselwörter für Dateinamen, Dateimagie (die eigentliche Dateierweiterung) und eingebettete URLs scannen. Da die CASE-Technologie die Nachrichten bis zu diesem Detailgrad analysiert, können Cisco Talos äußerst detaillierte Outbreak-Regeln erstellen, die einen präzisen Schutz vor Outbreaks mit minimalen Fehlalarmen bieten. CASE kann dynamisch aktualisierte Outbreak-Regeln empfangen, die einen effektiven Schutz vor den neuesten Outbreaks gewährleisten.

Zusätzlich zur Analyse von Nachrichten auf der Grundlage von Outbreak-Regeln scannt die CASE-Technologie auch Nachrichten auf der Grundlage adaptiver Regeln. Adaptive Regeln sind fein abgestimmte Heuristik und Algorithmen, die eingehende Nachrichten auf Missbildungen und Spoofing-Eigenschaften, die auf Viren hindeuten, untersuchen. Zusätzlich zu diesen Parametern werden Meldungen nach Adaptive Rules basierend auf dem SenderBase-Virenbewertungs (SBVS) bewertet. SBVS ist ein Ergebnis, das einer SenderBase-Reputationsbewertung (SBRS) ähnelt, jedoch mit einer Rangfolge, die auf der Wahrscheinlichkeit basiert, dass der Absender statt Spam virale E-Mails sendet. Ein Großteil der viralen E-Mails wird von bereits infizierten "Zombie"-Computern versendet. Die Identifizierung und Bewertung dieser Absender ist daher ein wesentlicher Faktor für die Entdeckung von Viren.

Mit der CASE-Technologie von Cisco Email Security können Virus-Outbreak-Filter Virenangriffe weit vor herkömmlichen Antivirus-Lösungen stoppen, da die Meldungen in der CASE auf verschiedene Weise untersucht werden. Es kann zahlreiche Eigenschaften wie Nachrichtenanhänge, Nachrichteninhalte und die Erstellung von Nachrichten analysieren und Nachrichten anhand ihrer Absender-Reputation analysieren. Da CASE auch als IronPort Anti-Spam- und Reputationsfilter-Engine fungiert, muss eine Nachricht nur einmal für alle diese Anwendungen gescannt werden.

Hohe Leistung, niedrige Kosten

Die Logik der CASE-Technologie kann sehr ausgefeilt sein und daher sehr CPU-intensiv zu verarbeiten sein. Um die Effizienz zu maximieren, verwendet CASE eine einzigartige "Early-Exit"-Technologie. Die Wirksamkeit der unzähligen von CASE verarbeiteten Regeln wird bei frühzeitigem Austritt priorisiert. Die CASE-Technologie führt die Regeln mit der höchsten Auswirkung und den niedrigsten Kosten zuerst aus. Wenn ein statistisches Urteil (positiv oder negativ) gefällt wird, werden keine zusätzlichen Regeln ausgeführt, wodurch Systemressourcen eingespart werden. Die Eleganz dieses Ansatzes ist ein gutes Verständnis der Wirksamkeit jeder Regel. CASE überwacht und passt die Reihenfolge der Regelausführung automatisch an, wenn sich die Wirksamkeit ändert.

Das Ergebnis einer vorzeitigen Beendigung ist, dass die CASE-Technologie Nachrichten etwa 100 Prozent schneller verarbeitet als ein herkömmlicher regelbasierter Filter. Dies bietet für große ISPs und Unternehmen deutliche Vorteile. Aber auch kleine und mittlere Unternehmen profitieren davon. Aufgrund der Effizienz von CASE und der Effektivität des AsyncOS-Betriebssystems von Cisco Email Security können ESAs mit AsyncOS- und CASE-Technologie mit sehr kostengünstiger Hardware implementiert werden, was die Kapitalkosten senkt.

Eine weitere Möglichkeit, die CASE-Technologie zu geringen Kosten führt, ist der Abbau von Verwaltungsaufwand. Die CASE wird automatisch angepasst und aktualisiert, und zwar tausende Male pro Tag. Cisco Talos stellt Ihnen geschulte, mehrsprachige Techniker und Statistiker zur Verfügung. Analysten von Cisco Talos verfügen über spezielle Tools, die Anomalien im E-Mail-

Fluss aufzeigen, die in den Netzwerken von Cisco Email Security-Kunden oder in globalen E-Mail-Verkehrsmustern festgestellt wurden. Cisco Talos generiert neue Regeln, die automatisch in Echtzeit in das System übertragen werden. Cisco Talos verfügt außerdem über ein riesiges Korpus aus "Spam und Schinken", das zur Schulung der verschiedenen von CASE verwendeten Regeln verwendet wird. Die automatisch aktualisierten CASE-Regeln bedeuten, dass Administratoren den Filter nicht anpassen und anpassen müssen oder keine Zeit mehr damit verbringen müssen, durch Spam-Quarantänen zu navigieren.

Zusammenfassung

Spam, Viren, Malware, Spyware, Denial-of-Service-Angriffe und Angriffe auf Verzeichnisse beruhen alle auf demselben Motiv: dem Profit. Diese Gewinne werden entweder durch den Verkauf oder die Werbung von Waren oder durch Diebstahl von Informationen erzielt. Profite aus diesen Umsätzen führen zu immer raffinierteren Angriffen, die von professionellen Technikern entwickelt wurden. Erweiterte E-Mail-Security-Systeme müssen eine Nachricht im größtmöglichen Kontext analysieren, um diesen Bedrohungen entgegenzuwirken. Die Cisco Email Security Context Adaptive Scanning Engine-Technologie stellt die vier grundlegenden Fragen: Wer, wo, Was und Wie -, um legitime Botschaften vor kombinierten Bedrohungen zu löschen.

- "Wer" ist die E-Mail-Reputation des Absenders, der die Nachricht gesendet hat.
- "Wo" ist die Reputation der Quelle, die die Website hostet - analysieren, wo der Link Sie führen würde.
- "Was" ist eine Analyse des Inhalts der Nachricht - was die Nachricht enthält (Systeme der ersten Generation verlassen sich oft nur auf die" Was"-Analyse).
- Schließlich ist "Wie" eine Analyse, wie die Nachricht erstellt wird.

Dieses grundlegende Framework zur Analyse von "Wer, Wo, Was und Wie" funktioniert bei der Blockierung von Spam ebenso gut wie bei der Vorbeugung von Virenangriffen, Phishing-Angriffen, E-Mail-basierter Spyware oder anderen Bedrohungen per E-Mail. Die Datensätze und Regelsätze für Analysen werden speziell auf die einzelnen Bedrohungen abgestimmt. Mit der CASE-Technologie kann die Cisco ESA eine Vielzahl von Bedrohungen mit der höchstmöglichen Effizienz stoppen, indem sie diese Bedrohungen auf einer einzigen Hochleistungs-Engine verarbeitet.