Cisco e-mailbeveiliging: Begrijpen van context-adaptieve scans-engine (CASE)

Inhoud

Inleiding

De toename van het aantal gemengde bedreigingen is dramatisch geweest. Veel van de belangrijkste uitbraken van het virus in de afgelopen twee jaar zijn in verband gebracht met het leveren van spam (wat betekent dat de lading voor het virus een leger 'zombie'-computers creëert), die gebruikt worden om spam, phishing, spyware en nog meer virussen te verzenden. Spyware via e-mail is iedere zes maanden verdubbeld en het is niet ongebruikelijk dat spammed URL's 'keyloggers' installeren die gebruikersnamen en wachtwoorden stelen. Virussen kunnen zelfs worden gebruikt om een netwerk van zombies te creëren om een massaal verspreid 'denial of service'-aanval te lanceren, zoals toen de Mydoom.B-variant de website van SCO offline veroverde met een gecoördineerde aanval.

Wat is de drijvende kracht achter de plotselinge toename van gemengde dreigingen? Kortom, het is het geld. Nu anti-spamtechnieken van de eerste generatie (zoals zwarte lijsten en contentfilters) breder zijn ingezet, zijn traditionele methoden (zoals het verzenden van spam van een vaste bank servers met een ‘bod' in de tekst van het bericht) minder rendabel geworden. Met meer netwerken die anti-spam technologie gebruiken, maken minder "eenvoudige" spamberichten het voorbij spamfilters en in de inbox van de ontvanger. Dit schaadt de winstmarges van spammers en dwingt hen zich aan deze veranderingen aan te passen.

Spammers pasten deze situatie op twee verschillende manieren aan:

1. Ze sturen zelfs nog meer spam in de hoop dat wat ze verliezen in de leveringstarieven, ze zullen inhalen in volume.
2. Ze wenden zich tot gemengde aanvallen om hun boodschap te verhullen en hun winst per boodschap te verhogen.

De tweede techniek wordt vaak een criminele activiteit. Er zijn georganiseerde criminele netwerken opgericht om aanvallen uit te voeren en te profiteren van virussen, phishing en andere bedreigingen. In 2004 werd een individu, John Dover genaamd, gearresteerd nadat hij had gehandeld in meer dan twee miljoen creditcardgegevens, die werden gestolen door phishing-aanvallen.

De technieken die worden gebruikt bij aanvallen met gemengde weefsels zijn ook steeds complexer geworden. Het Sober.N-virus had e-mail, webdownloads, trojans en zombies. Traditionele inhoud analyse filters zijn geen match voor deze intelligente bedreigingen. Veel gebruikers van anti-spamfilters van de eerste generatie hebben ontdekt dat ze de stijgende uren moeten doorbrengen om hun filters te "trainen" of nieuwe regels te schrijven. Ondanks deze inspanningen dalen hun vangstcijfers en hun productie echter allebei. Het gevolg is dat de kosten stijgen omdat er meer systemen nodig zijn om de lading bij te houden, terwijl er meer beheertijd wordt gebruikt om elk systeem te beheren.

Cisco Email Security heeft deze bedreigingen aangepakt met een unieke gemengde bedreiging defensietechnologie die bekend staat als de Context Adaptive Scanning Engine (CASE). Cisco Email Security-technologie wordt gebruikt om zowel traditionele spam- als geavanceerde zombieaanvallen te stoppen. Deze zelfde scantechnologie wordt ook gebruikt om virussen en malware zo'n 42 uur voor de beschikbaarheid van de handtekening te voorkomen - met één enkele geünificeerde scan voor efficiëntie.

Begrijpen van CASE, gemengde bedreigingen in context detecteren

De eerste generatie filters waren ontworpen om de inhoud van een bericht te bekijken en een beslissing te nemen. Bijvoorbeeld, als het woord "vrij" meer dan twee keer verscheen in een bericht, samen met het woord "kruiden", was het waarschijnlijk spam. Deze benadering is relatief makkelijk voor spammers om te verslaan door gebruik te maken van verborgen tekens of getallen in plaats van letters, zoals "f0r y0u" in plaats van "voor u." Tweede generatie technieken zoals Bayesiaanse filters probeerden deze beperking aan te pakken door te leren de kenmerken van spam en legitieme e-mail automatisch te differentiëren. Maar deze technieken bleken te uitdagend om te trainen, te laat om te reageren, en te langzaam om te scannen.

Gezien de geavanceerde verduisteringstechnieken die met de huidige spam worden gebruikt, moeten de meest geavanceerde filters de inkomende post in volledige context onderzoeken. CASE gebruikt geavanceerde machine learning-technieken die de logica volgen van een mens die de legitimiteit van een bericht beoordeelt. Een menselijke lezer, zowel als de CASE-technologie van Cisco Email Security, stelt vier fundamentele vragen:

1. Wie heeft me het bericht gestuurd?
2. Waar brengen de links in de boodschap me heen?
3. Hoe werd het bericht geconstrueerd?
4. Wat bevat het bericht?

Hierop volgt een onderzoek van elk geëvalueerd logisch gebied.

Wie?

Zoals eerder gezegd, de eerste generatie spam filters vertrouwden primair op sleutelwoordenzoekingen om spam te identificeren. In 2003 heeft Cisco (IronPort) de e-mailbeveiligingssector revolutionair veranderd door het concept van reputatieschade. Terwijl content filteren de vraag stelde, "Wat is er in de boodschap?", stelt reputatie-filteren de vraag: "Wie heeft het bericht gestuurd?" Dit eenvoudige maar krachtige concept verbreedde de context waarin bedreigingen worden beoordeeld. In 2005 had bijna elke belangrijke verkoper van commerciële beveiliging een of ander soort reputatiesysteem ingevoerd.

Het bepalen van reputatie omvat het onderzoeken van een brede reeks gegevens over het gedrag van een bepaalde afzender (een afzender wordt gedefinieerd als een IP adres dat post versturen). Cisco overweegt meer dan 120 verschillende parameters, waaronder e-mailvolume in de loop der tijd, het aantal "spamvallen" dat door deze IP is getroffen, het land van oorsprong, of de host gecompromitteerd is en nog veel meer. Cisco heeft een team statistici dat algoritmen ontwikkelt en onderhoudt, dat deze gegevens verwerkt om een reputatiescore te genereren. Deze reputatiescore wordt dan beschikbaar gesteld aan de ontvangende Cisco Email Security Appliance (ESA), die dan een zender kan gooien op basis van hun betrouwbaarheid. Kort samengevat: hoe meer "spammie" een sender verschijnt, hoe langzamer hij gaat. Reputatie-filtering houdt ook rekening met de problemen die gepaard gaan met het toenemend aantal e-mailberichten door verbindingen af te wijzen of te wentelen voordat het bericht wordt geaccepteerd, wat de prestaties en beschikbaarheid van het postsysteem dramatisch verbetert. Cisco ESA reputatiefilters stoppen meer dan 80 procent van de inkomende spam, ongeveer tweemaal het vangstpercentage van concurrerende systemen.

Waar?

Hoewel de combinatie van analyse van e-mailinhoud en reputatie in 2003 de stand van de techniek was, blijft de verfijning van de tactieken van spammer- en virusschrijvers toenemen. In antwoord hierop introduceerde Cisco (IronPort) het begrip Web reputatie - een cruciale nieuwe vector om de context te verbreden waarin een bericht wordt geëvalueerd. Overeenkomstig de benadering die wordt gebruikt bij het berekenen van de reputatie van een e-mail, kijkt Cisco Web Reputation naar meer dan 45 server-gerelateerde parameters om de reputatie van een bepaalde URL te beoordelen. De parameters omvatten het volume van HTTP-verzoeken naar de URL in de loop der tijd, of de URL wordt gehost op een IP-adres met een slechte reputatie-score, of deze URL wordt geassocieerd met een bekende "zombie" of geïnfecteerde PC-host, en de leeftijd van het domein dat wordt gebruikt door de URL. Net als bij e-mailreputatie wordt deze Web reputatie gemeten met behulp van een granulaire score, die het systeem in staat stelt om de dubbelzinnigheden van geraffineerde bedreigingen aan te pakken.

Hoe?

Een andere nieuwe benadering van de contextuele analyse van Cisco Email Security is om de constructie van een bericht te onderzoeken. Legitieme mailklanten, zoals Microsoft Outlook, construeren berichten op unieke manieren - met MIME-encodering, HTML of andere vergelijkbare middelen. Een onderzoek naar de constructie van een boodschap kan veel over zijn legitimiteit aan het licht brengen. Een veelzeggend voorbeeld hiervan is wanneer een spamserver probeert de constructie van een legitieme mailcliënt na te bootsen. Dit is moeilijk te doen en een imperfecte emulatie is een betrouwbare indicator van een onwettige boodschap.

Wat?

Een volledige contextuele analyse moet de inhoud van een bericht in overweging nemen, maar zoals eerder vermeld is inhoudanalyse op zichzelf niet voldoende om illegale post te identificeren. De CASE-technologie van Cisco e-mail Security voert een volledige inhoudanalyse uit met behulp van state-of-the-art technieken voor het leren van machines. Met deze technieken wordt de inhoud van de boodschap onderzocht en in verschillende categorieën gescand - is het financieel, pornografisch of bevat het inhoud waarvan bekend is dat deze samenhangt met andere spam? Deze contentanalyse wordt in CASE samen met de andere eigenschappen - de who, Where, How en What - meegenomen om de volledige context van de boodschap te evalueren.

GEVAL IN AANMERKING

Vanwege de breedte van de gegevens die door CASE zijn geanalyseerd, wordt de technologie gebruikt in een verscheidenheid aan beveiligingstoepassingen - waaronder IronPort Anti-Spam (IPAS), Graymail en Virus Outbreak Filters (VOF). Het onderstaande voorbeeld benadrukt hoe CASE wordt gebruikt om spam te stoppen. De inhoud van het bericht is vrijwel identiek aan de telefonische organisatie, zodat de inhoudelijke analyse van het bericht geen bedreigingen zou bevatten. Voor content-based filters lijkt dit bericht een legitieme communicatie te zijn. Om vast te stellen of dit bericht spam is, zouden filters die primair vertrouwen op het "Wat" gemakkelijk om de boodschap als legitiem te herkennen zijn. Een analyse van de volledige context van het bericht schildert echter een ander beeld.

- Het IP-adres van de verzendende mailserver is achterdochtig - het volume is plotseling gestegen en het domein accepteert geen mail.
- De URL van de e-mail wijst naar een server die in een consumentenbreedbandnetwerk lijkt te zijn.
- De URL die in het bericht wordt geadverteerd, is anders dan de "echte" URL waaraan de gebruiker is genummerd wanneer hij op de link klikt.

Als we alle drie deze factoren in hun context zien, wordt duidelijk dat dit geen legitieme boodschap is, maar een spamaanval.

Traditionele "contentfilters"
Welke CONTENTFILTERS zoeken

Wat? Berichtinhoud is legitiem.

Uitspraak: ONBEKEND

Adaptieve scannen van context
Wat stelt CASE in?

Wat? Berichtinhoud legitiem.
Hoe? Berichtenconstructie emuleert Microsoft Ou client.
Wie?
1) Een plotselinge toename van het aantal e-mailberichten dat wordt verstuurd.
2) In ruil hiervoor accepteert de mailserver geen r
3) Mail server gelegen in Oekraïne.

Waar?
1) Een mismatch tussen het URL-domein van dis en doel dat een dag geleden is geregistreerd.
2) Website georganiseerd op consumentenbreedbandnetwerk.
3) "Whois"-gegevens tonen de eigenaar van het domein als een bekend spammer.

Uitspraak: BLOKKEREN

Wanneer CASE wordt gebruikt in Filters voor uiteinden van virussen, worden dezelfde scoring en mogelijkheden voor machinaal leren toegepast - alhoewel op een afzonderlijk afgestemde gegevensset. Filters voor virusuitbraken zijn een preventieve anti-virusoplossing die door Cisco wordt aangeboden en door CASE-technologie wordt aangedreven. De oplossing van Outbreak Filters scant berichten tegen zowel "real-time" Outbreak Regels (uitgegeven door Cisco Talos specifieke uitbraken) en "altijd-on" adaptieve regels (die op CASE te allen tijde wonen), die gebruikers tegen uitbraken beschermen alvorens zij een kans hebben gehad om volledig te

vormen. CASE stelt Filters van virussen in staat om virusuitbraken op verschillende manieren nauwkeurig te detecteren en te beschermen tegen virusuitbraken. Eerst kan CASE snel berichten scannen op basis van parameters zoals bestandsextensie van bijlage, bestandsgrootte, bestandsnaam, bestandsnaam, bestandsnaam, sleutelwoorden, bestandsextensie (de eigenlijke extensie van een bestand) en ingesloten URL's. Omdat de technologie van CASE berichten aan dit niveau van detail analyseert, kunnen Cisco Talos zeer granulaire regels uitvaardigen die accuraat tegen een uitbraak beschermen met minimale valse positieven. CASE kan dynamisch bijgewerkte regels voor uitbraken ontvangen, die ervoor zorgen dat deze bescherming biedt tegen de nieuwste uitbraken.

Naast de analyse van berichten gebaseerd op regels van de Uitsplitsing, scant de technologie van de CASE ook berichten gebaseerd op Adaptieve Regels. Adaptieve regels zijn fijnafstemming van heuristiek en algoritmen die binnenkomende berichten voor misvorming en spoofing karakteristieken die wijzen op virussen onderzoeken. Naast deze parameters scoren Adaptieve Regels berichten op basis van hun SenderBase Virus Score (SBVS). SBVS is een score vergelijkbaar met een SenderBase Reputation Score (SBRS), maar met een ranglijst gebaseerd op de waarschijnlijkheid dat de verzendende partij virale e-mails verstuurt in plaats van spam. De meeste virale e-mail wordt verstuurd door eerder geïnfecteerde 'zombie'-machines, dus het identificeren en scannen van deze verzendende partijen is een belangrijke factor bij het vangen van virussen.

Met de CASE-technologie van Cisco e-mail security kunnen Filters van het virus de uitbraken van het virus ruim voor traditionele anti-virusoplossingen stoppen omdat de CASE berichten op meerdere manieren onderzoekt. Het heeft de mogelijkheid om talrijke kenmerken van berichtbijlagen, berichtinhoud en berichtenconstructie te analyseren, evenals de mogelijkheid om berichten te analyseren op basis van hun reputatie als afzender. En omdat CASE ook fungeert als de IronPort Anti-Spam en Reputation Filters machine, hoeft er slechts één bericht te worden gescand voor al deze toepassingen.

Hoge prestaties, lage kosten

De logica achter de CASE-technologie kan zeer geavanceerd zijn en dus intensief CPU-proces. Om de efficiëntie te maximaliseren, gebruikt CASE een unieke "vroege exit"-technologie. Vroege exit geeft prioriteit aan de effectiviteit van de talloze regels die verwerkt zijn door CASE. CASE-technologie runt de regels eerst met de hoogste impact en de laagste kosten. Indien een statistisch oordeel wordt bereikt (positief of negatief), worden geen extra regels uitgevoerd, waardoor de middelen van het systeem worden bespaard. De elegantie in deze benadering heeft een goed inzicht in de effectiviteit van elke regel. De CASE controleert en past de volgorde van uitvoering van de regel automatisch aan als de werkzaamheid verandert.

Het resultaat van vroege exit is dat CASE technologie berichten ongeveer 100 procent sneller verwerkt dan een traditioneel op regels gebaseerd filter. Dit heeft uitgesproken voordelen voor grote ISP's en ondernemingen. Maar het heeft ook voordelen voor kleine en middelgrote bedrijven. De efficiëntie van CASE, gekoppeld aan de effectiviteit van het AsyncOS-besturingssysteem van Cisco Email Security, betekent dat ESA’s met AsyncOS- en CASE-technologie kunnen worden geïmplementeerd op basis van zeer goedkope hardware-voeding, waardoor de kapitaalkosten omlaag kunnen worden gebracht.

Een andere manier waarop de CASE-technologie zich vertaalt in lage kosten is door het elimineren van administratieve overheadkosten. De CASE wordt automatisch aangepast en bijgewerkt, duizenden keren per dag. Cisco Talos biedt ingenieurs die zijn getraind, meertalige technici en statistici. Cisco Talos analisten hebben speciale tools die anomalieën in poststroom

markeren die worden gedetecteerd in het netwerk van de klant van Cisco e-mail security of mondiale e-mailverkeerspatronen. Cisco Talos genereert nieuwe regels die automatisch in real-time naar het systeem worden geduwd. Cisco Talos behoudt ook een enorm corpus van "spam en ham", dat wordt gebruikt om verschillende regels te trainen die door CASE worden gebruikt. De automatisch aangepaste CASE-regels betekenen dat beheerders de filter niet moeten afstemmen en de wachttijd van het filter of de invoertijd niet in spam-quarantaine moeten wijzigen.

Samenvatting

Spam, virussen, malware, spyware, het weigeren van service aanvallen en de aanvallen van telefoongidsen worden allemaal gedreven door dezelfde onderliggende motief - winsten. Deze winsten worden behaald door de verkoop of reclame van goederen of door informatie-diefstal. De winsten uit deze verkopen zijn de drijvende kracht achter steeds complexere aanvallen, die door professionele ingenieurs worden ontwikkeld. Geavanceerde systemen voor e-mail moeten een bericht in de breedst mogelijke context analyseren om deze bedreigingen te bestrijden. Cisco e-mail security context adaptieve scans engine technologie stelt de vier basisvragen: Wie, waar, wat en hoe - om legitieme boodschappen van gemengde dreigingen af te schudden.

- "Wie" is de e-mailreputatie van de afzender - die het bericht stuurde.
- "Where" is de reputatie van de bron die de website gastheer is - en hij analyseert waar de link je heen zou leiden.
- "Wat" is een analyse van de inhoud van het bericht - wat de boodschap bevat (systemen van de eerste generatie vertrouwen vaak alleen op het "Wat"-type analyse).
- Tenslotte is "How" een analyse van de manier waarop de boodschap is geconstrueerd.

Dit fundamentele raamwerk van het analyseren van Wie, Waar, Wat en Hoe werkt net zo goed voor het stoppen van spam als het doet voor het voorkomen van virusuitbraken, phishing aanvallen, e-mail-borne spyware, of andere e-mailbedreigingen. De datasets en de analysetoets worden specifiek aangepast voor elke bedreiging. Met de CASE-technologie kan Cisco ESA het breedste scala aan bedreigingen met de hoogste efficiëntie stoppen door deze bedreigingen op één hoge-prestatie motor te verwerken.