ESA ervaart een Bounce (NDR) Storm

Inhoud

Inleiding

Dit document beschrijft een ondervonden probleem waar uw e-mail security applicatie (ESA) een stuitstorm ervaart en een oplossing voor het probleem biedt.

Achtergrondinformatie

Een stormen is een neveneffect van een baan of een backscatter van e-mailspam.

Joe Job

Een gezamenlijke baan is een spamaanval die gebruik maakt van spoofed sender data en erop gericht is de reputatie van de klaarblijkelijke zender te schaden en/of de ontvangers ertoe aan te zetten actie te ondernemen tegen de klaarblijkelijke zender.

backscatter

Een backscatter is een neveneffect van e-mailspam, virussen en wormen waarin e-mailservers die spam en andere post ontvangen, berichten verzenden naar een onschuldige partij. Dit komt voor omdat de oorspronkelijke map van het bericht is vervalst om het e-mailadres van het slachtoffer te bevatten. Aangezien deze berichten niet door de ontvangers werden opgevraagd, grotendeels met elkaar vergelijkbaar zijn en in grote hoeveelheden worden geleverd, worden zij beschouwd als ongevraagde bulk-e-mail of spam. Als zodanig kunnen systemen die e-mailbackscatter genereren, worden opgenomen in verschillende Domain Name System Blacklists (DNSBL's) en treden deze in strijd met de servicevoorwaarden van internetproviders.

Probleem

Uw ESA heeft een stuitstorm ervaren waarbij een stortvloed aan berichten in de ESA is geïnjecteerd. Tijdens zo'n aanval valt het aantal aansluitingen toe. Het apparaat kan een back-up van de werkvoorraad ontwikkelen. Controleer of het apparaat aan een dergelijke aanval is onderworpen, en neem de e-mailbestanden naar het adres van de mail. Bounces (Non-Delivery Rapporten - NDR's) hebben een lege enveloppe post Vanaf adres.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Een apparaat dat aan een stuitstorm is blootgesteld, heeft de meeste berichten met de enveloppe Vanaf adres van '<>'.

Oplossing

Er zijn een aantal opties om een stuitstorm te beheersen.

Stapelverificatie

Om deze verkeerd geregisseerde aanvallen te bestrijden omvat AsyncOS Cisco Bounce Verificatie. Als deze functie is ingeschakeld, wordt het Envelope Sender-adres achtergelaten voor berichten die via de ESA worden verstuurd. De ontvanger van het geld voor een door de ESA ontvangen melding wordt vervolgens gecontroleerd op de aanwezigheid van dit label. Wanneer legitieme bounce worden ontvangen, wordt de tag die werd toegevoegd aan het adres van Envelope Sender verwijderd en de bounce wordt afgeleverd aan de ontvanger. Bounce berichten die de tag niet bevatten, kunnen afzonderlijk worden verwerkt.

AsyncOS beschouwt bounces als post met een ongeldige post Van adres (<>). Berichten die afkomstig zijn van adressen zoals mailer-daemon@example.com of postmaster@example.com worden door het systeem niet beschouwd als bounces en zijn niet onderworpen aan Bounce Verification.

Keekens van Bounce Verificatieadres configureren

De lijst met bellenings-toetsen van het verificatieadres toont de huidige toets en alle niet-gezuiverde toetsen die u in het verleden hebt gebruikt. Voltooi de volgende stappen om een nieuwe toets toe te voegen:

1. Op het Mail-beleid > Stapelverificatie Klik op Nieuwe sleutel.
2. Typ een tekststring en klik Indienen.
3. Breng je wijzigingen aan.

Doorvoertoetsen

U kunt de oude adrestoewijzing-toetsen verwijderen als u een regel voor het verwijderen in het

keuzemenu selecteert en op **Opslaan** klikt.

Cisco-verificatie-instellingen configureren

De controle-instellingen van de staak bepalen welke actie moet worden ondernomen wanneer een ongeldige bounce wordt ontvangen.

- Kies **Mail-beleid** > **Stapelverificatie**.
- Klik **Instellingen bewerken**.
- Selecteer of u ongeldige kortingen wilt afwijzen of een aangepaste header aan het bericht wilt toevoegen. Als u een header wilt toevoegen, typt u de naam en de waarde van de header.
- Optioneel: maak slimme uitzonderingen mogelijk. Deze instelling maakt het mogelijk binnenkomende e-mailberichten en berichten die door interne mailservers zijn gegenereerd automatisch vrij te stellen van de controle-verwerking in de openlucht (zelfs wanneer één enkele luisteraar wordt gebruikt voor zowel inkomende als uitgaande mail).
- Indienen en je wijzigingen begaan.

Cisco Bounce Verificatie met CLI configureren

U kunt de opdrachten **bvConfig** en **deconfiguratie** in de CLI gebruiken om verificatie te configureren. Deze opdrachten worden besproken in de Cisco AsyncOS CLI referentiegids.

Cisco-stuitverificatie en -clusterconfiguratie

De verificatie werkt in een clusterconfiguratie zolang beide Cisco-apparaten dezelfde "bounce-toets" gebruiken. Als je dezelfde toets gebruikt, moet elk systeem een legitieme terugkoppeling accepteren. De aangepaste header-tag/toets is niet specifiek voor elk Cisco-apparaat.

Mail-filter

Als u geen Bounce Verificatie kunt gebruiken omdat u afzonderlijke apparaten gebruikt voor ontvangst en levering, kunt u een berichtfilter instellen om berichten te blokkeren die een lege post hebben **Vanaf** adres.

postblok

Aangezien deze bounce berichten waarschijnlijk een niet-bestaand enveloppe adres van de ontvanger hebben, kunt u ongeldige adressen blokkeren via gesprek Lichtgewicht Directory Access Protocol (LDAP) ontvanger validatie om de impact van dergelijke berichten te verminderen.