عند إصدار رسالة من العزل، أين يتم تسجيل هذه الرسالة؟

المحتويات

المقدمة

يوضح هذا المستند كيفية عرض سجلات البريد لتحديد مصير رسالة تم إصدارها من العزل على جهاز أمان البريد الإلكتروني (ESA) من Cisco أو جهاز إدارة الأمان (SMA) من Cisco.

عند إصدار رسالة من العزل، أين يتم تسجيل هذه الرسالة؟

في ESA، عندما تقوم بإصدار رسالة من IronPort Spam Quarantine (ISQ) أو عزل النهج أو إجراء عزل مخصص آخر، يتم الإبلاغ عن هذا الإجراء والحدث المقترن في ملف سجلات البريد النصي (mail_log) ل IronPort. ينتسب إدخال السجل إلى MID الأصلي.

أفضل طريقة لنقترب من تتبع هذا هو أن نحصل إما *من*، *إلى*، أو *موضوع* الرسالة الأصلية التي تم الحجر الصحي عليها. بعد ذلك، ابحث عنه في السجل لمعرفة ما إذا كان قد تم إصداره من الفحص، ثم حدد ما إذا كان خادم البريد النهائي قد قبله أم قام برفعه.

على سبيل المثال، البحث في سجلات البريد عن المرسل "spam@test.com":

```
grep -i "spam@test.com" mail_logs <
<Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
<Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com
```

ستحتاج إلى الانتباه إلى معرف الرسالة (MID) ومعرف اتصال التسليم (DCID).

يمكننا أن نرى أن MID هذا تم إرساله إلى العزل العشوائي من Mail_LOG بالكامل، أو تعقب الرسائل:

```
Wed Aug 13 12:59:29 2014 Info: New SMTP ICID 10152 interface Management
address 75.111.22.123 reverse dns host spam.test.com verified yes (192.168.0.199)
Wed Aug 13 12:59:29 2014 Info: ICID 10152 RELAY SG RELAY_SG match 75.111.22.123
SBRS not enabled
Wed Aug 13 12:59:36 2014 Info: Start MID 1357 ICID 10152
<Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com
<Wed Aug 13 12:59:40 2014 Info: MID 1357 ICID 10152 RID 0 To: <end_user@domain.com
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: helo identity postmaster None
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
```

```
Wed Aug 13 12:59:57 2014 Info: MID 1357 SPF: pra identity None headers None
'<Wed Aug 13 12:59:57 2014 Info: MID 1357 Message-ID '<9afe3f$1ad@my_esa.domain.com
'?Wed Aug 13 12:59:57 2014 Info: MID 1357 Subject 'This is spam
<Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com
Wed Aug 13 12:59:57 2014 Info: MID 1357 matched all recipients for per-recipient
                                        policy DEFAULT in the outbound table
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim verdict using engine: CASE
                                                                    spam positive
Wed Aug 13 12:59:58 2014 Info: MID 1357 using engine: CASE spam positive
Wed Aug 13 12:59:58 2014 Info: ISQ: Tagging MID 1357 for quarantine
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim AV verdict using Sophos CLEAN
Wed Aug 13 12:59:58 2014 Info: MID 1357 antivirus negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 Outbreak Filters: verdict negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 DLP no violation
Wed Aug 13 12:59:58 2014 Info: MID 1357 queued for delivery
Wed Aug 13 13:00:02 2014 Info: RPC Delivery start RCID 161 MID 1357 to local IronPort
                                                                    Spam Quarantine
Wed Aug 13 13:00:08 2014 Info: ISQ: Quarantined MID 1357
Wed Aug 13 13:00:08 2014 Info: RPC Message done RCID 161 MID 1357
Wed Aug 13 13:00:08 2014 Info: Message finished MID 1357 done
Wed Aug 13 13:05:11 2014 Info: ICID 10152 close
```

وفيما يلي مثال على ما يجب البحث عنه في الرسالة التي يتم إصدارها من ISQ:

```
(Wed Aug 13 13:02:14 2014 Info: Start MID 1359 ICID 0 (ISQ Released Message
Wed Aug 13 13:02:14 2014 Info: ISQ: Reinjected MID 1357 as MID 1359
<Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 From: <spam@test.com
<Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 RID 0 To: <end_user@domain.com
'?Wed Aug 13 13:02:14 2014 Info: MID 1359 Subject '[SPAM] This is spam
<Wed Aug 13 13:02:14 2014 Info: MID 1359 ready 1445 bytes from <spam@test.com
Wed Aug 13 13:02:14 2014 Info: MID 1359 queued for delivery
Wed Aug 13 13:02:14 2014 Info: New SMTP DCID 165 interface 192.168.0.199 address
                                                                    port 25 192.168.0.200
[Wed Aug 13 13:02:15 2014 Info: Delivery start DCID 165 MID 1359 to RID [0
[Wed Aug 13 13:02:15 2014 Info: Message done DCID 165 MID 1359 to RID [0
Wed Aug 13 13:02:15 2014 Info: MID 1359 RID [0] Response '2.0.0 Ok: queued as
                                                                    '33B7380356
Wed Aug 13 13:02:15 2014 Info: Message finished MID 1359 done
Wed Aug 13 13:02:20 2014 Info: DCID 165 close
```

في هذا المثال، يتم إصدار الرسالة، والواجهة (192.168.0.199) هي وحدة الإصغاء على ESA، والتي تتصل ب (192.168.0.200) كخادم بريد نهاية التسليم النهائي.

عندما تنظر إلى سجلات العزل للبريد العشوائي (euq_log)، يظهر إجراء الإصدار ما يلي:

```
Wed Aug 13 13:02:14 2014 Info: ISQ: Releasing MID [1357] for all
Wed Aug 13 13:02:14 2014 Info: ISQ: Delivering released MID 1357 (skipping
                                                                    (work queue
Wed Aug 13 13:02:14 2014 Info: ISQ: Corpus status: 0
Wed Aug 13 13:02:15 2014 Info: ISQ: Released MID 1357 to end_user@domain.com
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleting MID [1357] for all
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleted MID 1357 for all
Wed Aug 13 13:02:15 2014 Info: ISQ: Cleared 8192 bytes (MIDs 1, for all
                                        .recipients) from database. Current bytes=0
```

وعلى نحو مماثل، إذا كانت الرسالة الأصلية قد وضعت في الحجر الصحي على السياسات، ثم تم إصدارها، فسوف ترى ما هو مشابه لهذا المثال:

```
(Wed Aug 13 13:09:27 2014 Info: MID 1361 released from quarantine "Policy" (manual
                                                                    t=29
```

```
Wed Aug 13 13:09:27 2014 Info: MID 1361 released from all quarantines
Wed Aug 13 13:09:27 2014 Info: MID 1361 matched all recipients for per-recipient
                                                    policy DEFAULT in the inbound table
   Wed Aug 13 13:09:27 2014 Info: MID 1361 interim AV verdict using Sophos CLEAN
                       Wed Aug 13 13:09:27 2014 Info: MID 1361 antivirus negative
                     Wed Aug 13 13:09:27 2014 Info: MID 1361 queued for delivery
Wed Aug 13 13:09:27 2014 Info: New SMTP DCID 169 interface 192.168.0.199 address
                                                                  port 25 192.168.0.200
      [Wed Aug 13 13:09:27 2014 Info: Delivery start DCID 169 MID 1361 to RID [0
        [Wed Aug 13 13:09:27 2014 Info: Message done DCID 169 MID 1361 to RID [0
      Wed Aug 13 13:09:27 2014 Info: MID 1361 RID [0] Response '2.0.0 Ok: queued
                                                                  'as C702980356
            Wed Aug 13 13:09:27 2014 Info: Message finished MID 1361 done
                                  Wed Aug 13 13:09:32 2014 Info: DCID 169 close
```

من "عزل النهج"، يتم إصدار الرسالة من "عزل النهج"، والواجهة (192.168.0.199) هي المستمع على ESA، وتتصل ب (192.168.0.200) كخادم بريد نهاية التسليم النهائي.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- ما هو معرف الرسالة (MID) أو معرف اتصال الحقن (ICID) أو معرف اتصال التسليم (DCID)؟
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).