How does the ESA handle bounce messages sent to 127.0.0.1?

Document ID: 117911

Contributed by Nasir Shakour and Enrico Werner, Cisco TAC Engineers.
Jul 10, 2014

Contents

Question:

How does the ESA handle bounce messages sent to 127.0.0.1?

When spammers send email, they occasionally originate the email from domain names that will resolve to one of the reserved IP loopback addresses (typically 127.0.0.1, although any address in the 127.0.0.0/8 block is reserved for loopback purposes). These addresses are also occasionally encountered in a mass−mailing worm, when the forged source domain name was never designed to receive mail and thus has an illegal IP address to discourage email.

The issue with such domain names resolving to loopback addresses is that an unsuspecting MTA might attempt to connect to the address to deliver the message. Since the loopback address connects back to the same MTA, a loop can be generated. Depending on how the headers are formed in a bounced message, the loop can be particularly costly, eventually getting large enough to consume all system resources.

The ESA avoids this pathological syndrome. When a DNS lookup results in a IP address in the loopback range (127.0.0.0/8), the AsyncOS SMTP client will not attempt to deliver such a message. You can observe this behavior by looking at the mail_logs log. The following log excerpt shows a message being sent with a return address domain name that resolves to the 127.0.0.1 IP address. When the message cannot be delivered, AsyncOS creates a bounce message, but does not try and deliver the bounced message because the DNS is pointing to the loopback address.

```
Thu Dec 9 22:06:03 2004 Info: Start MID 524 ICID 322
Thu Dec 9 22:06:03 2004 Info: MID 524 ICID 322 From:
<loopme@loopback.example.com>
Thu Dec 9 22:06:08 2004 Info: MID 524 ICID 322 RID 0 To:
<illegal99999@example.com>
Thu Dec 9 22:06:09 2004 Info: MID 524 Message−ID
'<3l57rh$gc@mail.example.com>'
Thu Dec 9 22:06:10 2004 Info: MID 524 ready 9 bytes from
<loopme@loopback.example.com>
Thu Dec 9 22:06:10 2004 Info: MID 524 matched all recipients
for per−recipientpolicy DEFAULT in the inbound table
Thu Dec 9 22:06:10 2004 Info: MID 524 Brightmail negative
Thu Dec 9 22:06:10 2004 Info: MID 524 antivirus negative
Thu Dec 9 22:06:10 2004 Info: MID 524 queued for delivery
Thu Dec 9 22:06:10 2004 Info: New SMTP DCID 160 interface
192.35.195.101 address 192.245.12.7
Thu Dec 9 22:06:10 2004 Info: Delivery start DCID 160 MID 524
```

```
to RID [0]
Thu Dec 9 22:06:10 2004 Info: Bounced: DCID 160 MID 524 to RID
0 − 5.1.0 − Unknown address error ('550', ['5.1.1 unknown or
illegal user: illegal99999@example.com'])
Thu Dec 9 22:06:10 2004 Info: MID 525 generated for bounce of
MID 524
Thu Dec 9 22:06:10 2004 Info: Start MID 525 ICID 0
Thu Dec 9 22:06:10 2004 Info: MID 525 ICID 0 From: <>
Thu Dec 9 22:06:10 2004 Info: MID 525 ICID 0 RID 0 To:
<loopme@loopback.opus1.com>
Thu Dec 9 22:06:10 2004 Info: MID 525 queued for delivery
Thu Dec 9 22:06:10 2004 Info: Message finished MID 524 done
Thu Dec 9 22:06:10 2004 Warning: nameserver resolution path
points to 0.x.x.x or 127.x.x.x address.
domain=loopback.example.com
Thu Dec 9 22:06:10 2004 Info: ICID 322 close
Thu Dec 9 22:06:15 2004 Info: DCID 160 close
```

Updated: Jul 10, 2014 Document ID: 117911