Dynamic Port 25 Blocking to Control SPAM Zombies

Jonathan E. Schmidt
Perftech, Inc.
3201 Cherry Ridge C-319
San Antonio, TX 78230
+1-210-349-7152
jon@perftech.com

ABSTRACT

This paper presents the results of a case study in which outbound SPAM, here referring to excessive amounts of bulk-generated e-mail, is suppressed using dynamic Port 25 blocking. Detection, blocking, and remediation are fully automated, relieving the provider's support center, and sparing the 99% of users who are non-abusing from any impact at all. SPAM is typically generated by an infected PC, referred to as a Zombie, whose owner is most often unaware of the infection.

INTRODUCTION

A Multiple Systems Operator (MSO) of 240,000 High Speed Internet subscribers had not imposed a universal block on Port 25 to external servers and was suffering the effects of accelerated SPAM Zombie activity: blacklisting problems and the expense of dealing with 600 abuse complaints each day. The MSO wanted to stop SPAM Zombie activity without a universal Port 25 block.

Why overall Port 25 blocking isn't a solution

The statistics on the percentage of subscribers who were legitimate users of external Port 25 services were unknown but anecdotal reports, specifically the Broadband Reports Forum from Bell South (1) users when their block was imposed, implied that a universal block would generate a volume of support center calls that would exceed the limits of the center for a long period. In addition, a significant part of the subscriber base would be deprived of a critical service.

THE PROPOSAL FOR A SOLUTION

The MSO had already installed a system at each POP for communicating with its subscribers through the use of a small, added frame in the browser. The frame's MSO-branded message displayed no matter which page the user browsed. The MSO proposed to extend this system by monitoring Port 25 connection activity with the expectation that signatures of activity would identify the Zombies and allow a subsequent blocking of their sending processes. It was anticipated that the system could automatically notify the affected subscribers of the reason why their outbound e-mail had been blocked and recommend steps for self-remediation. The latter would be available through a button-click in the browser message that would link to TrendMicro's free on-line virus and Trojan removal tool.

Test setup for analysis

One subnet of 20,000 subscribers was chosen for an analysis of e-mail sending patterns. The test was run in early 2005 for three months. No content was observed and only the statistics of activity on Port 25 was collected and analyzed.

CEAS 2006 – Third Conference on Email and Anti-Spam, July 27-28, 2006, Mountain View, California USA

Using existing bulletin messaging equipment

It was proposed that the existing subscriber messaging system at each POP be used for detection, blocking, and conveying remediation steps. The existing platform:

- Is subscriber-aware, that is, it tracks subscriber activity by subscriber ID (Cable Modem MAC address) and is not affected by ephemeral IP addresses
- Maintained an analysis by subscriber and a database of analytical results for each subscriber
- Was able to process all the traffic with no detectable latency impact on the network

Preliminary analysis

The preliminary analysis showed:

- A very pronounced knee in the curve of sending patterns of subscribers with regular periods of sending rates exceeding 10/second.
- Approximately 1% of the subscribers were among a group exceeding the stipulated limit.
- Approximately 5% of the subscribers were using external Port 25 services and not exceeding the limit.
- Less than 1% of the overall network bandwidth would be saved by eliminating all e-mail traffic emanating from those exceeding the limit.

Proposed active test

A test was proposed and initiated on the subnet of 20,000 subscribers as follows:

- Subscribers exceeding 40 Port 25 connections in any minute would be blocked
- Subscribers exceeding the limit would be presented an explanatory message
- Subscribers exceeding the limit would continue to be monitored and maintained in that mode as along as there were no one minute periods during which Port 25 activity exceeded 5/second. This hysteresis was empirically determined by examining the sending patterns of subscribers exceeding the limit.
- Subscribers subsequently dropping below the stipulated limit would be immediately unblocked.

RESULTS OF THE TEST

The test was operated from April 29, 2005 for two weeks during which the following was noted:

- There were no complaints registered in DSLREPORTS on the MSO's forum.
- Abuse complaints referring to the IP addresses in that subnet often dropped to zero/day from an average of nearly 100/day.
- There were five legitimate, high-volume senders who requested and received a waiver from blocking. The system had anticipated this requirement and the support technicians were provided with a simple GUI to enter the account identifications of those subscribers. Those subscribers were monitored and significant excessive activity relative to typical operation created e-mail alerts to the support center.
- The support group reported no contacts with subscribers about this process other than the five legitimate high-volume users. On the graph below, the activation of spam containment at 2:00 am is visibly noted. The solid color green denotes the actual e-mail output and the blue line denotes the output of Zombies which, after activation of the system, is suppressed.

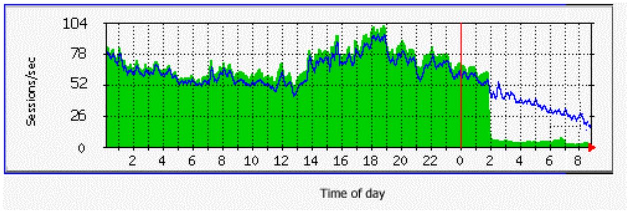

Figure 1: First test activation on 20,000-subscriber subnet

After two weeks, in the absence of the feared large volume of support calls, the MSO requested that all 240,000 subscribers be placed under the control of this system.

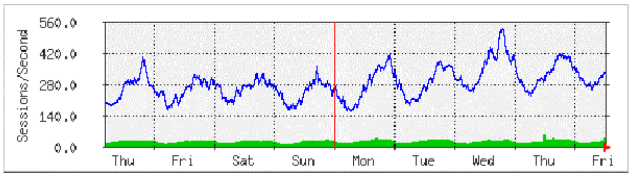

Figure 2: 24-hour cyclic blocked spam attempts

The Zombie activity, varying cyclically, over a 24-hour period is clearly evident by the upper blue line. The system e-mail output, dropping by over 95%, is shown in the solid green at the very bottom of the graph.

After the entire 240,000 subscriber-base was placed under the rate limiting/blocking control, results of this study include:

- Abuse complaints, which previously averaged 600 per day, dropped to single digits.
- The abuse team was disbanded and a single, part-time technician maintained that function.
- After one year, there have been no complaints registered in the DSLREPORTS.
- Bot infections, as measured by the percentage of subscribers flagged as Zombies, dropped from 1% to .2% of the base.

Sideline activity: Subscriber self-remediation

Subscriber self-remediation has been a partial success. The initial link to TrendMicro required a host header in the URL and would not work with an IP address directly. This neutralized the opportunity for the typically infected subscriber whose HOSTS file had been compromised by the virus and would not permit resolution of the TrendMicro domain name. A contact was made with TrendMicro personnel and this was resolved.

It was determined that a sizable portion of the subscriber base isn't using Port 25, likely a result of the popularity of Web-based e-mail services. The messages to those infected subscribers who do not respond with requests for remediation may require more detailed explanations to understand the benefits in performance and security that ridding their PCs of infection would produce.

Reduction of other infrastructure load

It was noted by the MSO that a reduction in DNS MX record lookup load had occurred. The actual statistics are being analyzed. It is expected that the load reduction results from two sources:

1. Slowdown in Zombie sending attempts due to timeouts from the block
2. Remediation of infections by subscribers utilizing TrendMicro's virus "scrub"

A test removing the control from a subnet

A test was undertaken to determine the results of removing a subnet of 20,000 from the entire network of 240,000 for a period of 60 days. The result was:

- A steady return to the pre-control SPAM sending rates
- After 60 days, that subnet again approached the 1% infection rate noted with the first, uncontrolled network. The majority of apparent infections recurred in the last quarter of the period. It is not certain as to the cause. However, it appears that the BOTs or infecting sources became more active in networks that produced positive results.

Future activities in analysis

The collected activity and actions taken over this period is retained in an SQL database and open to interesting queries. The query results are stimulating proposals for the follow-on design and tuning of subsequent tests. Analysis of self-remediation rates is being re-calculated now that the numeric IP address is useable.

Slow-dribble and other new Zombie behavior

It is anticipated that Zombie behavior will be modified to bypass the dynamic rate limiting. This and other circumventing behaviors, including the Zombie use of Port 587, are being analyzed.

Legitimate automatons such as surveillance Web cams, have been observed to be steady senders, yet they are easily ignored by the consistency of the destination address.

Connections with multiple addressees didn't appear to occur from Zombies. That may be due to modern servers rejecting such connections with large bogus addressees being flagged as SPAM.

REFERENCES

[1] http://www.dslreports.com/shownews/43478