SMTP:
Scotch Made Totally Practical

Flaw in the SMTP Protocol

- or -

How I learned to annoy spammers

SMTP Basics

- RFC 2821 – Simple Mail Transfer Protocol
-

"The communication between is an alternating dialogue, controlled by the sender. As such, the sender issues a command and the receiver responds with a reply. Unless other arrangements are negotiated through service extensions, the sender MUST wait for this response before sending further commands."

SMTP Responses

3 numbers, a space or dash, some text

Examples:
220 Ok

250-Text
250 Text

450 4.7.1 Rejected, Try again later

Example SMTP Transmission

220 comet.tesuji.org ESMTP Mailer v0.0.0.0
EHLO localhost
250-comet.tesuji.org, Hello localhost, pleased to meet you
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-AUTH BASIC LOGIN PLAIN
250-DELIVERY
250 HELP
MAIL From:<jonlin@tesuji.org>
250 2.1.0 Sender Ok.
RCPT To: <papers@summercon.org>
554 5.7.1 <papers@summercon.org> Relaying Denied

What's this have to do with Spam?

- Spammers will connect to anything that's listening to port 25
- Email address discovery
- Open relay testing/discovery
- Extra traffic on the network

A few more things about Spam

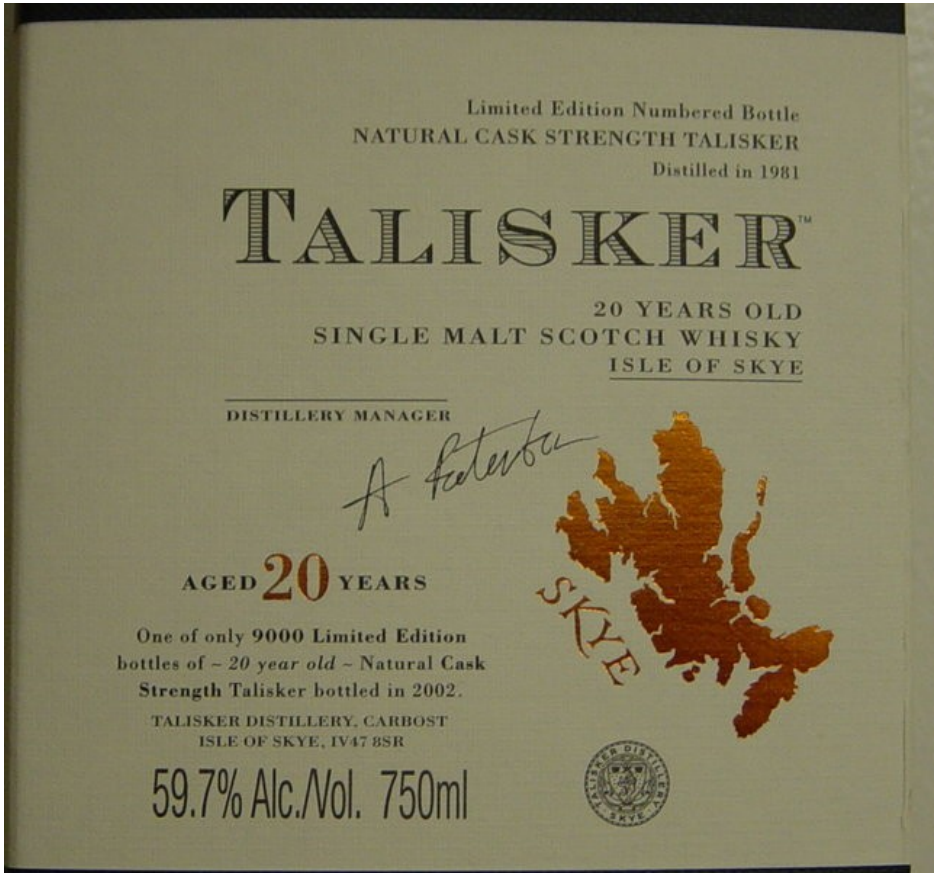
- Spam is mostly sent from compromised personal computers at the home or office
- Botnets
- Small unsophisticated programs usually running on a single thread of execution
- Generally very dumb and do not strictly adhere to the protocol definition

But, But...

- Most people don't run mail servers on non-MXed machines or machines that don't receive or send email
- Most people who do have properly configured mail servers
- Most people don't care about the extra traffic
- Most people don't drink Single Malt Scotch Whisky

Talisker

- Salty and peaty but not overpowering
- Can be found aged 10, 18, 20, 25, and 30 years.
- Peat is added to the malts as they are roasted
- The water source, Croc nan Speireag, flows through peat before it is used in distilling
- Johnnie Walker buys barrels of Talisker to be blended in their Green Label 15 year pure malt



Putting 2 and 2 together

- Spammers will connect to anything listening on port 25
- There are no definitions given in the SMTP standard for the length of multi-line server responses
- No commands can be issued by a client until the server's response to the previous command is transmitted
- The listing for ESMTP commands after the greeting happens before any type of discovery can be made by a spammer

The SMTP Honeypot

Goal

To try to keep spammers that are connecting to servers (which do not require a daemon listening on port 25) as busy doing absolutely nothing for as long as possible.

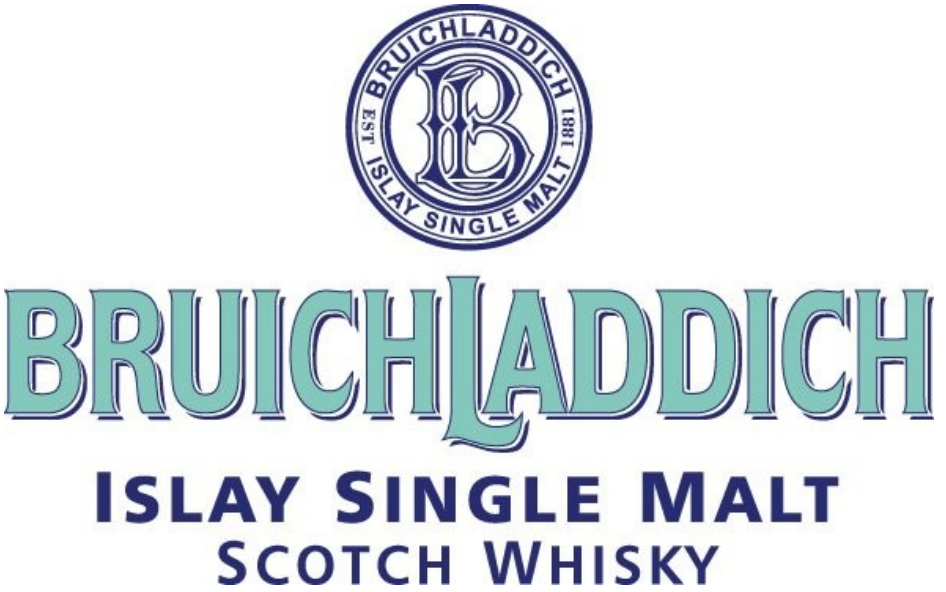
How does it work?

SMTP Extended commands listing, a flaw in the SMTP Protocol. (RFC 2821, Section 4.1.1.1)

SMTP Honey Pot in Action

Bruichladdich

- Distilled on Islay in the village of Bruichladdich
- A very ballanced sweet whisky, light on the peat and salt
- Can be found aged 10, 15, and 20 years
- Distilled in tall neck stills using steam as a heat source
- The distillery was being monitored by the U.S. Defense Threat Reduction Agency because they thought Bruichladdich was making chemical weapons.



Some stats

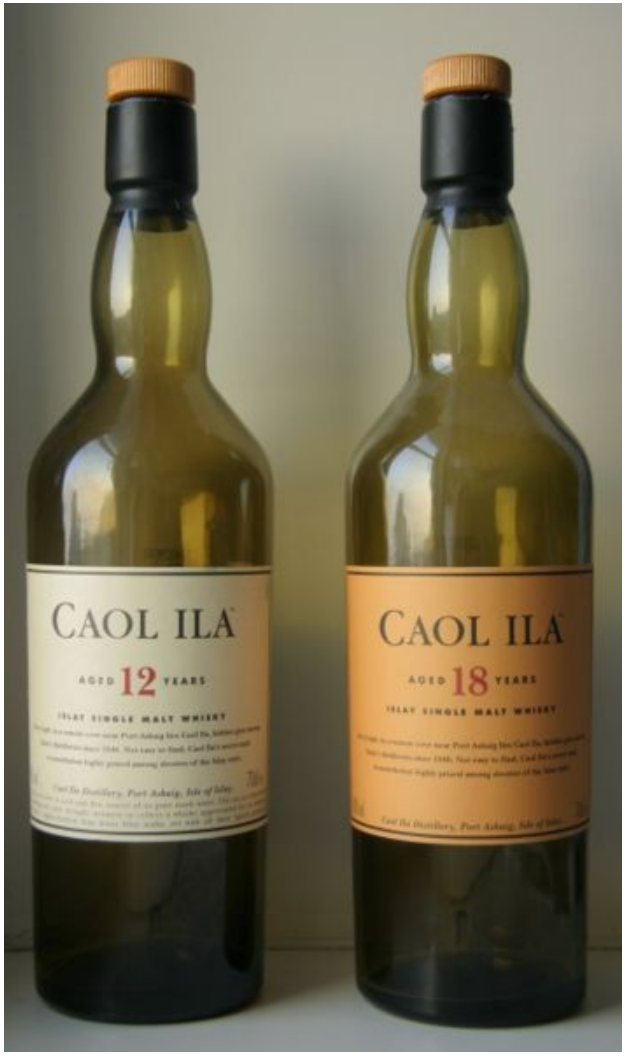
- Running on 8 servers:
- Each server accepted around 10 to 20 connections a day
- Of all the servers, the shortest transaction time was about 5 minutes (not unusual for a regular SMTP transaction)
- Of all the servers, the longest transaction time was over 3 months
- On average, transactions last a few days

Some more disturbing stats

- Affects Postfix and Sendmail (probably others too, I only tested these 2), up until the max transaction timeout is reached or the handler resources run out
- But the email is still in the queue so will attempt to resend
- Can DOS legitimate mail servers by attempting to send MANY emails to a honeypot and cause the server to run out of open files
- Probably more

Caol Ila

- Distilled near Port Askaig on Islay
- Good balance of Peat and Smoke
- Can be found in a variety of ages ranging from 9 to 23 years, as well as many special blends, 12 and 18 are common years imported into the states
- Has the highest production of all Islay distilleries
- Most of its barrels are sold directly to blenders like Johnnie Walker



If you want a copy of the Honeypot

http://www.tesuji.org/SMTPHoneyPot.java