Homeless Vikings

Cut it out. You’re just making it worse.

A marginally entertaining talk by Dave Josephsen

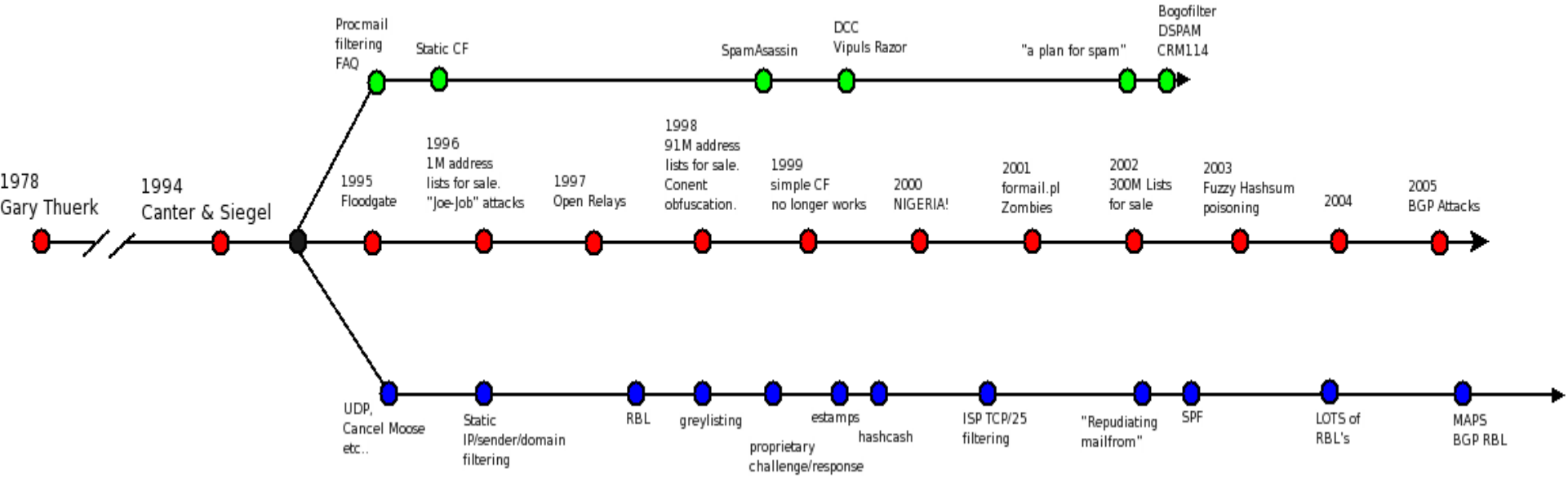
Who IS this guy?

- Dave. Sysadmin.
- Various (mostly useless) Certifications
- I wrote a book. You should buy it (I could use the $4)
- I write the monitoring column for ;login magazine.
- Use SourceMage!

You might find me at

- usenix LISA
- usenix security
- usenix tech
- NANOG
- defcon

It all went down sorta like this:



Conclusions I think we can draw from this

- There is no such thing as repudiating mail from
- Spammers *will* find a way to use your credentials
- Delivery countermeasures are broken, and have generally made things worse.
- Content filtering is NOT dead (contrary to popular belief).

What’s all this about BGP?

In short, Prefix Hijacks make the IPs of others, your own.
This isn't new

They've been used in the past to social engineer blocks of net-space away from unsuspecting RIR's, for the purpose of selling them to private enterprise who didn't know any better.

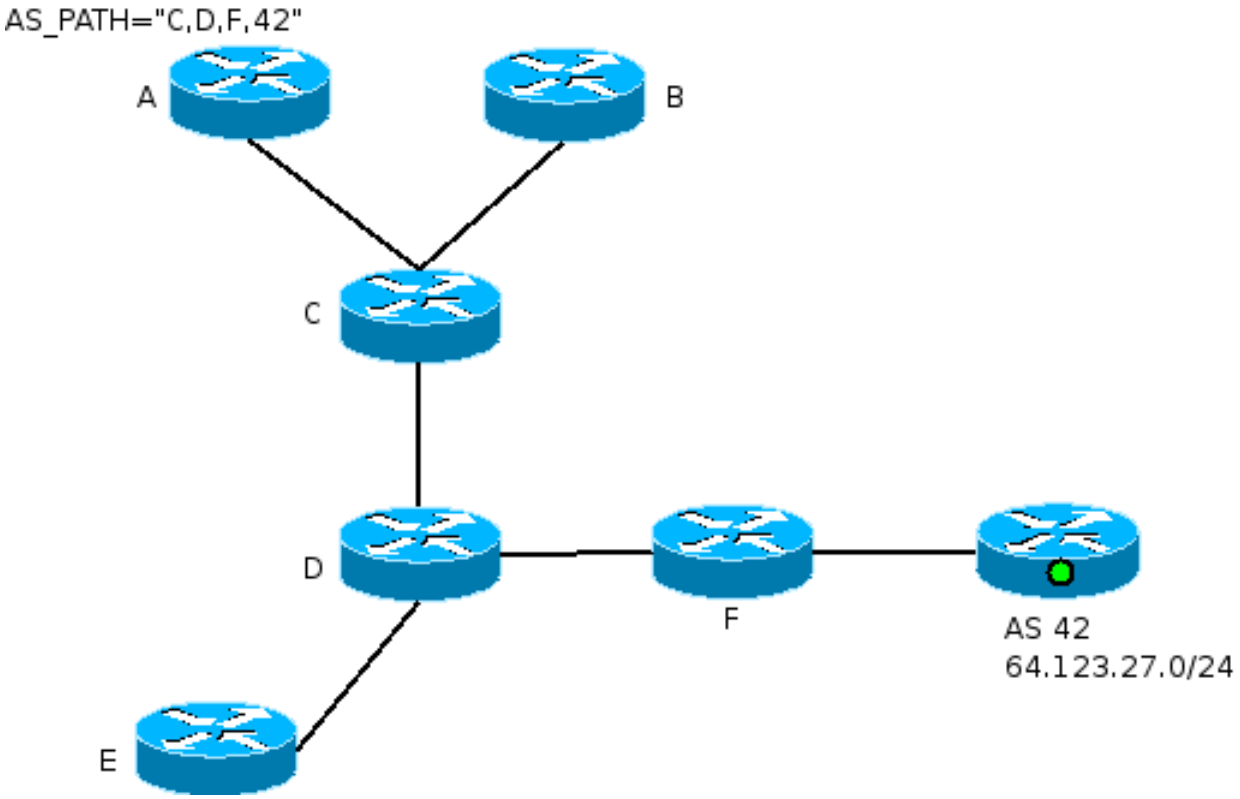
In the past few years, a new kind of prefix hijack has become more prevalent. These are hard to detect and trace because they last for around 15 minutes, and come with a lot of AS prepending

Why would you do this?

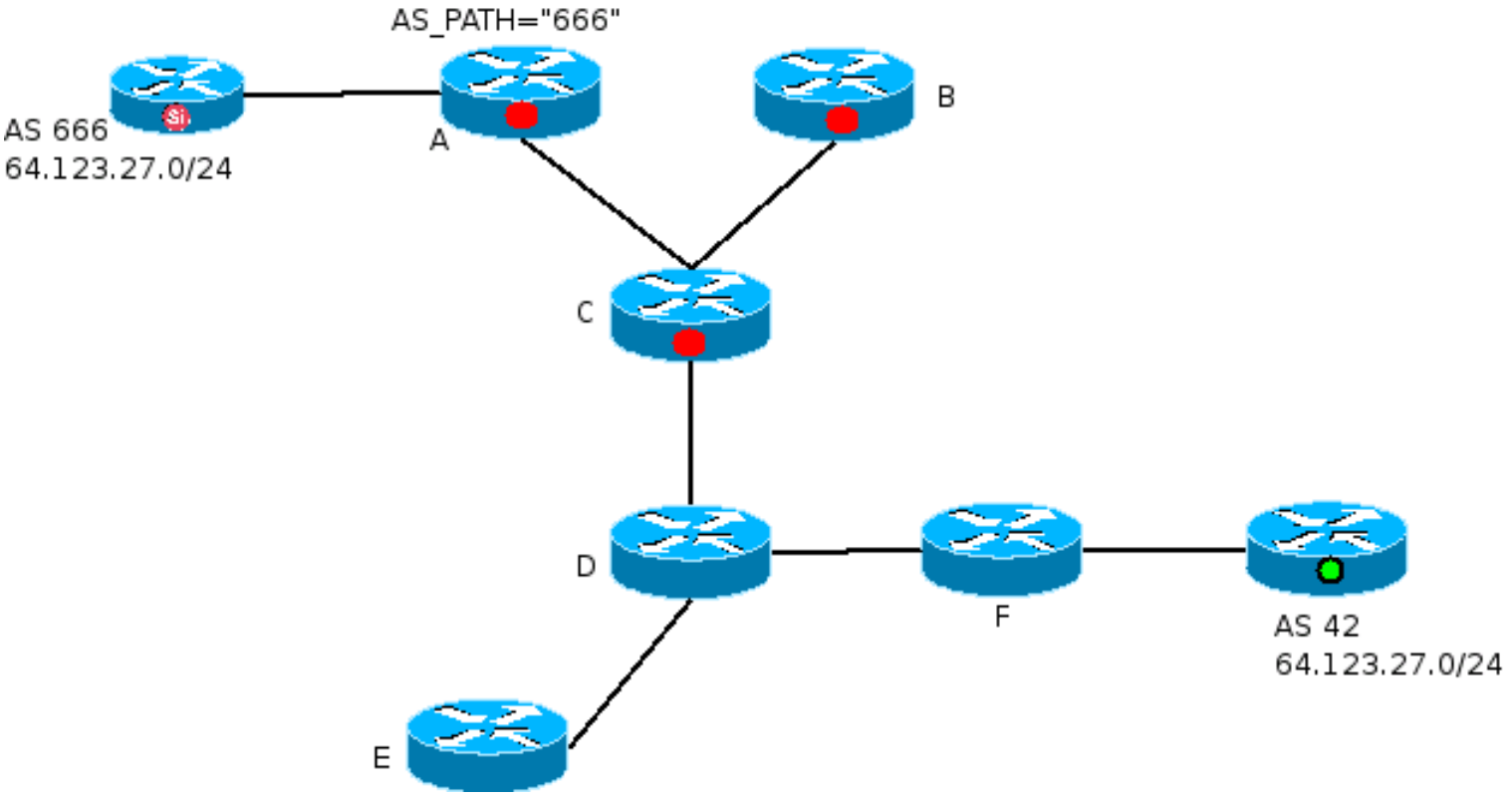
- NMap the NSA
- P2P MP3's
- DOS the RIAA
- Other Illegal acronyms

How does it work?

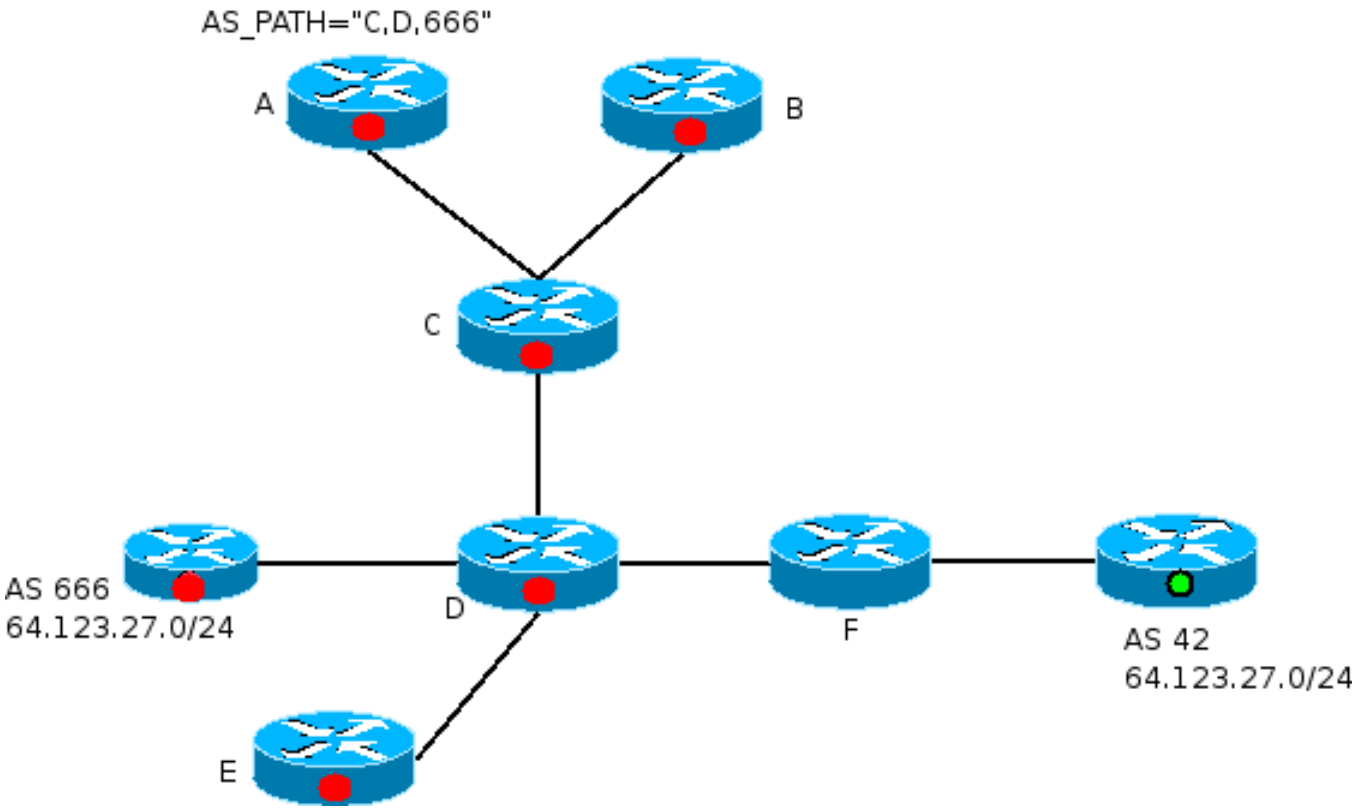
Usually, like this:



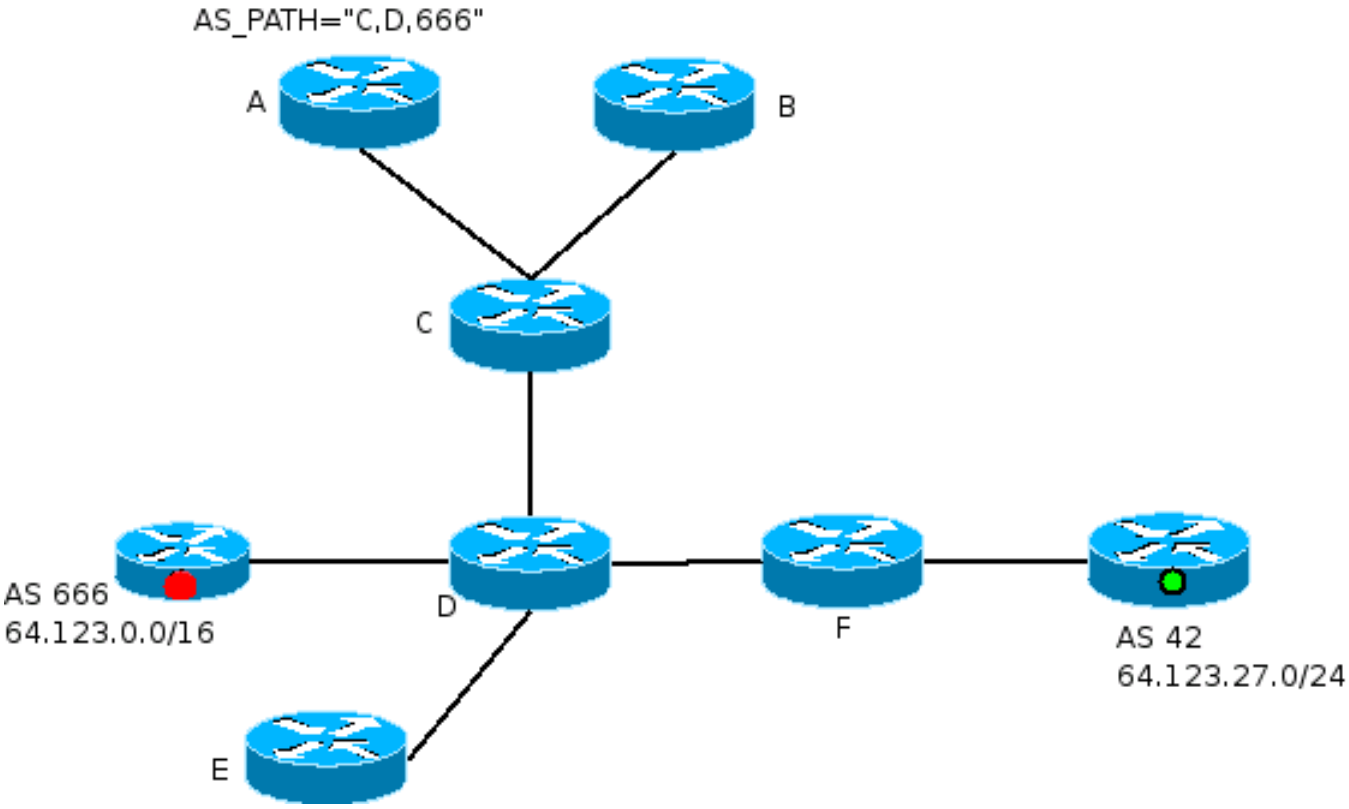
If someone doesn’t play nice:



Or is clever and not nice:



But spammers don’t care about your netblock anyway.



But there isn’t much unallocated IPV4 space right?