Miscreants, Hijacking, and Bogons – Oh My!

or,

"Love and (our) loss in the underground"

Rob Thomas, Cisco/Team Cymru

<robt@cymru.com>

23 OCT 2003

The excitement never ends

What has this to do with ARIN?

- The bad people.
- The bad deeds.
- The good efforts.
- Magic 8-ball says…

The Bad People
Just for fun

- Botnets, DoSnets, roots.
- “don’t call me a kid kthx”
- IRC, the packet magnet.

Meanwhile, the spammers look for willing (read: naive and eager) assistants.

The Bad People
Just for hire

- “need bgps will pay ccs and cvv2”
- route-views and the checklist.
- “lol ur hitting them both ?”

Poor monitoring and dated DBs equate to miscreant opportunity.

The Bad People
Just for cash

- $40,000.00 US.
- “woke up and had $1200 in my paypal”
- The spammers reap what they sow.
- Anti-spam, the packet magnet.

The Bad Deeds

BGP thievery

- Enter the bogons, aka the “safe ranges.”
- “no one notices”
- “kewl the other 1 doesnt filter”
- DDoS, hacking, scanning

Where are the best practices?

The Bad Deeds

The ever changing sources

- Getting caught is bad, getting filtered is worse.
- DDoS - “u cant spoof 10 and 192.168 ne more”
- Enter the ephemeral prefixes!
- “i sold it”

Proxies, prefixes, W32.Slanper

The Good Efforts

We can make a difference

- Sundry bogon projects.
- Sundry hijacked prefix tracking.
- uRPF, but don’t forget the filters.
- Coordination and communication makes correction ***probable***, e.g. nsp-security, INOC-DBA.

Magic 8-ball Says

- Where there is profit, there shall be profiteers.
- Documentation, the bane of the geek, becomes ever more critical.
- The increasing number of vulnerable devices decreases the requirements for spoofing and prefix hijacking. ***This is NOT** good news.* ☹

Thank you!

We’re here to help!

Feel free to contact us.

<http://www.cymru.com>