

# Team Cymru



<http://www.cymru.com/About/teamcymru.html>

# Team Members

Neil Long , [neil.long@cymru.com](mailto:neil.long@cymru.com)

Steve Gill, [gillsr@cymru.com](mailto:gillsr@cymru.com)

Dave Deitrich, [bigdave@cymru.com](mailto:bigdave@cymru.com)

Richard Perlotto , [perlotto@cymru.com](mailto:perlotto@cymru.com)

Rob Thomas , [robt@cymru.com](mailto:robt@cymru.com)

# Network Health Reports

- What are they?
  - An outsider's view of your network
  - Grouped by ASN
  - Weekly basis, ad hoc
    - Migrating to real time and on demand
  - NSP-SEC community only

# Network Health Reports

- What do they include?
  - Worm infected hosts
  - Open proxies
  - Owned Machines
  - Spam Sending Hosts
  - Smurf amplifiers
  - DNS Lamers
  - Inconsistent ASNs, Private ASNs

# Network Health Reports

- View of Active Botnets
  - Botnet status update
  - Goal: getting rid of the pesky ones
  - Malicious intent and monetary value

# Network Health Reports

- Methodology
  - Sniffer traces
  - Netflow
  - Logfiles
  - BGP (Whois, Private ASNs, Inconsistent ASNs)
  - Feedback: <1% false positives

# Network Health Reports

Out of time!

Questions?

[team-cymru@cymru.com](mailto:team-cymru@cymru.com)