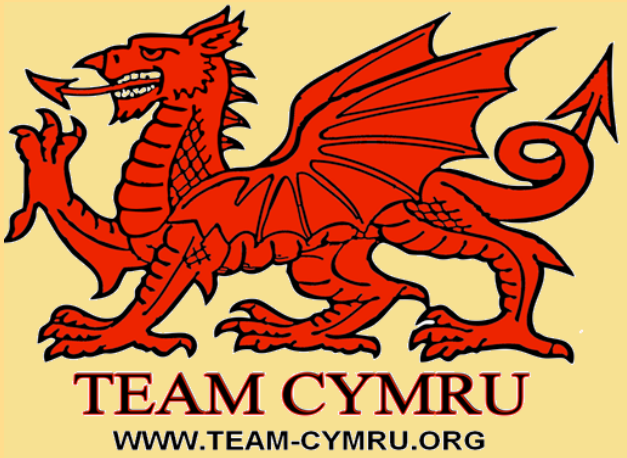
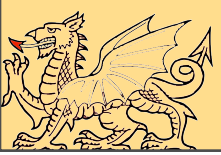
Sept 11th

Team Cymru Update



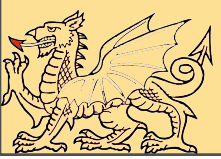
Neil Long

UKNOF 14
London



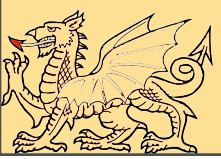
Getting the word out

- outreach@
- YouTube 5minute videos
- Twitter
- Wider than *NOG or nsp-sec



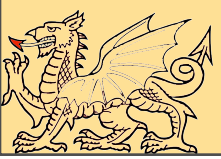
DRG

- NFP side of Team Cymru voluntary tradition (501(c)3 US Federal status)
- http://drg.team-cymru.org/
- Vetted membership
- Progressing - DRG Linux Distro

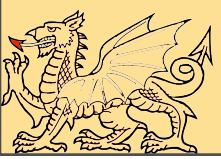


Update on newer feeds

- Open Resolvers
- Malware Hash Registry
- IP to ASN Mapping
- BIN Feed

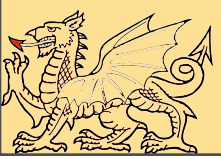


- http://www.team-cymru.org/Services/Resolvers/
- http://www.youtube.com/watch?v=XhSTIqYIQnI
- http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf
- http://www.team-cymru.org/ReadingRoom/Whitepapers/2009/recursion.pdf



Open Resolvers

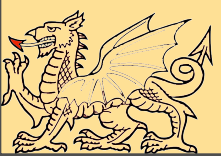
- Attack based on cache poisoning and loose DNS server configurations
- Continuation of work by JTK
- Instigated by major network attack (25Gbps +)
- Initial srcIPs = attack IP sources



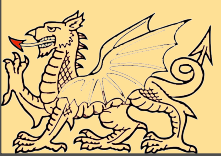
DNS Amplifier attack

DDoS attack uses over 1 million open recursive servers

- Data updated periodically
- ad hoc every few days, million or so random IP addresses

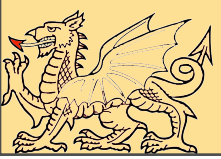


- Clearly lists of Open Resolvers is dangerous e.g. recall Smurf lists
- Data provided to owners of AS with email notification *if* there is data, otherwise silent.
- Solutions can be hard over short term.



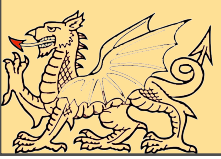
Malware Hash Registry

- Free for non-commercial use.
- Access via Whois, DNS, HTTP, HTTPS
- Query MD5 or SHA1 for known malware



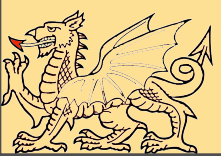
IP to ASN Mapping

- free for non-commercial use
- Whois, DNS, HTTP, HTTPS
- Bulk queries versus single queries
- Multiple BGP feeds, 4hr refresh
- IPv6 data



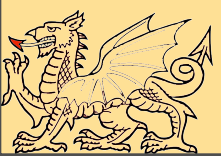
BIN Feed

- Free to bankers....



BATTLE

- Only available to LEOs
- IRC and HTTP Botnet data
- Non-evidential



How to contact:

- neil@cymru.com
- outreach@cymru.com
- team PGP key at www.cymru.com/teamcymrukey.txt