A day in the life of an Security Professional

Donald.Smith@qwest.com

NANOG33

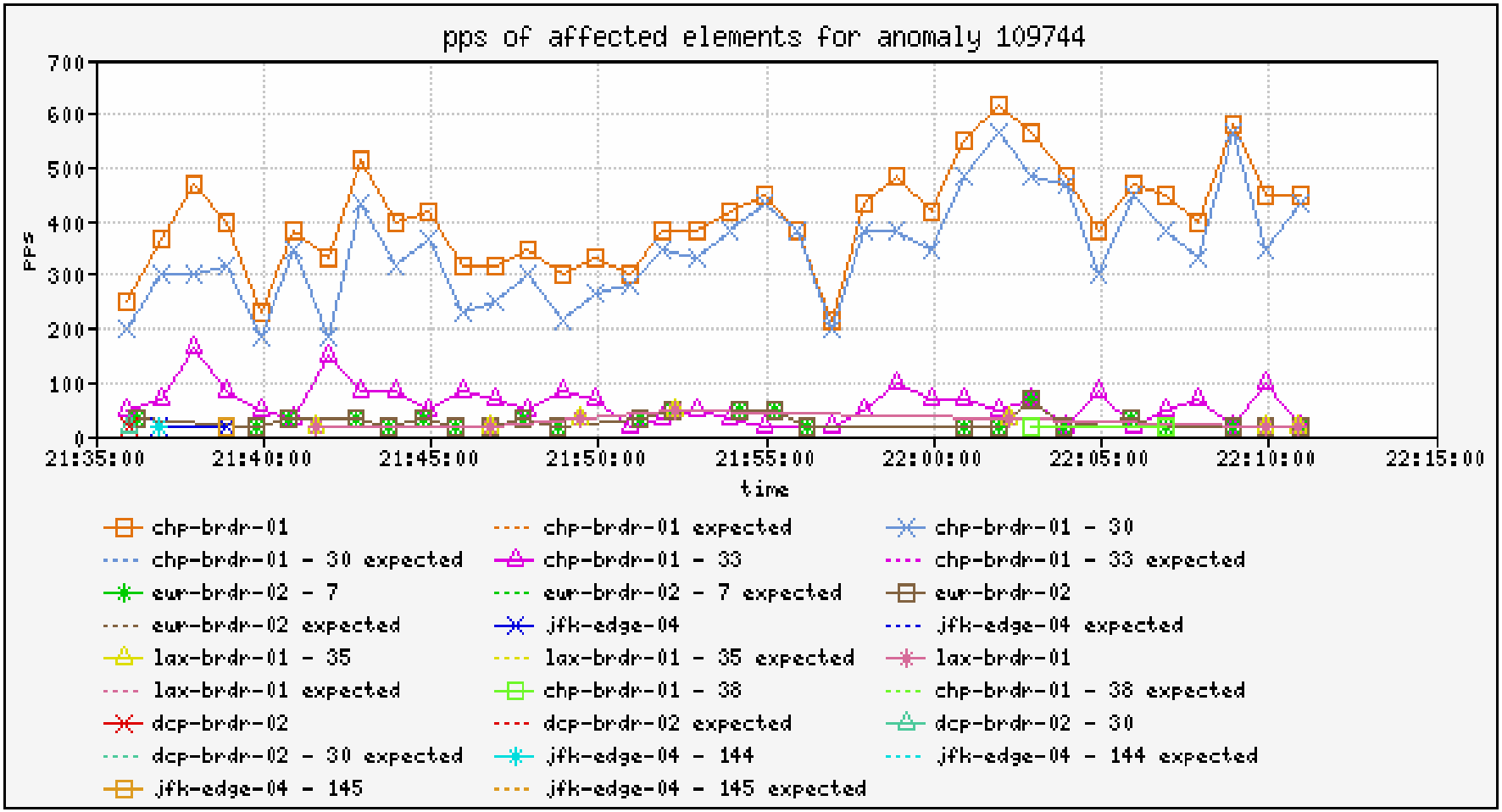
Jan 30th 2004

- Senior SP Qwest backbone
- Internet Storm Center volunteer handler.
- Early notification of new incidents, vulnerabilities, techniques and other security info.
- Coordinate analysis and responses with other SPs.
- Analysis
  - packets
  - malware

Got UDP weird fragments?

- NSP-Security and SANS/ISC handlers reporting weird UDP fragments.
- First seen in October.
- Gather Data

UDP weird fragment Analysis



UDP DNS fingerprinting?

- Probably not.
- RFC791 (Mike Poor)

UDP Direct attack?

- Targeting authoritative DNS servers.
- NO recon

Weird UDP Fragments “explained”

- Packets requesting .
- ISC handler **George Bakos** reconstructed the packet. Similar analysis by **Gerard White** aliant.ca and **Judy Novak (Sourcefire).**
- A broken tool?

Weird UDP Fragments “explained”

- 83.102.166.0/24 seen in hacker irc logs.
- Reflective dns attack with 10 to 1 amplification.
- Stealthy
- Flawed tool

Lab testing of Network Elements

- Preformed by Qwest Architecture Security Team.
- Free, Publicly available tools can be used for most of this testing.
- Testing is fun and interesting
  - Repeatedly crashed one NE with the 3y/o protos snmp test suite.
  - Accessed another NE without a valid login and can be rebooted with a overflow from non-privileged account.

Lab testing of Network Elements

- Vendors have been notified no vulnerability information has been released publicly.
- Mitigation steps are also recommend and tested.

Escalation of security events

- Escalated events include
  - attack Qwest routers.
  - unusual or new attacks
- Don’t be afraid to ask for help.

Notification of new vulnerabilities and exploits

- Early notification of vulnerabilities and exploits.
- review the announcement
- notify ISC, QCIRT and engineers.

!(possible(know_it_all))

- Team-work.
- Ask the experts.
- ISC and NSP resources.
- Sharing with other SPs

Q & A