Bro 2.5 Highlights

SMB Analyzer

NetControl

Intelligence Framework extensions

BroControl sets up “logger” node. Add to your node.cfg:

```
[logger]
type=logger
host=localhost
```

Analyzers

File entropy
Remote framebuffer protocol (VNC)
Radiotap header for 802.11
SSL handoff for IMAP, XMPP, IRC (STARTTLS)
VLAN IDs, MAC addresses
SSL updates

Refactored execution statistics

get_*_stats()

New plugins:

af_packet, kafka, myricom, pf_ring, postgresq, redis, tcprs

Broadmap

Bro Package Manager

- Central package repository on bro.org
- Move bro-plugins over
- Move parts of policy/* over

Bro Cluster (pushed back to 2.6/2.7)

Switch to Broker
New broctld model
Deep Cluster
Higher-level communication framework

Dynamic Configuration

Configuration Framework

Protocol parsing

Improved SMB
OCSP
STUN
WebSocket

osquery Integration

https://github.com/bro/bro-osquery

NetControl++