The Netflow Observatory
An Interactive 3-D Event Visualization

ihmc
VizSec 2013

Larry Bunch
Jeffrey M. Bradshaw
Michael Vignati

multiple maps enable meaningful separation of traffic types

http traffic

blacklisted IPs

all other traffic

Netflow Glyph
source country/ip/port
source tags
size or duration
event count
destination tags
destination country/ip/port

Source Map

Selecting Netflows Reveals Details

103.30.161.238:54500
KR
TCP 0.10KB/2p/4000000ms
184.182.233.47:22
cox.net
Pensacola, FL, US

Agents tag netflows to highlight possible concerns such as blacklisted IPs

05-Apr 18:55:00

05-Apr 18:54:00

05-Apr 18:53:00

05-Apr 18:52:00

http:80

https:443

Rings separate netflows by common attributes such as ports

Timeline Markers

Destination Map

likely intrusion attempts

precede as 'tells' for

horizontal scans

glyph colors indicate ports

IPv4 fractal maps

Research supported by the U.S. Department of Defense and the MIT Lincoln Laboratory

patent pending, application #12156480

glyph colors indicate IP addresses

vertical scans

DDoS attacks

domain map

184.182.233.2:5424
cox.net
Pensacola, FL, US
TCP 0.57KB/4f/11p/28304000ms
101.162.48.240:50260
Brisbane, 04, AU

16-Jul 18:10:00

mail:993

cmap:4447

cmap:4748

dns:53

https:443

http:80

glyph colors indicate countries

flooding / brute force attacks