Shahrulniza Musa, PhD
Malaysian Institute of Information Technology
University Kuala Lumpur, Malaysia

Prof. David J. Parish
High Speed Networks Research Group,
Electronic and Electrical Engineering Department
Loughborough University, United Kingdom

Using Time Series 3D AlertGraph and False Alert Classification to Analyse Snort Alerts

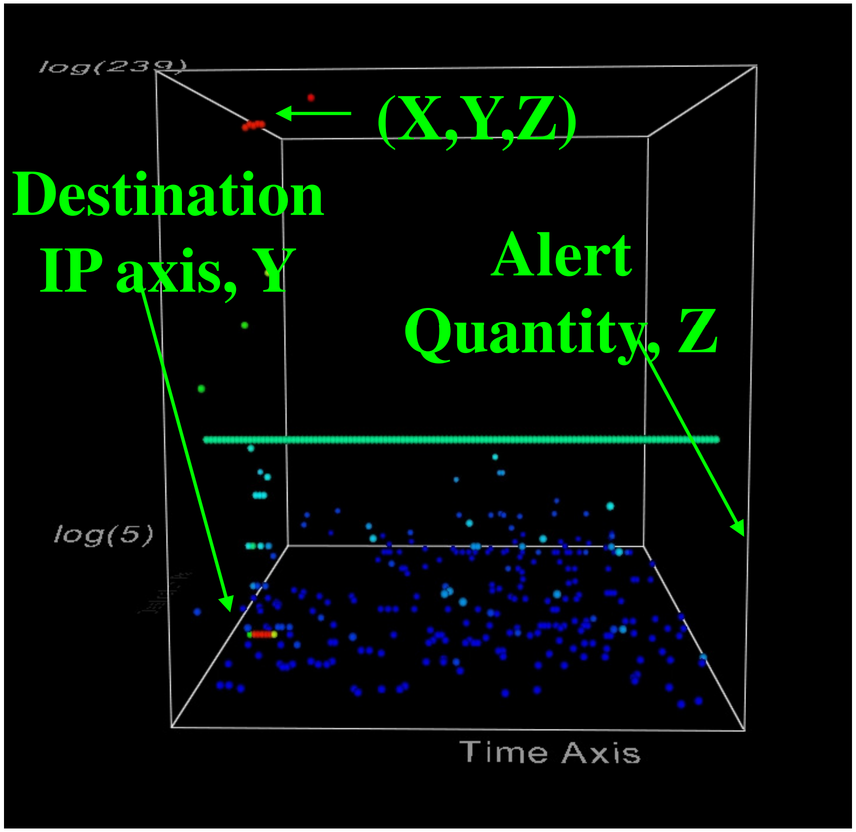
Introduction – Background to the Problem

- A lot of alerts
- Most of them are false
- A lot of information

```
[**] [1:1560:6] WEB-MISC /doc/ access [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
04/09-15:19:46.079304 197.218.177.69:16511 -> 172.16.114.50:80
TCP TTL:63 TOS:0x0 ID:5357 IpLen:20 DgmLen:298 DF
***AP*** Seq: 0x97531B46  Ack: 0xDADDDD8F  Win: 0x7D78  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0678][Xref =>
http://www.securityfocus.com/bid/318]
[**] [1:1560:6] WEB-MISC /doc/ access [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
04/09-15:19:46.299292 197.218.177.69:16521 -> 172.16.114.50:80
TCP TTL:63 TOS:0x0 ID:5377 IpLen:20 DgmLen:362 DF
***AP*** Seq: 0xD948F63F  Ack: 0x210D8B51  Win: 0x7D78  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0678][Xref =>
http://www.securityfocus.com/bid/318]
[**] [1:1560:6] WEB-MISC /doc/ access [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
04/09-15:19:46.318748 197.218.177.69:16586 -> 172.16.114.50:80
TCP TTL:63 TOS:0x0 ID:5392 IpLen:20 DgmLen:363 DF
***AP*** Seq: 0x7C311751  Ack: 0xBD4E2177  Win: 0x7D78  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0678][Xref =>
http://www.securityfocus.com/bid/318]
[**] [1:1411:10] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/09-15:19:48.253464 192.168.1.30:32770 -> 172.16.112.5:161
UDP TTL:254 TOS:0x0 ID:35978 IpLen:20 DgmLen:132 DF
Len: 104
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref =>
http:][Xref => http://www.securityfocus.com/bid/4089][Xref =>
http://www.securityfocus.com/bid/4088]
```

The 3D Time Series AlertGraph

- The time series plot of the quantity of alerts received by a destination IP in a time interval from the pair of source IP address and destination port



(X,Y,Z)

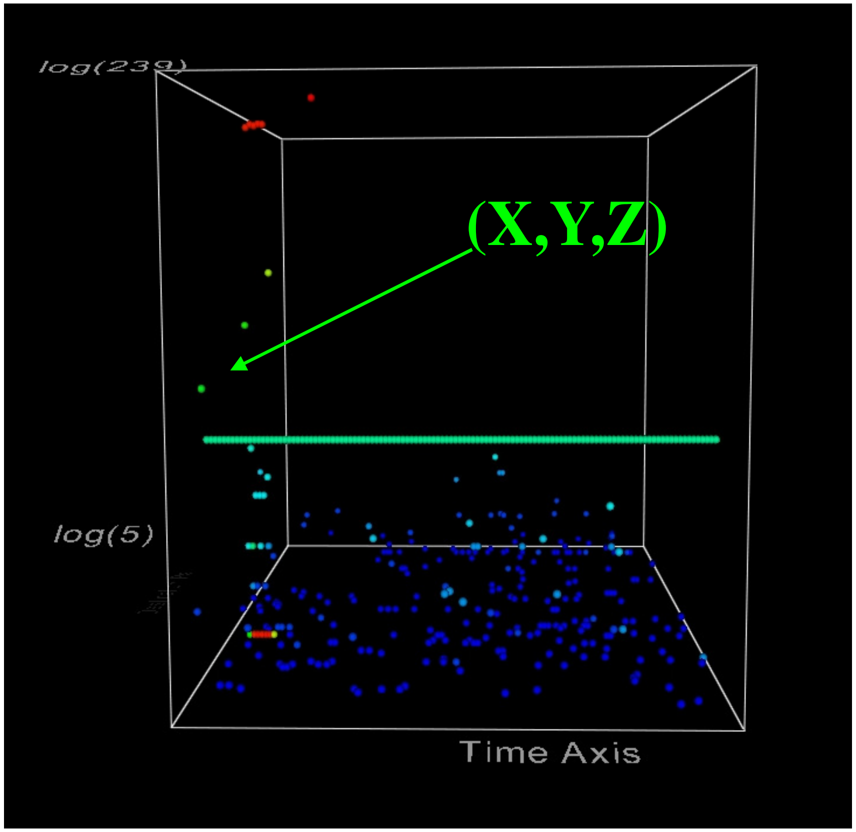
Destination IP axis, Y

Alert Quantity, Z

Time axis, X (default time interval=5 mn)

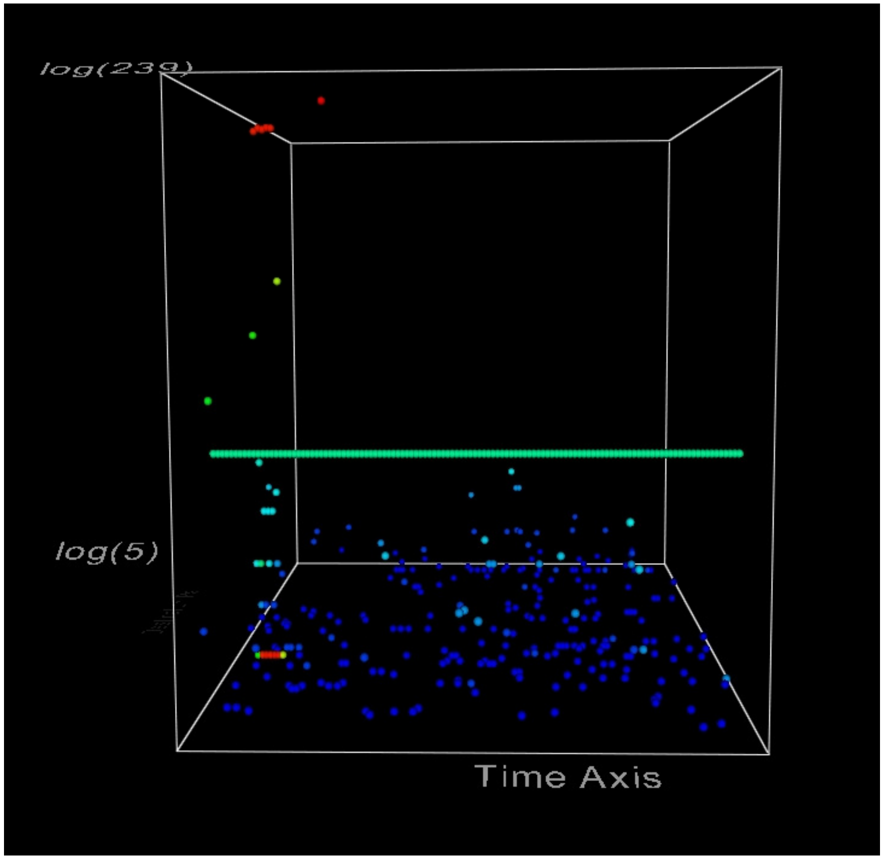
The Data Point - Sphere

- A coloured sphere means during the time interval X, the quantity of alerts Z were received by the destination host Y from source IP and destination port pair



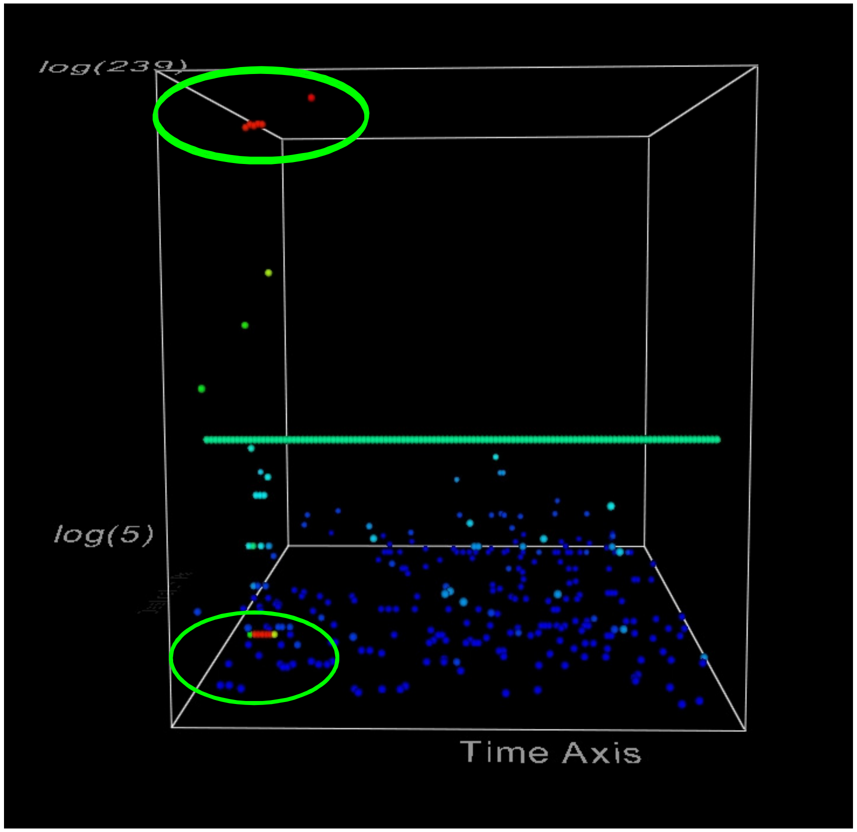
The Colour

- The colour of the sphere reveals the total quantity of alerts at the data point (sphere) - classifier mode : true alerts
- Lowest: Blue
- Highest: Red
- Colour varies from blue to red



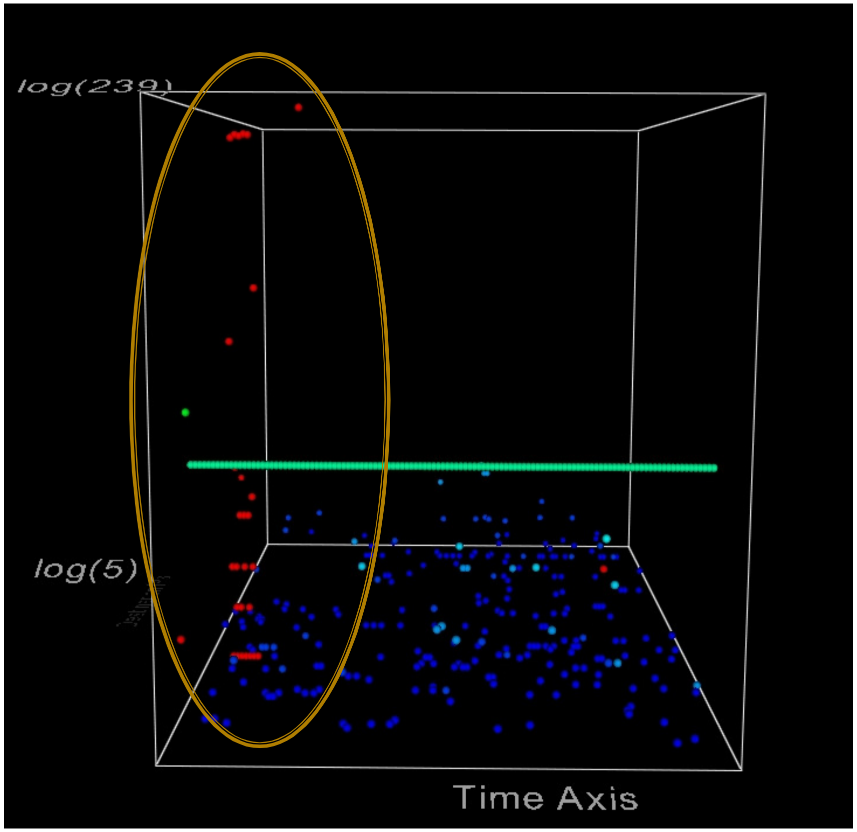
Example – without classifier

- The red spheres on the top : Many alerts in the interval with a unique source IP and destination port.
- The red spheres on the bottom: A single alert from many source IP and destination port pairs.

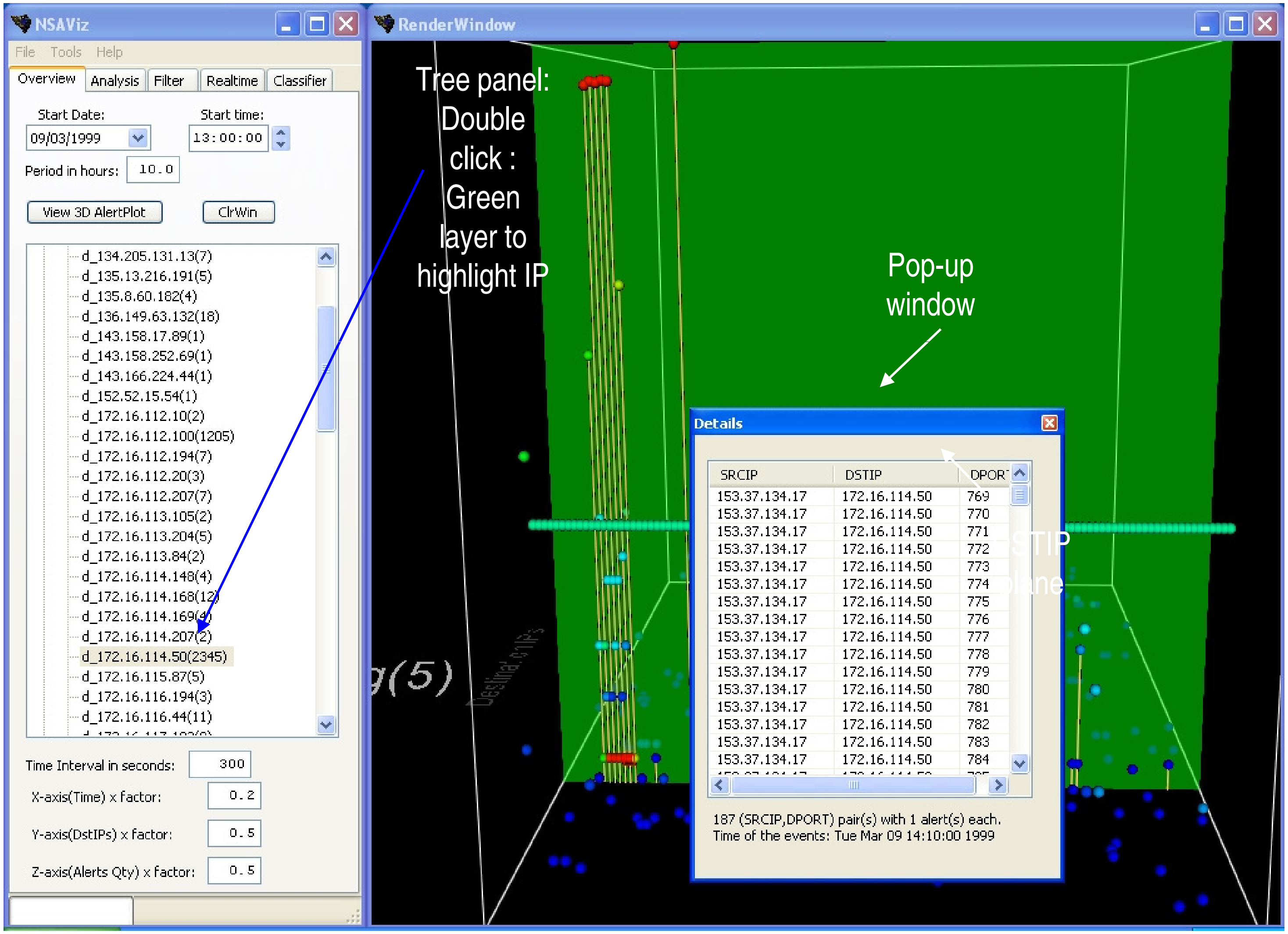


Previous Example with Classifier

- All the red spheres suggested true alerts



The Interaction



Start Date: 09/03/1999

Start time: 13:00:00

Period in hours: 10.0

```
d_134.205.131.13(7)
d_135.13.216.191(5)
d_135.8.60.182(4)
d_136.149.63.132(18)
d_143.158.17.89(1)
d_143.158.252.69(1)
d_143.166.224.44(1)
d_152.52.15.54(1)
d_172.16.112.10(2)
d_172.16.112.100(1205)
d_172.16.112.194(7)
d_172.16.112.20(3)
d_172.16.112.207(7)
d_172.16.113.105(2)
d_172.16.113.204(5)
d_172.16.113.84(2)
d_172.16.114.148(4)
d_172.16.114.168(12)
d_172.16.114.169(4)
d_172.16.114.207(2)
d_172.16.114.50(2345)
d_172.16.115.87(5)
d_172.16.116.194(3)
d_172.16.116.44(11)
```

Time Interval in seconds: 300

X-axis(Time) x factor: 0.2

Y-axis(DstIPs) x factor: 0.5

Z-axis(Alerts Qty) x factor: 0.5

SRCIP	DSTIP	DPOR
153.37.134.17	172.16.114.50	769
153.37.134.17	172.16.114.50	770
153.37.134.17	172.16.114.50	771
153.37.134.17	172.16.114.50	772
153.37.134.17	172.16.114.50	773
153.37.134.17	172.16.114.50	774
153.37.134.17	172.16.114.50	775
153.37.134.17	172.16.114.50	776
153.37.134.17	172.16.114.50	777
153.37.134.17	172.16.114.50	778
153.37.134.17	172.16.114.50	779
153.37.134.17	172.16.114.50	780
153.37.134.17	172.16.114.50	781
153.37.134.17	172.16.114.50	782
153.37.134.17	172.16.114.50	783
153.37.134.17	172.16.114.50	784

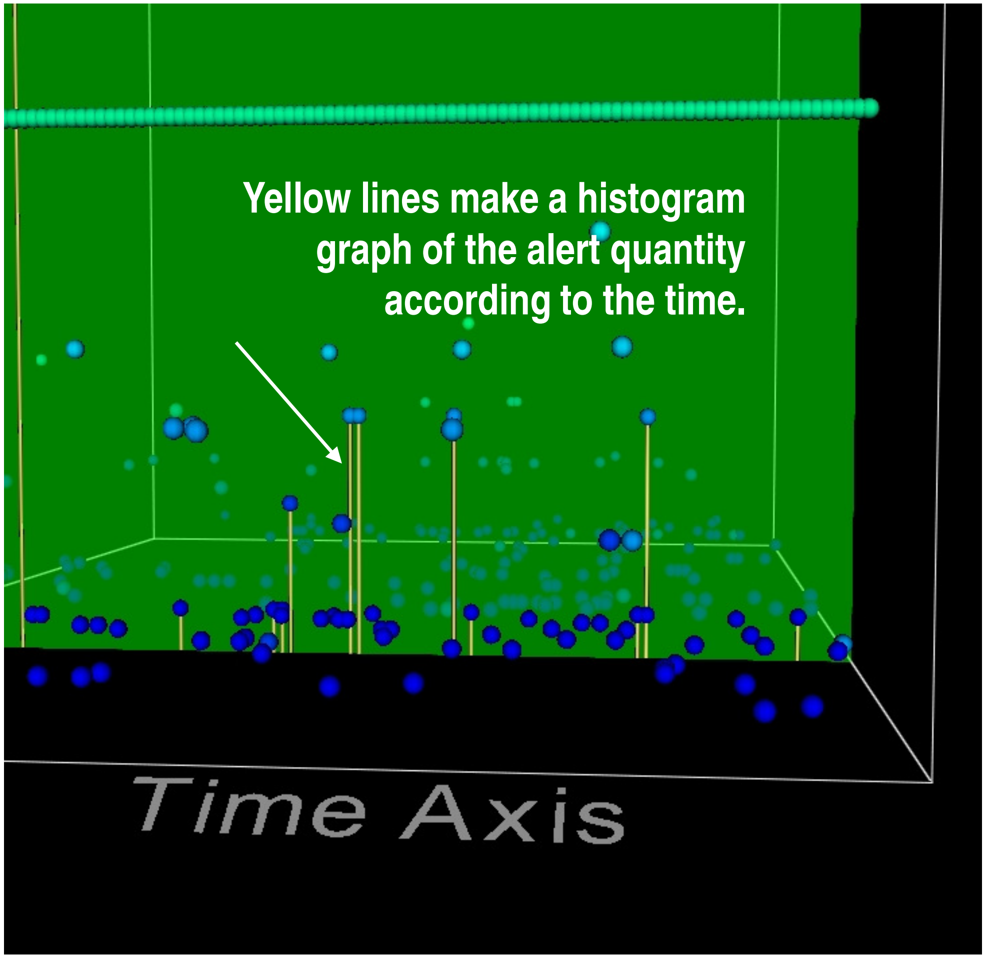
187 (SRCIP,DPORT) pair(s) with 1 alert(s) each.
Time of the events: Tue Mar 09 14:10:00 1999

Tree panel: Double click : Green layer to highlight IP

Pop-up window

DSTIP plane

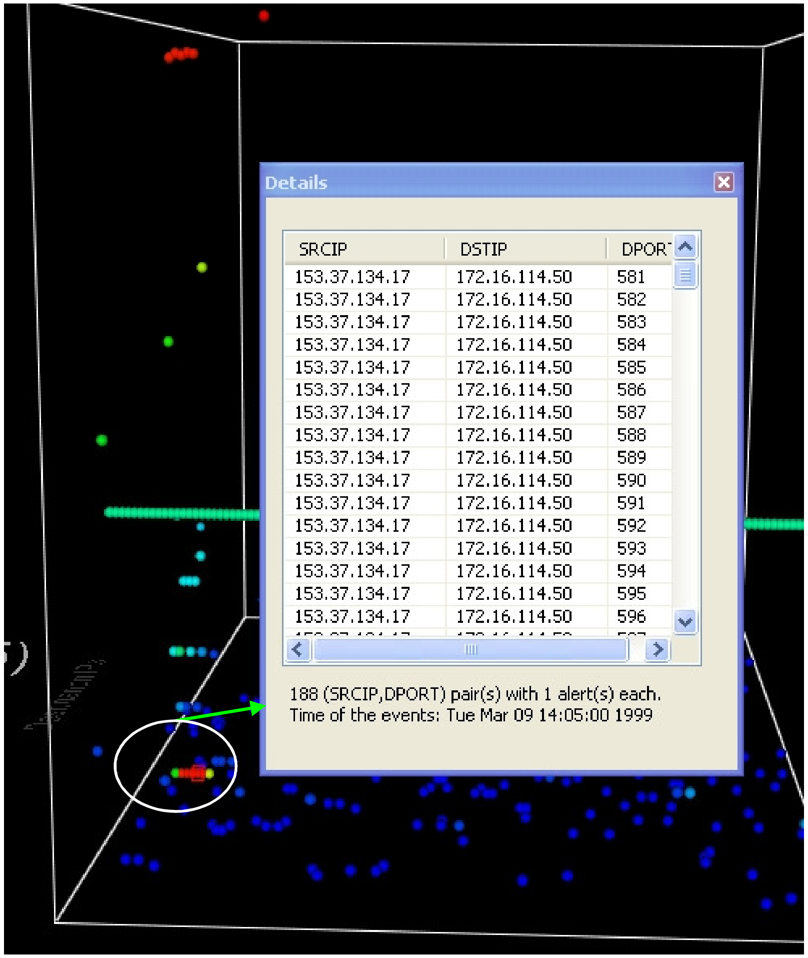
The Interaction



Yellow lines make a histogram graph of the alert quantity according to the time.

Example: Port Scan

- A unique source IP targeting many destination ports

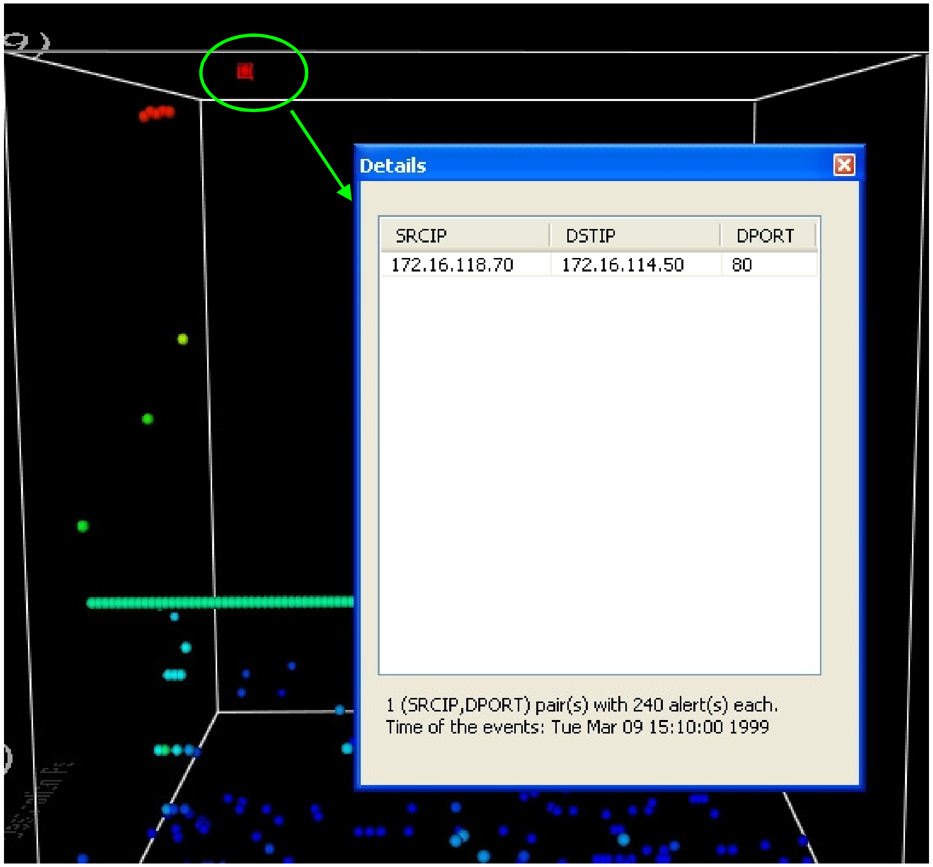


SRCIP	DSTIP	DPOR
153.37.134.17	172.16.114.50	581
153.37.134.17	172.16.114.50	582
153.37.134.17	172.16.114.50	583
153.37.134.17	172.16.114.50	584
153.37.134.17	172.16.114.50	585
153.37.134.17	172.16.114.50	586
153.37.134.17	172.16.114.50	587
153.37.134.17	172.16.114.50	588
153.37.134.17	172.16.114.50	589
153.37.134.17	172.16.114.50	590
153.37.134.17	172.16.114.50	591
153.37.134.17	172.16.114.50	592
153.37.134.17	172.16.114.50	593
153.37.134.17	172.16.114.50	594
153.37.134.17	172.16.114.50	595
153.37.134.17	172.16.114.50	596

188 (SRCIP,DPORT) pair(s) with 1 alert(s) each.
Time of the events: Tue Mar 09 14:05:00 1999

Example: DOS (BACK)

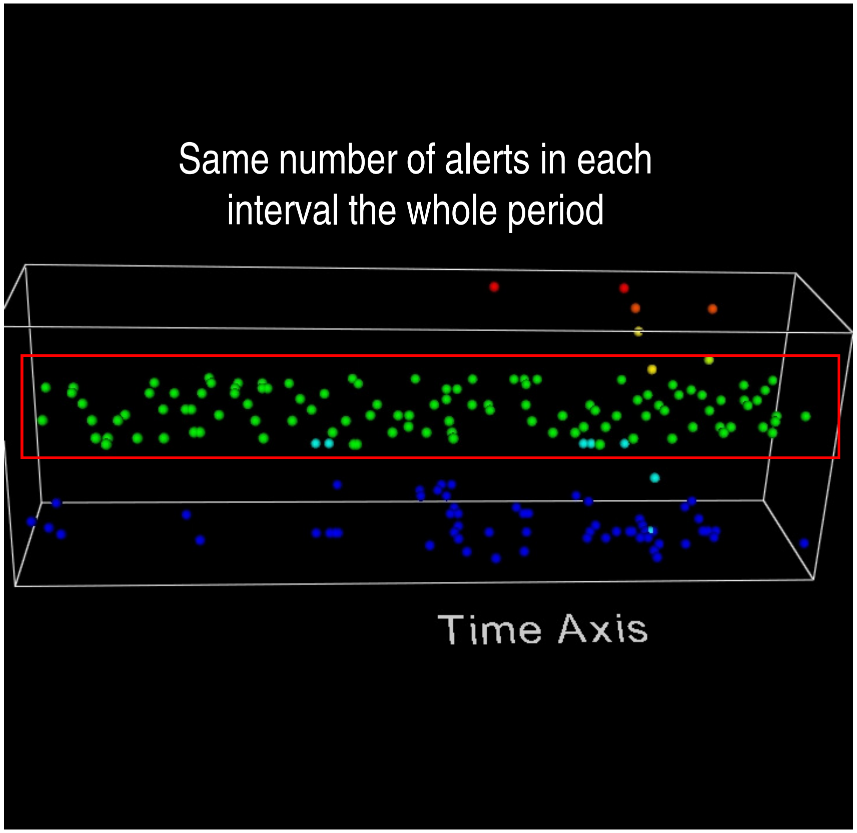
- Denial of service attack against apache webserver where a client requests a URL containing many backslashes.
- Many alerts from unique (srcip,dport)

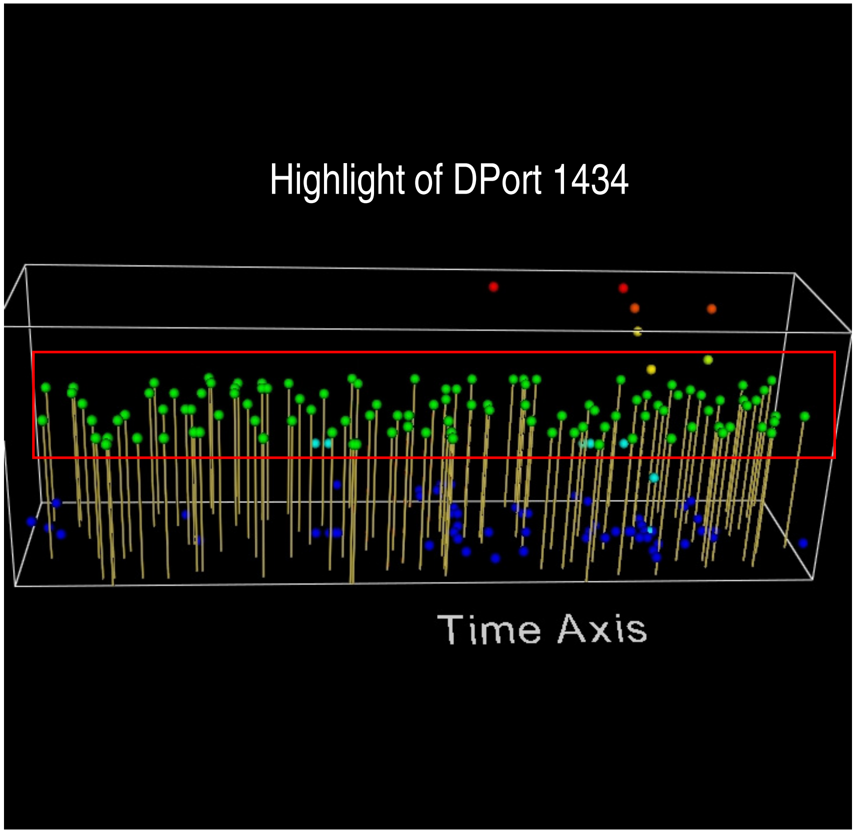


SRCIP	DSTIP	DPORT
172.16.118.70	172.16.114.50	80

1 (SRCIP,DPORT) pair(s) with 240 alert(s) each.
Time of the events: Tue Mar 09 15:10:00 1999

Example: Slammer Worm


Same number of alerts in each interval the whole period


Highlight of DPort 1434

Destination port 1434 was used in slammer worm propagation.

The Classifier

- Classification tree Algorithm
  - Based on C4.5 classification Algorithm
    - Decision tree based on information entropy theory
  - Post-Pruning (to avoid over-fitting)
  - The inputs were generalised
  - Using orange AI : open-source data mining and artificial intelligent module

The Classifier Inputs

Alert attributes	Generalisation
Src / Dst IP address	Local host Foreign host
Src / Dst port	Standard (< 1024) Ephemeral (between 1024 and 4999) Unassigned (> 5000) Unknown
Alert Classtype	Class type as specified by Snort
IP Datagram length	Actual byte value
IP protocol	UDP, TCP, ICMP, Reserve, Other

The Classifier Performance

- Performance Score

	Classification Accuracy (CA)	Brier Score (BS)	Area under the receiver operating characteristic (ROC) curve (AUC)
Scores	0.9857	0.0265	0.9892

- Confusion Matrix

	Negative (false) Predicted	Positive (true) Predicted
Negative (false) (273)	267 (TN=0.9780)	6 (FP=0.0220)
Positive (true) (288)	5 (FN=0.0174)	283 (TP=0.9826)

User Evaluation

- Usability Study
  - Neilson [68], 3-5 evaluators can identify 75-80% of all usability problems.
- Usability Problems found
  - Controlling 3D image
    - Suggestions: More training, Navigation control as in google map
  - Crowded GUI in Analysis panel
    - Suggestion: New organisation
  - Suggestion for mouse over information

Analysis of User Evaluation

no		Average	Std dev
A1	Overview	4.67	0.58
B1	Scatter plot	4.67	0.58
B2	Parallel plot	4.67	0.58
B3	Timeline view	3.67	1.53
B4	Plane view	4.00	1.73
B5	World globe	4.67	0.58
B6	World plane	4.67	0.58
C1	GUI - user friendly	4.33	0.58
C2	Interaction	4.67	0.58
C3	Classifier features	4.67	0.58
C4	Filter features	4.67	0.58
C5	Real-time	4.00	0.00
C6	Reporting features	4.67	0.58
C7	Comparison with similar tool	na	na
C8	Perform Security tasks	4.67	0.58

Advantages of 3D AlertGraph

- Highlights the true alerts
- Interaction tools for more information
- A huge numbers of alerts can be viewed in single display
- A temporal characteristic of attacks can be discovered

Q&A

Thank you
very much