Verifying Network IoC Hits

in Millions of Packets

Jasper Bongertz, Airbus CyberSecurity
@packetjay

Problem Scenario 1/2

- Scanning for network IoCs is relatively easy: use an IDS/IPS
  - snort, suricata, commercial appliances
- Perform live traffic analysis, or from PCAPs

Problem Scenario 2/2

- IDS scan can easily result in tons of alerts
- Alerts are often spread over hundreds of PCAPs, containing millions of packets
- **Main challenge**: alerts usually contain info about the matching packet only

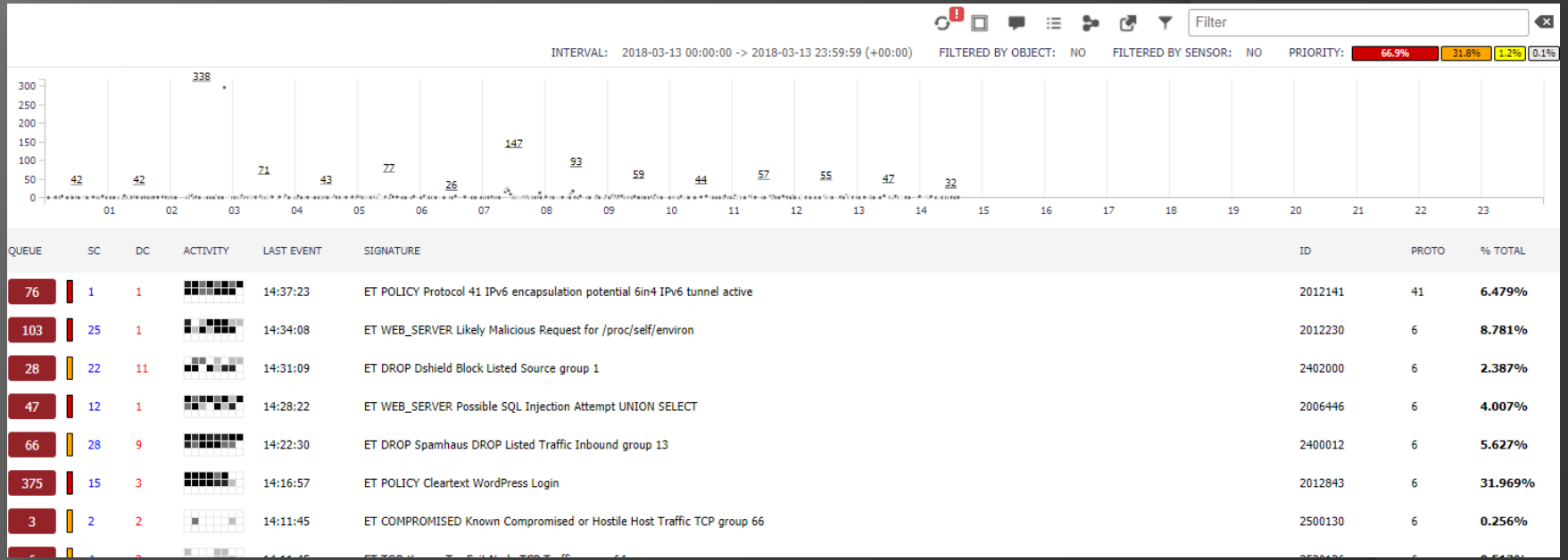
Alert Example

```
[**] [1:2101201:11] GPL WEB_SERVER 403 Forbidden [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/04-02:09:08.142211 81.209.179.120:80 -> 142.4.215.116:56182
TCP TTL:55 TOS:0x14 ID:19599 IpLen:20 DgmLen:412 DF
***A**** Seq: 0xD5D42DAC  Ack: 0x3C270191  Win: 0xA580  TcpLen: 32
```

- The newer unified2 format is a binary format, which does not contain the rule name (just the SID, e.g. 1:2101202:11)

Challenge

- The challenge is to get the full attack/alert context, e.g. the whole TCP conversation
- Searching in Wireshark using display filters:
  - Yup, it's possible of course
  - but it's no fun
  - and it's slooooooooow
- Even with tshark scripting: running over all files again and again for each conversation is not efficient


Filter
INTERVAL: 2018-03-13 00:00:00 -> 2018-03-13 23:59:59 (+00:00)
FILTERED BY OBJECT: NO
FILTERED BY SENSOR: NO
PRIORITY: 66.9% 31.8% 1.2% 0.1%
300
250
200
150
100
50
0
42 42 338 71 43 77 26 147 93 59 44 57 55 47 32
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
QUEUE SC DC ACTIVITY LAST EVENT SIGNATURE ID PROTO % TOTAL
76 1 1 14:37:23 ET POLICY Protocol 41 IPv6 encapsulation potential 6in4 IPv6 tunnel active 2012141 41 6.479%
103 25 1 14:34:08 ET WEB_SERVER Likely Malicious Request for /proc/self/environ 2012230 6 8.781%
28 22 11 14:31:09 ET DROP Dshield Block Listed Source group 1 2402000 6 2.387%
47 12 1 14:28:22 ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT 2006446 6 4.007%
66 28 9 14:22:30 ET DROP Spamhaus DROP Listed Traffic Inbound group 13 2400012 6 5.627%
375 15 3 14:16:57 ET POLICY Cleartext WordPress Login 2012843 6 31.969%
3 2 2 14:11:45 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 66 2500130 6 0.256%


TROOPERS
MAKE THE WORLD A SAFER PLACE

Thanks! Questions?

- TraceWrangler: www.tracewrangler.com
- Mail: jasper@packet-foo.com
- Blog: blog.packet-foo.com
- Twitter: @packetjay