New Search

```
index=botsv2 sourcetype=suricata earliest=0
| stats count by src_ip, dest_ip, alert.signature
| sort - count
| head 20
```

Time range: All time

✓ **325,191 events** (before 12/26/25 8:17:42.000 AM) No Event Sampling

Statistics (20)

src_ip	dest_ip	alert.signature	count
10.0.1.1	10.0.1.100	ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection	1547
10.0.1.101	71.39.18.121	ET POLICY RDP connection confirm	9
10.0.1.120	199.117.103.176	ET POLICY Vulnerable Java Version 1.8.x Detected	6
10.0.2.109	45.77.65.211	SURICATA TLS invalid handshake message	5
10.0.2.109	45.77.65.211	SURICATA TLS invalid record/traffic	5
45.77.65.211	10.0.2.109	SURICATA TLS invalid handshake message	5
45.77.65.211	10.0.2.109	SURICATA TLS invalid record/traffic	5
10.0.1.120	199.117.103.138	ET POLICY Vulnerable Java Version 1.8.x Detected	4
10.0.4.2	10.0.1.100	ET TROJAN OSX Backdoor Quimitchin DNS Lookup	4
10.0.2.107	45.77.65.211	SURICATA TLS invalid handshake message	3
10.0.2.107	45.77.65.211	SURICATA TLS invalid record/traffic	3
37.187.30.78	10.0.2.101	ET POLICY TLS possible TOR SSL traffic	3
45.77.65.211	10.0.2.107	SURICATA TLS invalid handshake message	3
45.77.65.211	10.0.2.107	SURICATA TLS invalid record/traffic	3
10.0.1.120	199.117.103.67	ET POLICY Vulnerable Java Version 1.8.x Detected	2
10.0.2.107	93.184.216.172	SURICATA TLS invalid handshake message	2
10.0.2.107	93.184.216.172	SURICATA TLS invalid record/traffic	2
138.68.174.81	10.0.2.101	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 127	2
37.187.30.78	10.0.2.101	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 358	2
93.184.216.172	10.0.2.107	SURICATA TLS invalid handshake message	2