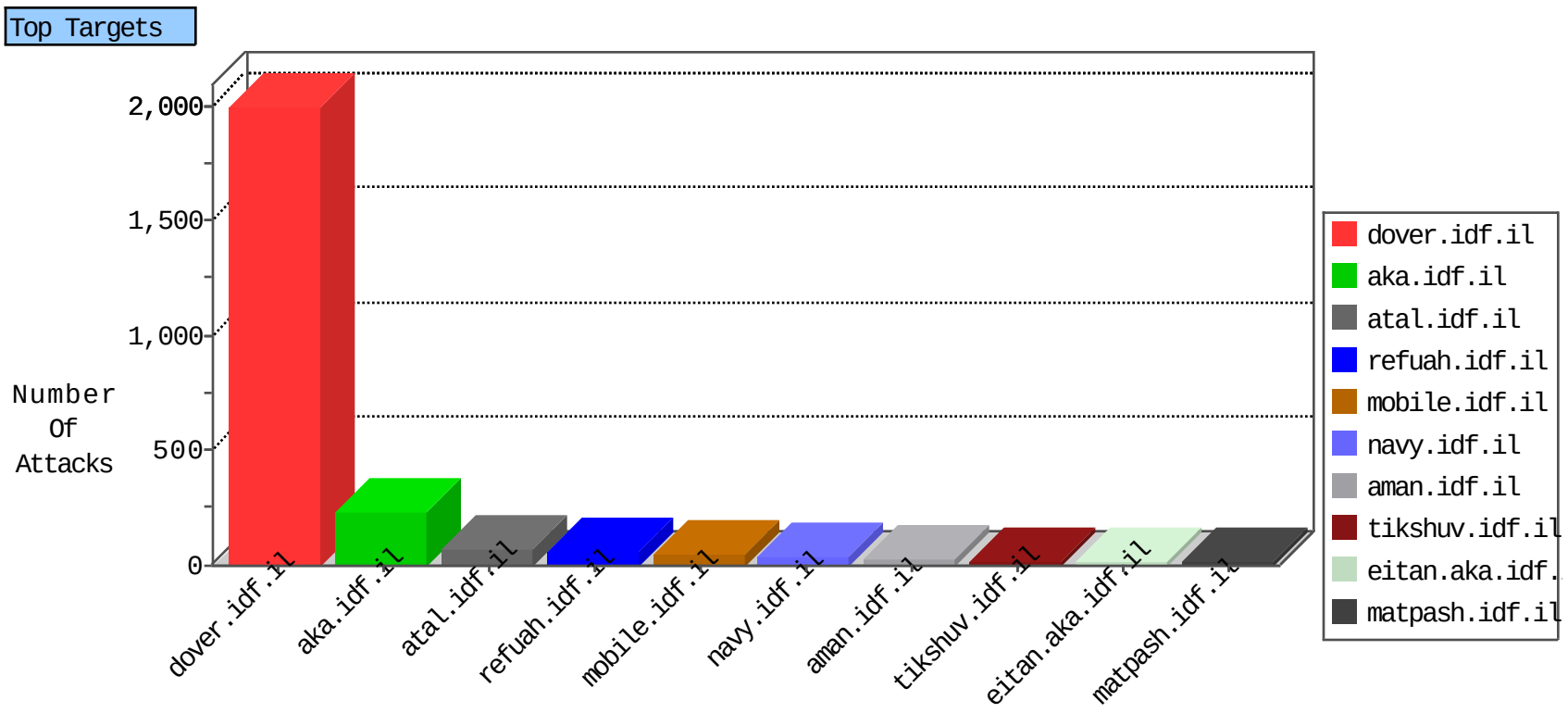
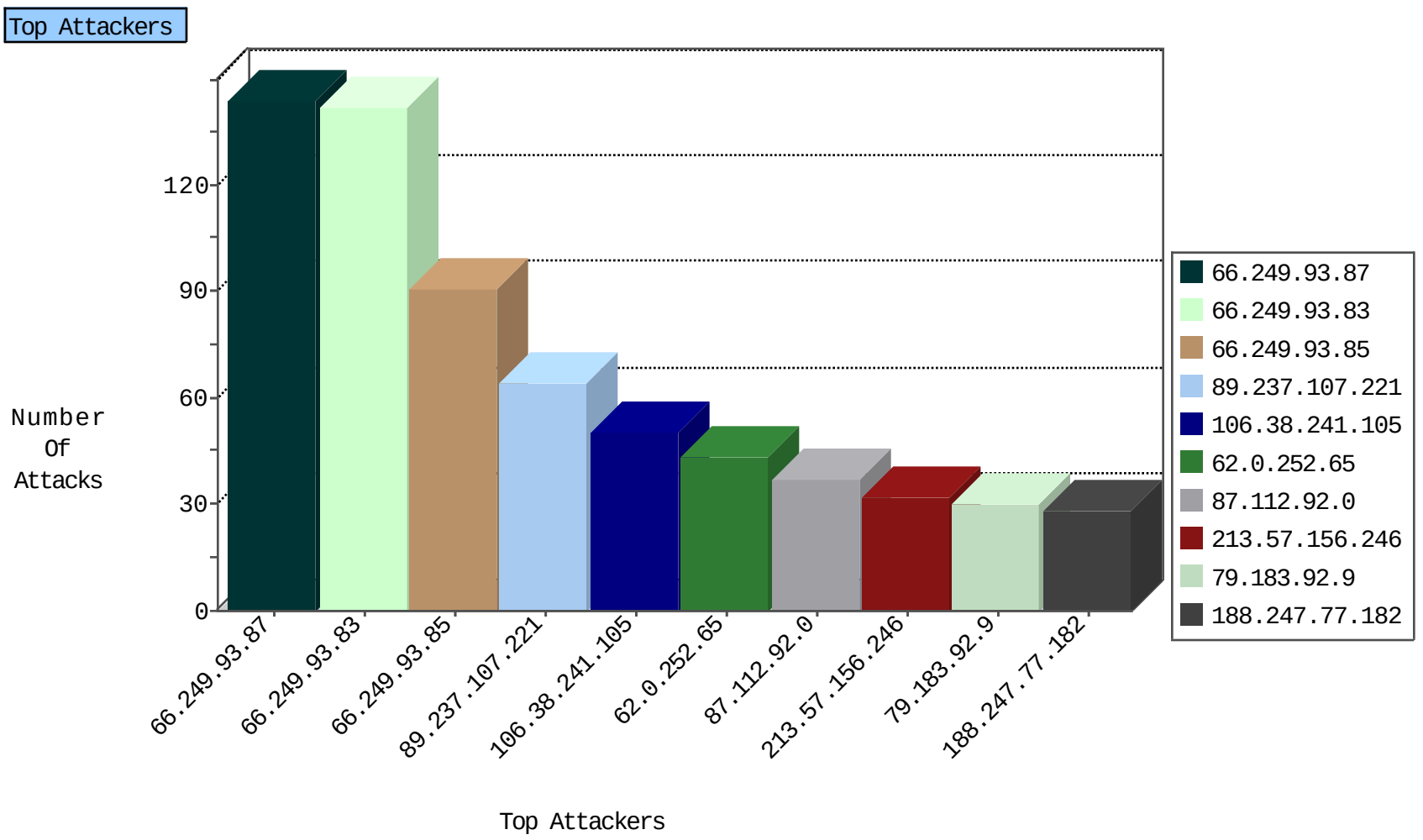
09-18-2016-19:04:05 to 09-18-2016-20:04:05

# IDF Under Attack Daily Report



09-18-2016-19:04:05 to 09-18-2016-20:04:05

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.117.245.12 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 198.133.224.147 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 198.82.160.238 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 178.39.218.11 | Switzerland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 129.93.229.138 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 130.217.77.2 | New Zealand | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 79.183.92.9 | Israel | 147.237.76.86 | navy.idf.il | Invalid TCP Flags | drop | 2 |
| 131.247.2.241 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 194.29.178.14 | Poland | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 130.194.252.8 | Australia | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.10.18.52 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 204.85.191.10 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 198.133.224.147 | United States | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 185.4.135.203 | Greece | 147.237.77.178 | e.matpash.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 139.78.141.243 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.32.84.160 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 204.12.220.84 | United States | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.193.252 | United States | 147.237.77.233 | atal.idf.il | block-sp-traf1 | forward | 1 |
| 194.29.178.14 | Poland | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 156.56.250.227 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.42.142.45 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 204.85.191.11 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 63.141.231.194 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | forward | 1 |
| 185.4.135.203 | Greece | 147.237.77.179 | e.mazi.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 141.22.213.34 | Germany | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 204.12.220.85 | United States | 147.237.77.234 | halag.idf.il | block-sp-traf1 | forward | 1 |
| 195.113.161.84 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 173.208.150.118 | United States | 147.237.77.235 | sviva.idf.il | block-sp-traf1 | forward | 1 |
| 128.223.8.113 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 208.110.84.68 | United States | 147.237.76.200 | eitan.aka.idf.il | block-sp-traf1 | forward | 1 |
| 198.204.224.238 | United States | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.242.194 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 192.33.90.69 | Switzerland | 147.237.72.156 | aman.idf.il | network flood IPv4 ICMP | drop | 1 |
| 142.54.174.86 | United States | 147.237.0.34 | tikshuv.idf.il | block-sp-traf1 | forward | 1 |
| 129.93.229.139 | United States | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 204.12.220.86 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 1 |
| 80.82.70.24 | Netherlands | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 1 |
| 134.197.113.3 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.223.8.114 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 200.19.159.34 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 63.141.242.196 | United States | 147.237.72.156 | aman.idf.il | block-sp-traf1 | forward | 1 |
| 153.90.1.34 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |

09-18-2016-19:04:05 to 09-18-2016-20:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 30 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 18 |
| 67.228.38.74 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 209.15.196.171 | Canada | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 2 |
| 89.248.167.131 | Netherlands | 147.237.77.61 | e.cogat.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

09-18-2016-19:04:05 to 09-18-2016-20:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 79.183.92.9 | 147.237.76.86 | Israel | navy.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 24 |
| 66.249.93.216 | 147.237.77.176 | Europe | matpash.idf.il | ET SCAN NMAP -sA (2) | 10 |
| 67.228.38.74 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 8 |
| 209.15.196.171 | 147.237.77.74 | Canada | law.idf.il | SQL Injection - Select From | 8 |
| 103.234.38.89 | 147.237.8.24 | Vietnam | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 7 |
| 91.201.236.158 | 147.237.76.31 | Ukraine | nakchal.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 223.149.201.85 | 147.237.8.24 | China | e.lifestyle.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.218.200.137 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.254.34.165 | 147.237.76.201 | Vietnam | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 40.114.15.49 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 176.47.117.187 | 147.237.77.216 | Saudi Arabia | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 113.240.250.154 | 147.237.77.170 | China | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.232.98.3 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.158 | 147.237.76.31 | Ukraine | nakchal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 62.210.189.248 | 147.237.72.167 | France | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.254.34.165 | 147.237.77.121 | Vietnam | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.141.192.67 | 147.237.8.45 | Russian Federation | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.240.250.154 | 147.237.77.227 | China | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.232.98.3 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 103.234.38.89 | 147.237.8.24 | Vietnam | e.lifestyle.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |

09-18-2016-19:04:05 to 09-18-2016-20:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 89.237.107.221 | France | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 64 |
| 66.249.93.83 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 45 |
| 66.249.93.83 | Europe | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 45 |
| 66.249.93.83 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 45 |
| 62.0.252.65 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 43 |
| 66.249.93.87 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 41 |
| 66.249.93.87 | Europe | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 41 |
| 66.249.93.87 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 41 |
| 87.112.92.0 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 37 |
| 66.249.93.85 | Europe | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 26 |
| 37.26.146.161 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 176.13.5.81 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 66.249.93.85 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 21 |
| 66.249.93.85 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 21 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 188.247.77.182 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 2.55.134.22 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 130.95.254.204 | Australia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.210.163.21 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.85.238 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.70 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 84.109.3.38 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 31.168.178.138 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 37.26.147.179 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 84.111.37.181 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 2.55.129.5 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 213.57.153.36 | Israel | 147.237.0.34 | tikshuv.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 12 |
| 192.114.105.254 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 213.57.156.246 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.253.207.113 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 11 |
| 89.237.100.222 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 5.102.253.67 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 141.226.217.239 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 79.179.104.20 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 176.13.21.134 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.116.112.203 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 9 |
| 79.181.210.188 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.19.86.115 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 66.249.93.85 | Europe | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 8 |
| 5.102.254.255 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 87.71.13.36 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 213.57.156.246 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.86.153 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 2.53.138.192 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 2.55.33.200 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 37.26.149.158 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.64 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 76.16.101.244 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 8 |
| 87.69.36.11 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 2.53.38.8 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |

09-18-2016-19:04:05 to 09-18-2016-20:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

09-18-2016-19:04:05 to 09-18-2016-20:04:05