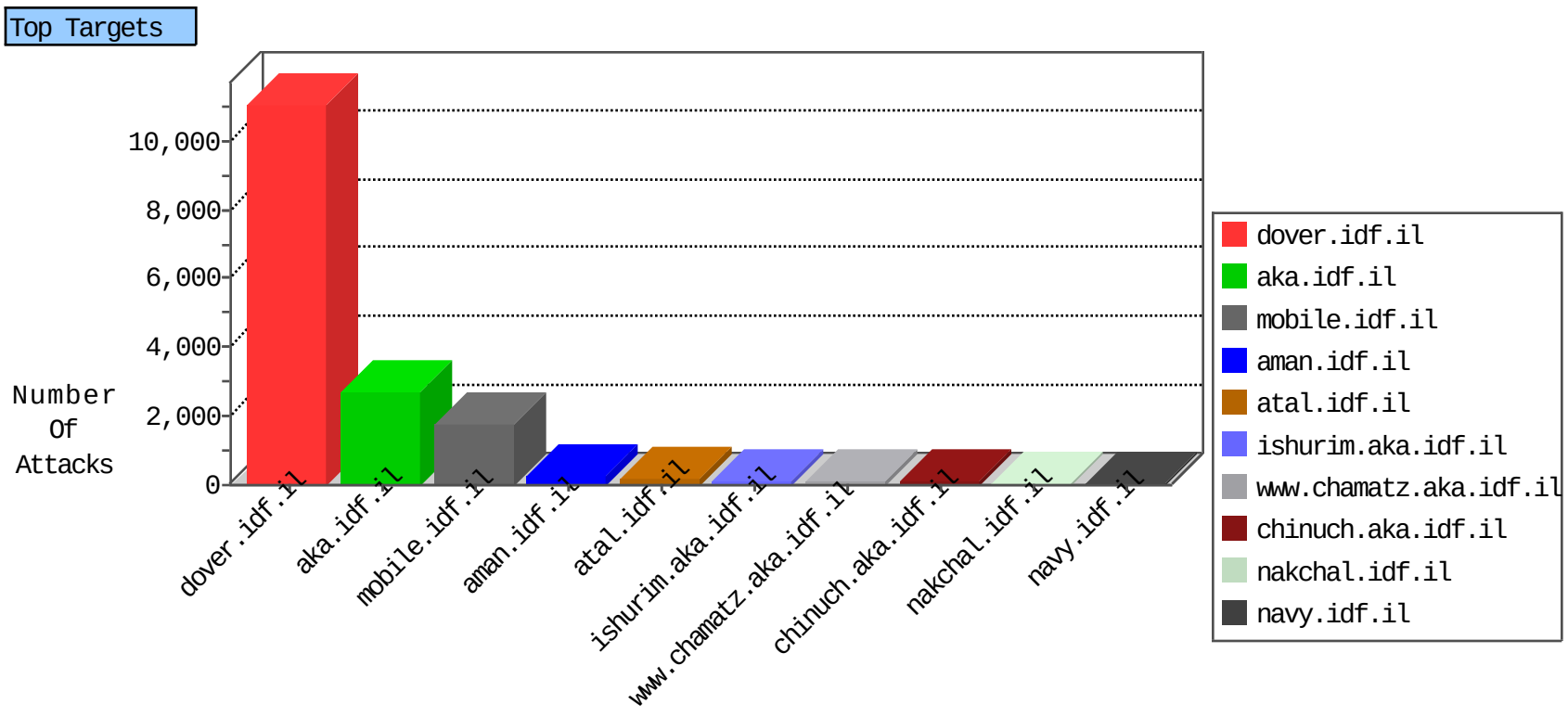
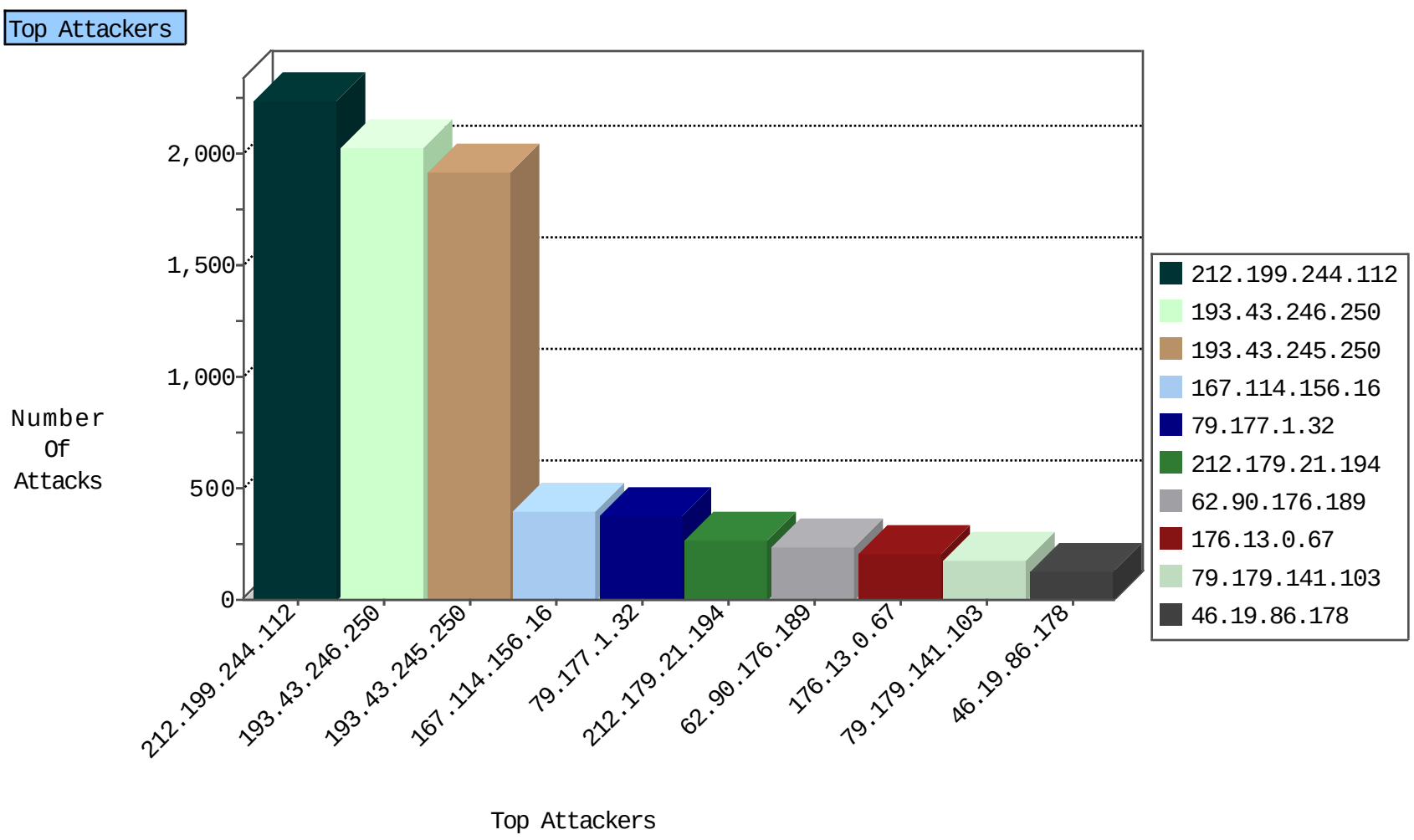
11-01-2015-16:04:05 to 11-01-2015-17:04:05

# IDF Under Attack Daily Report

Top Targets




Top Attackers



11-01-2015-16:04:05 to 11-01-2015-17:04:05

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3018 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 2709 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 682 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 602 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 226 |
| 149.78.118.180 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 22 |
| 109.64.212.130 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 20 |
| 176.12.142.249 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 19 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 18 |
| 79.183.208.88 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 15 |
| 149.78.118.180 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 12 |
| 46.116.138.222 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 12 |
| 176.12.140.128 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 109.65.125.142 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 68.41.54.48 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 84.228.253.17 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 31.168.155.39 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 178.135.109.9 | Lebanon | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 8 |
| 2.54.15.75 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 84.109.95.47 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 82.80.177.86 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 79.182.143.150 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 176.12.151.31 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 6 |
| 84.108.204.220 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 79.176.38.58 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 31.154.161.52 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 46.19.86.103 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 85.65.204.191 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 2.54.142.88 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 134.147.203.115 | Germany | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 4 |
| 5.29.28.100 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 46.19.86.218 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 85.250.101.169 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 185.13.192.85 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 2.54.56.223 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 185.13.192.85 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 192.117.138.210 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 2.54.130.223 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 79.177.29.176 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 82.81.7.178 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 193.43.244.102 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 81.20.191.202 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 176.13.22.171 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 109.226.91.13 | Russian Federation | 147.237.76.176 | test.ncore.idf.i | Block_Udp_All_Nets | drop | 3 |
| 31.168.20.111 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 3 |
| 84.94.21.76 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 176.13.11.126 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 82.81.7.178 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 79.182.143.150 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 3 |

11-01-2015-16:04:05 to 11-01-2015-17:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.108.217.193 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 178.135.109.9 | Lebanon | 147.237.77.216 | dover.idf.il | 12371: TCP: Hulk DDoS Tool | Block | 3 |
| 31.168.20.111 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |

11-01-2015-16:04:05 to 11-01-2015-17:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 79.178.164.99 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 109.64.212.130 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 86.97.144.204 | 147.237.77.216 | United Arab Emirates | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 109.65.27.38 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.138.95.59 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.229.169 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.11.16 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

11-01-2015-16:04:05 to 11-01-2015-17:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.199.244.112 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2246 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2018 |
| 193.43.245.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1909 |
| 62.90.176.189 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 231 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 206 |
| 87.69.128.231 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 106 |
| 69.195.57.206 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 103 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 82 |
| 178.135.109.9 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 81 |
| 139.162.202.59 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 72 |
| 47.17.217.216 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 65 |
| 212.25.105.8 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 57 |
| 89.138.95.59 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 55 |
| 31.168.233.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 54 |
| 77.127.170.119 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 108.217.190.3 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 116.220.166.124 | Japan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 42 |
| 46.19.85.44 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 41 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 213.57.160.27 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 34 |
| 138.110.228.203 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 31.168.155.39 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 46.19.86.219 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 176.12.140.128 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 85.250.178.137 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 176.13.0.67 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 28 |
| 176.13.12.232 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 80.217.101.34 | Sweden | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 26 |
| 109.64.212.130 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 82.166.145.177 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 46.19.85.218 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 2.54.33.185 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 100.100.44.11 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 24 |
| 149.78.118.180 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 46.19.85.218 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 23 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 151.80.31.112 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 2.54.34.142 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 46.19.86.103 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 46.19.86.178 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 79.176.51.137 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 81.218.196.22 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 37.26.148.164 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |

11-01-2015-16:04:05 to 11-01-2015-17:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.0.67 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 181 |
| 79.177.1.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 180 |
| 87.69.39.95 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 87.69.39.95 | Block | 105 |
| 46.19.86.178 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 105 |
| 2.54.7.149 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 90 |
| 79.179.141.103 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 90 |
| 79.177.1.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 90 |
| 79.179.141.103 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 90 |
| 185.32.179.2 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 90 |
| 79.177.1.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on aka.idf.il/ajax/updatestatus.php | Block | 87 |
| 213.151.35.218 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 75 |
| 2.52.163.112 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 75 |
| 79.183.58.250 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 60 |
| 82.166.22.35 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 60 |
| 79.183.58.250 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/ajax/updatestatus.php | Block | 60 |
| 176.13.5.234 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 60 |
| 82.166.22.35 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 60 |
| 77.127.170.119 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 60 |
| 176.13.10.216 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 60 |
| 2.54.44.198 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 176.13.22.73 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 45 |
| 176.12.145.172 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 82.80.177.86 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 176.13.16.207 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 176.12.146.151 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 212.179.21.194 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 45 |
| 37.26.146.209 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 45 |
| 62.90.94.84 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 45 |
| 2.54.17.22 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 176.13.21.197 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 45 |
| 84.108.217.193 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.108.217.193 | Block | 45 |
| 176.12.143.106 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 30 |
| 46.19.85.88 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 66.249.78.59 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 30 |
| 176.13.13.3 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 84.228.16.36 | Israel | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 30 |
| 77.125.104.87 | Israel | 147.237.72.166 | aka.idf.il | Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter | None | 30 |
| 31.154.91.148 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 30 |
| 84.109.3.210 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 30 |
| 54.244.22.103 | United States | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 30 |
| 84.228.16.36 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/ajax/updatestatus.php | Block | 30 |
| 82.81.31.100 | Israel | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 30 |
| 31.154.91.148 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 30 |
| 84.109.3.210 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 30 |
| 164.138.120.148 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/aman | Block | 30 |
| 176.13.18.248 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 30 |
| 84.228.50.41 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 82.81.31.100 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/ajax/updatestatus.php | Block | 30 |
| 87.69.134.156 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 87.69.134.156 | Block | 30 |

11-01-2015-16:04:05 to 11-01-2015-17:04:05