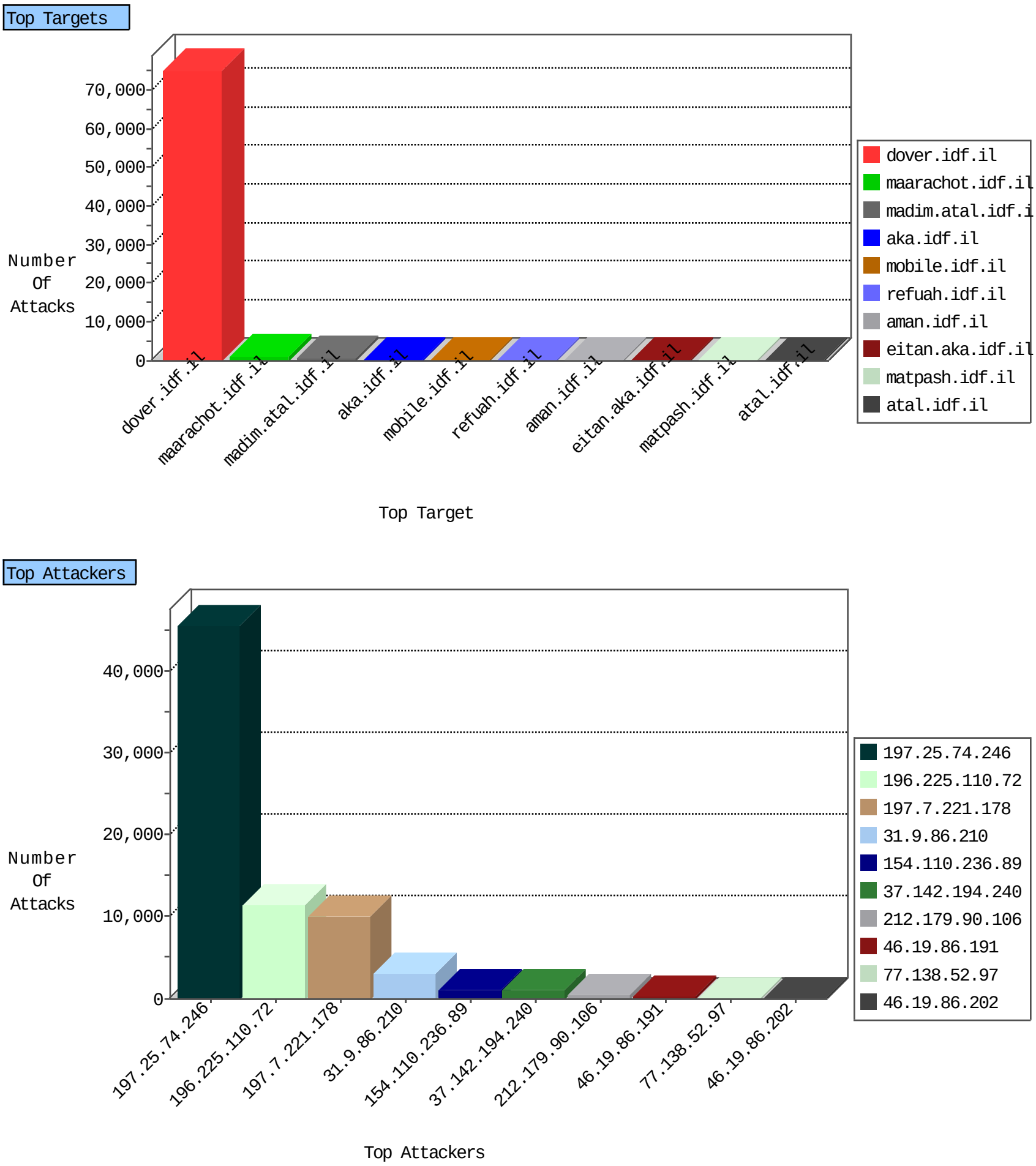
09-17-2016-22:04:04 to 09-17-2016-23:04:04

# IDF Under Attack Daily Report



09-17-2016-22:04:04 to 09-17-2016-23:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3540 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | DOS-HTTP-torshammer | forward | 940 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 474 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 26 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 26 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 9 |
| 141.22.213.34 | Germany | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 9 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 4 |
| 84.108.27.119 | Israel | 147.237.76.42 | refuah.idf.il | Black List | drop | 3 |
| 200.19.159.35 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 204.85.191.10 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 141.22.213.35 | Germany | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 2 |
| 195.113.161.83 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 160.80.221.39 | Italy | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 194.29.178.14 | Poland | 147.237.72.167 | ishurim.aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.22.150.78 | United States | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 143.225.229.236 | Italy | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 198.82.160.238 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 141.22.213.34 | Germany | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 157.55.39.20 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

09-17-2016-22:04:04 to 09-17-2016-23:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.130 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 9 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | C1000064: HTTP: Access to - admin.asp | Permit | 8 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | C1000016: HTTP: administrator in URI | Permit | 4 |
| 144.76.12.75 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.98 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.129 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 144.76.12.75 | Germany | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

09-17-2016-22:04:04 to 09-17-2016-23:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 197.7.221.178 | 147.237.77.216 | Tunisia | dover.idf.il | SERVER-WEBAPP login.htm access | 3 |
| 120.33.120.73 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 3 |
| 122.242.23.10 | 147.237.77.216 | China | dover.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 61.240.144.65 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 115.223.242.179 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 109.236.80.12 | 147.237.77.233 | Netherlands | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.60.153.178 | 147.237.77.19 | Russian Federation | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.60.153.178 | 147.237.76.147 | Russian Federation | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.193.74.175 | 147.237.77.243 | Gibraltar | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.193.74.175 | 147.237.76.200 | Gibraltar | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.64.99 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 179.43.141.228 | 147.237.76.176 | Switzerland | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 31.24.228.20 | 147.237.8.14 | United Kingdom | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.236.80.12 | 147.237.77.243 | Netherlands | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.236.80.12 | 147.237.77.205 | Netherlands | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.60.153.178 | 147.237.76.148 | Russian Federation | gqcenter.aka.idf.i | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 96.246.216.128 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.193.74.175 | 147.237.77.234 | Gibraltar | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.76.112 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 197.7.221.178 | 147.237.77.216 | Tunisia | dover.idf.il | SERVER-WEBAPP adminlogin access | 1 |
| 61.240.144.65 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |

09-17-2016-22:04:04 to 09-17-2016-23:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28788 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9045 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8146 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP SYN Modified Retransmission | Data received before SYN-ACK was acknowledged. Stripping all packet data. | drop | 5011 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3677 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | | monitor | 3645 |
| 31.9.86.210 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3147 |
| 154.110.236.89 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 986 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 807 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 583 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 576 |
| 37.142.194.240 | Israel | 147.237.77.170 | maarachot.idf.il | Block HTTP Non Compliant | Response out of state | monitor | 508 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 468 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 411 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 367 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP SYN Modified Retransmission | Data received before SYN-ACK was acknowledged. Stripping all packet data. | drop | 306 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 145 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 124 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 101 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 70 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 55 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP SYN Modified Retransmission | | drop | 50 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 50 |
| 41.253.191.103 | Libyan Arab Jamahiriya | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | alert | 49 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 49 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 48 |
| 109.67.178.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 47 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 38 |
| 89.139.134.241 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 62.24.252.133 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 35 |
| 213.151.48.123 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 34 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 33 |
| 156.204.16.63 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 79.177.162.202 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 207.46.13.66 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 85.250.214.228 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 26 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 24 |
| 68.180.229.223 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 84.94.160.41 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 213.151.39.193 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | | monitor | 22 |

09-17-2016-22:04:04 to 09-17-2016-23:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 556 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 548 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 548 |
| 196.225.110.72 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 548 |
| 37.142.194.240 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Abnormally Long Request | Block | 490 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Multiple Unknown HTTP Request Method from 197.25.74.246 | Block | 432 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Multiple Malformed URL from 197.25.74.246 | Block | 432 |
| 46.19.86.191 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 247 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 123 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 123 |
| 46.19.86.202 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 82 |
| 109.253.131.211 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 64 |
| 2.53.140.1 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 57 |
| 154.110.236.89 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 55 |
| 154.110.236.89 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 55 |
| 154.110.236.89 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 55 |
| 2.53.52.111 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 36 |
| 46.19.85.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 37.142.194.240 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Abnormally Long Request from 37.142.194.240 | Block | 18 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 197.7.221.178 | Block | 12 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 197.7.221.178 | Block | 11 |
| 79.178.152.230 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 9 |
| 77.138.80.92 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 5 |
| 165.225.80.104 | United Kingdom | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 4 |
| 62.219.136.251 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.220.207 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.12.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.19.206 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.180.163.243 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx | Block | 2 |
| 157.55.39.210 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx | Block | 2 |
| 2.53.20.216 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 5.28.137.123 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/homepage/<!doctype html public | Block | 1 |
| 79.181.59.205 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.76.81 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 95.86.83.28 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 2.53.48.222 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.177.107.12 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |
| 66.249.64.12 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 197.7.221.178 | Tunisia | 147.237.77.216 | dover.idf.il | Admin Blocking | Block | 1 |
| 5.28.146.243 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/watch | Block | 1 |
| 82.205.17.75 | Palestinian Territory Occupied | 147.237.77.216 | dover.idf.il | Unauthorized Method POST for 147.237.77.216/ | Block | 1 |
| 66.249.76.115 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 197.25.74.246 | Tunisia | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method When in URL harpoons, | Block | 1 |
| 66.249.64.45 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/eitan/tmuna/ | Block | 1 |
| 37.46.38.187 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 84.108.27.119 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 77.138.47.218 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/ | Block | 1 |
| 213.151.35.218 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/70283.pdf | Block | 1 |
| 85.64.173.91 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |

09-17-2016-22:04:04 to 09-17-2016-23:04:04