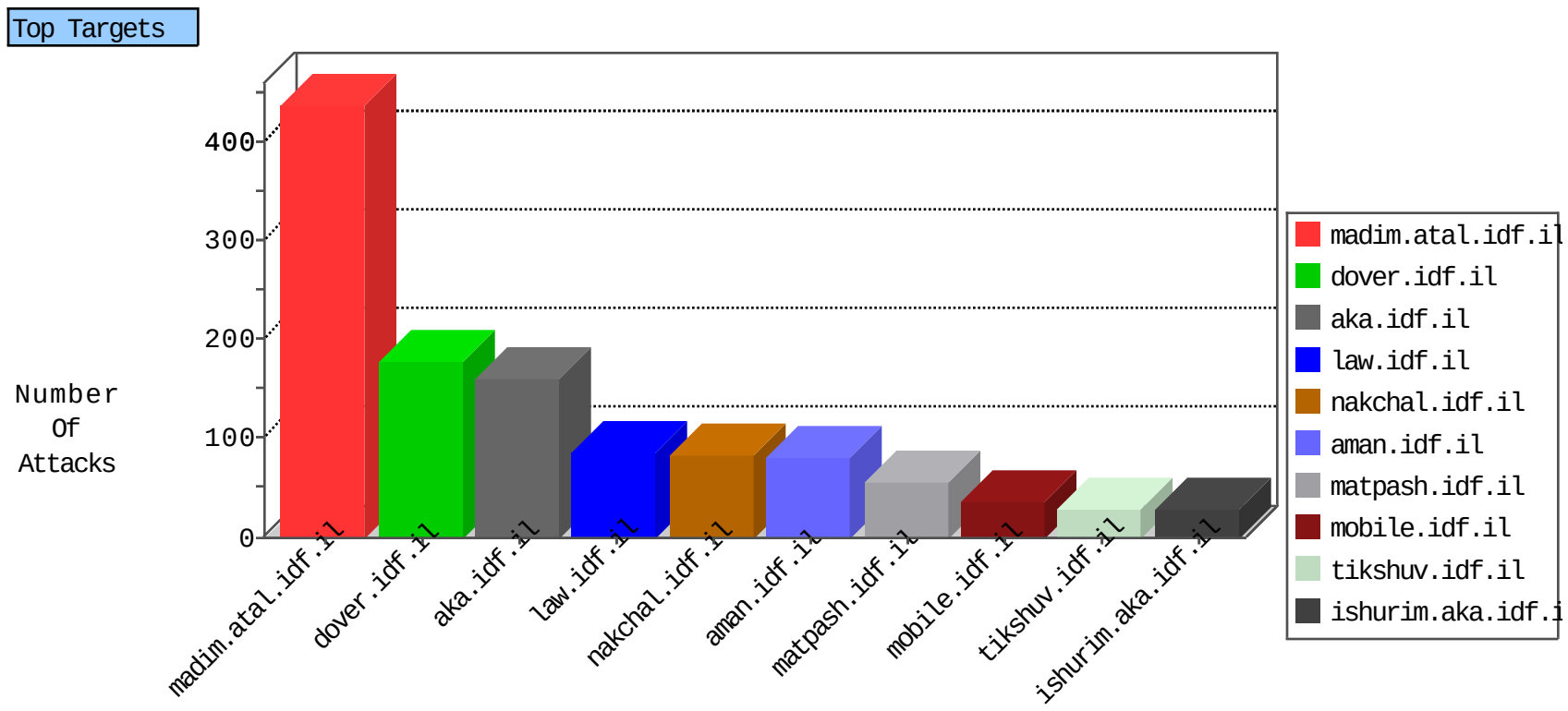
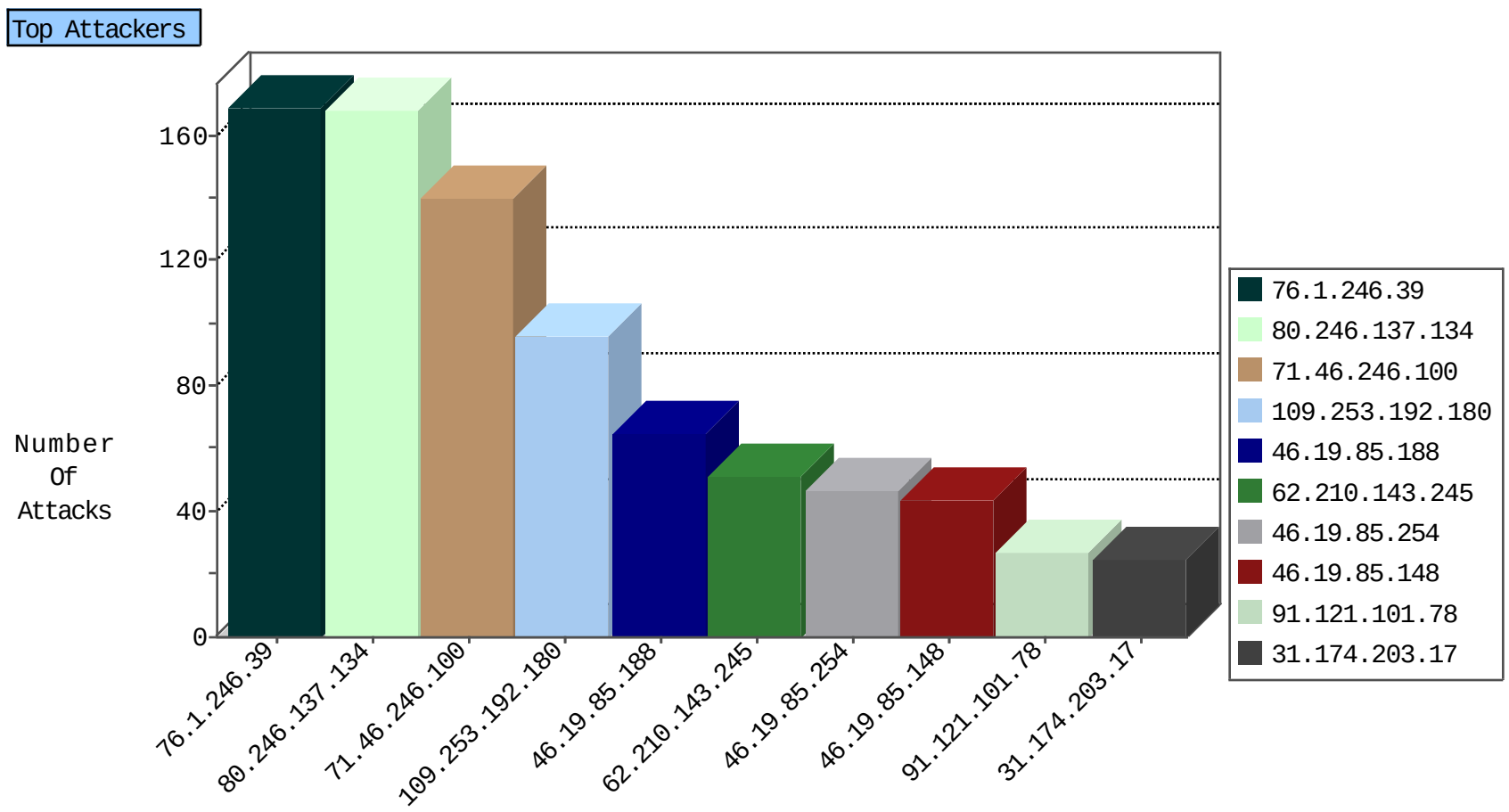
09-06-2016-14:04:02 to 09-06-2016-15:04:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-06-2016-14:04:02 to 09-06-2016-15:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.138.59.221 | France | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 176.13.12.188 | Israel | 147.237.72.167 | ishurim.aka.idf.il | DOSS-SSL-ClearText | drop | 1 |
| 69.27.168.124 | United States | 147.237.0.34 | tikshuv.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 66.240.192.138 | United States | 147.237.76.39 | mobile.meitav.idf.il | Black List | drop | 1 |
| 80.82.77.46 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |

09-06-2016-14:04:02 to 09-06-2016-15:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 62.210.143.245 | France | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 41 |
| 91.121.101.78 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 15 |
| 91.121.101.78 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 12 |
| 62.210.143.245 | France | 147.237.76.200 | eitan.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 62.210.143.245 | France | 147.237.77.170 | maarachot.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 109.186.81.55 | Israel | 147.237.72.166 | aka.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

09-06-2016-14:04:02 to 09-06-2016-15:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.121.78.198 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 46.19.86.39 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 37.48.93.217 | 147.237.77.226 | Netherlands | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.68.54.236 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.48.93.217 | 147.237.76.199 | Netherlands | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.65.165.100 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.48.93.217 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 82.81.13.88 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.55.171.213 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 196.47.173.21 | 147.237.0.15 | Cote D'Ivoire | kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 79.179.49.89 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.40.4.92 | 147.237.77.235 | Russian Federation | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.177.59.98 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 167.0.162.60 | 147.237.0.34 | Colombia | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 66.249.76.75 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.41.251 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.172.71.251 | 147.237.0.200 | Ukraine | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 37.142.7.158 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.32.50 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.48.93.217 | 147.237.76.199 | Netherlands | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.68.44.248 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.77.19 | United States | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.48.93.217 | 147.237.76.197 | Netherlands | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.64.86.161 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 199.203.108.173 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.48.93.217 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 79.181.109.160 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 196.47.173.21 | 147.237.0.15 | Cote D'Ivoire | kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 79.178.148.148 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.40.4.92 | 147.237.77.227 | Russian Federation | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.124.3.238 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.68.209.98 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 64.137.171.55 | 147.237.76.38 | Canada | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 93.158.203.196 | 147.237.0.33 | Netherlands | idf.il | ET SCAN NMAP -sS window 1024 | 1 |

09-06-2016-14:04:02 to 09-06-2016-15:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.19.85.148 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 21 |
| 46.117.76.68 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 15 |
| 141.0.14.145 | Europe | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.85.148 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 85.65.127.182 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 37.26.147.200 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 9 |
| 76.1.246.39 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 87.71.40.18 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 76.1.246.39 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 213.55.108.91 | Ethiopia | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 76.1.246.39 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 31.174.203.17 | Poland | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 76.1.246.39 | United States | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 76.1.246.39 | United States | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 71.46.246.100 | United States | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 71.46.246.100 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 46.19.86.125 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 76.1.246.39 | United States | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 71.46.246.100 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 76.1.246.39 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 76.1.246.39 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 76.1.246.39 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 76.1.246.39 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 71.46.246.100 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 71.46.246.100 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 62.0.247.129 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 71.46.246.100 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 76.1.246.39 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 76.1.246.39 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 71.46.246.100 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 31.174.203.17 | Poland | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 71.46.246.100 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 76.1.246.39 | United States | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 76.1.246.39 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 46.19.85.108 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 71.46.246.100 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 71.46.246.100 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 71.46.246.100 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 71.46.246.100 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 176.13.237.117 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 71.46.246.100 | United States | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 176.12.160.2 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |

09-06-2016-14:04:02 to 09-06-2016-15:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 80.246.137.134 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 168 |
| 109.253.192.180 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 96 |
| 46.19.85.188 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 65 |
| 46.19.85.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 39 |
| 79.176.52.182 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.176.52.182 | Block | 17 |
| 59.40.227.157 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 59.40.227.157 | Block | 17 |
| 2.53.17.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 16 |
| 85.250.248.24 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 9 |
| 46.19.85.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 8 |
| 176.13.241.73 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 84.109.64.150 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized HTTP Method | Block | 6 |
| 59.40.227.157 | China | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 6 |
| 77.138.168.98 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 4 |
| 192.115.252.2 | Israel | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 4 |
| 176.13.239.225 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.113 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.130.238 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 46.19.86.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.236.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 192.115.252.2 | Israel | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 192.115.252.2 | Block | 3 |
| 85.250.248.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.138.135 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 66.249.88.143 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 212.179.73.106 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 138.162.128.52 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 207.46.13.181 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 65.55.210.193 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.57.230.68 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.244.175 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 209.88.198.1 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc | Block | 2 |
| 80.246.133.236 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.57.230.68 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 2 |
| 147.161.10.221 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 79.176.52.182 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 2 |
| 46.19.86.61 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 212.179.21.194 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 2 |
| 77.138.53.6 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |
| 46.19.86.44 | Israel | 147.237.76.42 | refuah.idf.il | Abnormally Long Request method | Block | 1 |
| 66.249.66.243 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx | Block | 1 |
| 31.174.203.17 | Poland | 147.237.72.156 | aman.idf.il | Multiple Untraceable SSL Sessions from 31.174.203.17 (Open Mode) | None | 1 |
| 59.40.227.157 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.asp | Block | 1 |
| 216.244.66.236 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx | Block | 1 |
| 80.246.130.23 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 192.115.252.2 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/ | Block | 1 |
| 46.19.85.173 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 148.251.2.180 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 64.254.230.42 | Canada | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx | Block | 1 |
| 87.68.1.125 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 46.120.107.52 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 81.218.136.85 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 1 |

09-06-2016-14:04:02 to 09-06-2016-15:04:02