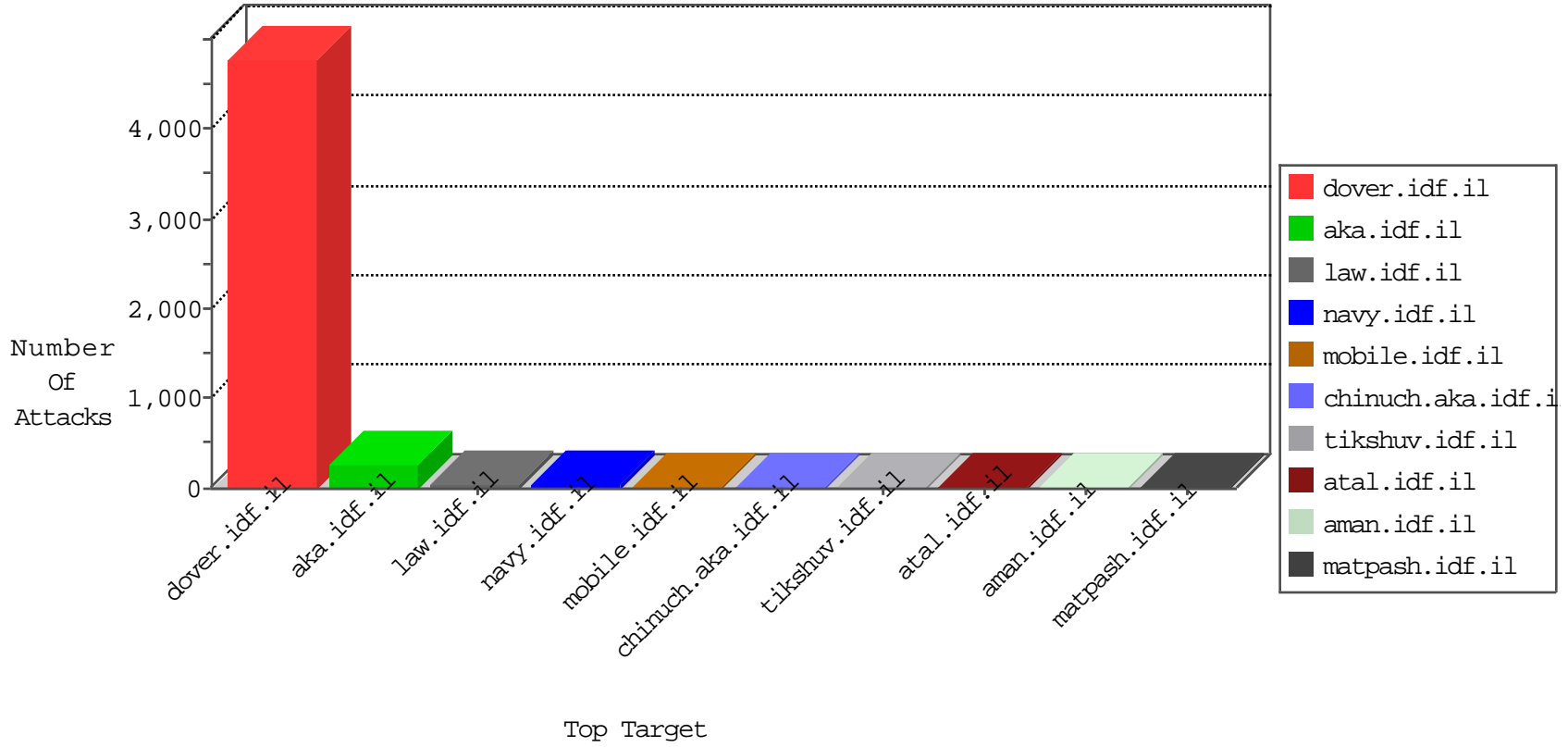


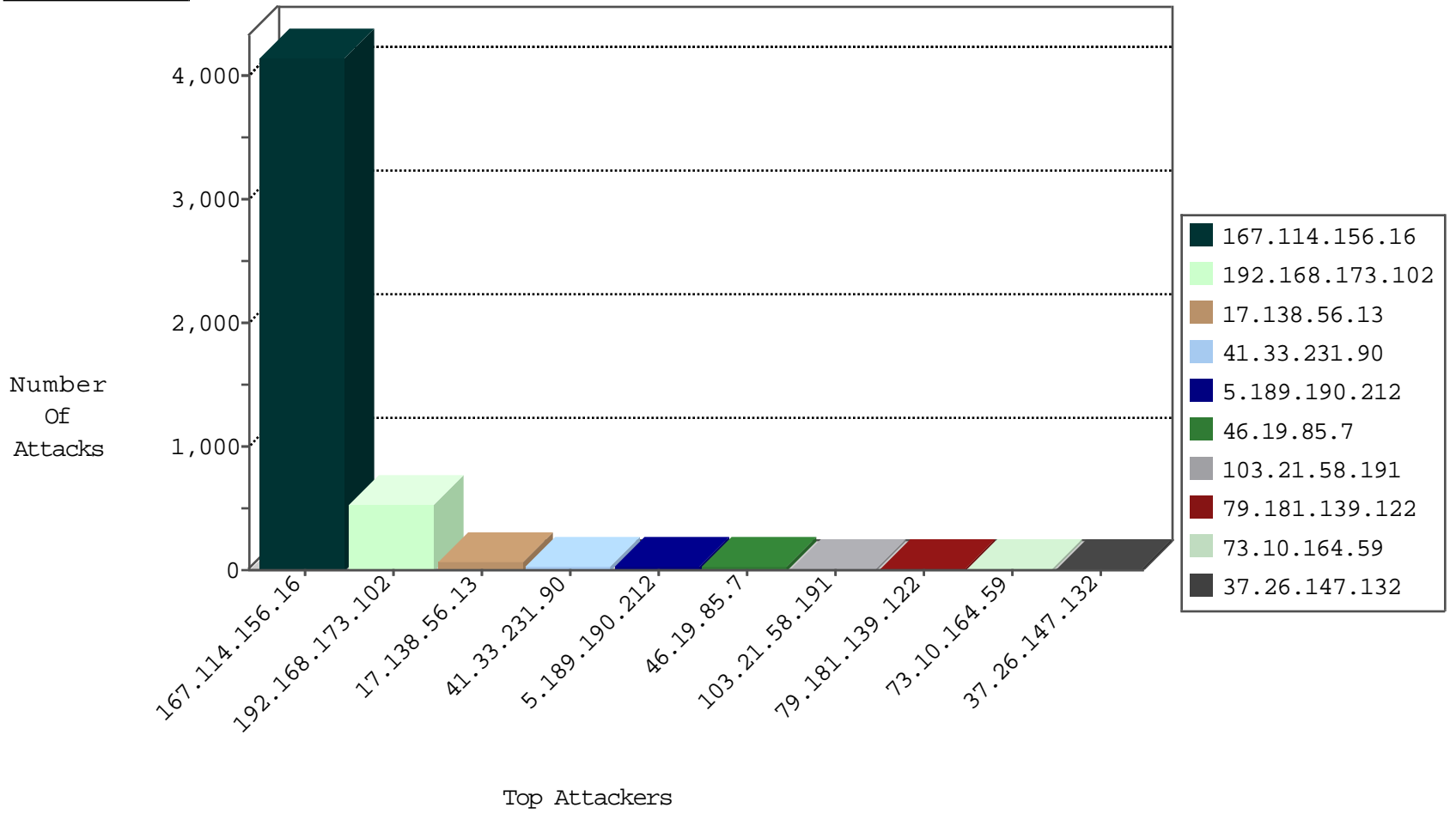
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------------------|--------------------------|---------------|-------|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 4142 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 4 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 117.205.131.205 | India | 147.237.76.86 | navy.idf.il | Invalid TCP Flags | drop | 2 |
| 104.156.240.205 | United States | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 1 |
| 91.15.193.249 | Germany | 147.237.0.35 | akaws.idf.il | Block_Ntp_All_Net | drop | 1 |
| 66.240.192.138 | United States | 147.237.77.243 | mobile.idf.il | Block_Udp_All_Nets | drop | 1 |
| 212.143.225.116 | Israel | 147.237.8.50 | e.tikshuv.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 184.105.139.106 | United States | 147.237.8.45 | e.eitan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.74 | United States | 147.237.77.205 | prisha.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.33 | idf.il | Block_Ntp_All_Net | drop | 1 |
| 91.15.193.249 | Germany | 147.237.0.16 | my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.122 | United States | 147.237.0.33 | idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.94 | United States | 147.237.77.74 | law.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.15 | kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.106 | United States | 147.237.77.233 | atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.82 | United States | 147.237.72.14 | dover.idf.il(old) | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.34 | tikshuv.idf.il | Block_Ntp_All_Net | drop | 1 |
| 91.15.193.249 | Germany | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.122 | United States | 147.237.8.28 | e.mobile-ks.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.102 | United States | 147.237.8.14 | e.orchot.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.16 | my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 82.145.219.139 | Europe | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 1 |
| 184.105.139.114 | United States | 147.237.8.50 | e.tikshuv.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.82 | United States | 147.237.72.166 | aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.35 | akaws.idf.il | Block_Ntp_All_Net | drop | 1 |
| 91.15.193.249 | Germany | 147.237.0.33 | idf.il | Block_Ntp_All_Net | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 212.143.225.116 | Israel | 147.237.8.46 | e.chinuch.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 184.105.139.102 | United States | 147.237.77.61 | e.cogat.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.70 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.215.17.228 | Germany | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 91.15.193.249 | Germany | 147.237.0.15 | kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.118 | United States | 147.237.77.234 | halag.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.82 | United States | 147.237.77.235 | sviva.idf.il | Block_Ntp_All_Net | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 106.38.241.149 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 103.21.58.191 | India | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 23.91.70.119 | United States | 147.237.0.34 | tikshuv.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 177.185.194.45 | Brazil | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 74.63.228.226 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 199.58.86.211 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 4 |
| 84.245.33.104 | Netherlands | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|--------------------|--|-------|
| 103.21.58.191 | 147.237.77.74 | India | law.idf.il | SQL Injection - Select From | 12 |
| 84.245.33.104 | 147.237.77.74 | Netherlands | law.idf.il | SQL Injection - Select From | 6 |
| 23.91.70.119 | 147.237.0.34 | United States | tikshuv.idf.il | SQL Injection - Select From | 6 |
| 177.185.194.45 | 147.237.77.74 | Brazil | law.idf.il | SQL Injection - Select From | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 74.63.228.226 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 2 |
| 120.199.111.137 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 93.183.201.2 | 147.237.77.243 | Ukraine | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 69.30.197.124 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 185.114.157.12 | 147.237.0.15 | Netherlands | kosher-kravi.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 120.199.111.137 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 93.183.201.2 | 147.237.0.33 | Ukraine | idf.il | ET SCAN Potential SSH Scan | 1 |
| 69.30.197.124 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 212.143.225.116 | 147.237.0.19 | Israel | medim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 185.114.157.12 | 147.237.0.15 | Netherlands | kosher-kravi.idf.i | ET SCAN NMAP -sS window 4096 | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|---------------------------------|----------------|--------------------|--|---|---------------|-------|
| 192.168.173.102 | | 147.237.77.216 | dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 366 |
| 192.168.173.102 | | 147.237.72.166 | aka.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 170 |
| 17.138.56.13 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 56 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 5.189.190.212 | Germany | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 27 |
| 79.181.139.122 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 73.10.164.59 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 109.64.38.68 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 37.26.146.173 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.147.132 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 110.171.55.59 | Thailand | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 176.13.21.37 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.147.132 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 130.193.178.236 | Iraq | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.7 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.7 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.182.225.222 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.55 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 54.75.228.43 | Ireland | 147.237.8.28 | e.mobile-ks.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 4 |
| 62.210.225.135 | France | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 4 |
| 66.76.174.2 | United States | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 4 |
| 5.28.191.62 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 164.138.23.232 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 82.205.56.106 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 213.57.242.127 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 164.138.23.232 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.85.17 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.236.25 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 141.8.142.1 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.4 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.70.53.233 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.120.125.29 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.236.129 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.142.57 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.235.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 93.158.152.49 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.18.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.29.184 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 194.28.115.226 | Netherlands | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 2.54.154.199 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.15.126 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 188.161.58.168 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.85.115 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 87.69.118.57 | Israel | 147.237.72.156 | anan.idf.il | drop | First packet isn't SYN | drop | 2 |
| 5.102.254.240 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |

04-09-2016-10:04:07 to 04-09-2016-11:04:07

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|--------------|------------------|------------------------|---------------|-------|
| 176.126.85.176 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.85.115 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------------|---|---------------|-------|
| 46.19.86.4 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 46.19.86.4 | Block | 5 |
| 91.200.12.58 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 4 |
| 91.200.12.58 | Ukraine | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 91.200.12.58 | Block | 3 |
| 37.26.148.198 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.224 | Block | 2 |
| 185.120.125.8 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 2 |
| 54.153.33.145 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 37.187.114.171 | France | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to /irj/portal | Block | 1 |
| 119.154.49.89 | Pakistan | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 66.249.69.34 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 46.19.85.174 | Israel | 147.237.76.86 | navy.idf.il | Unknown HTTP Request Method odzq; in URL __atuvc=1 | Block | 1 |
| 194.28.115.226 | Netherlands | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 54.153.33.145 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 40.77.167.31 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 157.55.39.205 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/watch | Block | 1 |
| 66.249.79.133 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/robots.txt | Block | 1 |
| 5.28.191.62 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/ | Block | 1 |
| 207.46.13.67 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ar/ | Block | 1 |
| 46.19.85.174 | Israel | 147.237.76.86 | navy.idf.il | Abnormally Long Request request version | Block | 1 |
| 177.242.161.48 | Mexico | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 84.108.88.60 | Israel | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 1 |
| 46.19.86.4 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 1 |
| 5.28.191.62 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/main/home/default.aspx | Block | 1 |
| 213.57.199.131 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 91.200.12.58 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 66.249.69.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/resources/scripts/ticker.js | Block | 1 |
| 46.19.85.174 | Israel | 147.237.76.86 | navy.idf.il | Illegal HTTP Version __atuvs=5708afdfbc59a7ca000;_atssc=facebook%3B1 | Block | 1 |
| 84.108.88.60 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to atal.idf.il/xmlrpc.php | Block | 1 |
| 46.120.201.183 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 119.154.49.89 | Pakistan | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 66.249.69.34 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;docId in www.aka.idf.il/giyus/login/ | None | 1 |
| 46.19.85.174 | Israel | 147.237.76.86 | navy.idf.il | Malformed URL __atuvc=1 | Block | 1 |
| 185.120.125.8 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/milluim/index | Block | 1 |
| 87.71.103.47 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct175 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |