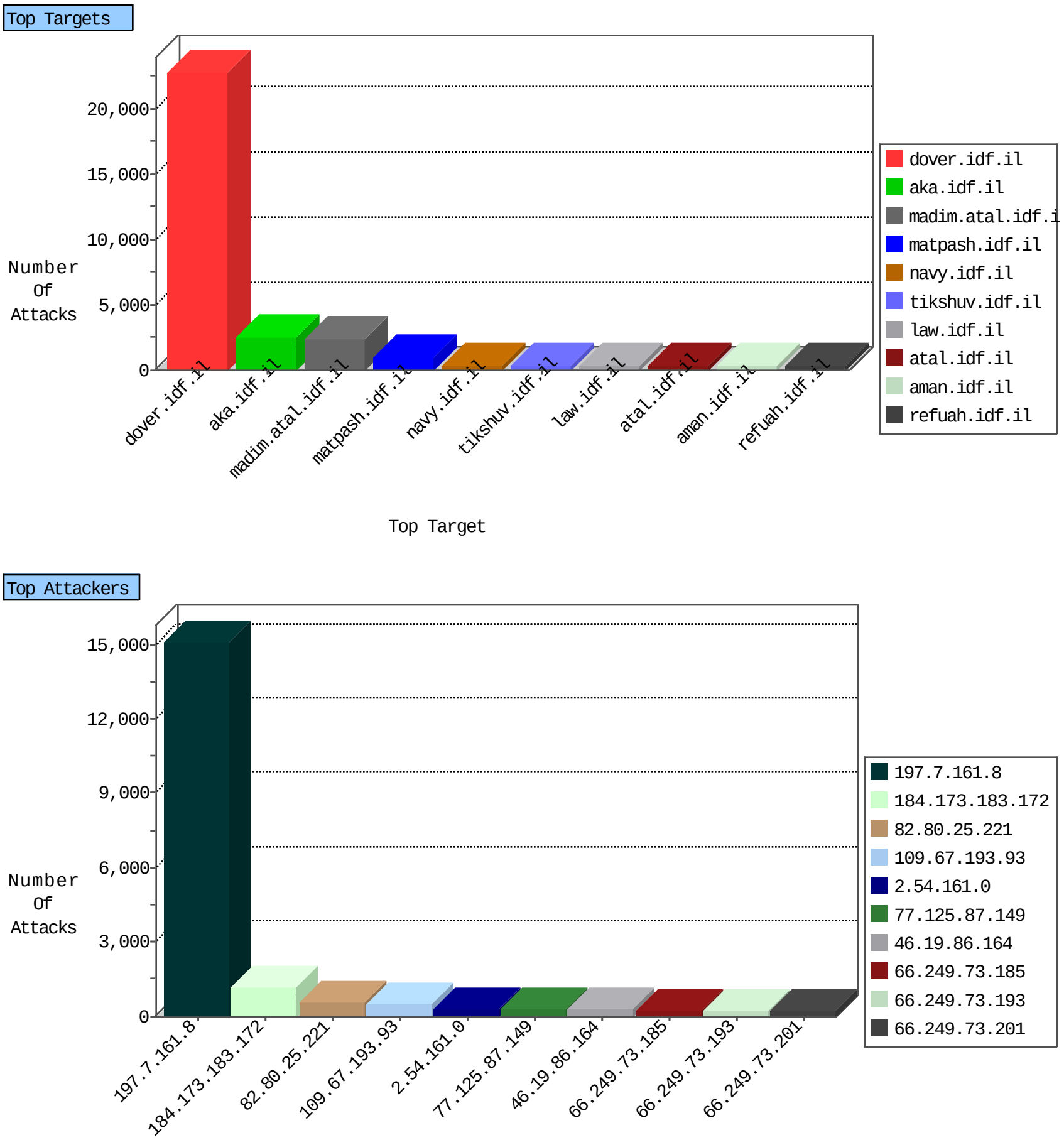
03-28-2015-00:00:05 to 03-29-2015-00:00:05

# IDF Under Attack Daily Report



03-28-2015-00:00:05 to 03-29-2015-00:00:05

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 89.138.11.240 | Israel | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 2119 |
| 85.250.202.142 | Israel | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 1830 |
| 46.121.113.212 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 241 |
| 84.108.88.76 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 230 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 205 |
| 84.108.148.10 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 190 |
| 2.54.43.164 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 179 |
| 82.102.251.11 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 170 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 146 |
| 46.120.239.9 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 145 |
| 109.64.109.183 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 118 |
| 66.249.75.13 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 104 |
| 207.46.13.16 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 96 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 87 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 84 |
| 46.19.85.223 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 83 |
| 31.210.186.141 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 78 |
| 94.159.221.97 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 77 |
| 37.26.147.170 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 77 |
| 109.253.142.28 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 76 |
| 79.183.170.147 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 73 |
| 207.46.13.5 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 72 |
| 2.54.191.130 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 71 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 69 |
| 85.65.217.66 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 65 |
| 46.19.85.189 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 64 |
| 188.165.15.148 | France | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 64 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 64 |
| 2.54.156.223 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 63 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 62 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 61 |
| 157.55.39.67 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 60 |
| 134.191.232.71 | Israel | 147.237.76.42 | refuah.idf.il | JLM_Purple_Con_Limit_Http | drop | 50 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 47 |
| 157.55.39.42 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 46 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 45 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 45 |
| 207.46.13.79 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 39 |
| 5.255.253.99 | Russian Federation | 147.237.77.74 | law.idf.il | unblock-sp-traf1 | forward | 34 |
| 66.249.75.5 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 34 |
| 66.249.75.13 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 33 |
| 68.180.228.232 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 29 |
| 188.161.114.98 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 28 |
| 108.215.221.246 | United States | 147.237.77.233 | atal.idf.il | unblock-sp-traf1 | forward | 26 |
| 5.255.253.124 | Russian Federation | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 21 |
| 66.249.75.117 | United States | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 21 |
| 37.140.141.27 | Russian Federation | 147.237.72.166 | aka.idf.il | unblock-sp-traf1 | forward | 21 |
| 24.79.123.181 | Canada | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 18 |
| 180.131.253.83 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 17 |
| 99.149.193.93 | United States | 147.237.77.216 | dover.idf.il | unblock-sp-traf1 | forward | 17 |

03-28-2015-00:00:05 to 03-29-2015-00:00:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 521 |
| 184.173.183.172 | United States | 147.237.77.176 | matpash.idf.il | DVRep_P-N_40-59 | Permit | 505 |
| 77.125.87.149 | Israel | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 298 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 216 |
| 184.173.183.172 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 189 |
| 77.125.87.160 | Israel | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 155 |
| 77.127.132.2 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 32 |
| 189.104.28.75 | Brazil | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 13 |
| 37.187.129.166 | France | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 8 |
| 193.43.246.250 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 7 |
| 91.207.4.22 | Ukraine | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 6 |
| 193.43.245.250 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 216.67.245.106 | United States | 147.237.77.216 | dover.idf.il | C003: HTTP: phpMyAdmin access | Block | 5 |
| 87.106.151.126 | Germany | 147.237.0.15 | kosher-kravi.idf.i | C003: HTTP: phpMyAdmin access | Block | 5 |
| 218.186.83.101 | Singapore | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 87.106.151.126 | Germany | 147.237.0.34 | tikshuv.idf.il | C003: HTTP: phpMyAdmin access | Block | 5 |
| 216.67.245.106 | United States | 147.237.0.15 | kosher-kravi.idf.i | C003: HTTP: phpMyAdmin access | Block | 5 |
| 87.106.151.126 | Germany | 147.237.77.216 | dover.idf.il | C003: HTTP: phpMyAdmin access | Block | 5 |
| 216.67.245.106 | United States | 147.237.0.34 | tikshuv.idf.il | C003: HTTP: phpMyAdmin access | Block | 5 |
| 87.69.134.201 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 58.59.239.46 | China | 147.237.72.167 | ishurim.aka.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 85.250.189.52 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 58.59.239.46 | China | 147.237.72.156 | aman.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 69.162.69.131 | United States | 147.237.77.176 | matpash.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 212.34.12.173 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 93.173.38.66 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 58.59.239.46 | China | 147.237.72.166 | aka.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 77.127.220.98 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 87.69.246.162 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 212.253.107.198 | Turkey | 147.237.77.176 | matpash.idf.il | 12373: HTTP: WordPress admin Login | Block | 3 |
| 223.25.242.100 | Malaysia | 147.237.76.31 | nakchal.idf.il | DVRep_P-N_40-59 | Permit | 3 |
| 212.253.107.198 | Turkey | 147.237.77.74 | law.idf.il | 12373: HTTP: WordPress admin Login | Block | 3 |
| 188.161.8.224 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 62.210.170.27 | France | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 79.182.187.217 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.123 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 37.26.147.129 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 85.25.43.94 | Germany | 147.237.77.19 | law-forum.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 85.25.43.94 | Germany | 147.237.8.50 | e.tikshuv.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 52.0.4.72 | United States | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 37.247.97.194 | Turkey | 147.237.76.197 | e.himush.idf.il | DVRep_P-N_40-59 | Permit | 2 |
| 67.80.231.181 | United States | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 85.25.43.94 | Germany | 147.237.76.176 | test.ncore.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 93.168.110.45 | Romania | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 85.25.43.94 | Germany | 147.237.76.30 | himush.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 84.153.66.198 | Germany | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 109.67.97.171 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 93.120.27.62 | Romania | 147.237.77.19 | law-forum.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 93.120.27.62 | Romania | 147.237.0.34 | tikshuv.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 46.19.85.154 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |

03-28-2015-00:00:05 to 03-29-2015-00:00:05

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 586 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 144 |
| 66.249.79.22 | United States | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sA (2) | 64 |
| 216.67.245.106 | United States | 147.237.77.216 | dover.idf.il | Admin login page scan - Havij | 27 |
| 216.67.245.106 | United States | 147.237.0.15 | kosher-kravi.idf.il | Admin login page scan - Havij | 21 |
| 216.67.245.106 | United States | 147.237.0.34 | tikshuv.idf.il | Admin login page scan - Havij | 21 |
| 87.106.151.126 | Germany | 147.237.0.15 | kosher-kravi.idf.il | Admin login page scan - Havij | 14 |
| 87.106.151.126 | Germany | 147.237.0.34 | tikshuv.idf.il | Admin login page scan - Havij | 11 |
| 87.106.151.126 | Germany | 147.237.77.216 | dover.idf.il | Admin login page scan - Havij | 10 |
| 85.250.202.142 | Israel | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sS window 1024 | 6 |
| 194.114.146.227 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 6 |
| 87.213.35.126 | Netherlands | 147.237.0.15 | kosher-kravi.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 89.138.11.240 | Israel | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sS window 1024 | 4 |
| 46.120.146.147 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 87.213.35.126 | Netherlands | 147.237.0.17 | m.my-kosher-kravi.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 85.250.238.251 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 5.22.130.149 | Israel | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 3 |
| 115.231.218.147 | China | 147.237.76.199 | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 3 |
| 132.74.95.19 | Israel | 147.237.77.170 | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 122.228.207.77 | China | 147.237.76.86 | navy.idf.il | ET SCAN Potential SSH Scan | 3 |
| 66.135.63.24 | United States | 147.237.77.176 | matpash.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 115.231.218.147 | China | 147.237.76.201 | e.atal.idf.il | ET SCAN Potential SSH Scan | 3 |
| 122.228.207.77 | China | 147.237.76.31 | nakchal.idf.il | ET SCAN Potential SSH Scan | 3 |
| 85.64.42.26 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 89.139.41.21 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 43.255.191.166 | Japan | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 84.108.110.139 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.181.39.139 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.95.58.220 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.19.85.14 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.179.8.109 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.75.68 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 61.240.144.64 | China | 147.237.76.34 | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 122.228.207.77 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 61.240.144.67 | China | 147.237.76.34 | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 77.125.223.164 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 61.240.144.64 | China | 147.237.0.35 | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 122.228.207.77 | China | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 176.228.202.39 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 87.69.64.66 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.77 | China | 147.237.72.166 | aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 109.65.158.124 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 80.246.133.80 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.77 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.102.254.211 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 157.55.39.227 | United States | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.109.209.149 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 61.240.144.66 | China | 147.237.76.38 | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 122.228.207.77 | China | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 79.181.225.246 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |

03-28-2015-00:00:05 to 03-29-2015-00:00:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5057 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | SAM rule | drop | drop | 4571 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | | drop | drop | 4345 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | Data received before SYN-ACK was acknowledged. Stripping all packet data. | Streaming Engine: TCP SYN Modified Retransmission | drop | 441 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 250 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 242 |
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 239 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 150 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 146 |
| 2.92.147.218 | Russian Federation | 147.237.77.233 | atal.idf.il | First packet isn't SYN | drop | drop | 116 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | | Bad TCP sequence | monitor | 105 |
| 46.115.156.113 | Germany | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 75 |
| 176.12.141.239 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 60 |
| 66.249.75.5 | United States | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 56 |
| 5.11.16.14 | Satellite Provider | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 50 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 50 |
| 109.253.133.254 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 48 |
| 87.7.187.180 | Italy | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 46 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 44 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 66.249.79.104 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.253.146.41 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 77.127.246.217 | Israel | 147.237.72.166 | aka.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 35 |
| 121.54.54.172 | Philippines | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 33 |
| 5.22.130.144 | Israel | 147.237.72.156 | aman.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 31 |
| 109.253.157.54 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 176.12.150.134 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 66.249.81.215 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 176.12.141.183 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 109.253.149.244 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 26 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 26 |
| 66.249.79.96 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.142.193 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 66.249.79.112 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.136.57 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 5.22.130.149 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN retransmit with different window scale | Bad TCP sequence | monitor | 23 |
| 173.192.238.44 | United States | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 22 |
| 5.22.130.144 | Israel | 147.237.72.156 | aman.idf.il | First packet isn't SYN | drop | drop | 21 |
| 109.253.132.160 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 20 |
| 37.142.194.240 | Israel | 147.237.77.216 | dover.idf.il | SAM rule | drop | drop | 19 |
| 176.12.150.236 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 109.253.142.111 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.147.161 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 93.172.30.229 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 109.253.142.188 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 109.253.129.148 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.143.235 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 109.253.136.52 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.143.253 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.67.193.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 487 |
| 2.54.161.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 332 |
| 46.19.86.164 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 274 |
| 46.19.86.150 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.86.150 | Block | 208 |
| 197.7.161.8 | Tunisia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 205 |
| 46.116.220.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.116.220.30 | Block | 198 |
| 2.52.171.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 185 |
| 176.12.144.90 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 176.12.144.90 | Block | 181 |
| 46.19.86.63 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 118 |
| 37.26.146.149 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 97 |
| 46.19.85.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.0 | Block | 89 |
| 109.253.135.214 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 109.253.135.214 | Block | 86 |
| 176.12.138.64 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 55 |
| 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 | 44 |
| 197.9.134.90 | Tunisia | 147.237.77.216 | dover.idf.il | Post Request - Missing Content Type from 197.9.134.90 | Block | 41 |
| 197.9.134.90 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 38 |
| 46.19.86.237 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 37 |
| 216.67.245.106 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 216.67.245.106 | Block | 33 |
| 216.67.245.106 | United States | 147.237.0.15 | kosher-kravi.idf.i | Multiple Unauthorized URL Access from 216.67.245.106 | Block | 33 |
| 216.67.245.106 | United States | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 216.67.245.106 | Block | 33 |
| 109.253.159.26 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 32 |
| 207.46.13.16 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.16 | Block | 30 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.196 | Block | 29 |
| 66.249.79.128 | United States | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 66.249.79.128 | Block | 24 |
| 66.249.79.136 | United States | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 66.249.79.136 | Block | 24 |
| 87.106.151.126 | Germany | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 87.106.151.126 | Block | 23 |
| 87.106.151.126 | Germany | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 87.106.151.126 | Block | 22 |
| 87.106.151.126 | Germany | 147.237.0.15 | kosher-kravi.idf.i | Multiple Unauthorized URL Access from 87.106.151.126 | Block | 22 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.112 | Block | 19 |
| 157.55.39.42 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 157.55.39.42 | Block | 17 |
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.201 | Block | 17 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.193 | Block | 16 |
| 66.249.79.120 | United States | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 66.249.79.120 | Block | 15 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 157.55.39.6 | Block | 12 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.185 | Block | 10 |
| 79.177.41.177 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 8 |
| 85.250.5.204 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 7 |
| 109.253.139.250 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 188.165.15.176 | France | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 188.165.15.176 | Block | 6 |
| 213.251.182.10 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 6 |
| 149.88.68.118 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 2.54.151.80 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 2.54.151.80 | Block | 6 |
| 68.180.228.117 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.228.117 | Block | 6 |
| 2.54.151.80 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432 | Block | 5 |
| 46.120.130.223 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 5 |
| 85.130.248.6 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 5 |
| 5.22.129.237 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 5 |
| 17.142.152.43 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.142.152.43 | Block | 4 |
| 94.180.61.227 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 94.180.61.227 | Block | 4 |
| 17.142.151.93 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.142.151.93 | Block | 4 |