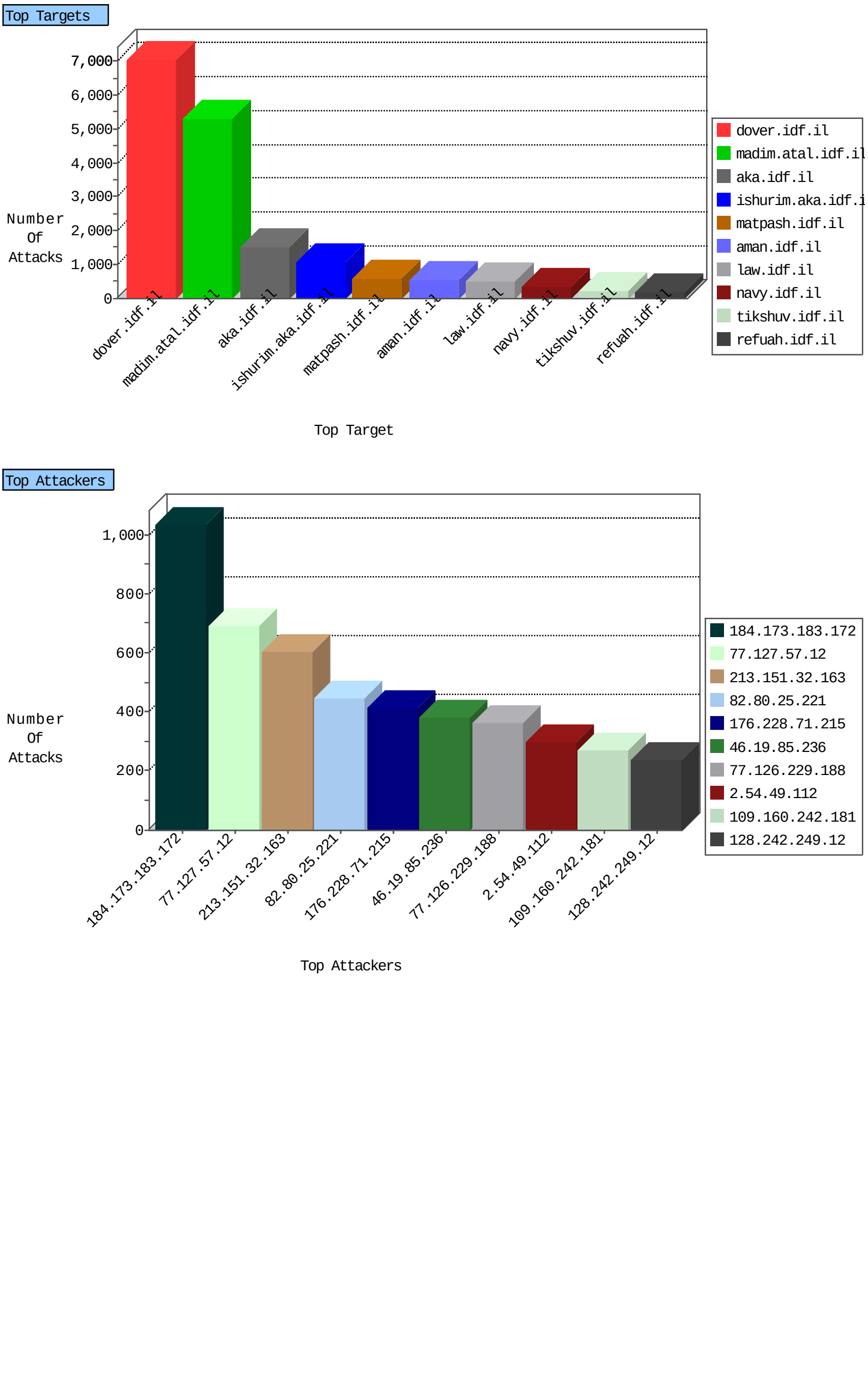
02-14-2015-00:00:04 to 02-15-2015-00:00:04

# IDF Under Attack
# Daily Report



02-14-2015-00:00:04 to 02-15-2015-00:00:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 66.249.69.98 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 7017 |
| 84.108.97.31 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1252 |
| 85.64.76.140 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 886 |
| 192.116.94.67 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 579 |
| 84.229.180.152 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 407 |
| 109.64.96.166 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 392 |
| 31.168.115.185 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 269 |
| 85.65.203.128 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 229 |
| 5.28.186.34 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 192 |
| 80.179.119.22 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 184 |
| 46.19.85.82 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 173 |
| 46.19.86.177 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 160 |
| 213.57.227.103 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 148 |
| 79.180.103.139 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 112 |
| 46.19.85.204 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 92 |
| 213.57.145.95 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 91 |
| 46.120.174.175 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 87 |
| 79.179.155.74 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 86 |
| 37.142.121.51 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 83 |
| 2.54.11.204 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 78 |
| 109.160.241.207 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 77 |
| 84.108.97.31 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 75 |
| 109.64.61.157 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 74 |
| 188.120.152.75 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 65 |
| 85.64.94.24 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 65 |
| 85.250.24.163 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 63 |
| 85.64.3.93 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 61 |
| 149.78.146.46 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 61 |
| 213.57.227.103 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 51 |
| 213.57.145.95 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 49 |
| 82.102.141.217 | Israel | 147.237.77.176 | matpash.idf.il | Invalid TCP Flags | drop | 46 |
| 193.109.199.154 | United Kingdom | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 30 |
| 82.102.141.215 | Israel | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 27 |
| 82.102.141.198 | Israel | 147.237.77.74 | law.idf.il | Invalid TCP Flags | drop | 26 |
| 82.102.141.218 | Israel | 147.237.72.166 | aka.idf.il | Invalid TCP Flags | drop | 25 |
| 82.102.141.198 | Israel | 147.237.76.31 | nakchal.idf.il | Invalid TCP Flags | drop | 20 |
| 82.145.217.180 | Europe | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 19 |
| 82.102.141.215 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Invalid TCP Flags | drop | 15 |
| 82.102.141.200 | Israel | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 15 |
| 82.102.141.217 | Israel | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 13 |
| 82.102.141.207 | Israel | 147.237.72.166 | aka.idf.il | Invalid TCP Flags | drop | 11 |
| 82.145.217.110 | Europe | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 10 |
| 82.102.141.216 | Israel | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 9 |
| 82.102.141.196 | Israel | 147.237.76.31 | nakchal.idf.il | Invalid TCP Flags | drop | 8 |
| 82.102.141.201 | Israel | 147.237.72.156 | aman.idf.il | Invalid TCP Flags | drop | 7 |
| 46.19.86.107 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 5 |
| 82.102.141.217 | Israel | 147.237.76.31 | nakchal.idf.il | Invalid TCP Flags | drop | 4 |
| 180.235.59.181 | Japan | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 4 |
| 134.147.203.115 | Germany | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 4 |
| 82.102.141.248 | Israel | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 3 |

02-14-2015-00:00:04 to 02-15-2015-00:00:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 184.173.183.172 | United States | 147.237.77.176 | matpash.idf.il | DVRep_P-N_40-59 | Permit | 471 |
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 439 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 239 |
| 184.173.183.172 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 126 |
| 46.116.219.74 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 54 |
| 180.76.5.193 | China | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 51 |
| 37.130.227.133 | United Kingdom | 147.237.0.34 | tikshuv.idf.il | DVRep_B-N_60_100 | Block | 26 |
| 188.65.115.185 | United Kingdom | 147.237.76.42 | refuah.idf.il | DVRep_P-N_40-59 | Permit | 13 |
| 37.130.227.133 | United Kingdom | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 11 |
| 180.76.5.193 | China | 147.237.72.156 | aman.idf.il | DVRep_P-N_40-59 | Permit | 8 |
| 89.31.57.5 | Italy | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 7 |
| 212.179.50.77 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 85.25.103.50 | Germany | 147.237.77.212 | e.dover.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 84.94.45.223 | Israel | 147.237.72.156 | aman.idf.il | DVRep_P-N_40-59 | Permit | 5 |
| 213.8.194.56 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 198.20.70.114 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 76.17.248.101 | United States | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 116.8.99.232 | China | 147.237.76.30 | himush.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 188.138.9.50 | Germany | 147.237.72.167 | ishurim.aka.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 116.8.99.232 | China | 147.237.76.31 | nakchal.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 188.138.9.50 | Germany | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 46.117.180.75 | Israel | 147.237.0.34 | tikshuv.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 116.8.99.232 | China | 147.237.76.42 | refuah.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 116.8.99.232 | China | 147.237.76.86 | navy.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 85.25.103.50 | Germany | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 85.25.103.50 | Germany | 147.237.0.35 | akaws.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 85.25.103.50 | Germany | 147.237.76.202 | e.halag.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 85.25.103.50 | Germany | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 85.25.103.50 | Germany | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.0.33 | idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.76.39 | mobile.meitav.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 85.25.103.50 | Germany | 147.237.76.197 | e.himush.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 46.19.85.242 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 198.20.70.114 | United States | 147.237.72.217 | e.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.76.30 | himush.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 46.19.85.238 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 198.20.70.114 | United States | 147.237.76.147 | chinuch.aka.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.76.199 | e.nakchal.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 93.120.27.62 | Romania | 147.237.8.27 | e.madim.atal.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 46.19.85.221 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 85.25.103.50 | Germany | 147.237.77.205 | prisha.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.76.201 | e.atal.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.77.61 | e.cogat.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.72.167 | ishurim.aka.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 79.179.15.19 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 109.67.15.108 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 198.20.70.114 | United States | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 198.20.70.114 | United States | 147.237.8.24 | e.lifestyle.idf.il | DVRep_B-N_60_100 | Block | 2 |

02-14-2015-00:00:04 to 02-15-2015-00:00:04

## 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 | 446 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 143 |
| 82.102.141.199 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 77.125.109.185 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 149.78.146.202 | United States | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 149.78.9.172 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 46.165.226.79 | Germany | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP Mambo upload.php access | 3 |
| 222.186.134.6 | China | 147.237.76.86 | navy.idf.il | ET SCAN Potential SSH Scan | 2 |
| 79.176.116.78 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.77 | China | 147.237.77.74 | law.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.29.129.47 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 222.186.134.6 | China | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 122.228.207.193 | China | 147.237.76.86 | navy.idf.il | ET SCAN Potential SSH Scan | 2 |
| 41.225.157.87 | Tunisia | 147.237.77.216 | dover.idf.il | SQL Injection - Select From | 2 |
| 85.64.116.61 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 149.78.103.137 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.63.133 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 109.64.51.48 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 212.129.52.90 | France | 147.237.77.227 | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 61.240.144.66 | China | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 37.142.240.84 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 149.78.19.122 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 58.20.54.249 | China | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 115.231.218.23 | China | 147.237.8.24 | e.lifestyle.idf.il | ET SCAN Potential SSH Scan | 2 |
| 89.138.205.205 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 31.168.244.9 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.109.86.171 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 95.86.86.7 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.193 | China | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 115.28.48.188 | China | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 115.231.218.147 | China | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 212.71.235.33 | United Kingdom | 147.237.77.216 | dover.idf.il | ET SCAN Potential SSH Scan | 2 |
| 122.228.207.193 | China | 147.237.8.14 | e.orchot.idf.il | ET SCAN Potential SSH Scan | 2 |
| 79.181.180.80 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 115.231.218.147 | China | 147.237.76.38 | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 212.71.235.33 | United Kingdom | 147.237.72.166 | aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 85.250.90.202 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 222.186.134.6 | China | 147.237.76.201 | e.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 79.181.129.152 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.121.83.227 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 111.95.148.194 | Indonesia | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 61.240.144.65 | China | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 122.228.207.77 | China | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 46.19.85.144 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 109.186.249.149 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 85.64.240.205 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 109.67.120.133 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 61.240.144.66 | China | 147.237.0.34 | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 85.64.89.8 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 149.78.84.137 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |

02-14-2015-00:00:04 to 02-15-2015-00:00:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.19.85.236 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 378 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 122 |
| 66.249.81.215 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 100 |
| 97.74.24.210 | United States | 147.237.77.74 | law.idf.il | SAM rule | drop | drop | 96 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 56 |
| 116.58.38.76 | Pakistan | 147.237.77.74 | law.idf.il | First packet isn't SYN | drop | drop | 55 |
| 38.111.147.86 | United States | 147.237.77.216 | dover.idf.il | | drop | drop | 49 |
| 46.42.39.106 | Russian Federation | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 48 |
| 97.74.24.210 | United States | 147.237.72.166 | aka.idf.il | SAM rule | drop | drop | 48 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 44 |
| 109.253.134.28 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 176.12.151.132 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 109.253.131.159 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 222.77.204.64 | China | 147.237.77.233 | atal.idf.il | SAM rule | drop | drop | 39 |
| 109.253.133.75 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 109.253.145.53 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 76.109.47.51 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 82.102.136.65 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 66.249.93.219 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 109.160.250.25 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 176.12.137.241 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 84.140.223.137 | Germany | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 80.169.112.194 | United Kingdom | 147.237.77.216 | dover.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 31 |
| 109.253.144.180 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 109.253.156.13 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 109.253.146.114 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 176.12.140.247 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 109.253.142.148 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 109.253.130.182 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 5.28.183.236 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 29 |
| 66.249.64.92 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 109.66.56.36 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 27 |
| 82.145.209.106 | Europe | 147.237.77.74 | law.idf.il | First packet isn't SYN | drop | drop | 27 |
| 109.253.136.44 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 26 |
| 176.12.147.141 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 26 |
| 109.253.130.78 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 79.181.54.134 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 24 |
| 176.12.136.53 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.147.209 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 157.55.39.187 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.133.46 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 79.181.54.134 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 24 |
| 176.12.143.199 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.132.74 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 176.12.141.99 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 176.12.142.98 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 176.12.141.148 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.135.103 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 176.12.140.39 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 91.186.231.87 | Jordan | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 23 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.127.57.12 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 690 |
| 213.151.32.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 601 |
| 176.228.71.215 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 176.228.71.215 | Block | 414 |
| 77.126.229.188 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 362 |
| 2.54.49.112 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 298 |
| 109.160.242.181 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 265 |
| 176.12.147.123 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 216 |
| 80.246.140.232 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 203 |
| 80.246.136.21 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 182 |
| 38.111.147.84 | United States | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 38.111.147.84 | Block | 169 |
| 80.246.140.151 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 141 |
| 176.12.147.146 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 127 |
| 176.12.141.220 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 176.12.141.220 | Block | 119 |
| 79.181.19.48 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 112 |
| 2.54.19.153 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 108 |
| 109.253.141.189 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 106 |
| 109.253.137.179 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 98 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 72 |
| 185.32.176.86 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 68 |
| 109.253.141.21 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 61 |
| 109.253.156.155 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 59 |
| 109.253.132.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 59 |
| 109.253.144.46 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 51 |
| 109.253.142.12 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 51 |
| 109.253.156.8 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 109.253.156.8 | Block | 50 |
| 176.12.140.123 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 48 |
| 176.12.142.165 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 46 |
| 109.253.133.14 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 45 |
| 109.253.133.29 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 39 |
| 109.253.141.51 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 35 |
| 176.12.138.125 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 33 |
| 109.253.142.217 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 33 |
| 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 | 33 |
| 217.126.129.8 | Spain | 147.237.77.216 | dover.idf.il | Multiple Illegal HTTP Version from 217.126.129.8 | Block | 33 |
| 176.12.142.182 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 33 |
| 109.253.142.232 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 109.253.142.232 | Block | 30 |
| 176.12.147.184 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 30 |
| 109.186.172.66 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 29 |
| 109.253.156.129 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 29 |
| 176.12.138.45 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 26 |
| 80.246.140.151 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 80.246.140.151 | Block | 24 |
| 2.54.178.220 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 23 |
| 109.253.140.36 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 22 |
| 109.253.156.203 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 22 |
| 79.179.141.17 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on 147.237.72.156//modiin/default.aspx | Block | 21 |
| 31.44.134.213 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 20 |
| 95.86.116.138 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 20 |
| 176.12.142.108 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 20 |
| 85.250.178.211 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 17 |
| 109.253.151.83 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 17 |