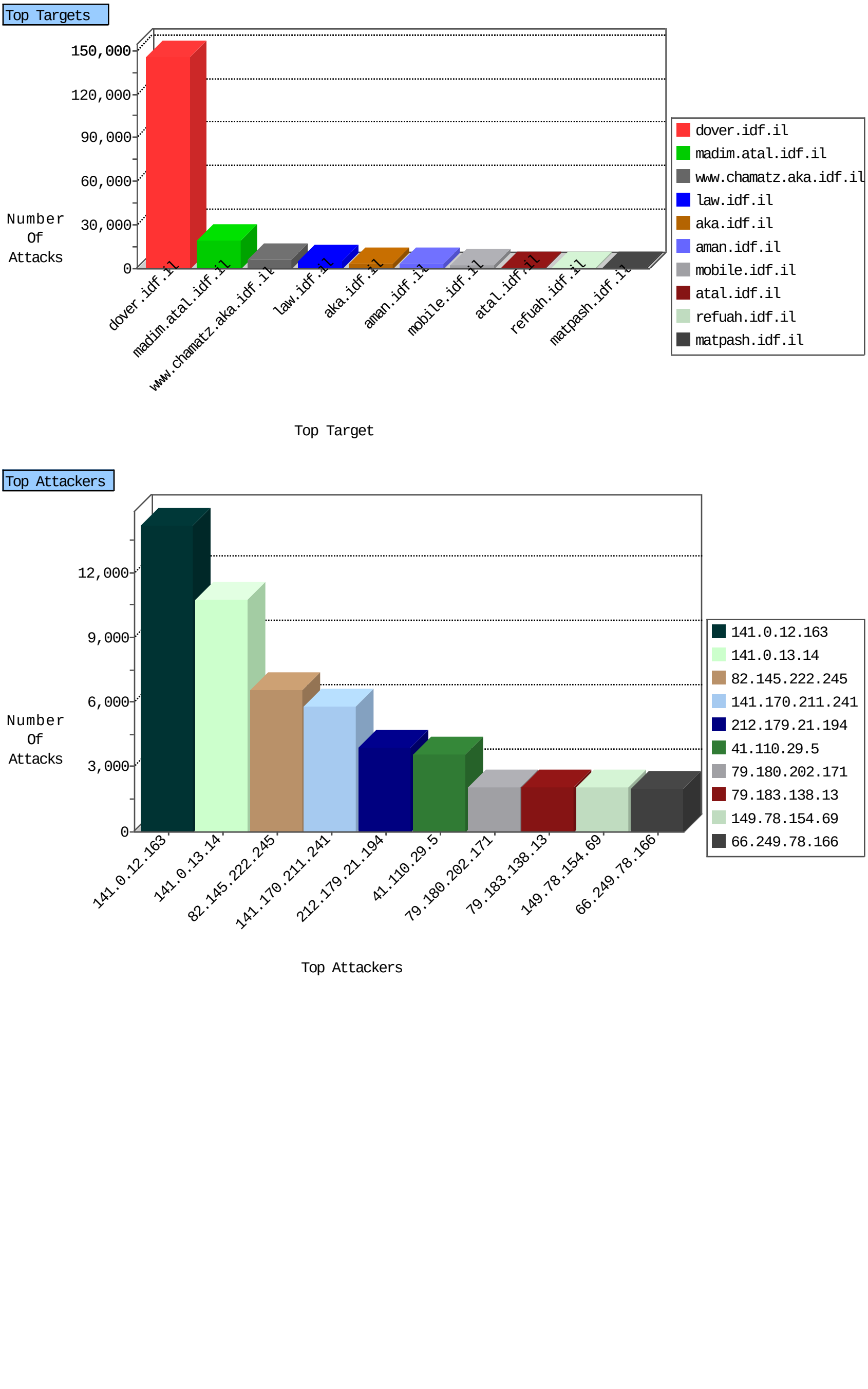
08-06-2015-00:00:07 to 08-07-2015-00:00:07

# IDF Under Attack Daily Report



08-06-2015-00:00:07 to 08-07-2015-00:00:07

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 141.0.13.14 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 16363 |
| 141.0.12.163 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 12170 |
| 108.46.49.77 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 11683 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 10780 |
| 141.0.12.163 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 10255 |
| 66.249.78.141 | Israel | 147.237.72.156 | aman.idf.il | TCP handshake violation, first packet not syn | drop | 9639 |
| 94.249.247.131 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 6009 |
| 66.249.64.173 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4153 |
| 190.24.146.71 | Colombia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3565 |
| 141.0.13.14 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3397 |
| 66.249.64.9 | Israel | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 2857 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 2536 |
| 176.223.82.30 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 2269 |
| 66.249.78.153 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 1834 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1116 |
| 66.249.67.67 | Israel | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 1043 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1001 |
| 141.170.211.241 | Algeria | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1000 |
| 81.218.241.26 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 937 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 638 |
| 85.64.124.32 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 534 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.il | HTTP-MISC-Havij-User-Agent | dest-reset | 521 |
| 109.64.60.69 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 507 |
| 147.235.236.1 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 505 |
| 79.176.127.87 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 492 |
| 108.69.25.167 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 458 |
| 82.211.18.89 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 455 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-product3 | dest-reset | 434 |
| 77.125.145.147 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 412 |
| 79.180.22.89 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 411 |
| 79.183.101.82 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 381 |
| 94.230.81.131 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 336 |
| 84.111.125.156 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 336 |
| 109.66.131.13 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 317 |
| 212.179.21.194 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 267 |
| 5.102.225.136 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 256 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.il | DOS-HTTP-torshammer | dest-reset | 254 |
| 141.170.211.241 | Algeria | 147.237.77.216 | dover.idf.il | DOS-HTTP-torshammer | dest-reset | 249 |
| 82.80.177.187 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 243 |
| 109.64.27.201 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 241 |
| 64.233.172.155 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 239 |
| 79.180.205.38 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 223 |
| 46.117.161.91 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 223 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 217 |
| 31.154.92.134 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 197 |
| 79.183.185.28 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 193 |
| 79.181.206.225 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 189 |
| 81.218.194.243 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 182 |
| 192.118.30.102 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 180 |
| 109.186.100.186 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 179 |

08-06-2015-00:00:07 to 08-07-2015-00:00:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 31.168.23.59 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 37 |
| 79.183.101.82 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 24 |
| 141.170.211.241 | Algeria | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 17 |
| 109.226.20.135 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 194.114.146.227 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 212.150.66.161 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 9 |
| 62.90.35.105 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 8 |
| 62.219.114.84 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 8 |
| 46.19.85.201 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 7 |
| 147.236.113.1 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 82.166.232.133 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 79.182.192.110 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 46.120.229.31 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 194.114.146.227 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 79.176.96.221 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.179 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 77.125.12.121 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 87.69.42.3 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 31.154.92.134 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.195 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 192.116.76.78 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 85.65.130.19 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 31.168.3.188 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 211.59.8.170 | Korea, Republic of | 147.237.72.166 | aka.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 79.177.154.78 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 62.219.197.160 | Israel | 147.237.77.216 | dover.idf.il | 19863: HTTP: WordPress Revslider/Showbiz PHP File Upload | Block | 3 |
| 176.13.17.28 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.116.128.101 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 209.49.53.38 | United States | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 147.236.138.212 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 85.250.215.23 | Israel | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.19.85.179 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 37.26.149.219 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.19.85.179 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 93.172.169.59 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 149.78.68.250 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 87.68.66.45 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.177 | Israel | 147.237.77.74 | law.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 85.64.240.67 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 109.186.173.134 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 91.178.50.168 | Belgium | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 79.182.64.189 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 84.94.200.249 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 194.176.105.144 | United Kingdom | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 192.114.23.18 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 82.166.29.226 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 85.250.185.100 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 109.66.99.2 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |

08-06-2015-00:00:07 to 08-07-2015-00:00:07

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 91 |
| 66.249.78.204 | United States | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 45.114.11.46 | | 147.237.77.233 | atal.idf.il | ET SCAN Potential SSH Scan | 4 |
| 45.114.11.46 | | 147.237.76.202 | e.halag.idf.il | ET SCAN Potential SSH Scan | 3 |
| 218.65.30.107 | China | 147.237.76.176 | test.ncore.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.46 | | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 3 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 3 |
| 188.138.9.51 | Germany | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sS window 1024 | 3 |
| 111.248.47.29 | Taiwan | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP Setup.php access | 3 |
| 218.65.30.107 | China | 147.237.76.202 | e.halag.idf.il | ET SCAN Potential SSH Scan | 3 |
| 41.100.71.190 | Algeria | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP TRACE attempt | 3 |
| 218.65.30.107 | China | 147.237.76.198 | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.48 | | 147.237.8.50 | e.tikshuv.idf.il | ET SCAN Potential SSH Scan | 2 |
| 188.138.9.51 | Germany | 147.237.76.177 | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 45.114.11.46 | | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.48 | | 147.237.0.34 | tikshuv.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.0.200 | m4u.idf.il | ET SCAN Potential SSH Scan | 2 |
| 168.167.132.2 | Botswana | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.67.23 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 94.102.48.193 | Netherlands | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 193.5.216.100 | Switzerland | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 218.65.30.107 | China | 147.237.77.170 | maarachot.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.196 | e.sviva.idf.il | ET SCAN Potential SSH Scan | 2 |
| 92.251.27.46 | Malta | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.48 | | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 45.114.11.46 | | 147.237.77.235 | sviva.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.77.19 | law-forum.idf.il | ET SCAN Potential SSH Scan | 2 |
| 41.100.71.190 | Algeria | 147.237.77.216 | dover.idf.il | SQL Injection - Select From | 2 |
| 45.114.11.46 | | 147.237.77.227 | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 2 |
| 132.74.95.21 | Israel | 147.237.77.170 | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 218.65.30.107 | China | 147.237.72.166 | aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.72.217 | e.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.72.14 | dover.idf.il(old) | ET SCAN Potential SSH Scan | 2 |
| 177.107.103.150 | Brazil | 147.237.76.198 | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.76.197 | e.himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 2 |
| 41.142.89.116 | Morocco | 147.237.0.34 | tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 218.65.30.107 | China | 147.237.77.212 | e.dover.idf.il | ET SCAN Potential SSH Scan | 2 |
| 178.65.17.106 | Russian Federation | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.65.30.107 | China | 147.237.0.35 | akaws.idf.il | ET SCAN Potential SSH Scan | 2 |
| 79.176.42.169 | Israel | 147.237.72.166 | aka.idf.il | http_inspect: MULTIPLE HOST HEADERS DETECTED | 2 |
| 218.65.30.107 | China | 147.237.77.176 | matpash.idf.il | ET SCAN Potential SSH Scan | 2 |
| 92.251.27.46 | Malta | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 177.107.103.150 | Brazil | 147.237.77.243 | mobile.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.64.242 | United States | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 218.65.30.107 | China | 147.237.77.121 | e.navy.idf.il | ET SCAN Potential SSH Scan | 2 |

08-06-2015-00:00:07 to 08-07-2015-00:00:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 141.0.12.163 | Norway | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 14091 |
| 141.0.13.14 | Norway | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 10629 |
| 82.145.222.245 | Europe | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6544 |
| 141.170.211.241 | Algeria | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 5101 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 3624 |
| 41.110.29.5 | Algeria | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 2104 |
| 79.183.138.13 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 2070 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 2063 |
| 212.179.162.114 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1546 |
| 190.24.146.71 | Colombia | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1518 |
| 82.145.222.207 | Europe | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1515 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1005 |
| 2.54.173.227 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 966 |
| 2.52.20.26 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 912 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 864 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 850 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 786 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 777 |
| 46.19.86.248 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 664 |
| 66.249.93.168 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 638 |
| 66.249.84.182 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 626 |
| 66.249.84.194 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 622 |
| 66.249.84.188 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 613 |
| 66.249.93.164 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 606 |
| 193.106.52.21 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 597 |
| 66.249.93.160 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 590 |
| 109.67.188.251 | Israel | 147.237.72.156 | aman.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 588 |
| 188.165.15.152 | France | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 586 |
| 84.111.155.155 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 571 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 564 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 560 |
| 31.44.137.50 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 530 |
| 79.181.136.79 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 529 |
| 2.54.31.107 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 497 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 464 |
| 37.26.148.155 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 458 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 455 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 433 |
| 213.204.103.36 | Lebanon | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 425 |
| 2.54.2.215 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 411 |
| 207.46.13.29 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 400 |
| 149.255.201.246 | Iraq | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 385 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 382 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 379 |
| 94.249.247.193 | Germany | 147.237.77.74 | law.idf.il | First packet isn't SYN | drop | drop | 374 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 372 |
| 2.54.188.73 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 369 |
| 207.46.13.36 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 363 |
| 84.109.116.107 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 363 |
| 2.52.141.46 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 358 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.202.171 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 2073 |
| 109.67.56.127 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 109.67.56.127 | Block | 1934 |
| 176.13.21.180 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1623 |
| 176.12.144.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1077 |
| 85.250.20.18 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1010 |
| 176.12.137.174 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 921 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.173 | Block | 897 |
| 46.19.86.213 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 876 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 831 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 813 |
| 37.26.146.255 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 762 |
| 2.54.21.70 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 2.54.21.70 | Block | 708 |
| 176.13.19.184 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 707 |
| 80.246.139.155 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 660 |
| 176.12.142.117 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 636 |
| 46.19.85.252 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 624 |
| 109.64.43.79 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 109.64.43.79 | Block | 624 |
| 46.19.86.188 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 612 |
| 149.78.176.14 | United States | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 149.78.176.14 | Block | 606 |
| 132.76.10.45 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 504 |
| 85.65.216.87 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 500 |
| 46.19.85.104 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 417 |
| 185.32.179.157 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 405 |
| 37.26.146.239 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 300 |
| 2.52.21.61 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword | Block | 267 |
| 176.12.149.195 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 246 |
| 212.235.8.225 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 231 |
| 212.235.8.225 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 212.235.8.225 | Block | 213 |
| 176.13.17.34 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 207 |
| 176.13.14.171 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 183 |
| 2.54.140.211 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 174 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp | Block | 162 |
| 176.13.19.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 159 |
| 176.12.150.193 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 141 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_text.asp | Block | 138 |
| 80.246.136.227 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 135 |
| 46.19.85.154 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 126 |
| 176.12.151.4 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 126 |
| 93.172.104.225 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 120 |
| 212.179.21.194 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 117 |
| 46.19.85.13 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 114 |
| 84.228.125.65 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 105 |
| 176.13.0.18 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 81 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp | Block | 81 |
| 46.19.85.74 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 75 |
| 93.173.239.55 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 72 |
| 176.13.1.135 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 72 |
| 176.13.9.166 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 69 |
| 176.12.137.219 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 69 |
| 46.19.85.104 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.85.104 | Block | 60 |