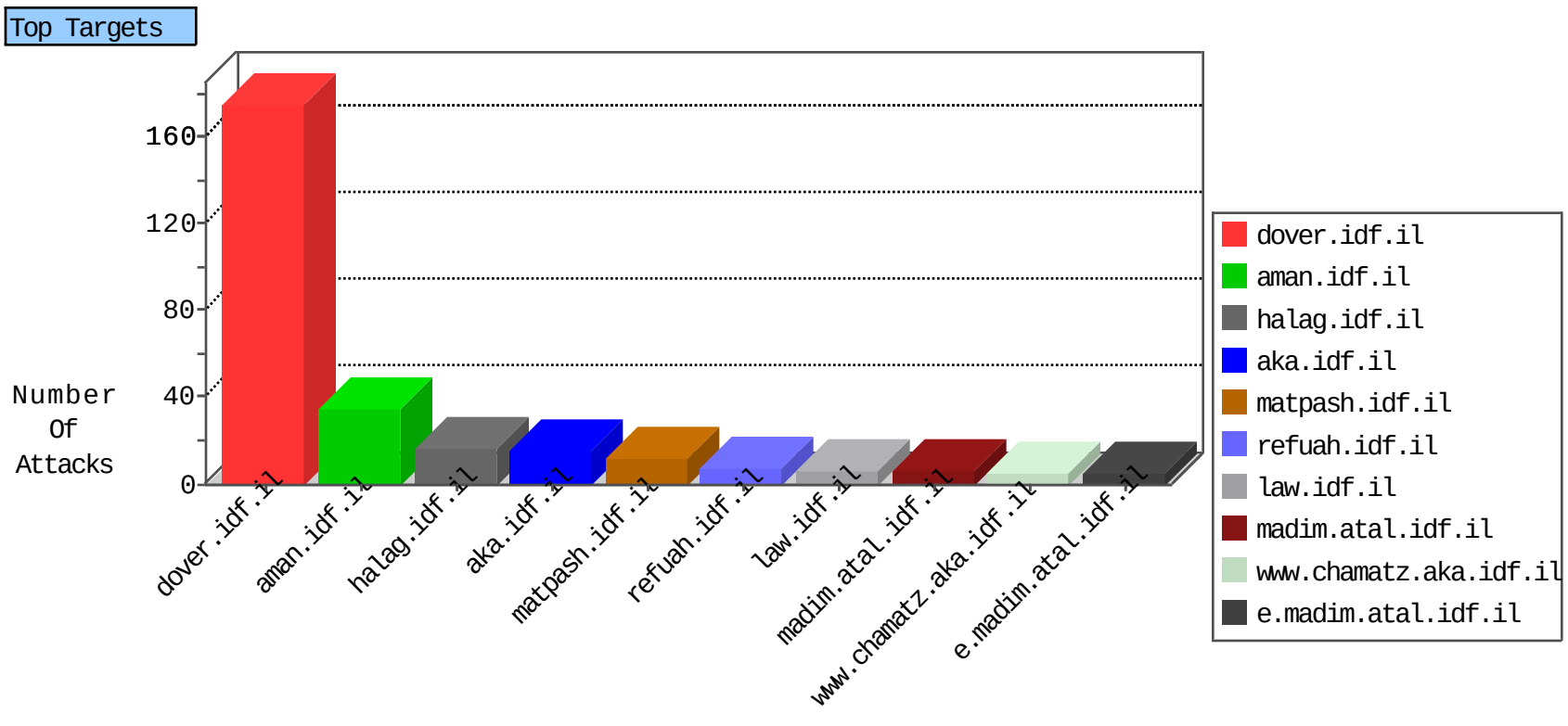
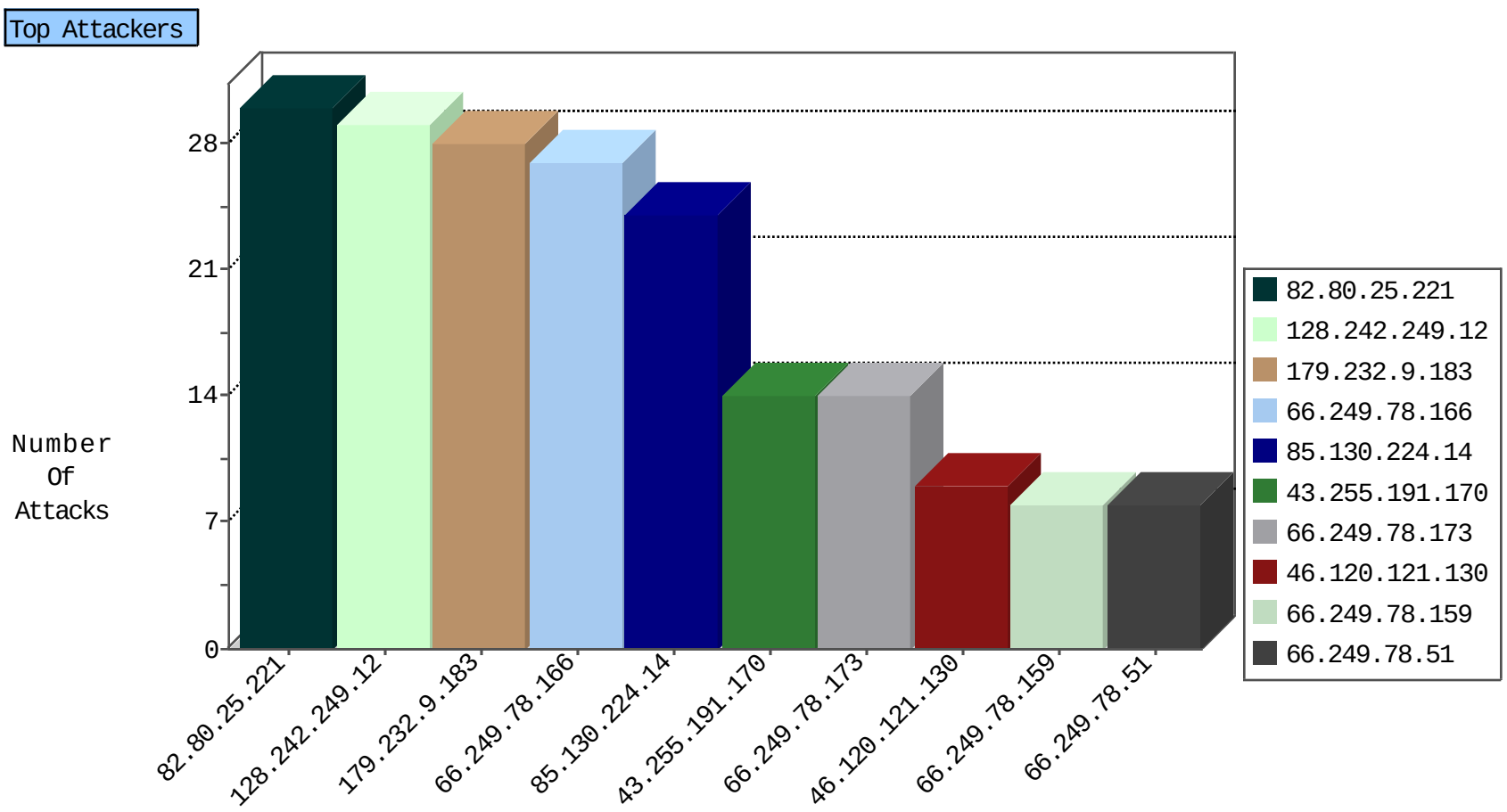
03-31-2015-02:03:04 to 03-31-2015-03:03:04

# IDF Under Attack
# 03-31-2015-02:03:04



03-31-2015-02:03:04 to 03-31-2015-03:03:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 85.130.224.14 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 130 |
| 46.120.121.130 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 78 |
| 71.6.165.200 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

03-31-2015-02:03:04 to 03-31-2015-03:03:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 29 |
| 85.250.146.221 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 69.197.186.210 | United States | 147.237.76.42 | refuah.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 4 |
| 77.127.132.2 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 175.44.5.185 | China | 147.237.77.74 | law.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 2 |
| 85.25.103.50 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.243 | mobile.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.236.119 | United States | 147.237.8.14 | e.orchot.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.0.15 | kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.236.119 | United States | 147.237.76.31 | nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.0.35 | akaws.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.43.94 | Germany | 147.237.77.74 | law.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.177 | ncore.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.19 | madim.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.236.119 | United States | 147.237.77.234 | halag.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.44 | e.refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.8.28 | e.mobile-ks.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.177 | ncore.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.234 | halag.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.61 | e.cogat.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.135.131 | United States | 147.237.77.170 | maarachot.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.72.167 | ishurim.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |

03-31-2015-02:03:04 to 03-31-2015-03:03:04

## 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 | 30 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 6 |
| 43.255.191.170 | Japan | 147.237.77.176 | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.76.147 | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.76.42 | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.72.14 | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 222.69.94.13 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 43.255.191.170 | Japan | 147.237.0.35 | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.77.178 | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.76.201 | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.76.86 | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.76.38 | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.69.94.13 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 43.255.191.170 | Japan | 147.237.8.27 | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.69.94.13 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 43.255.191.170 | Japan | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 128.61.240.66 | United States | 147.237.72.14 | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.77.234 | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 43.255.191.170 | Japan | 147.237.77.179 | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |

03-31-2015-02:03:04 to 03-31-2015-03:03:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 179.232.9.183 | Brazil | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 26 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 14 |
| 66.249.78.51 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 8 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 46.19.85.63 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 5 |
| 188.225.183.149 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 5 |
| 85.130.224.14 | Israel | 147.237.72.156 | aman.idf.il | Invalid ACK number | Bad TCP sequence | alert | 5 |
| 85.130.224.14 | Israel | 147.237.72.156 | aman.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 5 |
| 46.19.86.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 37.247.36.91 | Netherlands | 147.237.8.27 | e.madim.atal.idf.il | Geo-location inbound enforcement | Geo-location enforcement | drop | 4 |
| 75.146.123.25 | United States | 147.237.72.217 | e.idf.il | Geo-location inbound enforcement | Geo-location enforcement | drop | 4 |
| 66.249.78.37 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 4 |
| 5.102.254.222 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 75.119.249.208 | Canada | 147.237.77.226 | www.chamatz.aka.idf.il | First packet isn't SYN | drop | drop | 3 |
| 75.119.249.208 | Canada | 147.237.77.74 | law.idf.il | First packet isn't SYN | drop | drop | 2 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 207.241.237.106 | United States | 147.237.77.216 | dover.idf.il | Web Servers Slow HTTP Denial of Service | Web Server Enforcement Violation | reject | 2 |
| 66.249.78.44 | United States | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 46.19.86.30 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 2.54.41.4 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 85.130.230.214 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 37.26.147.216 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 188.138.17.205 | France | 147.237.77.212 | e.dover.idf.il | Geo-location inbound enforcement | Geo-location enforcement | drop | 1 |
| 5.22.129.188 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 1 |
| 141.212.122.12 | United States | 147.237.76.147 | chinuch.aka.idf.il | | drop | drop | 1 |
| 46.120.190.177 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 5.22.129.188 | Israel | 147.237.72.166 | aka.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 1 |
| 173.208.203.138 | United States | 147.237.77.176 | matpash.idf.il | Failed to handle connection data | Block HTTP Non Compliant | monitor | 1 |
| 46.19.85.225 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 37.26.147.216 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 1 |
| 188.120.148.196 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |

03-31-2015-02:03:04 to 03-31-2015-03:03:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.255.253.124 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 5.255.253.124 | Block | 3 |
| 31.184.238.128 | Russian Federation | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 31.184.238.128 | Block | 2 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.196 | Block | 2 |
| 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 | 2 |
| 77.127.95.169 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.78.82 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf | Block | 1 |
| 157.55.39.66 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 1 |
| 74.102.91.142 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 188.165.15.148 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 188.165.15.148 | Block | 1 |
| 79.182.129.63 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd | Block | 1 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 1 |
| 173.36.113.105 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 75.146.123.25 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 31.184.238.128 | Russian Federation | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 84.111.6.81 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/relativecontact.aspx | None | 1 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/history/future3.stm | Block | 1 |
| 173.208.203.138 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/readme.asp | Block | 1 |
| 75.146.123.25 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 46.19.123.125 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/alnajah/alnajah.stm | Block | 1 |
| 95.86.126.37 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/p | Block | 1 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm | Block | 1 |
| 176.12.136.120 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 77.125.216.194 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd | Block | 1 |
| 66.249.75.7 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx | Block | 1 |
| 207.241.237.103 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx | Block | 1 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/dover/site/homepage.asp | Block | 1 |
| 188.165.15.148 | France | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

03-31-2015-02:03:04 to 03-31-2015-03:03:04