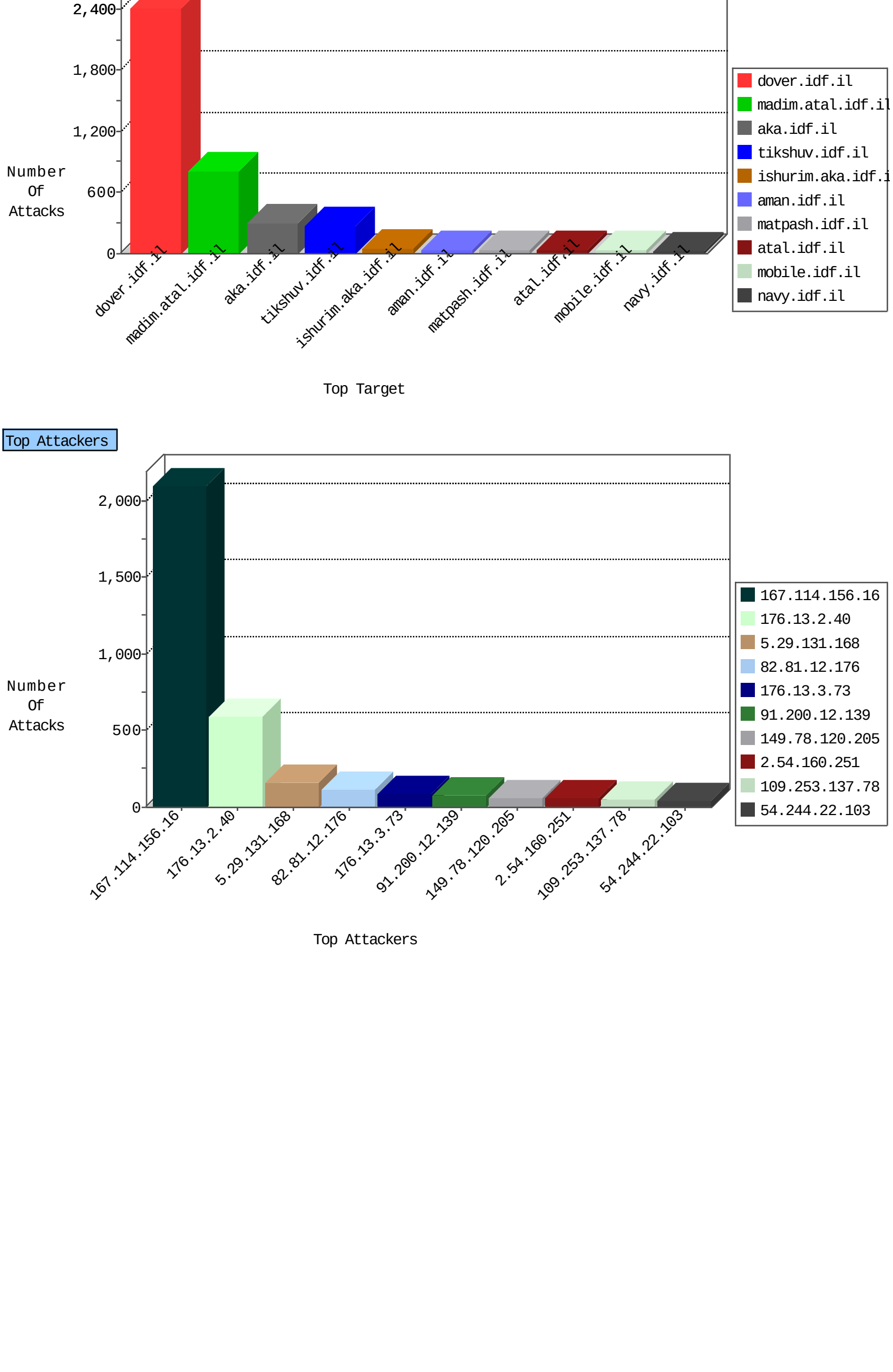
01-20-2016-08:04:03 to 01-20-2016-09:04:03

# IDF Under Attack Daily Report



01-20-2016-08:04:03 to 01-20-2016-09:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3079 |
| 82.81.12.176 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 119 |
| 204.42.253.2 | United States | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.146.244 | Germany | 147.237.76.147 | chinuch.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 204.42.253.2 | United States | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.146.244 | Germany | 147.237.76.199 | e.nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 204.42.253.2 | United States | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 204.42.253.2 | United States | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.160.18.169 | Vietnam | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 204.42.253.2 | United States | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.146.244 | Germany | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 1 |

01-20-2016-08:04:03 to 01-20-2016-09:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 140.101.20.1 | United States | 147.237.0.34 | tikshuv.idf.il | C212: HTTP: prefix 1.01 in the URL | Block | 5 |
| 93.63.188.181 | Italy | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 87.106.184.160 | Germany | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |

01-20-2016-08:04:03 to 01-20-2016-09:04:03

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | **Signature** | **Count** |
|---|---|---|---|---|---|

01-20-2016-08:04:03 to 01-20-2016-09:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.253.137.78 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 47 |
| 202.3.255.143 | French Polynesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 34 |
| 54.244.22.103 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 31 |
| 105.230.24.243 | Kenya | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 19 |
| 2.52.11.238 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 192.117.153.118 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 46.19.85.3 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 207.46.13.133 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 10 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 109.253.202.23 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 2.54.9.83 | Israel | 147.237.77.243 | mobile.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 212.150.214.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 212.150.214.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 185.32.179.1 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.46 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 54.244.22.103 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 8 |
| 37.142.168.233 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.127 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.46 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 31.168.140.228 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.86.127 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 46.19.86.127 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 31.168.140.228 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.64.163 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.52.187.129 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 31.168.140.228 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 2.52.187.129 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 105.230.24.243 | Kenya | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.86.127 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.253.208.126 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 46.19.86.127 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 109.65.117.81 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 194.90.178.146 | Israel | 147.237.77.170 | maarachot.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 195.244.23.42 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.26.148.212 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.86.127 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 5 |
| 37.142.168.233 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 195.244.23.42 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 213.8.204.62 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.54.189.223 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.42.39 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 46.19.85.181 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.189.223 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 64.31.44.6 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 4 |
| 176.13.2.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid sequence number | alert | 3 |
| 23.91.70.94 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |

01-20-2016-08:04:03 to 01-20-2016-09:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.2.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 176.13.2.40 | Block | 287 |
| 176.13.2.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 176.13.2.40 | Block | 163 |
| 5.29.131.168 | Israel | 147.237.0.34 | tikshuv.idf.il | Too Many of the Same Response Code (404) in Session from 5.29.131.168 | Block | 161 |
| 176.13.2.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 133 |
| 176.13.3.73 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 90 |
| 149.78.120.205 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 60 |
| 2.54.160.251 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 56 |
| 185.32.179.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 38 |
| 2.52.177.2 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 14 |
| 91.200.12.139 | Ukraine | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 8 |
| 91.200.12.139 | Ukraine | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 6 |
| 91.200.12.139 | Ukraine | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 6 |
| 109.186.151.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/ | Block | 6 |
| 91.200.12.139 | Ukraine | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 6 |
| 194.90.178.146 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Unauthorized HTTP Method | Block | 5 |
| 91.200.12.139 | Ukraine | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 4 |
| 91.200.12.139 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 4 |
| 194.90.178.146 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 194.90.178.146 | Block | 4 |
| 46.19.86.225 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 91.200.12.139 | Ukraine | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 3 |
| 37.26.147.150 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.176.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 81.218.241.25 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 81.218.241.25 | Block | 3 |
| 2.52.166.171 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.197 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 91.200.12.139 | Ukraine | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 2 |
| 37.26.147.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.0.34 | tikshuv.idf.il | Distributed PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 2 |
| 46.19.86.39 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.76.200 | eitan.aka.idf.il | PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.0.15 | kosher-kravi.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 91.200.12.139 | Block | 2 |
| 176.13.4.142 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 91.200.12.139 | Ukraine | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 2 |
| 109.253.150.74 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.76.86 | navy.idf.il | Distributed PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.0.15 | kosher-kravi.idf.il | PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 2 |
| 37.26.146.151 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |
| 109.253.200.218 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 84.109.11.141 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.158.46 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 105.155.163.105 | Morocco | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 105.155.163.105 | Block | 1 |
| 91.200.12.139 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/wp-login.php | Block | 1 |

01-20-2016-08:04:03 to 01-20-2016-09:04:03