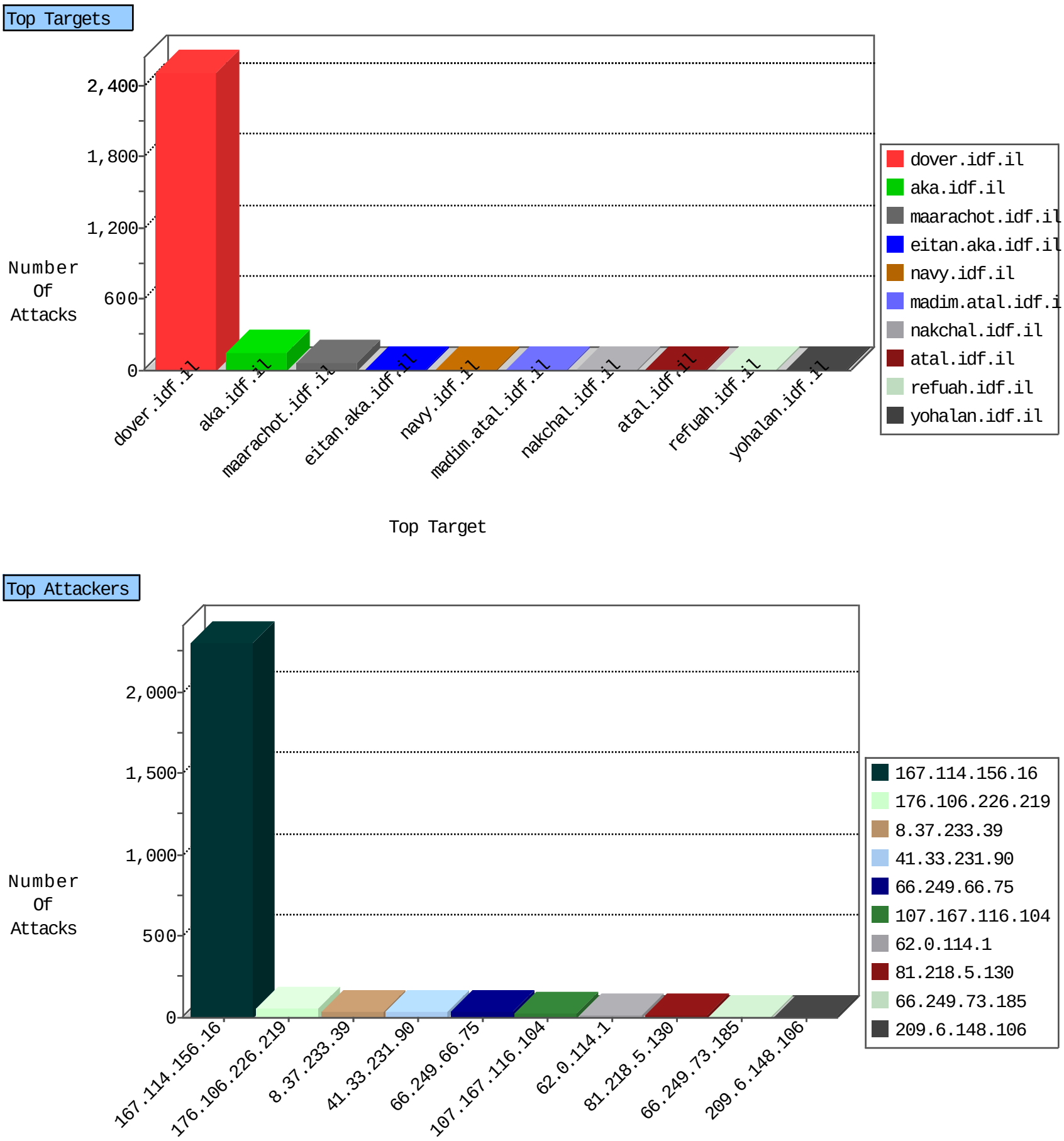
11-26-2015-01:12:28 to 11-26-2015-02:12:28

# IDF Under Attack Daily Report



11-26-2015-01:12:28 to 11-26-2015-02:12:28

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.66.75 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 9261 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 4277 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 371 |
| 81.218.5.130 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 14 |
| 113.108.21.16 | China | 147.237.76.197 | e.himush.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 93.174.93.151 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 52.27.97.133 | United States | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.174.93.151 | Netherlands | 147.237.76.38 | e.e.meitav.idf.i | Block_Udp_All_Nets | drop | 1 |
| 93.174.93.151 | Netherlands | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

11-26-2015-01:12:28 to 11-26-2015-02:12:28

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 60.56.228.138 | Japan | 147.237.76.86 | navy.idf.il | C025: HTTP: access to administrator/index.php -> Quarantine | Block | 1 |

11-26-2015-01:12:28 to 11-26-2015-02:12:28

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 183.60.48.25 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.131.21.69 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.131.21.69 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.131.21.69 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 121.21.232.248 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 31.6.71.154 | 147.237.77.216 | Poland | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.60.48.25 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.131.21.69 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.131.21.69 | 147.237.76.177 | China | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 134.219.148.12 | 147.237.8.46 | United Kingdom | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.195 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-26-2015-01:12:28 to 11-26-2015-02:12:28

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 8.37.233.39 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 176.106.226.219 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | alert | 28 |
| 176.106.226.219 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 28 |
| 107.167.116.104 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 26 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 20 |
| 62.0.114.1 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 209.6.148.106 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 207.46.13.49 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.85.79 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 66.249.66.61 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.59.101 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.103 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 40.77.167.14 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.86.15 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 66.249.64.75 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 77.126.51.122 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 192.116.242.249 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.108.176.250 | Israel | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 37.26.146.213 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.182.31.127 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.86.250 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 80.246.130.32 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 109.67.160.53 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.68.59.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 62.0.114.1 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 5.255.253.188 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.142.49 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 157.55.39.180 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 195.154.200.30 | France | 147.237.76.34 | yohalan.idf.il | drop | | drop | 2 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 188.95.127.237 | Czech Republic | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 40.77.167.35 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 80.246.137.252 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 137.227.175.206 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 2 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 2.54.142.49 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 2 |
| 68.156.149.62 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.86.44 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 137.227.175.206 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 94.159.181.187 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.126.163.240 | Ukraine | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 64.125.239.137 | United States | 147.237.72.217 | e.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.121.182 | United States | 147.237.8.46 | e.chinuch.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.85.64 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |

11-26-2015-01:12:28 to 11-26-2015-02:12:28

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 194.187.168.22 | Poland | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 107.167.116.104 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx | Block | 2 |
| 46.116.137.51 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 2 |
| 80.246.136.223 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 2.54.59.101 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar | Block | 2 |
| 176.13.15.2 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 5.29.242.54 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 80.246.130.32 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 60.56.228.138 | Japan | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 8.37.70.135 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1514-en/dover.aspx&usg=alkjrhi0fatgzxyham9ad57e0egxs3xepw | Block | 1 |
| 194.102.58.66 | Romania | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 1 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1065-he/dover.aspx | Block | 1 |
| 149.78.166.151 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 60.56.228.138 | Japan | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/wp-login.php | Block | 1 |
| 208.184.112.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 194.102.58.66 | Romania | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 1 |
| 8.37.233.39 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/shael, idfspokeperson | Block | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.67.251 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter 5cf35968 in aka.idf.il/news/ | None | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx | Block | 1 |
| 46.121.64.254 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 81.223.254.34 | Austria | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to /robots.txt | Block | 1 |
| 66.249.66.28 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 40.77.167.14 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.73.201 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/ | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 46.175.254.19 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/international_training/catalog.asp | Block | 1 |
| 5.29.160.26 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.126.163.240 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 88.117.101.132 | Austria | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 207.46.13.49 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar | Block | 1 |
| 40.77.167.35 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 79.182.31.127 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 54.147.177.102 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 178.255.215.87 | France | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 95.86.80.41 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx&sa=u&ved=0ahukewi46jiw4azjahugtxqkhz3dd3aqfggqmae&sig2=f_ymuzl2ozdfdzcb7fg_jq&usg=afqjcnf_b016rnmdjafppqlxngfli8du6w | Block | 1 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/1159-he/chinuch.aspx | Block | 1 |
| 40.77.167.76 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/sip_storage/ | Block | 1 |

11-26-2015-01:12:28 to 11-26-2015-02:12:28