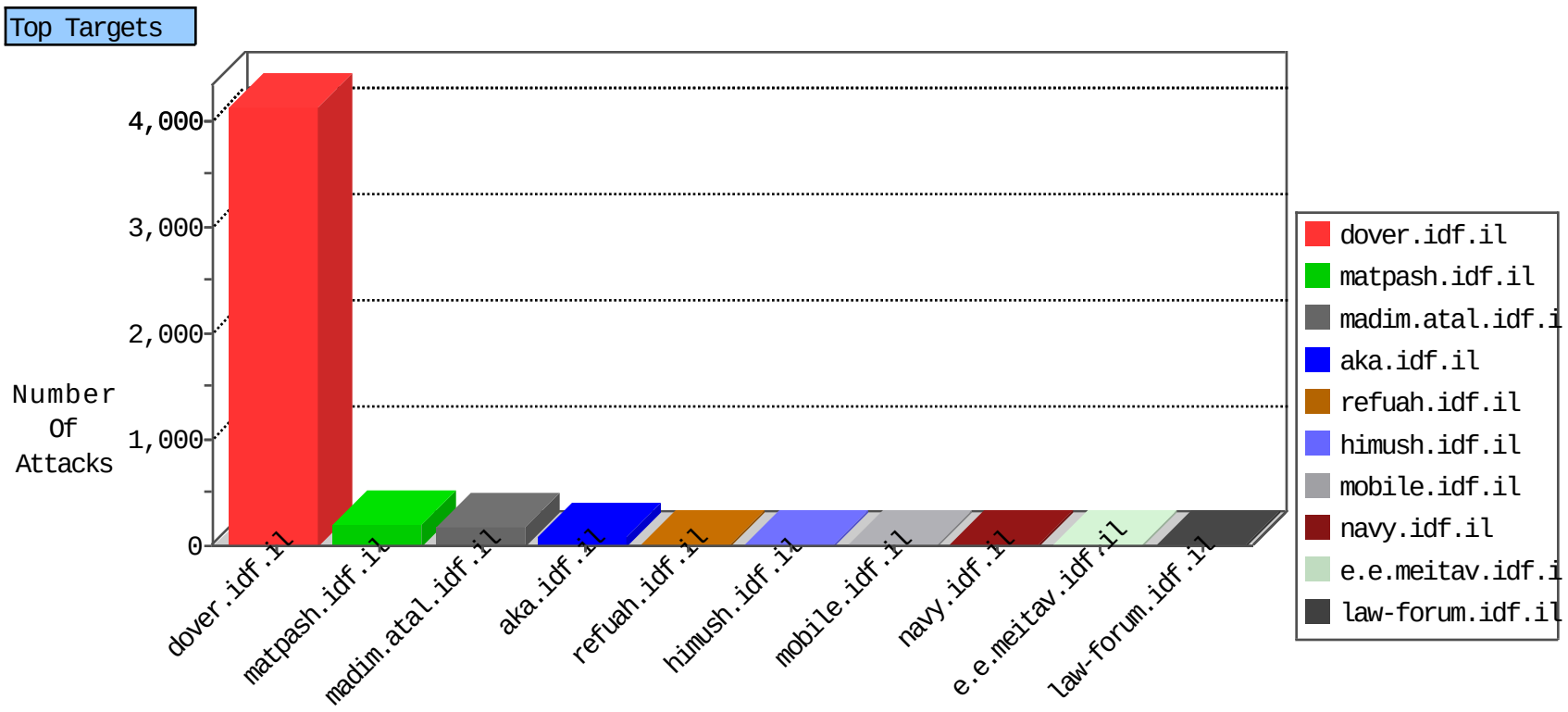
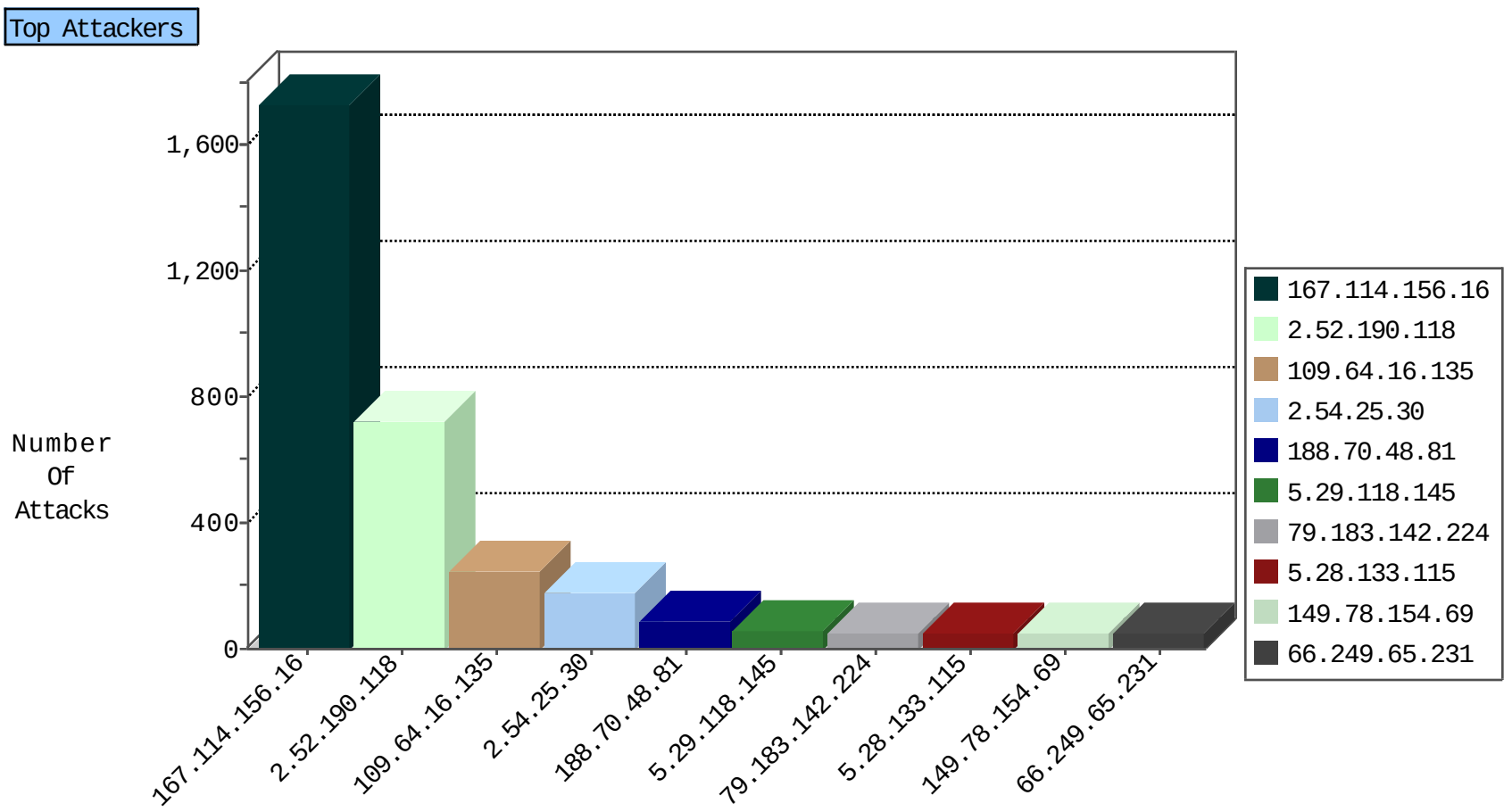
11-07-2015-00:04:01 to 11-07-2015-01:04:01

# IDF Under Attack Daily Report

Top Targets




Top Attackers



11-07-2015-00:04:01 to 11-07-2015-01:04:01

## 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 | 2837 |
| 220.181.108.81 | China | 147.237.76.86 | navy.idf.il | TCP handshake violation, first packet not syn | drop | 278 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 21 |
| 46.116.159.165 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 19 |
| 84.228.144.166 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 19 |
| 100.14.33.8 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 2.54.182.164 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 37.26.147.211 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 77.127.178.43 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 100.14.33.8 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 62.219.254.22 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 37.238.180.14 | Iraq | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 188.161.178.66 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 5.8.66.69 | Russian Federation | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 96.45.232.46 | United States | 147.237.76.30 | himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 172.87.128.131 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 84.94.79.247 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 5.8.66.69 | Russian Federation | 147.237.76.197 | e.himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 207.46.13.184 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 85.25.103.50 | Germany | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

11-07-2015-00:04:01 to 11-07-2015-01:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

11-07-2015-00:04:01 to 11-07-2015-01:04:01

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 6 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.67.122 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 78.142.19.47 | 147.237.72.217 | Bulgaria | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 78.142.19.47 | 147.237.0.33 | Bulgaria | idf.il | ET SCAN Potential SSH Scan | 1 |
| 78.142.19.47 | 147.237.0.16 | Bulgaria | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 78.142.19.47 | 147.237.76.38 | Bulgaria | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 78.142.19.47 | 147.237.72.166 | Bulgaria | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 78.142.19.47 | 147.237.0.17 | Bulgaria | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 188.138.9.51 | 147.237.77.19 | Germany | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-07-2015-00:04:01 to 11-07-2015-01:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.52.190.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 723 |
| 109.64.16.135 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 245 |
| 188.70.48.81 | Kuwait | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 88 |
| 5.29.118.145 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 55 |
| 5.28.133.115 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 79.183.142.224 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 40.77.167.35 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 66.249.65.231 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 34 |
| 66.249.93.200 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 68.4.93.63 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 109.200.30.154 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 54.224.21.23 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 77.127.178.43 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 66.249.93.196 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 86.67.9.88 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 46.116.159.165 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 41.109.225.178 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 66.249.93.192 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 84.94.208.173 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 183.79.221.13 | Japan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 84.228.144.166 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 198.58.102.95 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.13.19.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 2.54.25.30 | Israel | 147.237.0.19 | madim.atal.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 79.177.148.51 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 173.52.85.106 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 12 |
| 37.238.180.14 | Iraq | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 31.13.109.117 | Ireland | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 10 |
| 31.13.100.118 | Ireland | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 10 |
| 173.252.81.112 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 10 |
| 105.99.16.225 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 173.252.81.119 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 10 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.54.25.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 128 |
| 2.54.25.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 2.54.25.30 | Block | 27 |
| 176.12.137.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.12.142.14 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | 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 |
| 159.255.163.132 | Iraq | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 2 |
| 79.181.147.149 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 66.249.64.56 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/scriptresource.axd | Block | 1 |
| 69.171.231.226 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 66.249.67.54 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 1 |
| 31.154.145.255 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 87.68.157.177 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.67.242 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 66.249.65.14 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465 | Block | 1 |
| 69.171.231.227 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/favicon.ico | Block | 1 |
| 66.249.67.59 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 46.19.86.100 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 87.69.241.92 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 1 |
| 66.249.67.250 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 208.115.113.89 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx | Block | 1 |
| 66.249.67.65 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 46.117.146.161 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.67.56.239 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in URL /mivtza>×¡×Ÿ×•×¦×˜×›×?×›Ã¼×?×žœ ×¡×?×™×¢×•</a>, ×¡×žפ×?×?×?×žœ ×″×›Ã¿ â€Ž×¢×˜×¥ ×¦×•×› ×•×™. <p> <table cellspacing= | Block | 1 |
| 66.249.65.237 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-15693-he/dover.aspx | Block | 1 |
| 5.28.171.57 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 77.237.138.51 | Czech Republic | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to / | Block | 1 |
| 66.249.67.132 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter 5cf35968 in aka.idf.il/news/ | None | 1 |
| 64.19.78.242 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 5.255.253.157 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/kesher/ | Block | 1 |
| 217.132.54.20 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |

11-07-2015-00:04:01 to 11-07-2015-01:04:01