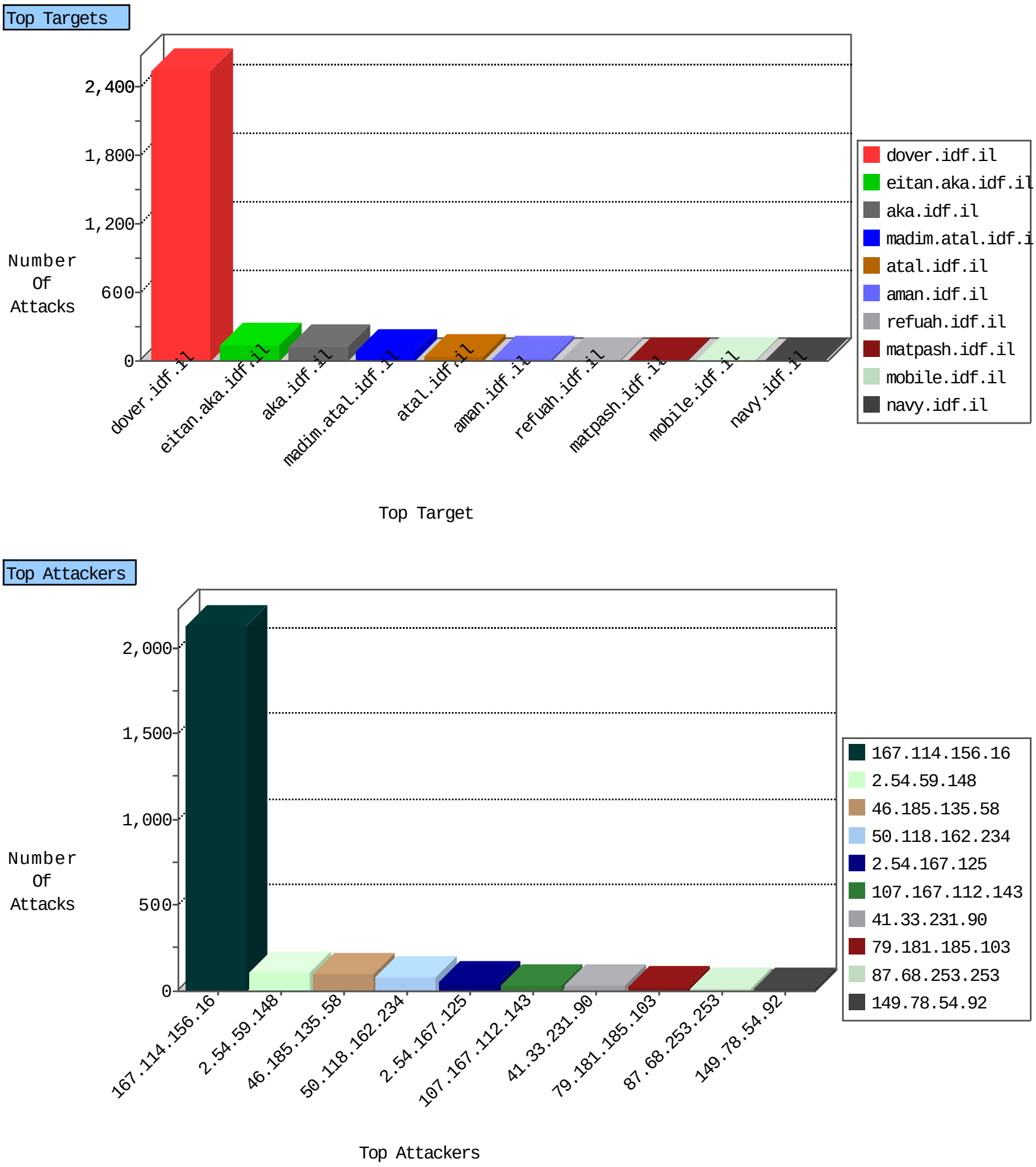
01-22-2016-17:04:06 to 01-22-2016-18:04:06

# IDF Under Attack Daily Report



01-22-2016-17:04:06 to 01-22-2016-18:04:06

## 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 | 3040 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Product | dest-reset | 87 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Url | dest-reset | 8 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 199.255.210.118 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Product | dest-reset | 3 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 198.20.70.114 | United States | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |
| 74.91.28.62 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | drop | 1 |
| 142.54.160.214 | United States | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | drop | 1 |

01-22-2016-17:04:06 to 01-22-2016-18:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 172.245.218.130 | United States | 147.237.72.166 | aka.idf.il | 0543: HTTP: php.cgi Access | Block | 1 |
| 172.245.218.130 | United States | 147.237.77.216 | dover.idf.il | 0543: HTTP: php.cgi Access | Block | 1 |

01-22-2016-17:04:06 to 01-22-2016-18:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 54.205.186.101 | 147.237.77.176 | United States | matpash.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 3 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.66.81 | 147.237.76.30 | United States | himush.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.65.34 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 109.253.207.238 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 85.93.5.65 | 147.237.77.212 | Germany | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 169.50.77.72 | 147.237.76.38 | Switzerland | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 162.242.245.138 | 147.237.8.24 | United States | e.lifestyle.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 119.81.188.158 | 147.237.8.27 | Hong Kong | e.madim.atal.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 108.168.185.133 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.81.12.132 | 147.237.72.167 | Israel | ishurim.aka.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 167.0.190.135 | 147.237.0.34 | Colombia | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 159.8.109.19 | 147.237.77.233 | Netherlands | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

01-22-2016-17:04:06 to 01-22-2016-18:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.54.59.148 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 108 |
| 46.185.135.58 | Jordan | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 100 |
| 107.167.112.143 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 35 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 79.181.185.103 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 87.68.253.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 93.172.164.45 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 14 |
| 79.207.41.129 | Germany | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 10 |
| 176.13.11.171 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 176.13.11.171 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.253.207.238 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 178.154.189.201 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.147.135 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.3.147.111 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.102.254.226 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 198.100.144.55 | Canada | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.207.238 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 84.228.8.17 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 31.210.186.46 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 93.169.137.10 | Romania | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 212.157.35.146 | France | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 77.125.145.166 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.52.50.211 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 79.180.112.65 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 84.229.245.25 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.146.214 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.179.101.140 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.89.217.229 |  | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.223.162 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.126.247 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 195.154.146.225 | France | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 3 |
| 79.181.202.76 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.161.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 217.66.240.199 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop |  | drop | 3 |
| 79.180.100.167 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.78.230 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.178.138.117 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 41.176.195.140 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 40.77.167.63 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 185.3.147.161 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 217.66.240.199 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 31.210.187.243 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 79.180.112.65 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 85.64.184.241 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 185.3.147.111 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |

01-22-2016-17:04:06 to 01-22-2016-18:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.54.167.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 54 |
| 149.78.54.92 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized HTTP Method | Block | 14 |
| 81.218.57.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 5.28.171.203 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 85.64.240.137 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 85.64.240.137 | None | 5 |
| 172.245.218.130 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 172.245.218.130 | Block | 3 |
| 199.30.25.101 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.253.90.5 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 2 |
| 201.156.142.136 | Mexico | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 2 |
| 79.179.120.254 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.179.120.254 | Block | 2 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 50.118.162.234 | Block | 2 |
| 37.26.146.221 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.19.85.65 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 120.29.66.5 | Philippines | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/menu-ending.gif | Block | 1 |
| 41.237.101.190 | Egypt | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php | Block | 1 |
| 217.66.240.199 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 84.111.191.49 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 31.13.113.77 | Ireland | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 79.178.188.111 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.78.216 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1890 | Block | 1 |
| 185.3.146.214 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 109.65.6.215 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.181.185.103 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx | None | 1 |
| 40.77.167.63 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx | Block | 1 |
| 207.46.13.78 | United States | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/ | Block | 1 |
| 2.54.155.224 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 197.49.65.10 | Egypt | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp | Block | 1 |
| 66.249.65.37 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 41.237.101.190 | Egypt | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 31.168.150.46 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/sidebar/bullet purple.gif | Block | 1 |
| 185.89.217.229 | | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 109.67.52.48 | Israel | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 1 |
| 79.181.188.44 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 1 |
| 41.176.195.140 | Egypt | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 213.8.204.40 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 197.49.65.10 | Egypt | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 69.30.205.251 | United States | 147.237.77.74 | law.idf.il | Suspicious Response Code | Block | 1 |
| 66.249.78.97 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 41.237.101.190 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 85.250.198.247 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 79.179.120.254 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx | Block | 1 |
| 204.13.201.138 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 190.104.220.126 | Argentina | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 109.67.52.48 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/xmlrpc.php | Block | 1 |
| 50.118.162.234 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he/tahuzbj5 | Block | 1 |
| 79.181.188.44 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/xmlrpc.php | Block | 1 |

01-22-2016-17:04:06 to 01-22-2016-18:04:06