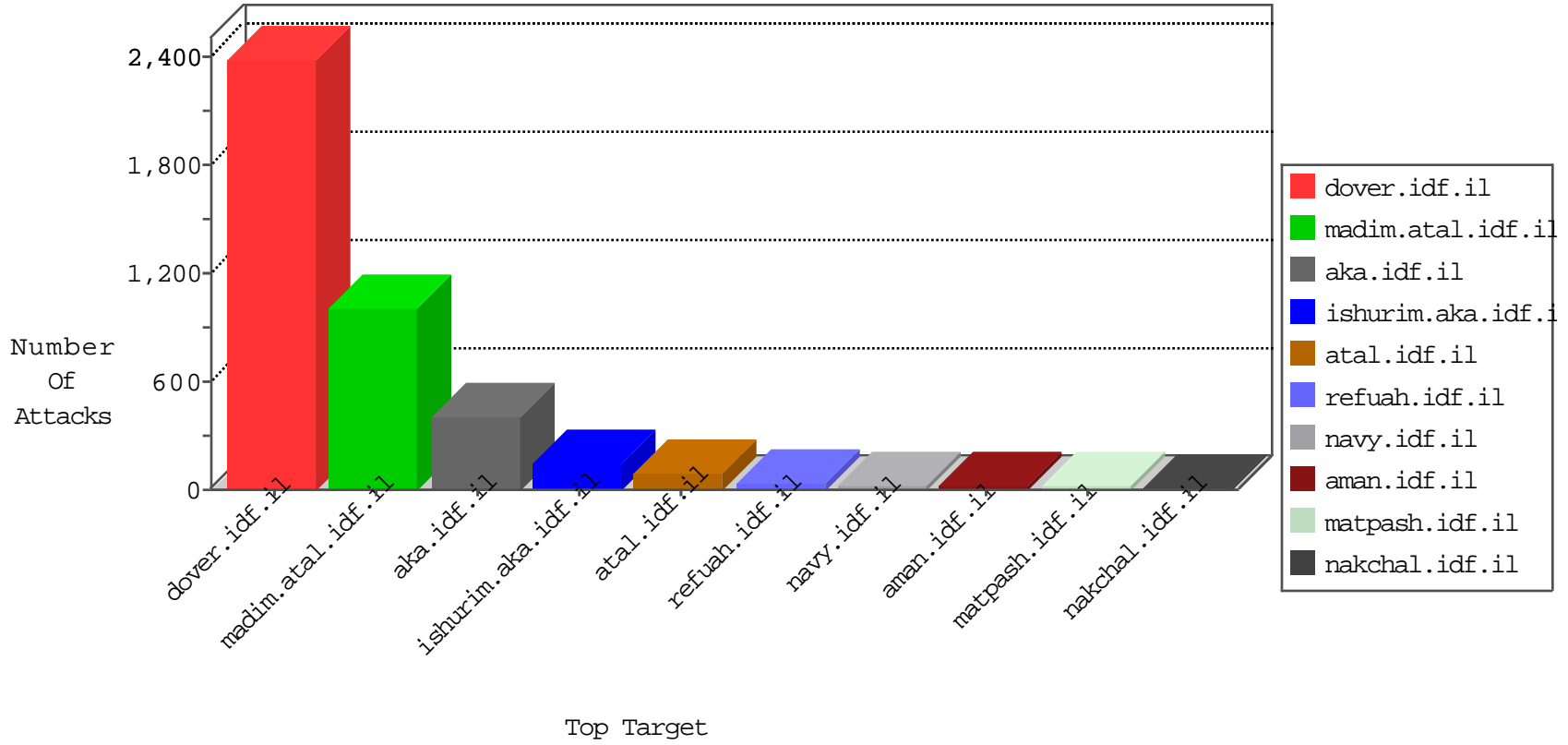


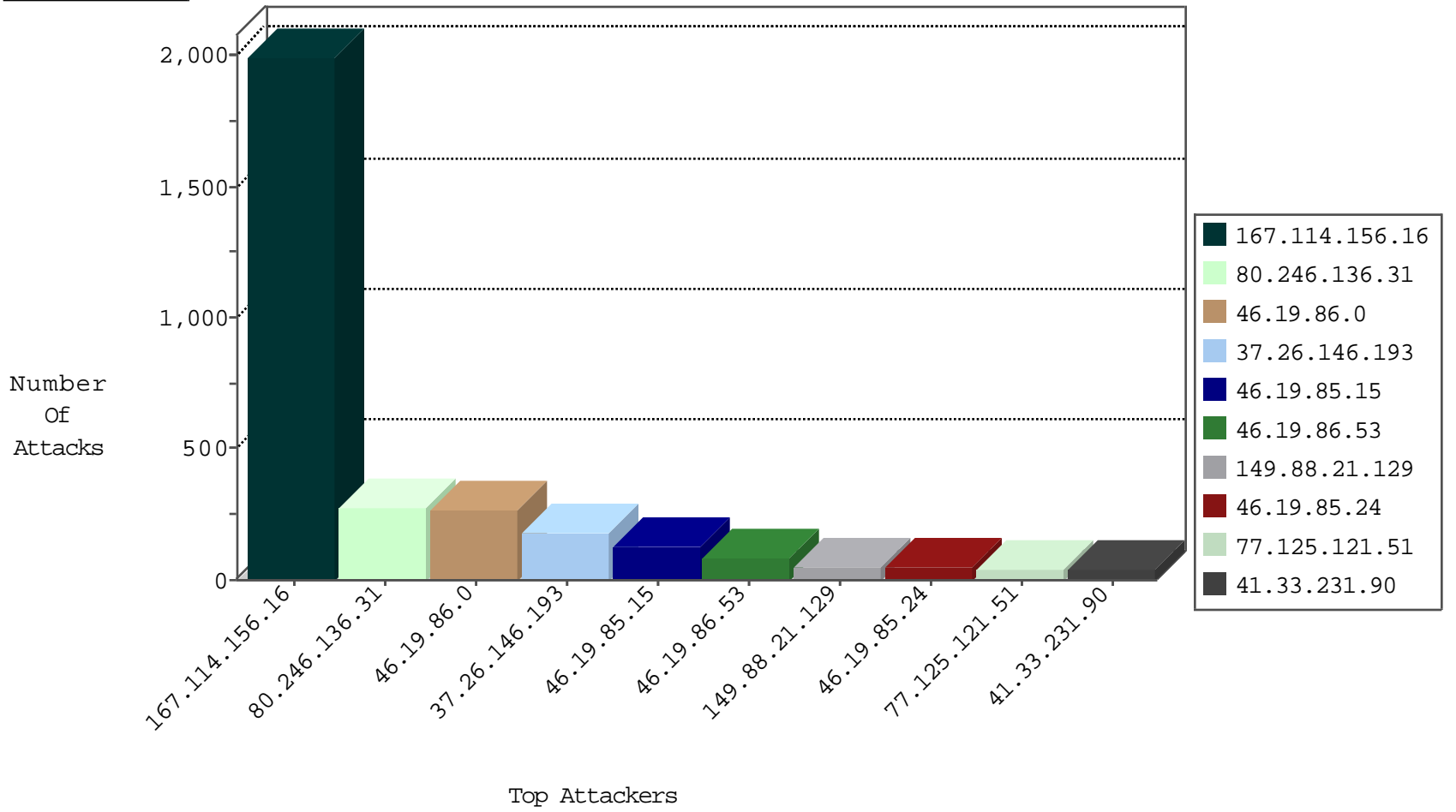
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | 3122 |
| 207.232.36.181 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 111 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |

12-17-2015-13:04:09 to 12-17-2015-14:04:09

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------|------------------------------|---------------|-------|
| 62.210.148.247 | France | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 1 |
| 151.80.31.115 | Italy | 147.237.77.233 | atal.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |

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 | 2 |
| 192.162.100.148 | 147.237.0.34 | Russian Federation | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 166.63.125.149 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 80.246.133.3 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 46.19.86.138 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.142.64.75 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.199.172.154 | 147.237.77.243 | Lithuania | mobile.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 183.14.7.252 | 147.237.77.216 | China | dover.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 81.218.89.58 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.183.135.8 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.212.62.139 | 147.237.72.166 | Belarus | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.147.167 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.177.148 | 147.237.77.216 | Israel | dover.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|--------------------|--|---|---------------|-------|
| 46.19.86.53 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 80 |
| 149.88.21.129 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 48 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 77.125.121.51 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 33 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 46.19.85.66 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 19 |
| 207.241.229.104 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 18 |
| 207.241.229.104 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 18 |
| 46.19.86.67 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 213.57.135.165 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 82.80.196.44 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 185.3.146.117 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 192.114.105.254 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 109.226.22.157 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 37.26.146.193 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 46.19.85.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.85.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 80.179.125.162 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 80.179.125.162 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 11 |
| 82.80.30.90 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 11 |
| 82.80.30.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 82.80.196.44 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 66.249.93.180 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 66.249.93.182 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 46.19.86.151 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 37.26.148.236 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 2.54.12.83 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 89.139.20.70 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 2.54.34.205 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 80.179.125.162 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 80.246.133.3 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 199.203.226.21 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 7 |
| 62.0.200.129 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 77.127.133.245 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 31.168.8.110 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 80.179.69.146 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 6 |
| 130.207.203.56 | United States | 147.237.8.28 | e.mobile-ks.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 6 |
| 46.19.85.119 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 80.246.136.185 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 80.246.133.3 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 37.26.149.131 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 5 |
| 46.19.85.119 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 80.246.136.174 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 73.195.248.179 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.54.12.83 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 188.120.148.160 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.49 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 141.0.15.243 | Norway | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------------|---|---------------|-------|
| 46.19.86.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 152 |
| 80.246.136.31 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 143 |
| 80.246.136.31 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 135 |
| 46.19.86.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 37.26.146.193 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 94 |
| 46.19.85.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 61 |
| 37.26.146.193 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 61 |
| 46.19.85.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 57 |
| 46.19.85.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 46.19.86.84 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 34 |
| 176.12.141.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 176.13.15.71 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 5.102.254.95 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 37.26.146.145 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 37.26.146.241 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.19.86.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 46.19.86.0 | Block | 5 |
| 192.116.172.33 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.52.26.224 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 84.111.184.168 | Israel | 147.237.76.147 | chinuch.aka.idf.il | PHP Attempt | Block | 3 |
| 84.111.184.168 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php | Block | 3 |
| 46.19.85.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 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 | 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 | 2 |
| 192.118.10.10 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.118.10.10 | Block | 2 |
| 90.148.174.170 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 90.148.174.170 | Block | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 90.148.174.170 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 2.54.25.186 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 54.186.248.49 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-he/www.idf.il | Block | 1 |
| 185.3.146.117 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 87.68.240.180 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 141.212.121.176 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 82.80.196.44 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 212.199.107.106 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.26.149.131 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 139.130.251.253 | Australia | 147.237.72.166 | aka.idf.il | Abnormally Long Request method | Block | 1 |
| 69.171.228.122 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.33.241 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 84.111.184.168 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php | Block | 1 |
| 46.19.86.187 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 46.19.86.187 | Block | 1 |
| 176.12.160.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 139.130.251.253 | Australia | 147.237.72.166 | aka.idf.il | Malformed URL k[[#14]]ÅsÅ¼o[[#11]]Å¼°æ°Å»Èe9[[#6]]bÅž a[[#21]][[#17]]Åšâ,~Å?Å'x£[[#19]]æwÅ¼'x?[[#31]]xæ æž2È†]i2Å²x³Ö,[[#12]]x?x"xžÅ¼¹Å»È†Öµæ°Ö²Ö³aæ°aÅ·mx -lÅ?y | Block | 1 |
| 81.218.241.25 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/style/shared/layout.css | None | 1 |
| 109.65.217.109 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 79.183.185.158 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 212.179.177.148 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to static.link4u.co.il/cache/w_news/img_287_3.jpg | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation pageNum in www.idf.il/1379-he/dover.aspx | Block | 1 |
| 185.27.105.176 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct125 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 89.138.209.68 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |