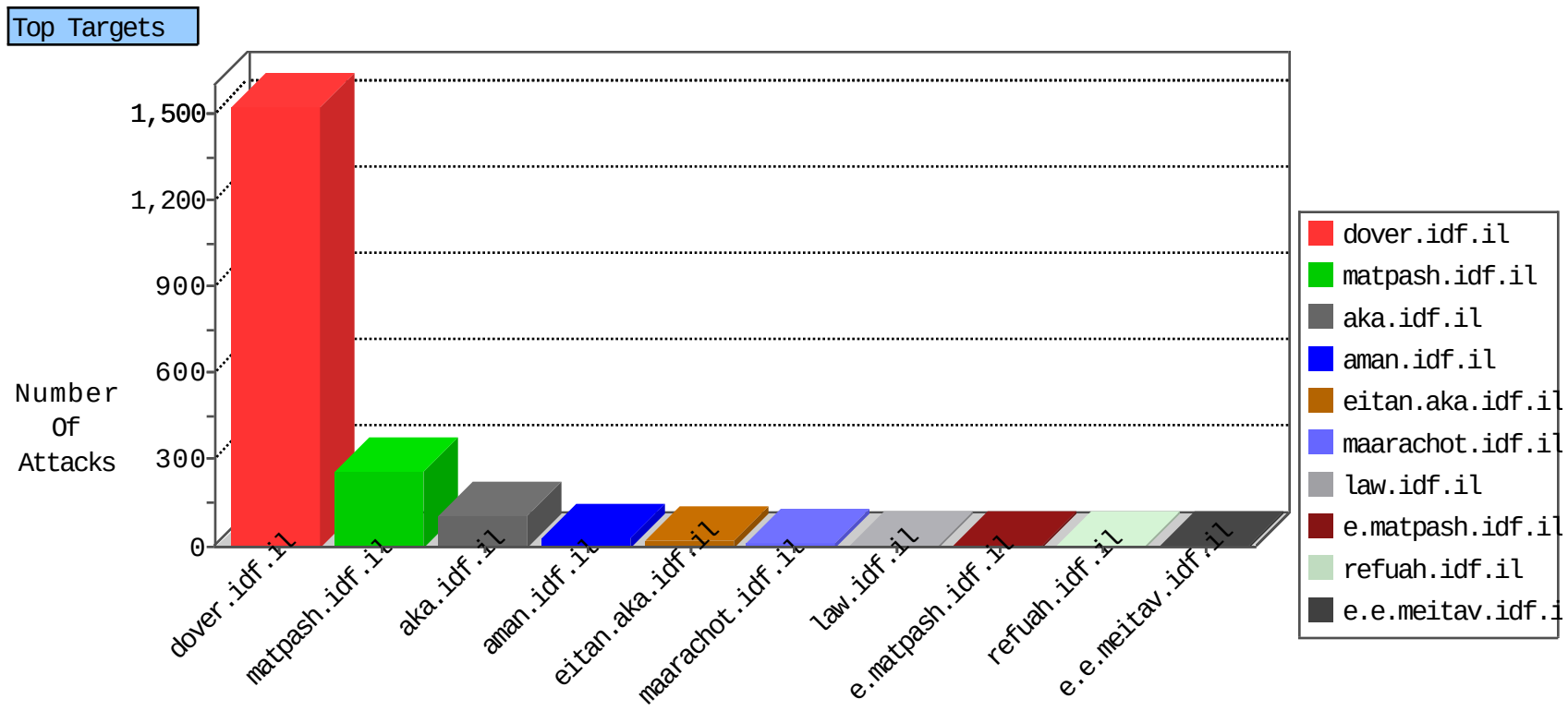
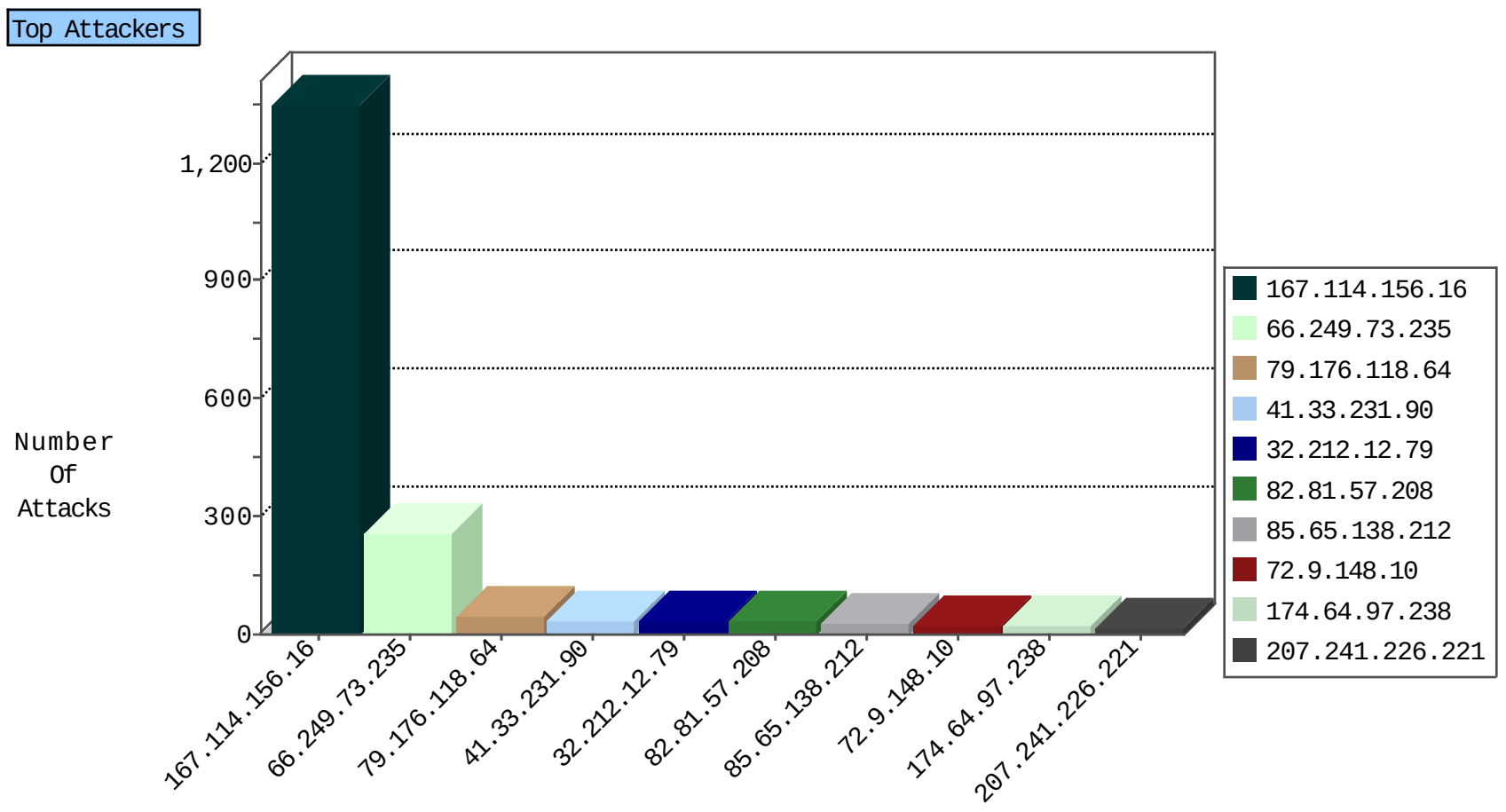
01-02-2016-03:04:05 to 01-02-2016-04:04:05

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



01-02-2016-03:04:05 to 01-02-2016-04:04:05

## 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 | 3023 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |

01-02-2016-03:04:05 to 01-02-2016-04:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 62.212.73.211 | Netherlands | 147.237.72.166 | aka.idf.il | C1000106: HTTP: majestic bot | Block | 1 |
| 69.30.203.166 | United States | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 1 |

01-02-2016-03:04:05 to 01-02-2016-04:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.73.235 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sA (2) | 255 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.66.53 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 36.72.228.72 | 147.237.77.178 | Indonesia | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 5.149.248.251 | 147.237.76.30 | Netherlands | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 169.50.71.13 | 147.237.76.200 | Switzerland | eitan.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 91.201.236.113 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 36.72.228.72 | 147.237.77.178 | Indonesia | e.matpash.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 36.72.228.72 | 147.237.77.178 | Indonesia | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 194.165.155.114 | 147.237.77.179 | Jordan | e.mazi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 93.189.26.18 | 147.237.8.50 | Austria | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.113 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |

01-02-2016-03:04:05 to 01-02-2016-04:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 79.176.118.64 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 174.64.97.238 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 22 |
| 207.241.226.221 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 18 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 16 |
| 32.212.12.79 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 32.212.12.79 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 14 |
| 85.65.138.212 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 85.65.138.212 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 79.176.118.64 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 77.127.243.193 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 10 |
| 46.19.85.137 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 185.27.105.156 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 72.9.148.10 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 4 |
| 5.29.104.197 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.45.254.225 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.38.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.138 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 72.9.148.10 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 2 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 70.81.6.15 | Canada | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 176.126.252.12 | Romania | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 46.19.85.47 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.170 | United States | 147.237.77.212 | e.dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.149.248.251 | Netherlands | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 185.130.5.231 | | 147.237.76.39 | mobile.meitav.idf.i | drop | SAM rule | drop | 1 |
| 77.125.147.25 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.130.5.224 | | 147.237.76.39 | mobile.meitav.idf.i | drop | SAM rule | drop | 1 |
| 52.90.147.148 | United States | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 171.25.193.20 | Sweden | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 93.189.26.18 | Austria | 147.237.72.217 | e.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 198.45.200.18 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 185.130.5.224 | | 147.237.76.199 | e.nakchal.idf.il | drop | SAM rule | drop | 1 |
| 71.6.165.200 | United States | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 178.17.174.99 | Moldova, Republic of | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 46.19.85.47 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 5.149.248.251 | Netherlands | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 185.130.5.231 | | 147.237.76.197 | e.himush.idf.il | drop | SAM rule | drop | 1 |
| 2.54.167.27 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.130.5.224 | | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 66.230.230.230 | United States | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 109.201.133.100 | Netherlands | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 198.45.200.18 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.130.5.224 | | 147.237.76.201 | e.atal.idf.il | drop | SAM rule | drop | 1 |
| 5.79.68.161 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 149.202.47.181 | Germany | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 5.175.26.46 | Germany | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 1 |
| 93.115.95.204 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.81.57.208 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized HTTP Method | Block | 31 |
| 32.212.12.79 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 87.68.60.182 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 2 |
| 5.29.104.197 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 85.65.138.212 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 149.78.23.30 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 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 | 1 |
| 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 |
| 77.237.146.28 | Czech Republic | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to / | Block | 1 |
| 62.210.105.116 | France | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 2.54.146.233 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 193.239.44.212 | Poland | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 89.138.165.35 | Israel | 147.237.72.166 | aka.idf.il | Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.78.187 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized URL Access on nakhal.idf.il/page.asp | Block | 1 |
| 37.187.129.166 | France | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 77.247.181.162 | Netherlands | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 66.249.66.61 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 2.54.170.179 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 193.239.44.212 | Poland | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 93.160.60.22 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english | Block | 1 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 37.187.129.166 | France | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 109.66.54.41 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.97 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 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 | 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 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx | Block | 1 |
| 46.166.188.250 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 109.253.143.210 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.78.146 | Block | 1 |
| 32.212.12.79 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 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 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx | Block | 1 |
| 52.90.147.148 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/ | Block | 1 |