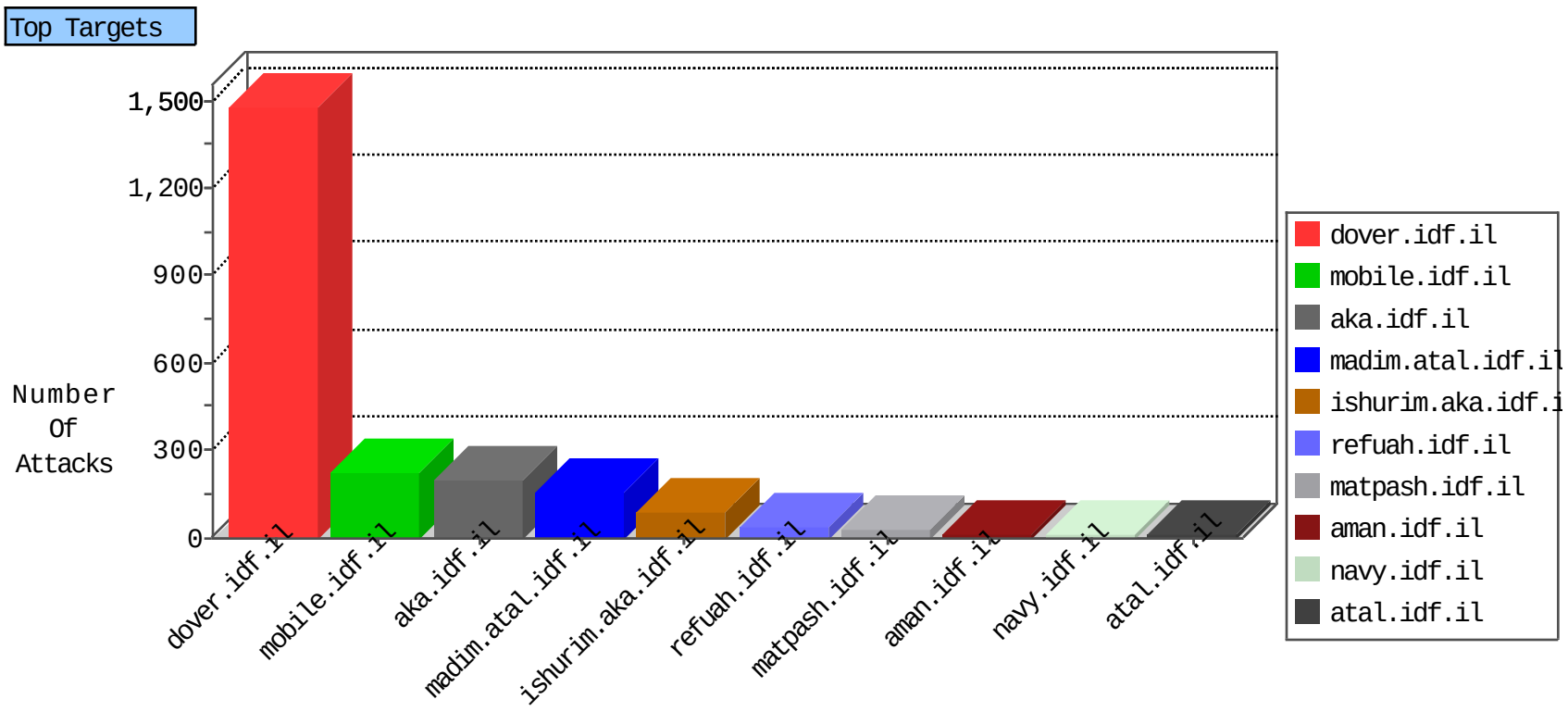
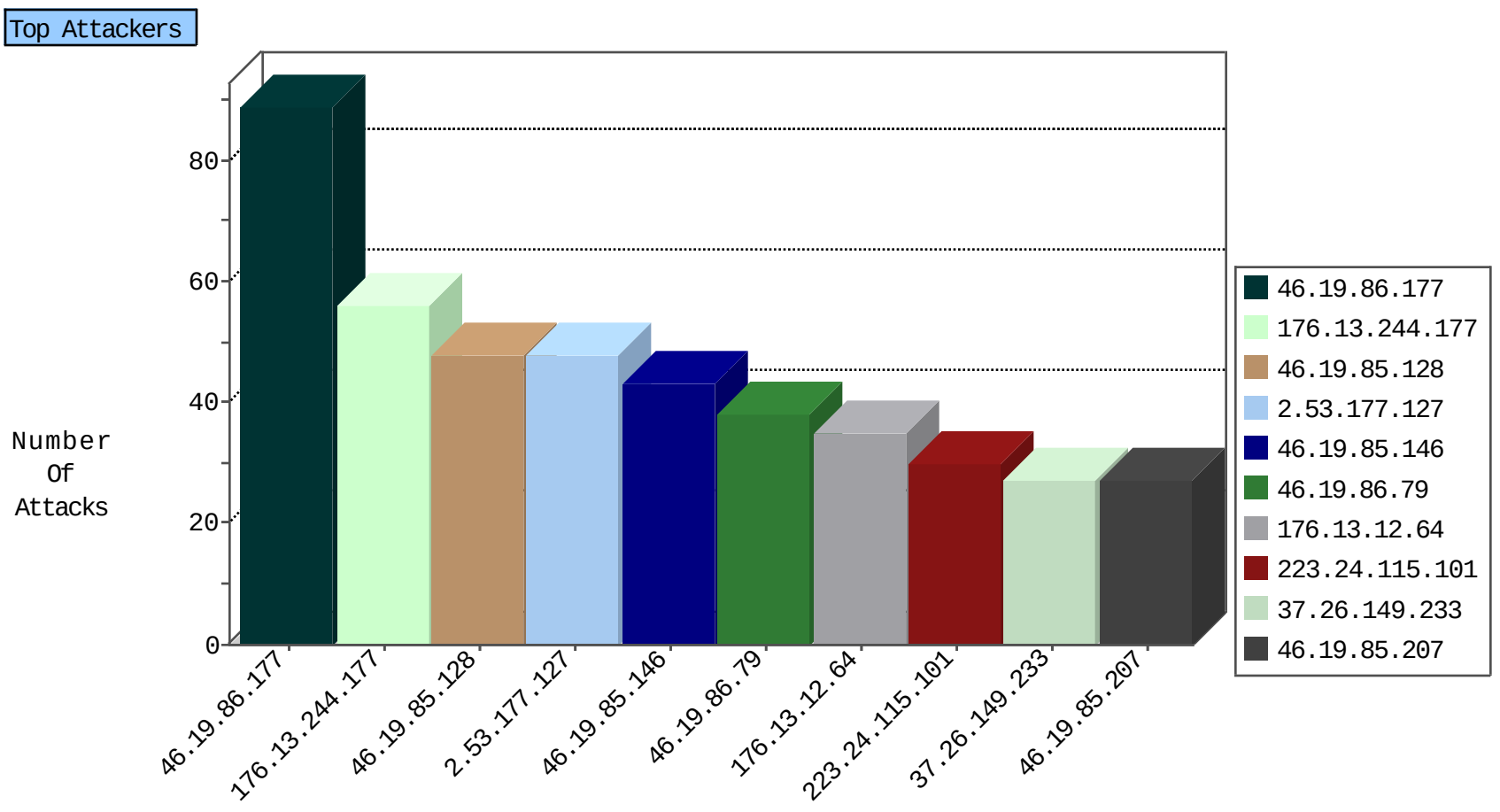
09-29-2016-14:04:05 to 09-29-2016-15:04:05

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-29-2016-14:04:05 to 09-29-2016-15:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 41 |
| 46.19.85.117 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 5 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 176.13.226.99 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 87.69.119.75 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 89.139.198.48 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 173.208.213.198 | United States | 147.237.76.31 | nakchal.idf.il | block-sp-traf1 | forward | 2 |
| 46.19.86.11 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 66.249.93.83 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 173.208.207.130 | United States | 147.237.72.166 | aka.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.193.250 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | forward | 1 |
| 46.19.85.226 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 188.120.154.231 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 63.141.250.157 | United States | 147.237.76.30 | himush.idf.il | block-sp-traf1 | forward | 1 |
| 79.180.91.7 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 192.187.118.68 | United States | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | forward | 1 |
| 94.102.52.10 | Netherlands | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 37.59.232.247 | France | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 176.13.19.34 | Israel | 147.237.72.167 | ishurim.aka.idf.il | DOSS-SSL-ClearText | drop | 1 |
| 80.246.133.121 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 46.19.86.90 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 198.204.247.221 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.198.14 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 66.249.93.85 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |

09-29-2016-14:04:05 to 09-29-2016-15:04:05

## Top Attackers In IPS

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

09-29-2016-14:04:05 to 09-29-2016-15:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 62.219.114.242 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 147.236.28.31 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.186 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 120.27.116.133 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.26.148.223 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.214.50 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.55.139.155 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.254.162.27 | 147.237.77.216 | Poland | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.255.81.225 | 147.237.0.15 | Moldova, Republic of | kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 213.151.39.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.70.6.79 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.29.203.226 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.140.205 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.129.160.229 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 77.124.38.16 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 163.172.129.15 | 147.237.0.17 | United Kingdom | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.244 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 141.0.13.162 | 147.237.77.216 | Norway | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.61 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 113.240.250.154 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.29.14.198 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.65.54.194 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.139.167.122 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.71.3.128 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.42.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.250.94.11 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.129.160.229 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 77.127.31.152 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 163.172.129.15 | 147.237.0.33 | United Kingdom | idf.il | ET SCAN NMAP -sS window 1024 | 1 |

09-29-2016-14:04:05 to 09-29-2016-15:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.53.177.127 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 48 |
| 46.19.85.128 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 32 |
| 223.24.115.101 | Thailand | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 37.26.149.233 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 27 |
| 107.167.116.74 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 24 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 141.0.13.162 | Norway | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 19 |
| 87.68.17.4 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 18 |
| 46.19.86.177 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 46.19.86.177 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 147.236.238.22 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 16 |
| 46.19.86.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 46.19.85.128 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 16 |
| 62.0.212.209 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 16 |
| 66.249.93.83 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.19.86.79 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 185.3.147.128 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.178 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 14 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 84.95.21.211 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 89.237.103.125 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 176.13.16.255 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.53.47.244 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.120.124.13 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.86.6 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.13.248.65 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.86.79 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 192.115.177.202 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 11 |
| 46.19.85.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 46.19.85.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 46.19.85.73 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 176.13.226.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 46.19.85.73 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 213.151.35.216 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 109.66.187.50 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 79.182.86.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 46.19.86.166 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 62.219.162.230 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.19.85.110 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 212.150.128.10 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.19.85.110 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 185.3.147.208 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 46.19.85.28 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 109.253.199.232 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.79 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.86.219 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 141.226.162.134 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 109.65.142.220 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 8 |

09-29-2016-14:04:05 to 09-29-2016-15:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.244.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 53 |
| 46.19.85.146 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 35 |
| 176.13.12.64 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 35 |
| 37.26.147.183 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 46.19.85.102 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 212.199.118.19 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 212.199.118.19 | Block | 5 |
| 46.19.85.14 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 77.126.18.29 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.126.18.29 | Block | 3 |
| 37.26.148.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.15.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.120.177.84 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx | Block | 2 |
| 176.13.246.58 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 2 |
| 176.13.226.47 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.53.32.110 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Untraceable SSL Sessions: Open Mode | None | 2 |
| 2.53.57.146 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 212.179.46.189 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal Byte Code Character in Query String [[#12]]jX¾œ˜lG ₧<·#Ↄ6 no «¿ | Block | 1 |
| 213.8.204.35 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 79.182.121.21 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.102.9.26 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/home/default.aspx | Block | 1 |
| 46.19.86.105 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Unknown HTTP Request Method Õu›ßß,°•®'÷Ž*Šd in URL | Block | 1 |
| 116.15.138.254 | Singapore | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 2.53.166.243 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.76.81 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp | Block | 1 |
| 54.210.93.172 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal Byte Code Character in URL [[#20]]( | Block | 1 |
| 213.8.204.35 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/xmlrpc.php | Block | 1 |
| 80.246.130.184 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 66.249.65.11 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx | Block | 1 |
| 176.13.248.65 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 46.19.86.166 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal Byte Code Character in Header Name [[#26]]Ð½ùrpâfÅ8[ç£µÕÕà | Block | 1 |
| 5.28.138.40 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 212.199.118.19 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/images/1.he/back.png | Block | 1 |
| 176.13.226.209 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/71772.pdf‍ | Block | 1 |
| 62.219.145.163 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/275-he/patzar.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal HTTP Version | Block | 1 |
| 2.53.32.110 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 217.194.197.80 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 81.218.251.252 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/960.css | Block | 1 |
| 66.249.65.63 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx | None | 1 |
| 183.129.160.229 | China | 147.237.77.234 | halag.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | NULL Character in Method | Block | 1 |
| 46.19.86.166 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method Dover.aspx in URL | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal Byte Code Character in Method Õu›ßß,°•®'÷Ž*Šd | Block | 1 |
| 213.8.204.16 | Israel | 147.237.76.42 | refuah.idf.il | PHP Attempt | Block | 1 |
| 77.139.252.131 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |

09-29-2016-14:04:05 to 09-29-2016-15:04:05