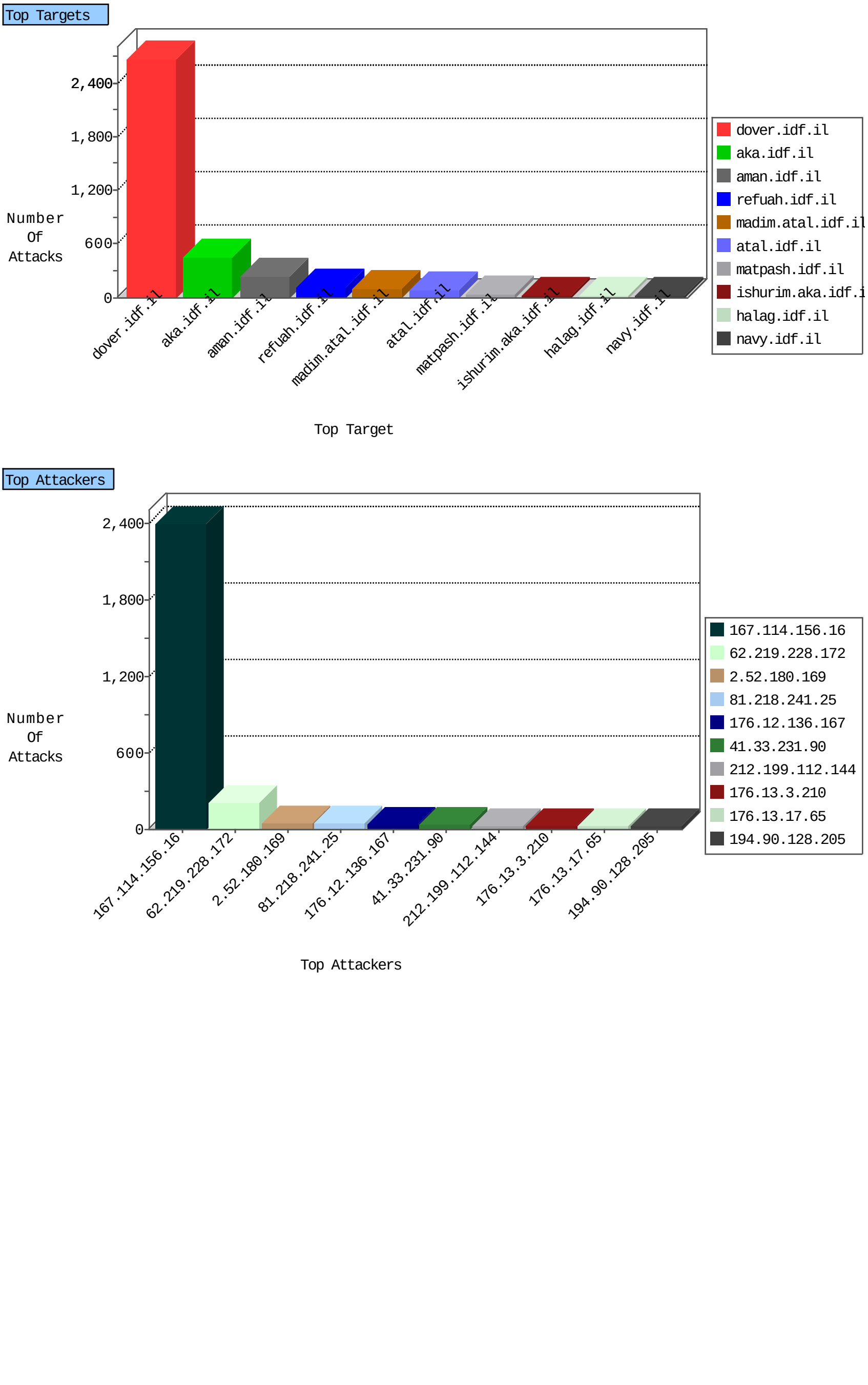
12-21-2015-12:04:03 to 12-21-2015-13:04:03

# IDF Under Attack Daily Report



12-21-2015-12:04:03 to 12-21-2015-13:04:03

## 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 | 3327 |
| 212.199.112.144 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 228 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 211 |
| 183.80.210.154 | Vietnam | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 183.80.210.154 | Vietnam | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.35.62.148 | Switzerland | 147.237.76.197 | e.himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.124.85.7 | | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

12-21-2015-12:04:03 to 12-21-2015-13:04:03

## Top Attackers In IPS

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

12-21-2015-12:04:03 to 12-21-2015-13:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 176.12.136.167 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 52.6.202.63 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.90 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.143.82.50 | 147.237.76.38 | Netherlands | e.e.meitav.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 217.132.61.30 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 31.168.51.114 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.227.7 | 147.237.76.176 | Ukraine | test.ncore.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 182.75.6.126 | 147.237.77.121 | India | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.95.102 | 147.237.0.33 | Netherlands | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 66.249.78.172 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 52.6.202.63 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.85.102 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.147.129 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.55.176.227 | 147.237.77.216 | Switzerland | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.114.185.100 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.1.201 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.245.127 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.69.209.221 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

12-21-2015-12:04:03 to 12-21-2015-13:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 72 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 60 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 48 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 194.90.128.205 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 27 |
| 176.12.136.167 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 27 |
| 15.90.166.12 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 26 |
| 199.203.173.198 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 26 |
| 66.249.64.250 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 213.57.143.220 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 20 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 19 |
| 62.0.197.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 176.12.136.167 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 13 |
| 80.246.130.160 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 12 |
| 46.19.85.247 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 46.19.85.102 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 147.236.232.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.52.180.169 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 2.52.180.169 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 2.52.180.169 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 2.52.180.169 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 62.0.200.198 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 2.52.180.169 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 81.218.0.133 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | | monitor | 8 |
| 2.52.149.167 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 212.235.105.53 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.52.148.46 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.52.1.125 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 2.54.160.190 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.39.91 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 193.106.52.34 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.126.97.63 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.115 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.8 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 193.106.54.34 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 5.102.254.221 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.176.50.57 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 46.19.85.115 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.182.99.117 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.142.90 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.127 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.144 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.26.146.208 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.15 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.178 | 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 |

12-21-2015-12:04:03 to 12-21-2015-13:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.17.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 176.13.3.210 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 22 |
| 80.246.136.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 19 |
| 185.32.179.137 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 176.13.0.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 212.90.148.93 | Germany | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 212.90.148.93 | Block | 3 |
| 176.13.13.89 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.221.211 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 109.253.221.211 | None | 3 |
| 176.13.3.32 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.190.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 217.194.207.105 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 192.114.1.131 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 80.246.139.205 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.86.132 | Israel | 147.237.77.234 | halag.idf.il | Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.19.86.132 | Block | 1 |
| 132.64.160.186 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 79.170.40.167 | United Kingdom | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/ | Block | 1 |
| 210.157.22.25 | Japan | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/wp-admin/ | Block | 1 |
| 41.189.47.10 | Cote D'Ivoire | 147.237.77.216 | dover.idf.il | eMail Hoarding | Block | 1 |
| 106.51.232.203 | India | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 195.221.21.235 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/style/shared/data:image/gif | Block | 1 |
| 46.19.86.204 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.13.20.155 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 82.213.13.62 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx | Block | 1 |
| 46.19.86.19 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 157.55.39.221 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 80.246.136.148 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.172 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 207.241.226.230 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/style/shared/data:image/gif | Block | 1 |
| 37.26.149.178 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 109.67.48.102 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 87.68.23.143 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 194.90.128.205 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il./homas | Block | 1 |
| 2.54.131.177 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 81.218.101.2 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.19.86.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.15 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 138.134.192.10 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/milnet | Block | 1 |
| 79.176.50.57 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 5.175.13.138 | Germany | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/aman | Block | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.66.150 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined | Block | 1 |
| 199.203.173.198 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/text.css | Block | 1 |
| 46.19.86.213 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.228.45.161 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.52.0.6 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 84.94.60.75 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.94.60.75 | Block | 1 |
| 46.19.86.97 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |

12-21-2015-12:04:03 to 12-21-2015-13:04:03