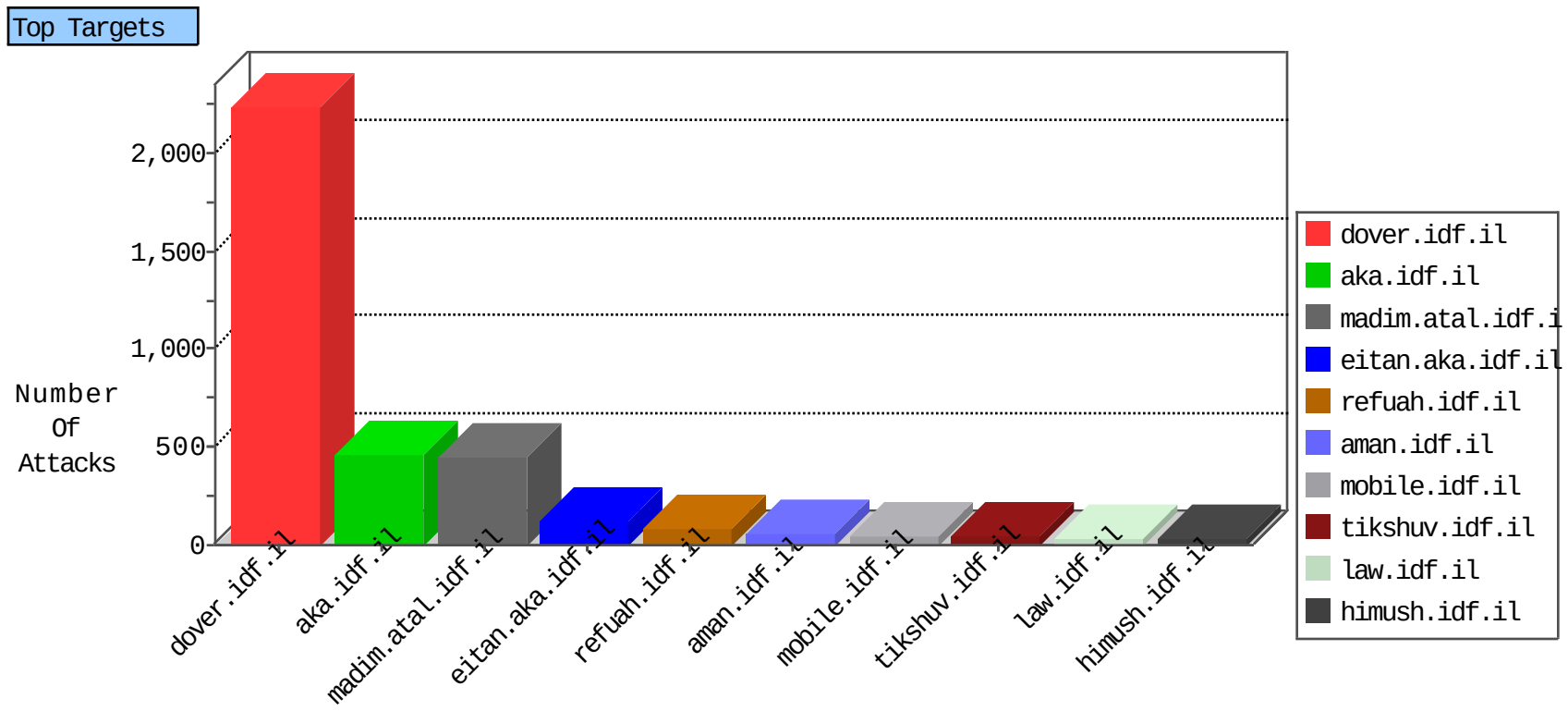
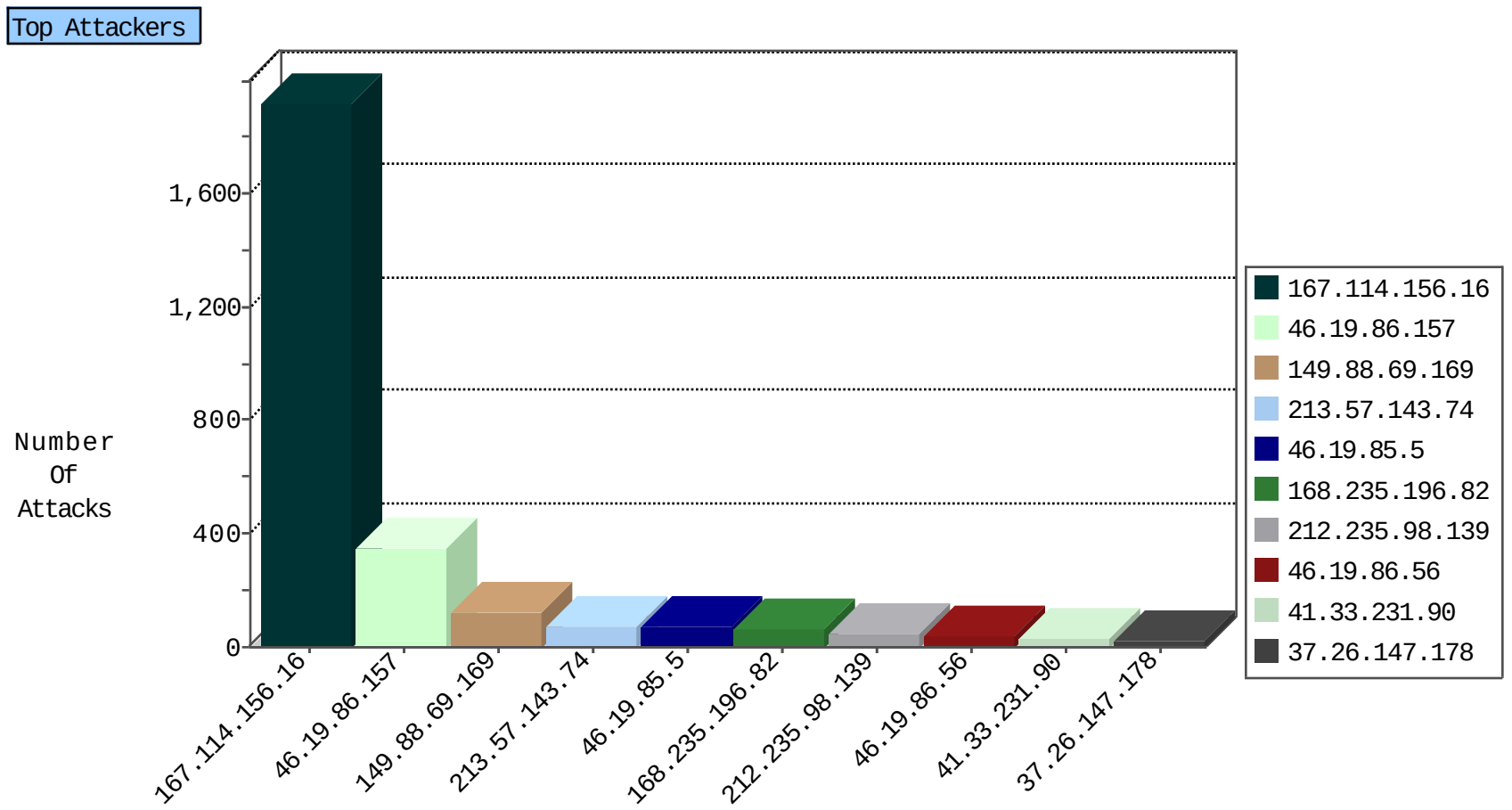
12-15-2015-17:04:07 to 12-15-2015-18:04:07

# IDF Under Attack Daily Report

Top Targets




Top Attackers



12-15-2015-17:04:07 to 12-15-2015-18:04:07

## 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 | 3250 |
| 82.80.157.174 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 3 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 168.235.196.82 | United States | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Http | drop | 1 |
| 168.235.196.82 | United States | 147.237.77.216 | dover.idf.il | JLM_Dover_Con_Limit_Https | drop | 1 |

12-15-2015-17:04:07 to 12-15-2015-18:04:07

## Top Attackers In IPS

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

12-15-2015-17:04:07 to 12-15-2015-18:04:07

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 | 4 |
| 59.46.193.114 | 147.237.77.227 | China | e.hamaz.idf.il | GPL SCAN nmap TCP | 2 |
| 107.167.184.195 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.39.222.253 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 107.167.184.195 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 95.86.106.134 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.235.98.139 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.81.31.15 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.178.215.172 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.120.126.24 | 147.237.77.216 |  | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.182.174.235 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 120.150.29.211 | 147.237.72.156 | Australia | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 107.167.184.195 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.26.148.131 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 107.167.184.195 | 147.237.77.234 | United States | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 14.150.77.119 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 107.167.184.195 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.29.76.74 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.219.238.10 | 147.237.77.170 |  | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.24.171.223 | 147.237.77.227 | China | e.hamaz.idf.il | GPL SCAN nmap TCP | 1 |
| 85.65.61.152 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 196.47.173.21 | 147.237.77.121 | Cote D'Ivoire | e.navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 80.246.136.44 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.227.7 | 147.237.77.243 | Ukraine | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.70.230 | 147.237.8.50 | Netherlands | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.106.94.66 | 147.237.0.33 |  | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 79.179.52.122 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 108.30.83.8 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.85.98 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 107.167.184.195 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.26.146.231 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

12-15-2015-17:04:07 to 12-15-2015-18:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.196.82 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 58 |
| 212.235.98.139 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 48 |
| 46.19.86.56 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 36 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 213.57.143.74 | Israel | 147.237.0.34 | tikshuv.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 27 |
| 109.67.115.55 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 82.145.219.176 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 19 |
| 149.78.136.33 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 19 |
| 37.26.147.178 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 213.57.143.74 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 213.57.143.74 | Israel | 147.237.0.34 | tikshuv.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 13 |
| 176.13.3.1 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.228.187.129 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 176.13.17.83 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 176.13.17.83 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 10 |
| 41.250.227.224 | Morocco | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 213.57.143.74 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 79.177.104.209 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 80.246.139.182 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 109.64.234.242 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 185.32.179.21 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.68 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 213.57.143.74 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |
| 176.13.23.13 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 109.64.186.23 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 176.13.23.13 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 79.181.7.133 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.68 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.178.25.28 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 93.173.254.79 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 66.220.159.116 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 79.183.119.106 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.209.88 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.178.49.43 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.67.104.38 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.22.129.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.176.170.98 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 190.242.47.19 | Colombia | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 66.220.159.119 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 213.8.118.14 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 37.26.148.131 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 185.3.144.95 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 94.230.86.244 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 109.65.138.63 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 93.172.33.8 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 2.54.2.72 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 37.26.148.131 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 5 |
| 37.26.148.131 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 91.200.12.106 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |

12-15-2015-17:04:07 to 12-15-2015-18:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.157 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 184 |
| 46.19.86.157 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 162 |
| 149.88.69.169 | Israel | 147.237.76.200 | eitan.aka.idf.il | Too Many of the Same Response Code (404) in Session from 149.88.69.169 | Block | 122 |
| 46.19.85.5 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 69 |
| 212.25.102.57 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 212.25.102.57 | Block | 14 |
| 2.52.55.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 176.13.13.6 | Israel | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 46.120.255.68 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 9 |
| 41.250.227.224 | Morocco | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 79.180.237.184 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 79.180.237.184 | Block | 7 |
| 80.246.139.242 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 6 |
| 37.26.147.178 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 208.115.111.74 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.136.200 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 66.249.66.77 | Israel | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.12.141.174 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.120.166.24 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 208.115.113.93 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 31.44.128.156 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 2 |
| 212.227.29.47 | Germany | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 212.227.29.47 | Block | 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 |
| 80.246.139.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 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 |
| 207.46.13.104 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 149.88.237.68 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 84.109.192.130 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 157.55.39.3 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.139.214 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.65.174.162 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.102 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 62.219.226.71 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx | Block | 1 |
| 185.32.179.186 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 85.250.119.60 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 79.183.217.81 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |
| 46.19.86.64 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 157.55.39.43 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/index.php/hairloss/site_css | Block | 1 |
| 79.177.154.45 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.49.226.232 | Netherlands | 147.237.77.216 | dover.idf.il | eMail Hoarding | Block | 1 |
| 2.54.130.84 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | 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 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/valtam | 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 |
| 46.120.167.202 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.68 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 79.181.128.195 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 213.151.37.219 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 1 |
| 109.67.115.55 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 101 cookies | Block | 1 |
| 66.249.64.218 | Israel | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 188.106.104.39 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |

12-15-2015-17:04:07 to 12-15-2015-18:04:07