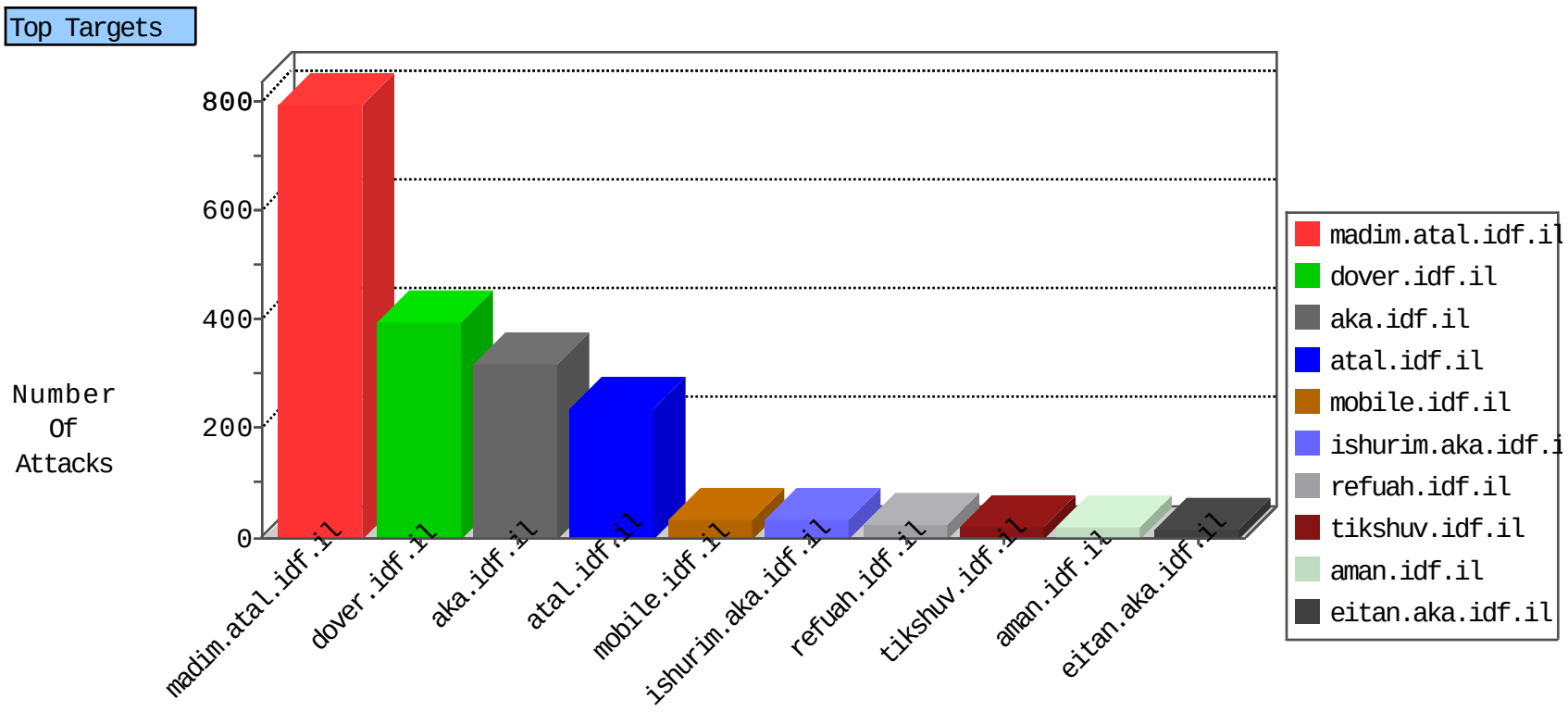
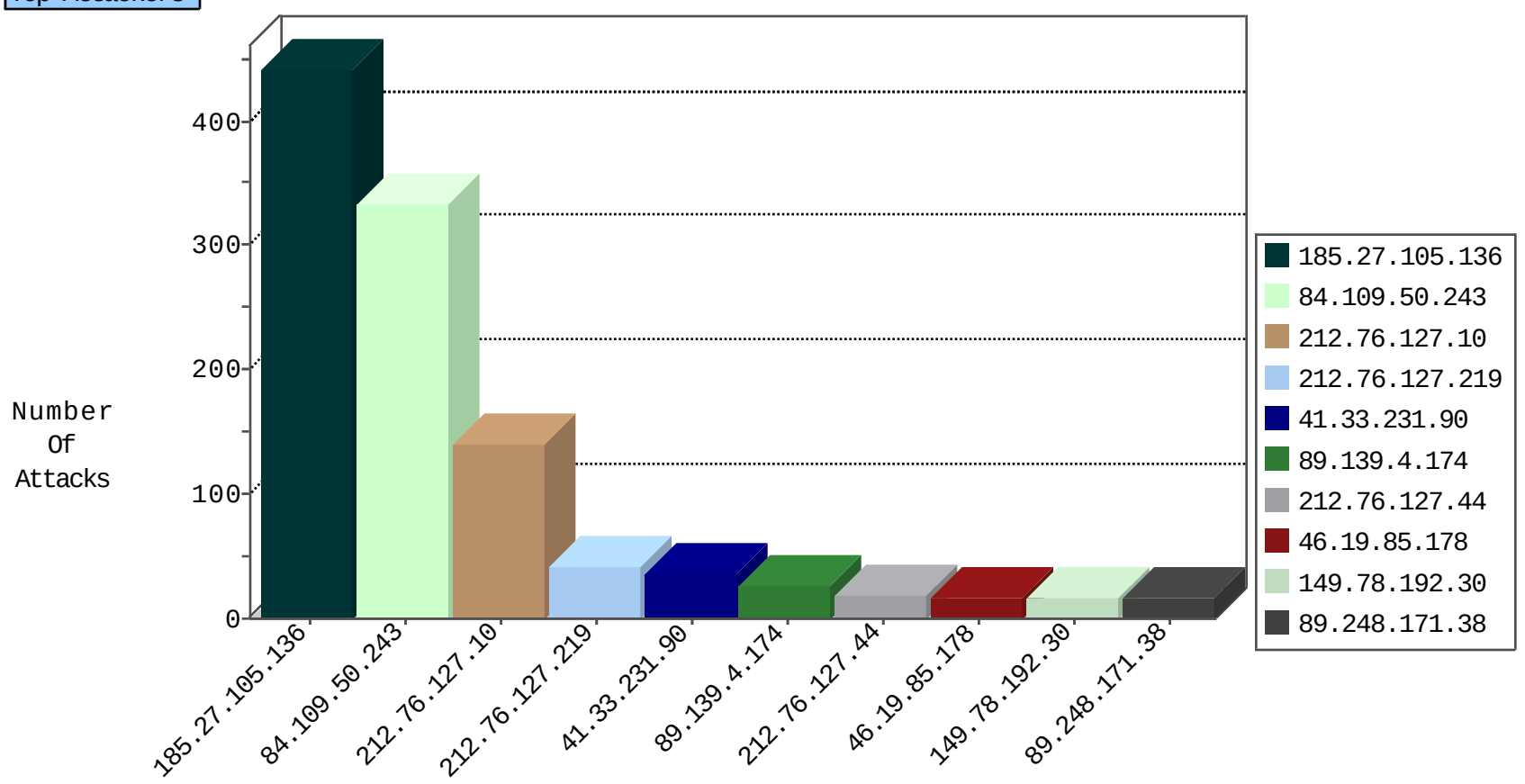
02-21-2016-22:04:03 to 02-21-2016-23:04:03

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-21-2016-22:04:03 to 02-21-2016-23:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.142.84 | Israel | 147.237.0.34 | tikshuv.idf.il | Block_Udp_All_Nets | drop | 3 |
| 79.180.142.84 | Israel | 147.237.77.170 | maarachot.idf.il | Block_Udp_All_Nets | drop | 3 |
| 146.185.239.100 | Russian Federation | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | drop | 1 |
| 151.67.188.141 | Italy | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 104.238.129.180 | | 147.237.76.34 | yohalan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 151.67.188.141 | Italy | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 104.245.97.224 | | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |

02-21-2016-22:04:03 to 02-21-2016-23:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.109.68.240 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 79.180.217.32 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 7 |
| 106.120.173.109 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 149.202.48.240 | Germany | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 79.183.63.205 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 149.202.48.240 | Germany | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 149.202.48.240 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 144.76.12.78 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 212.235.40.29 | Israel | 147.237.77.216 | dover.idf.il | C1000008: HTTP: Xenu UserAgent | Block | 1 |
| 188.165.15.205 | France | 147.237.76.31 | nakchal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

02-21-2016-22:04:03 to 02-21-2016-23:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 95.86.121.217 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 5 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.93.128 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 74.201.85.87 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 74.201.85.87 | 147.237.8.27 | United States | e.madim.atal.idf.i | ET SCAN Potential SSH Scan | 1 |
| 46.116.204.153 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 177.226.155.227 | 147.237.76.31 | Mexico | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 110.34.192.186 | 147.237.0.33 | Thailand | idf.il | ET SCAN Potential SSH Scan | 1 |
| 82.117.208.243 | 147.237.72.14 | | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 74.201.85.87 | 147.237.8.28 | United States | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 74.201.85.87 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.121.141.166 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.65 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.83.170.26 | 147.237.0.33 | France | idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.241.53.120 | 147.237.0.34 | Mexico | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 110.34.192.186 | 147.237.0.35 | Thailand | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |

02-21-2016-22:04:03 to 02-21-2016-23:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.76.127.10 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 141 |
| 212.76.127.219 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 42 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 212.76.127.44 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 18 |
| 89.248.171.38 | Netherlands | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 149.78.192.30 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |
| 176.13.18.165 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.19.85.178 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 46.19.85.4 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 46.19.85.209 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 212.76.127.111 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 79.179.10.245 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.149 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.159 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 94.159.178.232 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 89.138.66.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 89.139.4.174 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 8 |
| 46.19.85.230 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 79.181.153.244 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 37.26.146.156 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.15 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.178.25.94 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 84.228.0.241 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.28.189.84 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.159.117 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.139 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.15 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.197 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.55 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.178 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.139 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 31.168.29.65 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.230 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.57 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.4 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.149 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.54.147.129 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.128.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.209 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.223 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 89.139.4.174 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.85.157 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 2.54.142.214 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 188.120.148.97 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 89.139.4.174 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 46.19.85.53 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 89.139.4.174 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.142.192.250 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |

02-21-2016-22:04:03 to 02-21-2016-23:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.27.105.136 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 185.27.105.136 | Block | 308 |
| 84.109.50.243 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 203 |
| 185.27.105.136 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 133 |
| 84.109.50.243 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 131 |
| 109.253.192.56 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 37.26.148.156 | Israel | 147.237.76.39 | mobile.meitav.idf.il | Cookie Tampering on cookie .ASPNETAUTH: Expected 01027A767513003BD308FE7AEEB6DE023BD308000932003000390037003700360033003000310000012F00FF, Observed 01020689D90E003BD308FE06011BDA023BD308000932003000390037003700360033003000310000012F00FF | None | 10 |
| 87.69.245.27 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 87.69.245.27 | Block | 6 |
| 87.69.245.27 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/mainsachar | Block | 6 |
| 79.181.147.97 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/giyus | Block | 6 |
| 85.64.154.3 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 95.172.233.91 | United Kingdom | 147.237.77.233 | atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 167.114.64.100 | Canada | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/. | Block | 4 |
| 37.236.188.24 | Iraq | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ar/adminitem.asp | Block | 4 |
| 5.29.40.123 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 5.29.40.123 | Block | 4 |
| 37.236.188.24 | Iraq | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 37.236.188.24 | Block | 4 |
| 89.139.4.174 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 176.13.6.43 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$87 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 3 |
| 85.65.71.200 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 3 |
| 217.132.64.140 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 3 |
| 46.210.168.45 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.94.40.115 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 2 |
| 109.93.13.139 | | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 2 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 2 |
| 68.180.228.175 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8903-he/refuah.aspx | Block | 2 |
| 109.66.144.9 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 2 |
| 5.28.186.130 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 2 |
| 80.246.136.169 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 2 |
| 2.54.15.31 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 2 |
| 84.94.40.115 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 84.94.40.115 | Block | 2 |
| 109.93.13.139 | | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 2 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 2 |
| 141.212.122.129 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to /x | Block | 2 |
| 37.26.148.156 | Israel | 147.237.76.39 | mobile.meitav.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 5.29.40.123 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 2 |
| 188.120.130.73 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 2 |
| 95.86.121.217 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx | Block | 2 |
| 157.55.39.55 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 2 |
| 84.94.40.115 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php | Block | 2 |
| 213.8.204.11 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 2 |
| 80.178.148.158 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 2 |
| 46.19.85.115 | Israel | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 2 |
| 79.181.8.103 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 2 |
| 77.126.15.216 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx | Block | 2 |
| 141.212.122.129 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to /x | Block | 2 |
| 37.236.188.24 | Iraq | 147.237.77.216 | dover.idf.il | Admin Blocking | Block | 2 |
| 188.120.130.73 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 188.120.130.73 | Block | 2 |
| 79.181.210.109 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 2 |
| 176.13.11.52 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 40.77.167.50 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 2 |

02-21-2016-22:04:03 to 02-21-2016-23:04:03