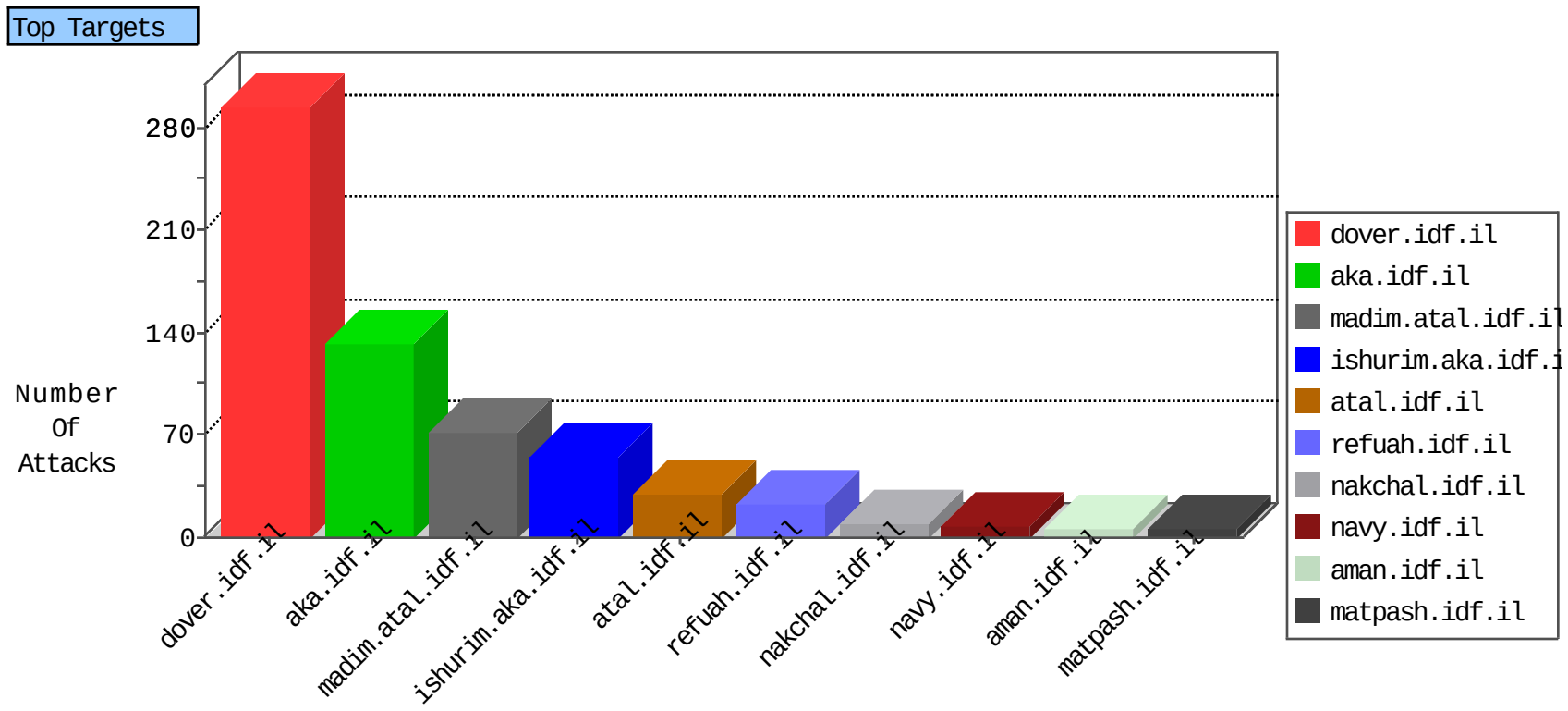
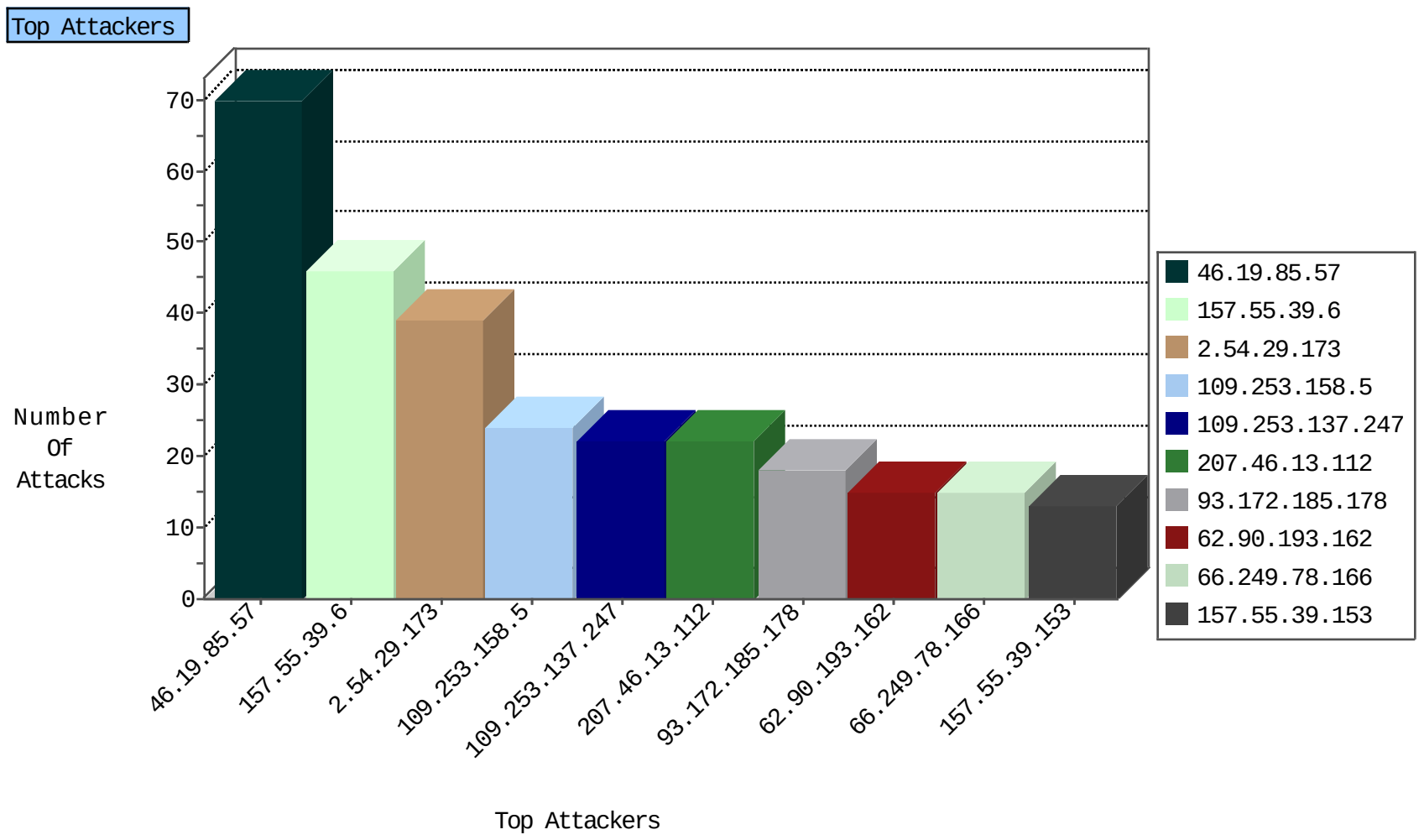
03-29-2015-13:03:00 to 03-29-2015-14:03:00

# IDF Under Attack
# 03-29-2015-13:03:00

Top Targets




Top Attackers



03-29-2015-13:03:00 to 03-29-2015-14:03:00

## Top Attackers In DDoS-Defence

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

03-29-2015-13:03:00 to 03-29-2015-14:03:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.64.81.84 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 80.70.130.5 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 93.120.27.62 | Romania | 147.237.0.35 | akaws.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 46.19.85.209 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 93.172.32.122 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 79.179.100.125 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 178.217.187.39 | Poland | 147.237.76.86 | navy.idf.il | DVRep_B-N_60_100 | Block | 1 |

03-29-2015-13:03:00 to 03-29-2015-14:03:00

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 5 |
| 59.106.108.116 | Japan | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 84.110.2.232 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.240.144.65 | China | 147.237.76.34 | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 176.12.160.2 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 58.20.54.249 | China | 147.237.0.200 | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.253.149.170 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 95.86.68.14 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 1 |
| 2.52.10.40 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.250.137.164 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.64.177.241 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 1 |
| 83.130.118.146 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.143.79 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.160.224.130 | China | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 192.117.100.81 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 58.20.54.249 | China | 147.237.8.46 | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 114.255.149.210 | China | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.201 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.57.79 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 36.72.228.72 | Indonesia | 147.237.77.178 | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.250.190.229 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.65.34.103 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

03-29-2015-13:03:00 to 03-29-2015-14:03:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 44 |
| 109.253.158.5 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 109.253.137.247 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 22 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 20 |
| 93.172.185.178 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 14 |
| 2.54.29.173 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | monitor | 13 |
| 2.54.29.173 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid sequence number | Bad TCP sequence | monitor | 13 |
| 2.54.29.173 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | alert | 13 |
| 157.55.39.153 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 109.253.130.151 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 109.253.141.74 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 81.168.55.171 | United Kingdom | 147.237.77.216 | dover.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 11 |
| 85.250.145.38 | Israel | 147.237.77.233 | atal.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 11 |
| 109.253.129.226 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 10 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 10 |
| 62.90.193.162 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid sequence number | Bad TCP sequence | monitor | 8 |
| 176.12.142.187 | Israel | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 8 |
| 62.90.193.162 | Israel | 147.237.72.166 | aka.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 7 |
| 109.253.158.158 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 46.19.85.14 | Israel | 147.237.76.42 | refuah.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 5 |
| 193.106.206.10 | Israel | 147.237.77.233 | atal.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 46.19.86.59 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 196.217.160.53 | Morocco | 147.237.76.42 | refuah.idf.il | | drop | drop | 4 |
| 46.19.85.14 | Israel | 147.237.76.42 | refuah.idf.il | Invalid ACK number | Bad TCP sequence | alert | 4 |
| 212.199.251.227 | Israel | 147.237.76.31 | nakchal.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 62.219.161.123 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 176.12.147.42 | Israel | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 4 |
| 149.78.200.61 | United States | 147.237.77.233 | atal.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 4 |
| 193.106.206.10 | Israel | 147.237.77.233 | atal.idf.il | Invalid ACK number | Bad TCP sequence | alert | 4 |
| 37.46.39.154 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 3 |
| 146.185.56.190 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | alert | 3 |
| 146.185.56.190 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 3 |
| 84.95.193.106 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN retransmit with different window scale | Bad TCP sequence | monitor | 3 |
| 213.8.38.42 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3 |
| 79.180.142.182 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 2 |
| 46.19.86.192 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | alert | 2 |
| 2.187.253.17 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 65.55.210.15 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 212.199.99.30 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 46.19.86.192 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 66.249.75.74 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 61.135.190.71 | China | 147.237.0.200 | m4u.idf.il | Geo-location inbound enforcement | Geo-location enforcement | drop | 2 |
| 199.30.16.182 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 212.199.251.235 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 46.19.86.248 | Israel | 147.237.76.42 | refuah.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 2.187.253.17 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 2 |
| 64.246.165.50 | United States | 147.237.77.216 | dover.idf.il | header rejection pattern found in request | Header Rejection | monitor | 2 |
| 81.218.178.50 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 2 |
| 178.214.65.127 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 2 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.57 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 70 |
| 46.121.198.182 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 87.69.173.109 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.196 | Block | 4 |
| 37.26.146.247 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 213.8.71.146 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 3 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 3 |
| 79.180.142.113 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 207.46.13.112 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.112 | Block | 2 |
| 157.55.39.42 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 157.55.39.42 | Block | 2 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 2 |
| 176.12.142.187 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 77.125.5.20 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il//894-en/idfgdover.aspx | Block | 2 |
| 212.199.69.213 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 2 |
| 37.142.157.2 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 37.142.157.2 | Block | 2 |
| 46.116.184.122 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/ | Block | 1 |
| 207.46.13.16 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.16 | Block | 1 |
| 109.253.144.97 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 5.29.118.48 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 1 |
| 180.76.5.153 | China | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/1058-en/cogat.aspx | Block | 1 |
| 87.68.228.80 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx | None | 1 |
| 176.12.139.56 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 62.219.24.52 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx | None | 1 |
| 213.8.100.81 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx | None | 1 |
| 149.78.5.84 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 109.253.136.255 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 37.142.157.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/kapatz/accepted.aspxhttp:/www.aka.idf.il/main/kapatz/default.asp | Block | 1 |
| 192.116.50.122 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/ | Block | 1 |
| 176.12.145.80 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 85.64.121.146 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/101503-5.stm | Block | 1 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 1 |
| 109.253.147.3 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 27.159.249.10 | China | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/901-11564-en/shared/usercontrols/headerupper/ | Block | 1 |
| 188.138.17.205 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 87.68.228.80 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$paySlipsSignAll in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 79.183.32.157 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-he | Block | 1 |
| 176.12.140.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 149.78.58.217 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 62.219.236.52 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 109.253.137.190 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 194.90.15.61 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |
| 2.54.165.208 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx | Block | 1 |
| 176.12.147.42 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 85.64.125.248 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 54.90.239.205 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arafat/terrorism2/english/main_index.stm | Block | 1 |
| 212.179.217.217 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 132.72.172.138 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx | None | 1 |
| 188.165.15.176 | France | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9785-he/refuah.aspx | Block | 1 |
| 80.246.130.19 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

03-29-2015-13:03:00 to 03-29-2015-14:03:00