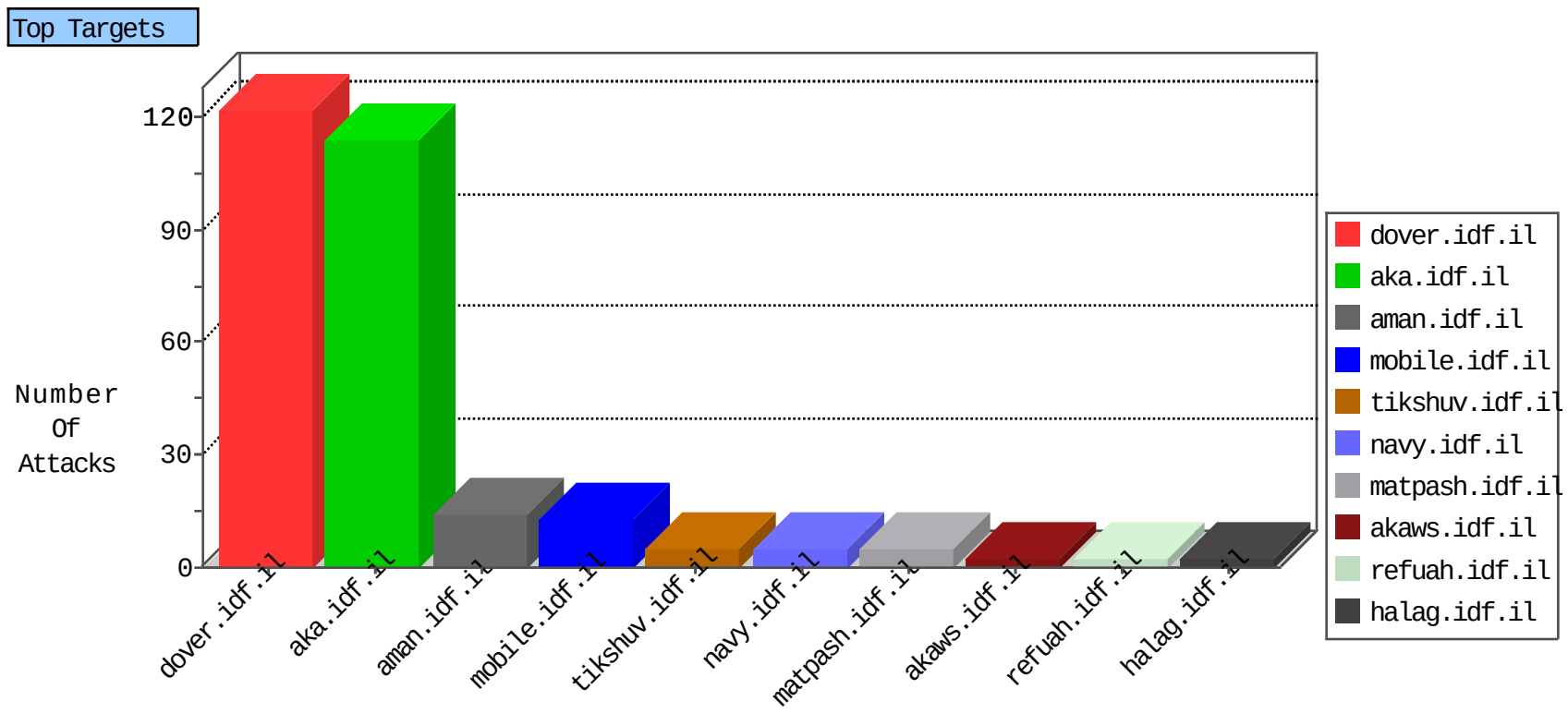
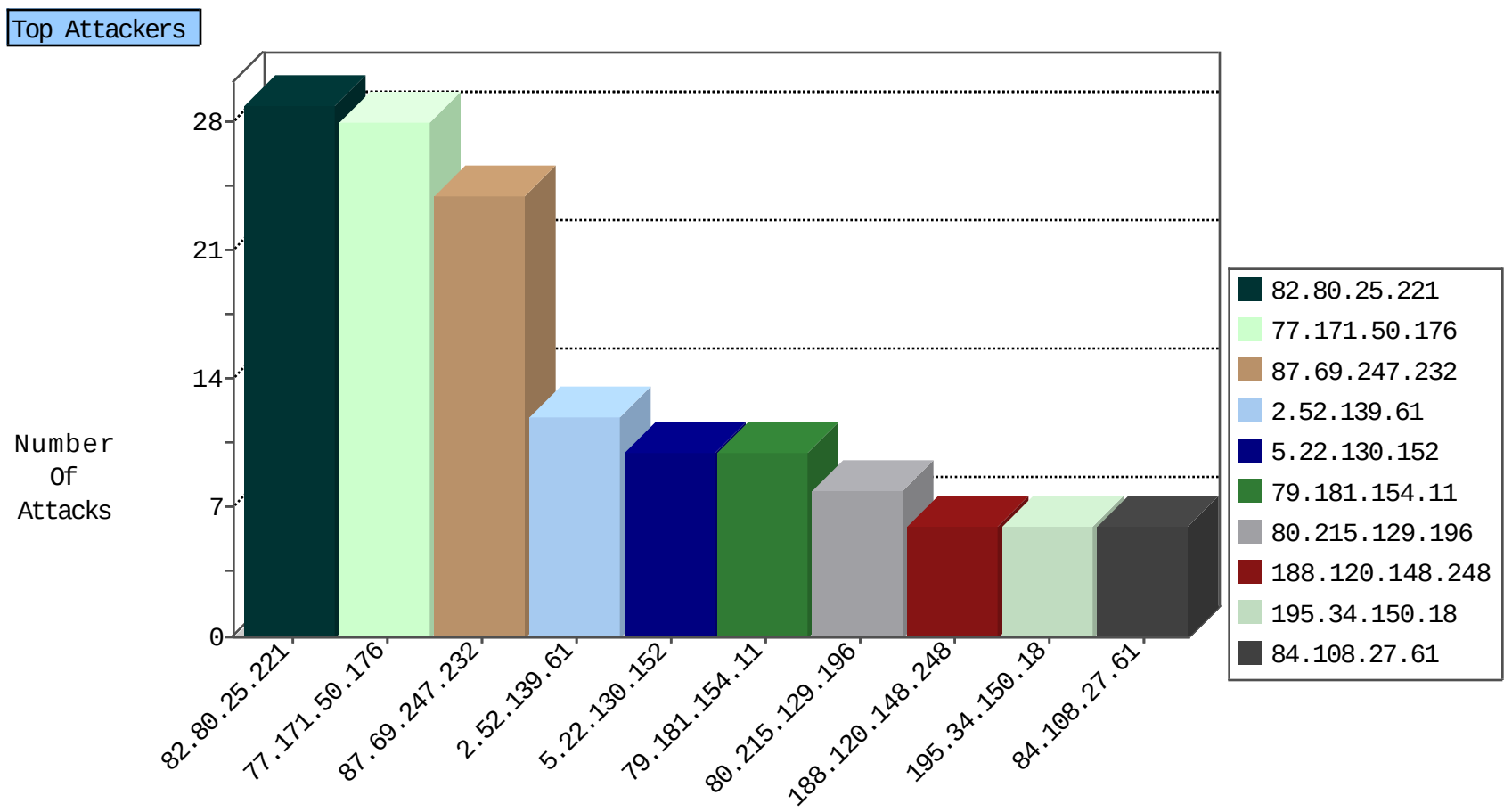
03-27-2015-16:03:02 to 03-27-2015-17:03:02

# IDF Under Attack
# 03-27-2015-16:03:02

Top Targets




Top Attackers



03-27-2015-16:03:02 to 03-27-2015-17:03:02

## Top Attackers In DDoS-Defence

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

03-27-2015-16:03:02 to 03-27-2015-17:03:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.111.60.184 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 192.116.162.182 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 46.19.85.106 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 84.228.222.104 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 46.19.85.123 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 85.25.43.94 | Germany | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 77.127.132.2 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 85.25.43.94 | Germany | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 79.180.37.233 | Israel | 147.237.72.156 | aman.idf.il | 3643: HTTP: Nikto HTTP Request | Block | 1 |
| 85.250.189.52 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |

03-27-2015-16:03:02 to 03-27-2015-17:03:02

## 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 | 29 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 6 |
| 192.116.162.182 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 194.114.146.227 | Israel | 147.237.77.216 | dover.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 3 |
| 183.136.216.7 | China | 147.237.76.34 | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.74.17.72 | India | 147.237.8.45 | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 131.221.105.25 | | 147.237.0.35 | akaws.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 61.240.144.65 | China | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.101.38.165 | Russian Federation | 147.237.8.14 | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.196.147.122 | Germany | 147.237.76.201 | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 198.20.69.74 | United States | 147.237.76.176 | test.ncore.idf.i | ET DROP Dshield Block Listed Source | 1 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 182.74.17.72 | India | 147.237.8.45 | e.eitan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 131.221.105.25 | | 147.237.0.35 | akaws.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 60.162.63.176 | China | 147.237.0.33 | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |

03-27-2015-16:03:02 to 03-27-2015-17:03:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 77.171.50.176 | Netherlands | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 87.69.247.232 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 24 |
| 5.22.130.152 | Israel | 147.237.72.156 | aman.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 7 |
| 188.120.148.248 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 6 |
| 80.215.129.196 | France | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 79.181.154.11 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5 |
| 83.244.143.62 | United Kingdom | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5 |
| 79.181.154.11 | Israel | 147.237.77.243 | mobile.idf.il | First packet isn't SYN | drop | drop | 5 |
| 2.52.139.61 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | alert | 4 |
| 2.52.139.61 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 31.210.186.129 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 2.52.139.61 | Israel | 147.237.72.166 | aka.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 4 |
| 176.12.142.52 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 4 |
| 89.139.21.94 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 3 |
| 5.22.130.152 | Israel | 147.237.72.156 | aman.idf.il | First packet isn't SYN | drop | drop | 3 |
| 80.246.139.78 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | alert | 2 |
| 46.19.86.92 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 80.246.139.78 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 85.250.116.191 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 2 |
| 80.246.139.78 | Israel | 147.237.72.166 | aka.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 2 |
| 188.165.15.22 | France | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 2 |
| 73.44.233.147 | United States | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 2 |
| 73.44.233.147 | United States | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 46.19.86.38 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 188.120.148.168 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 85.130.233.224 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 79.182.126.52 | Israel | 147.237.72.166 | aka.idf.il | Invalid checksum. Packet dropped. | Streaming Engine: TCP Invalid Checksum | drop | 1 |
| 222.186.21.112 | China | 147.237.76.147 | chinuch.aka.idf.il | | drop | drop | 1 |
| 109.253.136.131 | Israel | 147.237.77.243 | mobile.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 79.180.218.182 | Israel | 147.237.77.170 | maarachot.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 8.37.227.70 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Response out of state | Block HTTP Non Compliant | monitor | 1 |
| 66.249.84.137 | United States | 147.237.77.176 | matpash.idf.il | directory traversal overflow | Directory Traversal | monitor | 1 |
| 142.158.254.202 | Canada | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 80.215.129.196 | France | 147.237.77.216 | dover.idf.il | Invalid sequence number | Bad TCP sequence | alert | 1 |
| 31.210.186.237 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 203.90.244.62 | Hong Kong | 147.237.0.200 | m4u.idf.il | Geo-location inbound enforcement | Geo-location enforcement | drop | 1 |
| 80.215.129.196 | France | 147.237.77.216 | dover.idf.il | Invalid sequence number | Bad TCP sequence | monitor | 1 |
| 188.120.148.168 | Israel | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 1 |
| 85.64.21.235 | Israel | 147.237.76.42 | refuah.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 79.181.199.9 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 1 |
| 212.179.102.163 | Israel | 147.237.72.156 | aman.idf.il | First packet isn't SYN | drop | drop | 1 |
| 109.253.136.131 | Israel | 147.237.77.243 | mobile.idf.il | Invalid ACK number | Bad TCP sequence | alert | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 217.132.111.156 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd | Block | 5 |
| 84.108.27.61 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/gigus | Block | 4 |
| 79.176.215.11 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 213.251.182.10 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 3 |
| 17.142.151.205 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 17.142.151.205 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.142.151.205 | Block | 2 |
| 84.108.27.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | 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 |
| 207.46.13.114 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 2 |
| 149.78.5.229 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 5.29.109.152 | 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 | 2 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/poland/poland.stm | Block | 1 |
| 66.249.73.244 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar | Block | 1 |
| 46.116.174.201 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 87.69.132.88 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 1 |
| 84.108.6.244 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 68.180.228.117 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/1216-2.stm | Block | 1 |
| 207.46.13.30 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/captcha.ashx | Block | 1 |
| 54.159.134.239 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 109.64.80.5 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 84.111.190.194 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 37.26.148.228 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 1 |
| 2.54.191.153 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 79.177.138.173 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 1 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.79.66 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.116.206.201 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/viewpniot.aspx | None | 1 |
| 89.138.245.21 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 17.142.151.205 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arafat/terrorism2/english/main_index.stm | Block | 1 |
| 109.67.111.38 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/resource/userfollowresource/create/ | Block | 1 |
| 54.161.155.142 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/announcements/2002/january/11.stm and january/11.stm | Block | 1 |
| 84.228.170.172 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails | Block | 1 |
| 37.26.148.228 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/default.aspx | None | 1 |
| 5.29.44.253 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |
| 79.182.116.164 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 188.165.15.181 | France | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx | Block | 1 |
| 66.249.79.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.117.7.235 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 92.36.150.187 | Bosnia and Herzegovina | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 31.168.68.51 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx | None | 1 |
| 79.176.112.87 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 212.150.183.161 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx | Block | 1 |
| 54.172.196.207 | United States | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 85.65.221.186 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 37.142.190.6 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 80.230.110.146 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails | Block | 1 |
| 188.165.15.196 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.196 | Block | 1 |
| 66.249.81.209 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/home/aspx | Block | 1 |
| 46.117.40.210 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 93.173.56.105 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |