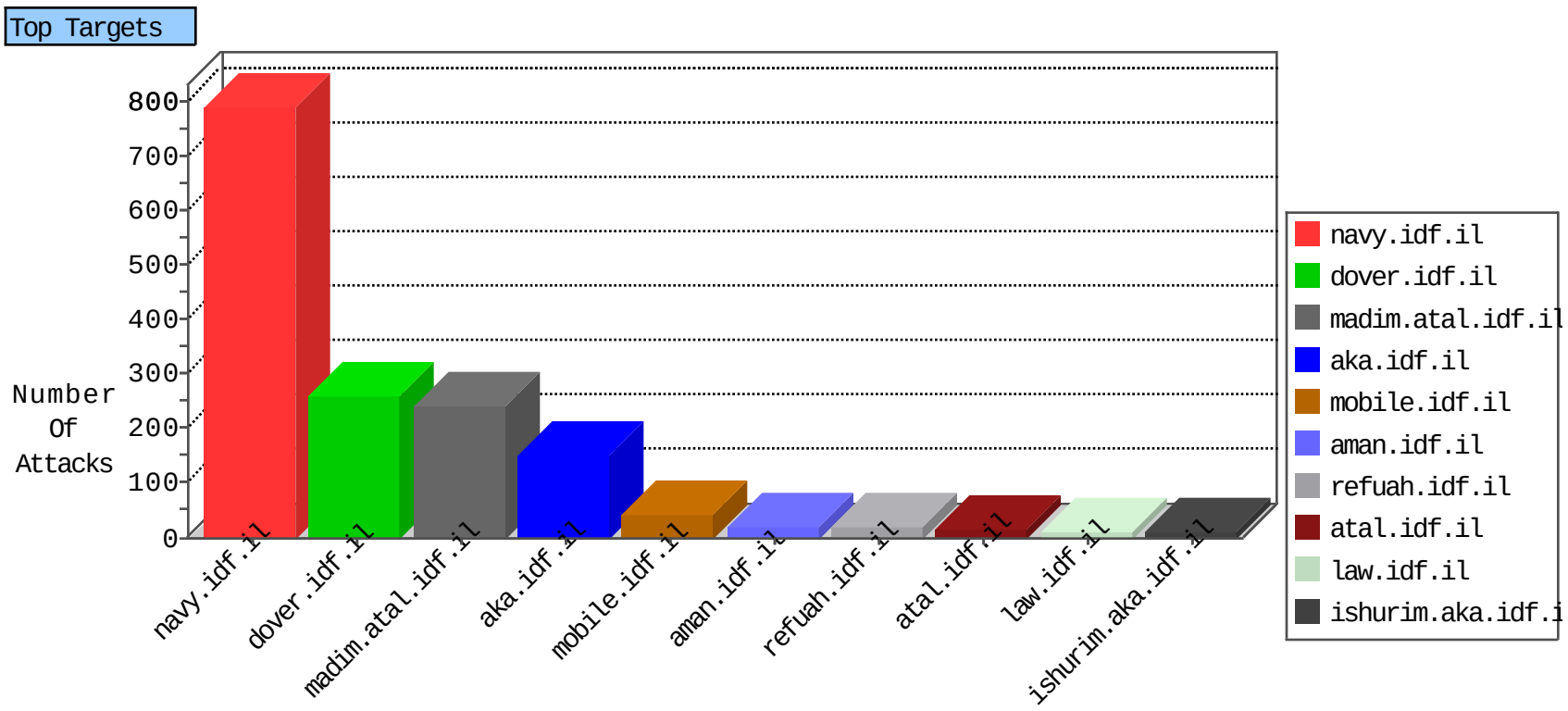
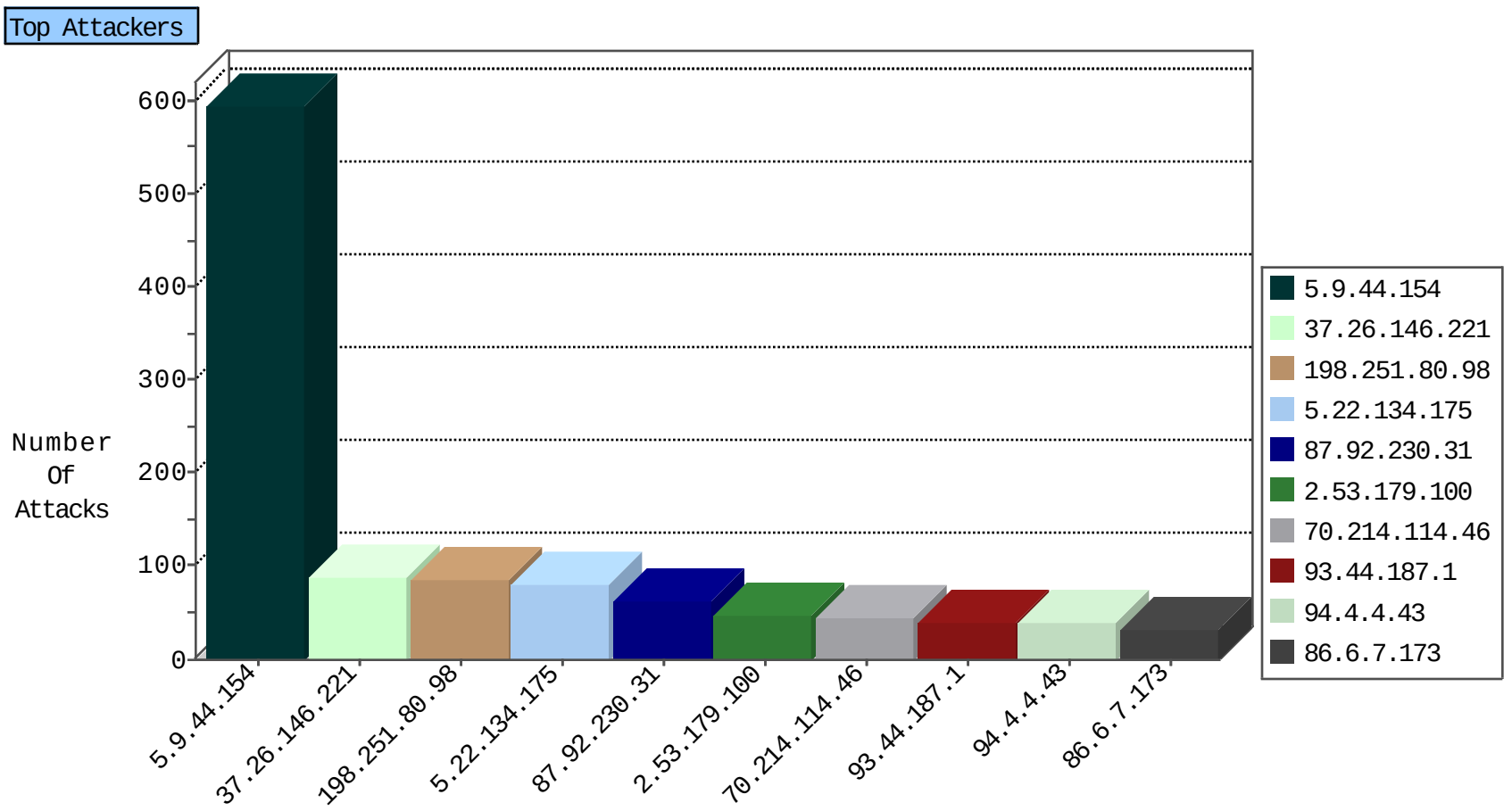
09-22-2016-19:04:09 to 09-22-2016-20:04:09

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



09-22-2016-19:04:09 to 09-22-2016-20:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.151.149.222 | China | 147.237.76.147 | chinuch.aka.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 185.94.111.1 | Russian Federation | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 71.6.146.185 | United States | 147.237.76.44 | e.refuah.idf.il | Black List | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |
| 183.60.48.25 | China | 147.237.76.39 | mobile.meitav.idf.il | JLM_Under_Attack_Con_Tcp | drop | 1 |

09-22-2016-19:04:09 to 09-22-2016-20:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.98 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.98 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 198.20.69.74 | United States | 147.237.77.61 | e.cogat.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

09-22-2016-19:04:09 to 09-22-2016-20:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.120.218.75 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 45.40.135.12 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 180.97.106.37 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 24.173.213.138 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.199 | United Kingdom | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 139.162.187.89 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 111.68.107.43 | 147.237.0.15 | Pakistan | kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 111.68.107.43 | 147.237.0.15 | Pakistan | kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 82.81.128.225 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 211.149.222.5 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 64.137.168.128 | 147.237.77.19 | Canada | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 45.40.135.12 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 180.97.106.161 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 42.112.238.213 | 147.237.0.16 | Vietnam | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 180.97.106.37 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 163.172.169.150 | 147.237.76.30 | United Kingdom | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.31.41.199 | 147.237.76.196 | Vietnam | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 111.68.107.43 | 147.237.0.15 | Pakistan | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.43.123.180 | 147.237.77.176 | Romania | matpash.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 212.76.123.207 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.240.213.93 | 147.237.77.205 | United States | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.36.35.241 | 147.237.8.27 | Russian Federation | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |

09-22-2016-19:04:09 to 09-22-2016-20:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 5.9.44.154 | Germany | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 590 |
| 87.92.230.31 | Finland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 93.44.187.1 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 40 |
| 94.4.4.43 | United Kingdom | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 39 |
| 86.6.7.173 | United Kingdom | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 32 |
| 77.126.58.14 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 70.214.114.46 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 23 |
| 198.251.80.98 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 21 |
| 198.251.80.98 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 20 |
| 70.214.114.46 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 198.251.80.98 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 84.94.119.108 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 198.251.80.98 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 198.251.80.98 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 13 |
| 2.53.179.100 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 37.26.149.191 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.53.179.100 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 2.53.179.100 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 12 |
| 2.53.179.100 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 12 |
| 46.19.85.10 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 2.53.58.33 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 2.53.131.222 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 79.178.254.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.10 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 93.172.148.82 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 84.109.75.25 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 201.200.0.140 | Costa Rica | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 6 |
| 46.19.85.10 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.10 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 70.214.114.46 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 6 |
| 46.166.188.214 | Netherlands | 147.237.8.50 | e.tikshuv.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 6 |
| 66.102.9.149 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.210.170.210 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 46.19.85.45 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 5 |
| 46.19.85.45 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 108.29.95.72 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 72.89.53.120 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 66.102.9.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 72.89.53.120 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 72.89.53.120 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.13.228.240 | Israel | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 79.178.254.141 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 213.57.215.16 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 109.67.131.115 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 100.92.17.242 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 79.178.254.141 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 109.253.206.251 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 84.229.8.189 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 37.26.147.163 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |

09-22-2016-19:04:09 to 09-22-2016-20:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.26.146.221 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 88 |
| 5.22.134.175 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 80 |
| 5.102.242.102 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 19 |
| 46.19.86.37 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 13 |
| 89.237.118.28 | France | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 87.69.246.69 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 46.116.197.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 46.19.86.172 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 46.19.86.172 | Block | 4 |
| 51.254.67.122 | France | 147.237.76.31 | nakchal.idf.il | Distributed PHP Attempt | Block | 4 |
| 51.254.67.122 | France | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 51.254.67.122 | Block | 4 |
| 176.13.6.46 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.98 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.66.114.20 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 51.254.67.122 | France | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 2 |
| 2.53.4.105 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 2 |
| 77.139.17.95 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/ | Block | 2 |
| 2.53.177.111 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 109.253.243.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.55.41.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.111.172.88 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.26.148.251 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.172 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 85.64.151.174 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/text.css | Block | 1 |
| 37.26.149.150 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 79.176.1.174 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 213.151.38.175 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 66.249.66.182 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8746-he/refuah.aspx | Block | 1 |
| 82.80.203.20 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 37.142.177.162 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$txtOtherQuestion in www.aka.idf.il/main/giyus/faq.aspx | None | 1 |
| 79.181.171.148 | Israel | 147.237.77.233 | atal.idf.il | Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx | Block | 1 |
| 66.249.76.61 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json | Block | 1 |
| 109.253.143.202 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 31.154.251.65 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/1/ | Block | 1 |
| 82.166.159.136 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 207.46.13.63 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 66.102.9.8 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 46.4.74.42 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp | Block | 1 |
| 80.179.122.185 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.76.63 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association | Block | 1 |
| 84.94.119.108 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 77.139.100.227 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 1 |
| 213.8.204.68 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 1 |
| 66.249.64.41 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg | Block | 1 |
| 104.175.212.142 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx | Block | 1 |
| 80.246.135.51 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 67.83.103.153 | United States | 147.237.77.216 | dover.idf.il | Distributed Parameter Type Violation on www.idf.il/error.htm parameter aspxerrorpath | Block | 1 |
| 113.110.233.3 | China | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 77.139.155.48 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx | Block | 1 |
| 213.8.204.68 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php | Block | 1 |

09-22-2016-19:04:09 to 09-22-2016-20:04:09