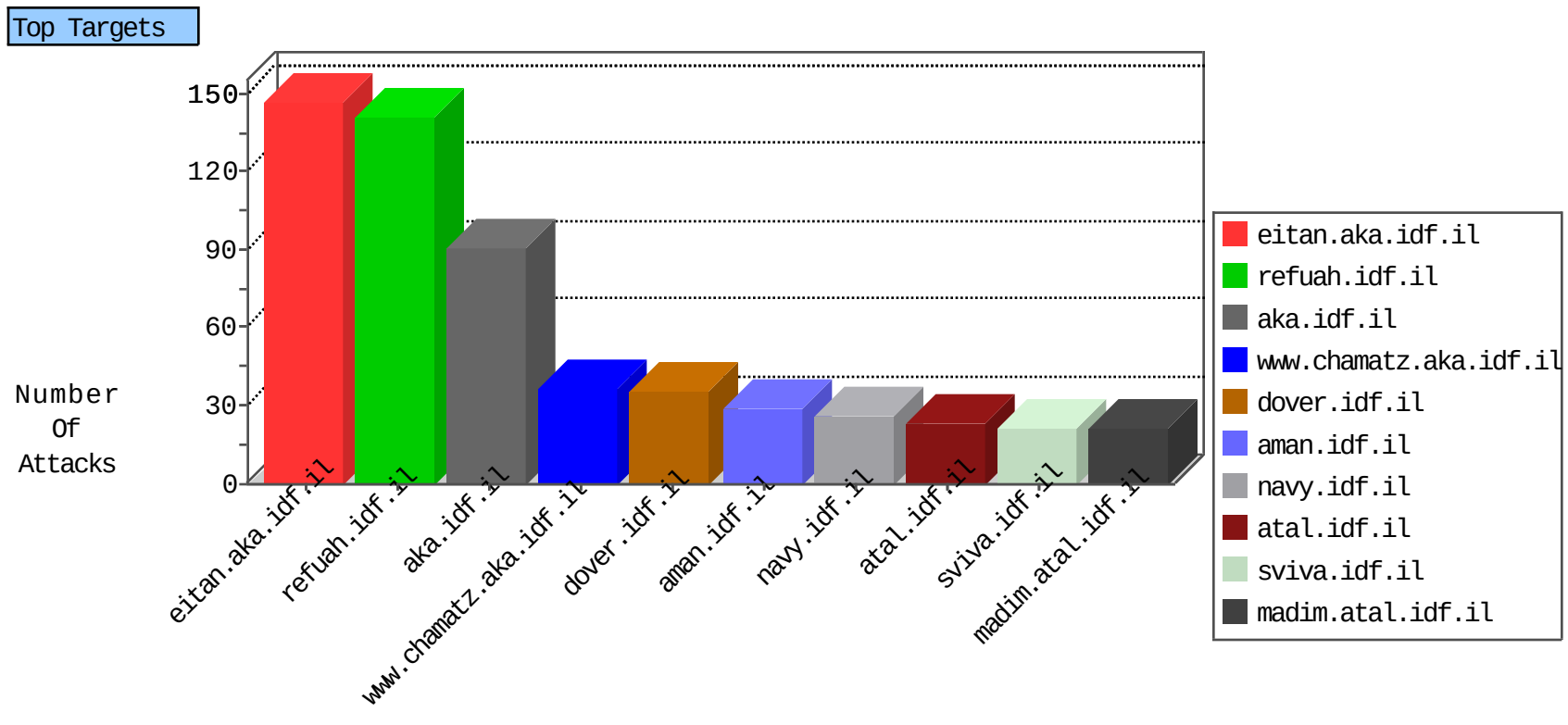
09-11-2016-01:06:35 to 09-11-2016-02:06:35

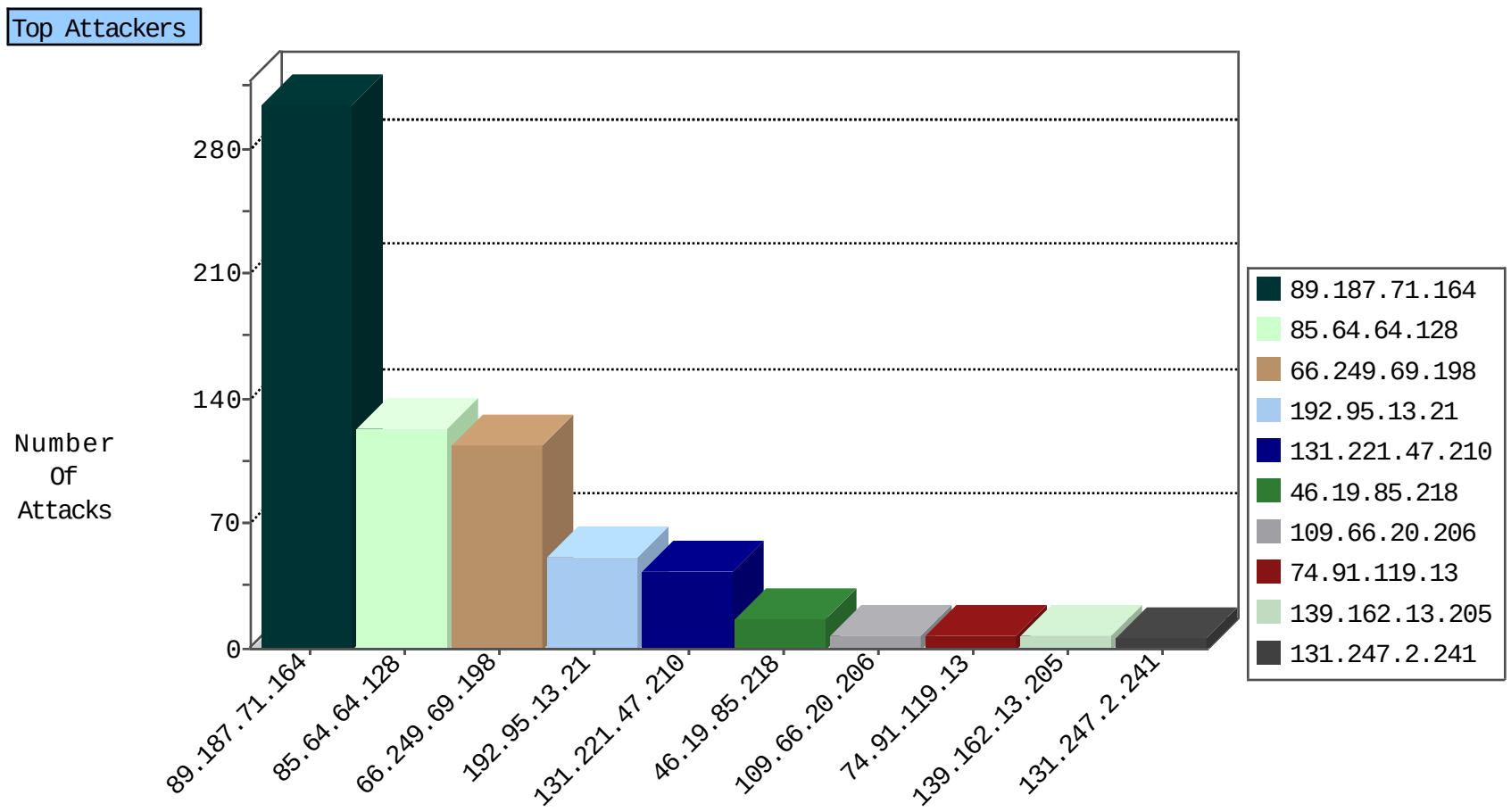
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

09-11-2016-01:06:35 to 09-11-2016-02:06:35

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 131.247.2.241 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 6 |
| 156.56.250.227 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 139.78.141.243 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.97.74.12 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.32.84.160 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 128.10.18.52 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 130.195.4.69 | New Zealand | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 204.85.191.11 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 153.90.1.34 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 195.113.161.84 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.8.126.111 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 216.48.80.12 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 130.194.252.8 | Australia | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.223.8.112 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 198.82.160.238 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.32.84.160 | United States | 147.237.72.167 | ishurim.aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 192.33.90.67 | Switzerland | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 128.223.8.114 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 200.19.159.34 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 141.22.213.34 | Germany | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.42.142.45 | United States | 147.237.72.167 | ishurim.aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 193.166.167.4 | Finland | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 130.217.77.2 | New Zealand | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.10.120.193 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.97.74.14 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.208.4.197 | United States | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |

09-11-2016-01:06:35 to 09-11-2016-02:06:35

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.97 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 123.126.68.101 | China | 147.237.77.74 | law.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

09-11-2016-01:06:35 to 09-11-2016-02:06:35

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.69.198 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 114 |
| 198.58.110.199 | 147.237.72.217 | United States | e.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 178.220.165.231 | 147.237.76.39 | | mobile.meitav.idf.i | ET SCAN NMAP -sS window 4096 | 1 |
| 178.220.165.231 | 147.237.76.39 | | mobile.meitav.idf.i | ET SCAN NMAP -f -sS | 1 |
| 94.102.48.195 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.149 | 147.237.0.33 | Ukraine | idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 178.220.165.231 | 147.237.76.39 | | mobile.meitav.idf.i | ET SCAN NMAP -sS window 2048 | 1 |
| 152.234.169.27 | 147.237.76.176 | Brazil | test.ncore.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 69.24.208.162 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

09-11-2016-01:06:35 to 09-11-2016-02:06:35

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 85.64.64.128 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 124 |
| 89.187.71.164 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 89.187.71.164 | United Kingdom | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 89.187.71.164 | United Kingdom | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 89.187.71.164 | United Kingdom | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 89.187.71.164 | United Kingdom | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 89.187.71.164 | United Kingdom | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 46.19.85.218 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 46.19.85.218 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 139.162.13.205 | Singapore | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 7 |
| 109.66.20.206 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 65.55.210.16 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.95.13.21 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 5.22.134.191 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 131.221.47.210 | Brazil | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 192.95.13.21 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 131.221.47.210 | Brazil | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 131.221.47.210 | Brazil | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 109.67.253.180 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 131.221.47.210 | Brazil | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 131.221.47.210 | Brazil | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 192.95.13.21 | Canada | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 46.19.85.66 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 131.221.47.210 | Brazil | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 74.91.119.13 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 2 |
| 131.221.47.210 | Brazil | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 192.95.13.21 | Canada | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 192.95.13.21 | Canada | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 131.221.47.210 | Brazil | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 131.221.47.210 | Brazil | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 89.237.126.36 | France | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 185.27.105.74 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 74.91.119.13 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 2 |

09-11-2016-01:06:35 to 09-11-2016-02:06:35

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.201 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 3 |
| 77.139.192.160 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.139.192.160 | Block | 3 |
| 84.111.234.107 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx | None | 1 |
| 157.55.39.124 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-15554-he/dover.aspx-title= | Block | 1 |
| 77.139.35.108 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp | Block | 1 |
| 88.128.80.105 | Germany | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on aka.idf.il/giyus/ | Block | 1 |
| 66.249.66.174 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 106.184.21.64 | Japan | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/giyus/ | Block | 1 |
| 66.249.66.251 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/gen...px | Block | 1 |
| 77.139.192.160 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim | Block | 1 |
| 2.53.169.114 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 109.64.33.204 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 77.138.216.8 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.138.216.8 | Block | 1 |
| 77.237.138.202 | Czech Republic | 147.237.77.235 | sviva.idf.il | Unauthorized Method HEAD for / | Block | 1 |
| 5.22.134.191 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/home/giyus | Block | 1 |
| 109.66.20.206 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 77.138.216.8 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 1 |

09-11-2016-01:06:35 to 09-11-2016-02:06:35