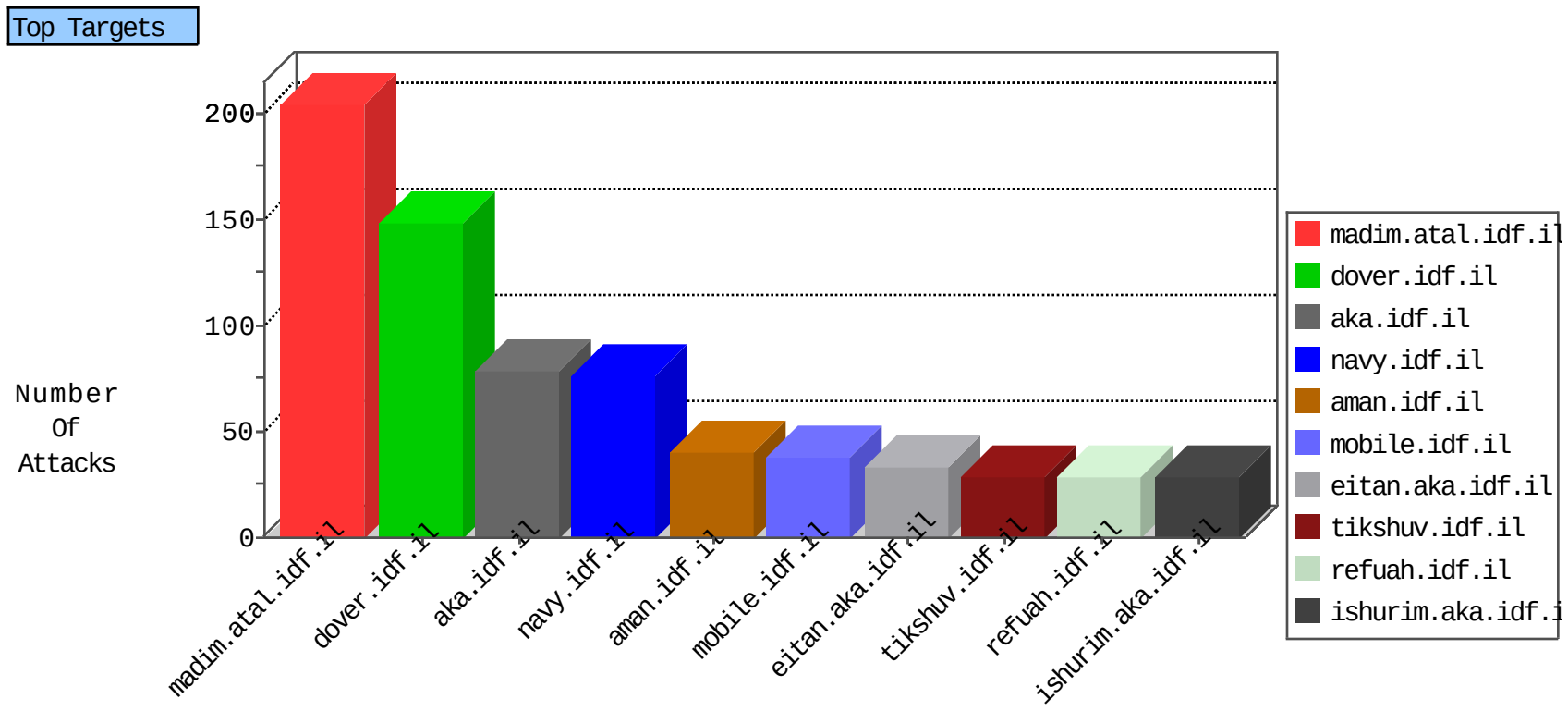
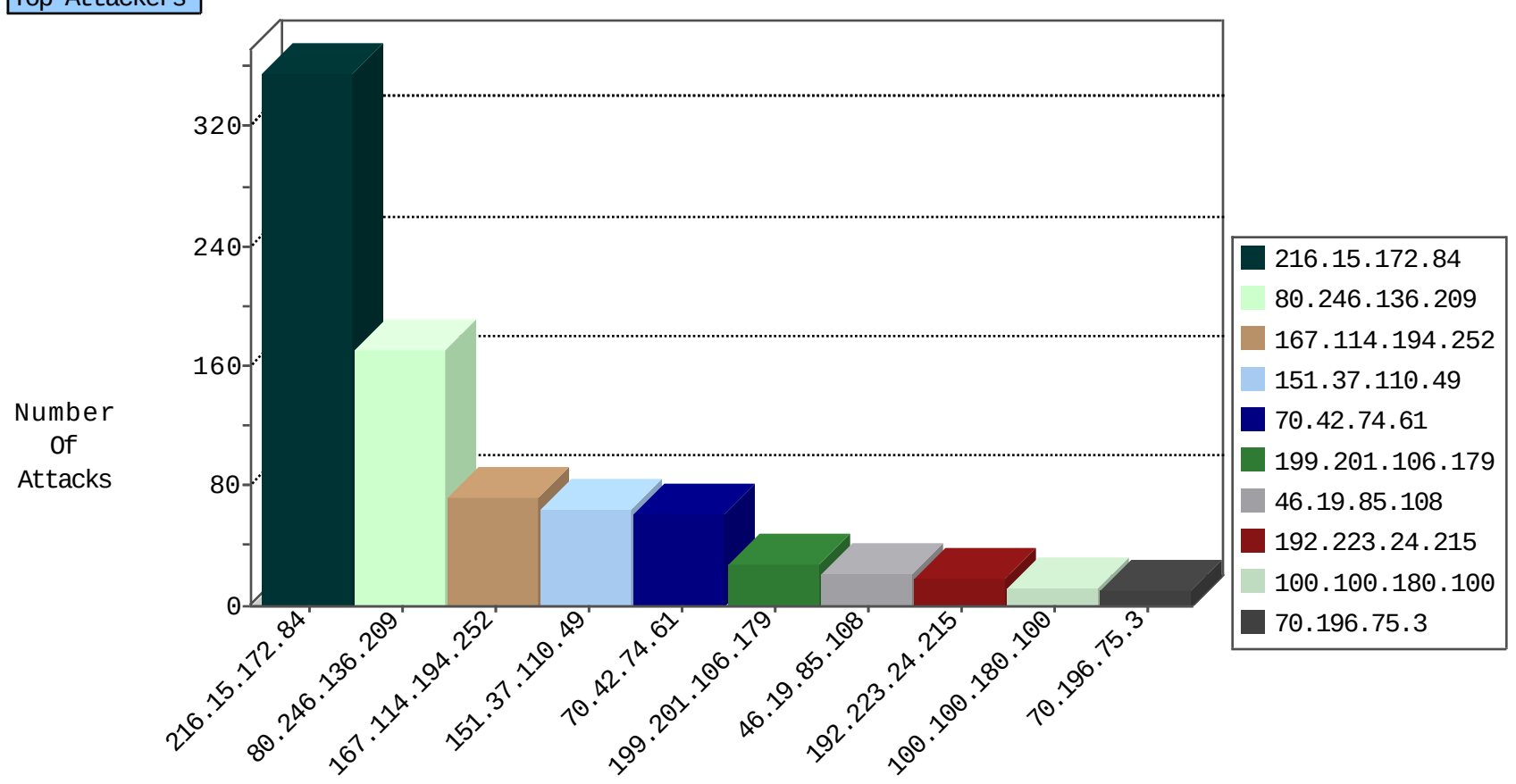
09-01-2016-00:04:00 to 09-01-2016-01:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-01-2016-00:04:00 to 09-01-2016-01:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.210.224 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 2 |
| 93.158.200.97 | Netherlands | 147.237.76.200 | eitan.aka.idf.il | Black List | drop | 1 |
| 186.229.64.153 | Brazil | 147.237.77.243 | mobile.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 82.221.105.6 | Iceland | 147.237.76.198 | e.yohalan.idf.il | Black List | drop | 1 |
| 93.158.200.97 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |

09-01-2016-00:04:00 to 09-01-2016-01:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.100 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 5 |

09-01-2016-00:04:00 to 09-01-2016-01:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.120.122.219 | 147.237.72.166 | Israel | aka.idf.il | Xenu Link Sleuth User Agent | 2 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 2 |
| 183.82.106.200 | 147.237.77.176 | India | matpash.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 123.192.104.236 | 147.237.76.30 | Taiwan | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 104.232.98.38 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 66.249.76.117 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 211.141.78.56 | 147.237.8.24 | China | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.149 | 147.237.76.177 | Ukraine | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 186.229.64.153 | 147.237.0.19 | Brazil | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 183.82.106.200 | 147.237.77.176 | India | matpash.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 104.232.98.38 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 97.105.173.114 | 147.237.72.167 | United States | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.155 | 147.237.77.176 | Ukraine | matpash.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 193.201.225.149 | 147.237.77.61 | Ukraine | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.82.46.210 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.149 | 147.237.8.14 | Ukraine | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |

09-01-2016-00:04:00 to 09-01-2016-01:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 151.37.110.49 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 199.201.106.179 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 28 |
| 46.19.85.108 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 216.15.172.84 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 216.15.172.84 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 216.15.172.84 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 216.15.172.84 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 216.15.172.84 | United States | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 216.15.172.84 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 216.15.172.84 | United States | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 100.100.180.100 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 192.223.24.215 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 196.137.77.48 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 70.196.75.3 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 8 |
| 80.246.136.209 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 192.223.24.215 | United States | 147.237.76.86 | navy.idf.il | SYN Attack |  | monitor | 7 |
| 80.246.137.17 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 130.193.50.14 | Russian Federation | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 93.172.202.147 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.180.164.221 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 167.114.194.252 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 167.114.194.252 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 80.246.136.209 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 167.114.194.252 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 167.114.194.252 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 167.114.194.252 | Canada | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 83.220.238.11 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 167.114.194.252 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 213.8.204.8 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 167.114.194.252 | Canada | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 167.114.194.252 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 87.204.52.13 | Poland | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 89.139.151.92 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 99.236.29.26 | Canada | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 70.42.74.61 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |

09-01-2016-00:04:00 to 09-01-2016-01:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 80.246.136.209 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 157 |
| 84.229.38.190 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 2.53.136.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 151.37.110.49 | Italy | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/italiano/ | Block | 2 |
| 62.212.110.206 | France | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 2 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/ | Block | 1 |
| 207.14.66.21 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 1 |
| 77.138.173.84 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 1 |
| 66.102.9.24 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 85.64.147.144 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 66.249.76.115 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-19825-he/dover.aspx | Block | 1 |
| 46.19.86.229 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 216.244.66.231 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 77.139.40.206 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/giyus/ | Block | 1 |
| 66.249.66.197 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 87.204.52.13 | Poland | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.76.117 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.120.122.219 | Block | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 70.52.8.86 | Canada | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx | Block | 1 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 80.246.137.17 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 180.97.106.162 | China | 147.237.0.15 | kosher-kravi.idf.i | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 70.53.249.78 | Canada | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/dover/sote/homepage/asp | Block | 1 |

09-01-2016-00:04:00 to 09-01-2016-01:04:00