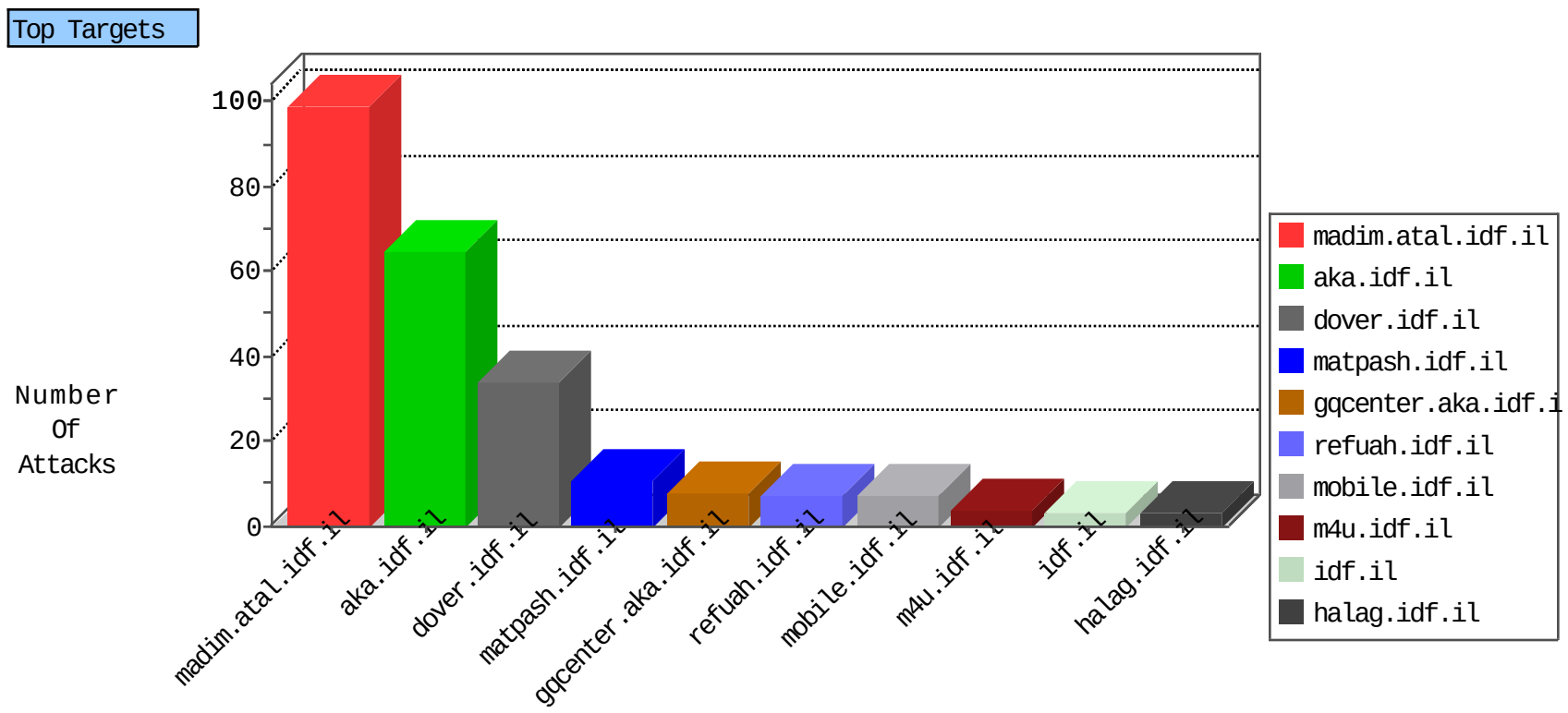
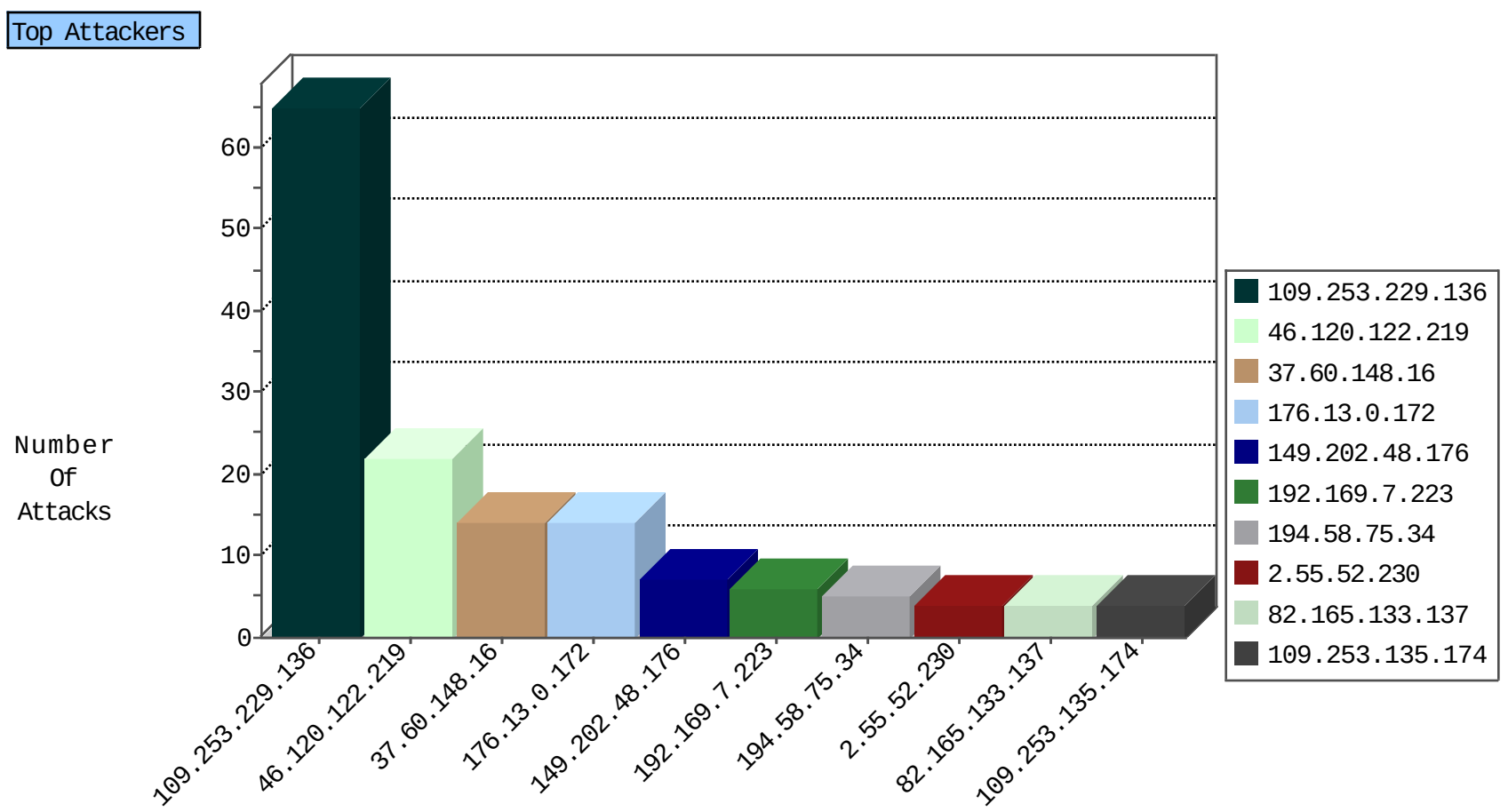
08-30-2016-07:04:08 to 08-30-2016-08:04:08

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-30-2016-07:04:08 to 08-30-2016-08:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.80.78.2 | Israel | 147.237.77.176 | matpash.idf.il | Black List | drop | 2 |
| 109.64.147.8 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 2 |
| 79.180.242.95 | Israel | 147.237.77.234 | halag.idf.il | Black List | drop | 1 |

08-30-2016-07:04:08 to 08-30-2016-08:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 149.202.48.176 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 5 |
| 149.202.48.176 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

08-30-2016-07:04:08 to 08-30-2016-08:04:08

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 | 12 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 2 |
| 46.120.122.219 | 147.237.77.170 | Israel | maarachot.idf.il | Xenu Link Sleuth User Agent | 2 |
| 66.249.93.16 | 147.237.77.226 | Europe | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 197.211.244.181 | 147.237.0.200 | Zimbabwe | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.204.245 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 116.12.175.233 | 147.237.72.167 | Singapore | ishurim.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 50.116.123.135 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.253.131.236 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.224.160.106 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.16 | Netherlands | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.28.187.177 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.165.133.137 | 147.237.76.202 | Germany | e.halag.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 82.165.133.137 | 147.237.0.33 | Germany | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 217.118.23.124 | 147.237.72.156 | Germany | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.178.170.69 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 197.211.244.181 | 147.237.0.200 | Zimbabwe | m4u.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 66.249.93.13 | 147.237.77.226 | Europe | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 190.147.75.207 | 147.237.8.28 | Colombia | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.218.204.245 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 116.12.175.233 | 147.237.72.167 | Singapore | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.227.67.172 | 147.237.0.16 | Sweden | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.77.179 | Netherlands | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.76.38 | Netherlands | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.102.253.31 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.108.50.179 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.17.229 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.165.133.137 | 147.237.76.30 | Germany | himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 82.165.133.137 | 147.237.0.19 | Germany | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 201.38.68.132 | 147.237.0.35 | Brazil | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-30-2016-07:04:08 to 08-30-2016-08:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.60.148.16 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 37.60.148.16 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 5 |
| 46.19.85.81 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 194.58.75.34 | Russian Federation | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 37.232.111.149 | Georgia | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 85.130.183.197 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 95.35.138.67 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 194.58.75.34 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.21.195 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 2 |
| 85.130.183.197 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 2 |
| 141.212.122.126 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 176.13.241.16 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.197.178 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 62.0.197.205 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 169.229.3.91 | United States | 147.237.72.217 | e.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.77.243 | mobile.idf.il | drop | SAM rule | drop | 1 |
| 109.253.198.223 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 66.249.64.19 | Israel | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 176.13.11.249 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.131.51 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 184.105.247.232 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 109.253.203.2 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 85.114.108.65 | Palestinian Territory, Occupied | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 109.253.139.107 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 188.161.150.114 | Palestinian Territory, Occupied | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 141.212.122.125 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 213.6.148.130 | Palestinian Territory, Occupied | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 176.13.225.166 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.194.194 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.253.229.136 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 65 |
| 176.13.0.172 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 14 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.120.122.219 | Block | 6 |
| 2.55.52.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 109.253.135.174 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 4 |
| 37.46.41.194 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.53.170.255 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 93.172.246.194 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.103 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.147.197 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 79.177.239.233 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.177.239.233 | Block | 2 |
| 77.138.211.194 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/ | Block | 1 |
| 192.169.7.223 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized Method HEAD for 147.237.76.42/ | Block | 1 |
| 66.249.65.19 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/undefined | Block | 1 |
| 91.199.69.254 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter sbredirect in www.aka.idf.il/main/sachar/ | None | 1 |
| 79.180.242.95 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.85.51 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 141.226.218.12 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 1 |
| 77.139.34.200 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 195.167.10.2 | Greece | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 1 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx | Block | 1 |
| 91.227.71.250 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 79.181.23.203 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.93.82 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 148.251.2.180 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/piwik.php | Block | 1 |
| 77.139.87.71 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 1 |
| 204.79.180.174 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp | Block | 1 |
| 66.249.76.116 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-22805-he/idfgdover.aspx | Block | 1 |
| 79.181.59.162 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 77.138.78.39 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx | Block | 1 |
| 46.120.238.81 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 84.111.244.200 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 213.57.183.133 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 66.249.85.41 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 24.232.179.138 | Argentina | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/sites/home/default.asp | Block | 1 |
| 79.183.88.149 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 77.138.207.94 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/sachar | Block | 1 |
| 62.219.195.139 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 85.64.144.11 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 79.177.239.233 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx | Block | 1 |
| 66.249.85.46 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |

08-30-2016-07:04:08 to 08-30-2016-08:04:08