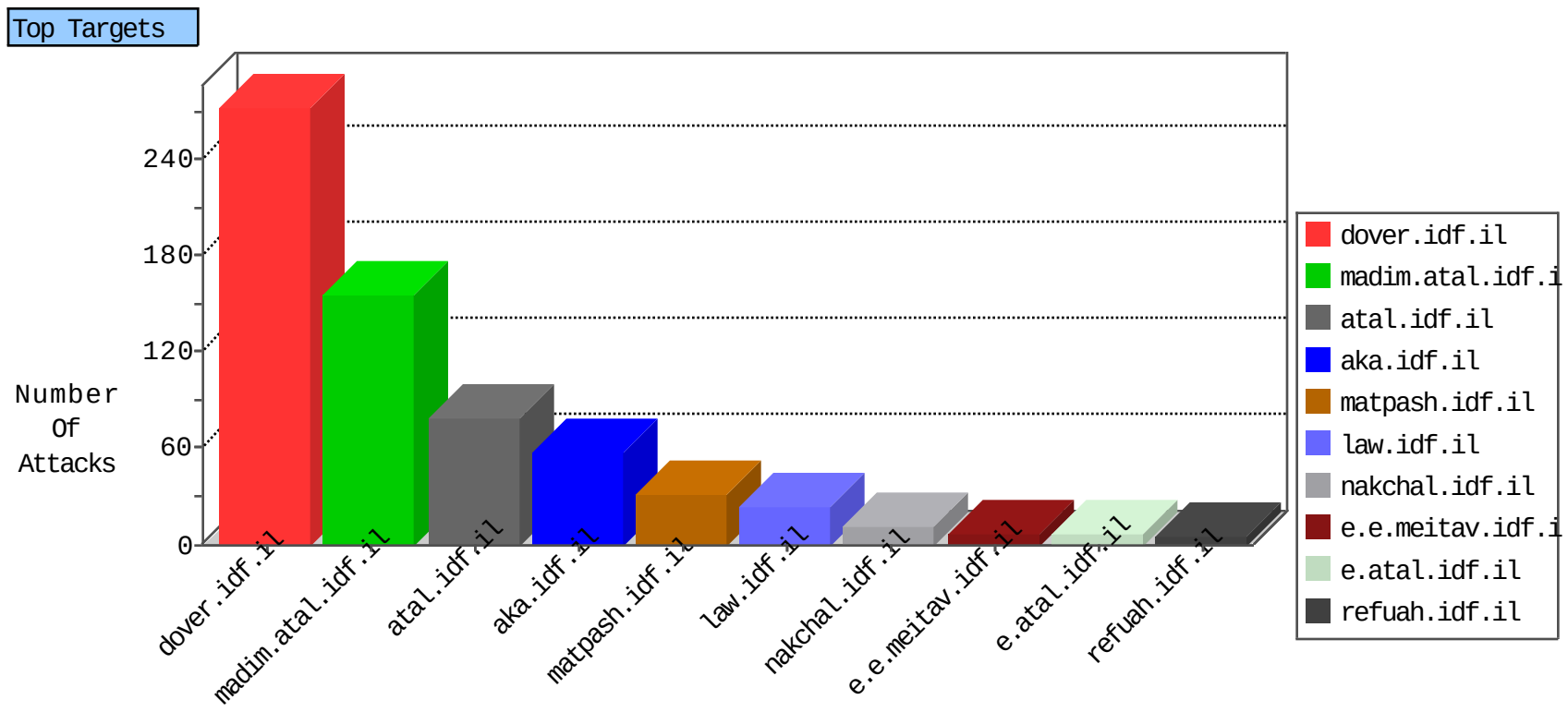
08-24-2016-15:07:32 to 08-24-2016-16:07:32

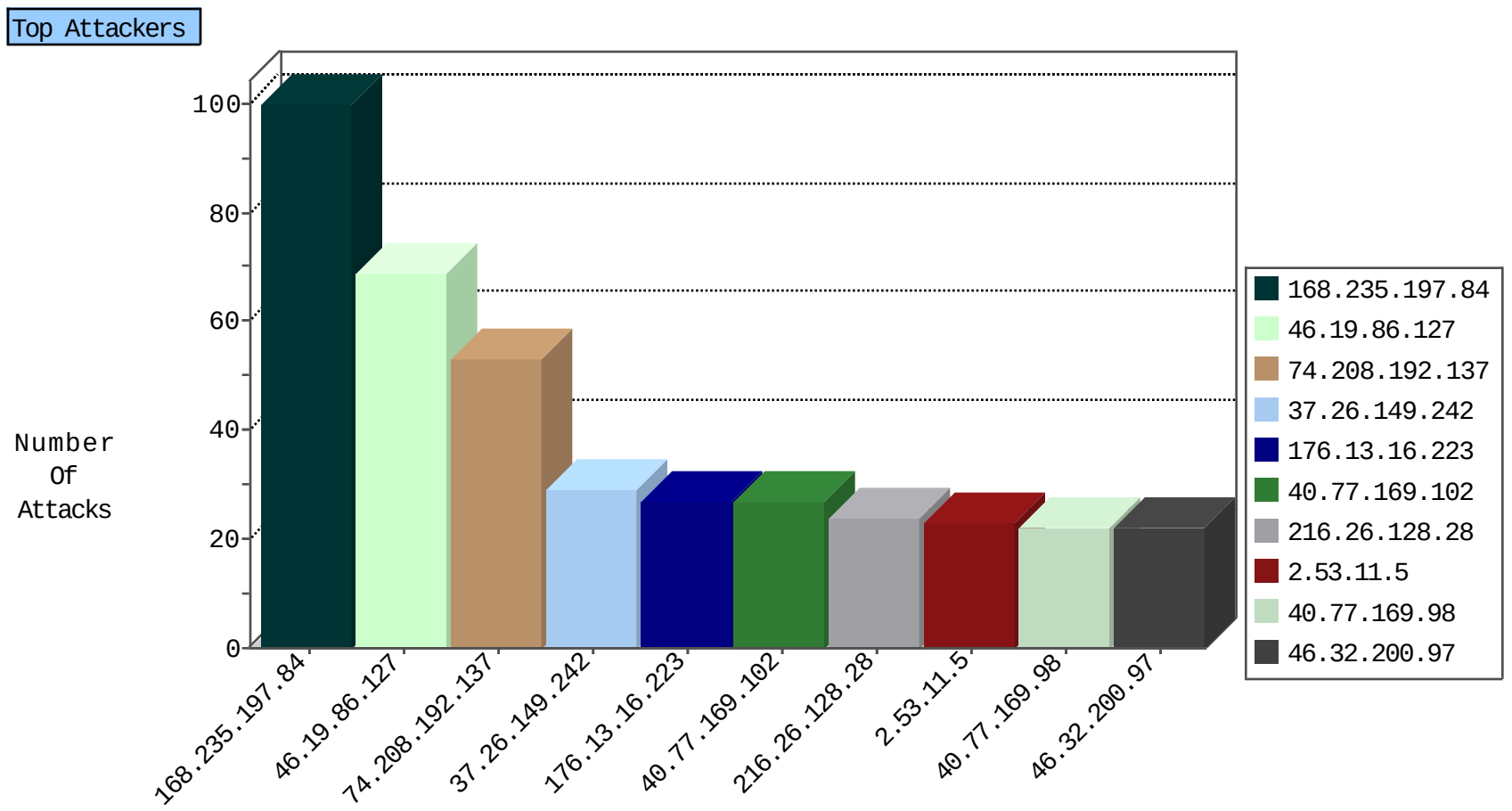
# IDF Under Attack
# Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

08-24-2016-15:07:32 to 08-24-2016-16:07:32

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.16.223 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 27 |
| 109.67.162.104 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 2.53.132.237 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 168.235.197.84 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 212.25.74.130 | Israel | 147.237.77.233 | atal.idf.il | Black List | drop | 3 |
| 98.139.14.250 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 212.25.74.130 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 2 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 195.160.242.40 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 93.174.93.156 | Netherlands | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 114.185.83.162 | Japan | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.77.176 | matpash.idf.il | Black List | drop | 1 |
| 93.174.93.156 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Black List | drop | 1 |
| 93.158.200.166 | Netherlands | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |
| 93.158.200.166 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Black List | drop | 1 |
| 2.53.38.138 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |

08-24-2016-15:07:32 to 08-24-2016-16:07:32

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 178.137.160.45 | Ukraine | 147.237.72.166 | aka.idf.il | C1000016: HTTP: administrator in URI | Permit | 8 |
| 74.208.192.137 | United States | 147.237.77.233 | atal.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 216.26.128.28 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 74.208.192.137 | United States | 147.237.77.233 | atal.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 6 |
| 74.208.192.137 | United States | 147.237.77.233 | atal.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 6 |
| 213.60.255.71 | Spain | 147.237.77.233 | atal.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 151.80.31.182 | France | 147.237.72.166 | aka.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

08-24-2016-15:07:32 to 08-24-2016-16:07:32

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 74.208.192.137 | 147.237.77.233 | United States | atal.idf.il | SQL Injection - Select From | 35 |
| 216.26.128.28 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 18 |
| 213.60.255.71 | 147.237.77.233 | Spain | atal.idf.il | SQL Injection - Select From | 9 |
| 151.80.41.177 | 147.237.72.166 | France | aka.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 3 |
| 46.120.122.219 | 147.237.72.166 | Israel | aka.idf.il | Xenu Link Sleuth User Agent | 2 |

08-24-2016-15:07:32 to 08-24-2016-16:07:32

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.197.84 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 97 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 16 |
| 46.32.200.97 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 16 |
| 40.77.169.96 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 10 |
| 155.55.50.19 | Norway | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 8 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 8 |
| 62.0.211.129 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 40.77.169.102 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 7 |
| 139.162.13.205 | Singapore | 147.237.76.38 | e.e.meitav.idf.il | drop | SAM rule | drop | 7 |
| 139.162.13.205 | Singapore | 147.237.76.201 | e.atal.idf.il | drop | SAM rule | drop | 7 |
| 46.32.200.97 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 62.0.211.129 | Israel | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 5 |
| 40.77.169.100 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 5 |
| 46.19.85.254 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 62.0.197.205 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 2.53.38.138 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 80.74.118.200 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop |  | drop | 4 |
| 46.43.92.6 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 5.43.205.22 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 37.8.124.141 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 98.139.14.250 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 101.178.206.92 | Australia | 147.237.0.35 | akaws.idf.il | drop |  | drop | 1 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 66.102.9.131 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 31.168.11.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 92.124.239.7 | Russian Federation | 147.237.0.200 | m4u.idf.il | drop |  | drop | 1 |
| 62.0.197.205 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.131.138 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 73.197.100.12 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.0.20 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 92.124.239.7 | Russian Federation | 147.237.76.148 | gqcenter.aka.idf.il | drop |  | drop | 1 |
| 74.82.47.47 | United States | 147.237.0.200 | m4u.idf.il | drop |  | drop | 1 |
| 178.238.229.218 | Germany | 147.237.76.34 | yohalan.idf.il | drop |  | drop | 1 |
| 184.105.247.230 | United States | 147.237.0.35 | akaws.idf.il | drop |  | drop | 1 |

08-24-2016-15:07:32 to 08-24-2016-16:07:32

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.127 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 69 |
| 37.26.149.242 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 46.19.86.181 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 17 |
| 2.53.11.5 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 212.117.140.170 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 3 |
| 192.116.232.69 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 192.116.232.69 | Block | 3 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 2.53.152.115 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il | Block | 2 |
| 85.64.124.129 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/matash | Block | 2 |
| 212.235.62.200 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized HTTP Method | Block | 2 |
| 167.220.232.104 | Japan | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 46.19.86.108 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 212.235.62.200 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal | Block | 2 |
| 192.116.98.164 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/9/size338x0/3209.jpg | Block | 2 |
| 84.111.165.132 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 40.77.169.99 | United States | 147.237.77.170 | maarachot.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 212.143.91.229 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd | None | 1 |
| 123.125.71.86 | China | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg | Block | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter sOpenLinkIn in www.aka.idf.il/iturim/asp/displayonesoldier.asp | None | 1 |
| 192.116.232.69 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.116.232.69 | Block | 1 |
| 46.117.145.144 | Israel | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation txtContent in www.tikshuv.idf.il/modules/forums.frm/frmmessage.aspx | Block | 1 |
| 40.77.169.99 | United States | 147.237.77.176 | matpash.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 212.179.146.134 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx | Block | 1 |
| 157.55.39.182 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/reserve | Block | 1 |
| 79.177.155.42 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 46.19.86.46 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 192.116.232.69 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png | Block | 1 |
| 37.26.149.154 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |
| 109.64.5.216 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/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/rabanut/general.aspx | Block | 1 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 80.179.20.132 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 194.90.128.185 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png | Block | 1 |
| 109.66.107.233 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.102.9.76 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/drushim/ | Block | 1 |
| 84.108.190.247 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 109.253.144.153 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.76.70 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/apple-app-site-association | Block | 1 |
| 40.77.169.103 | United States | 147.237.77.176 | matpash.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 2.53.14.112 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |

08-24-2016-15:07:32 to 08-24-2016-16:07:32