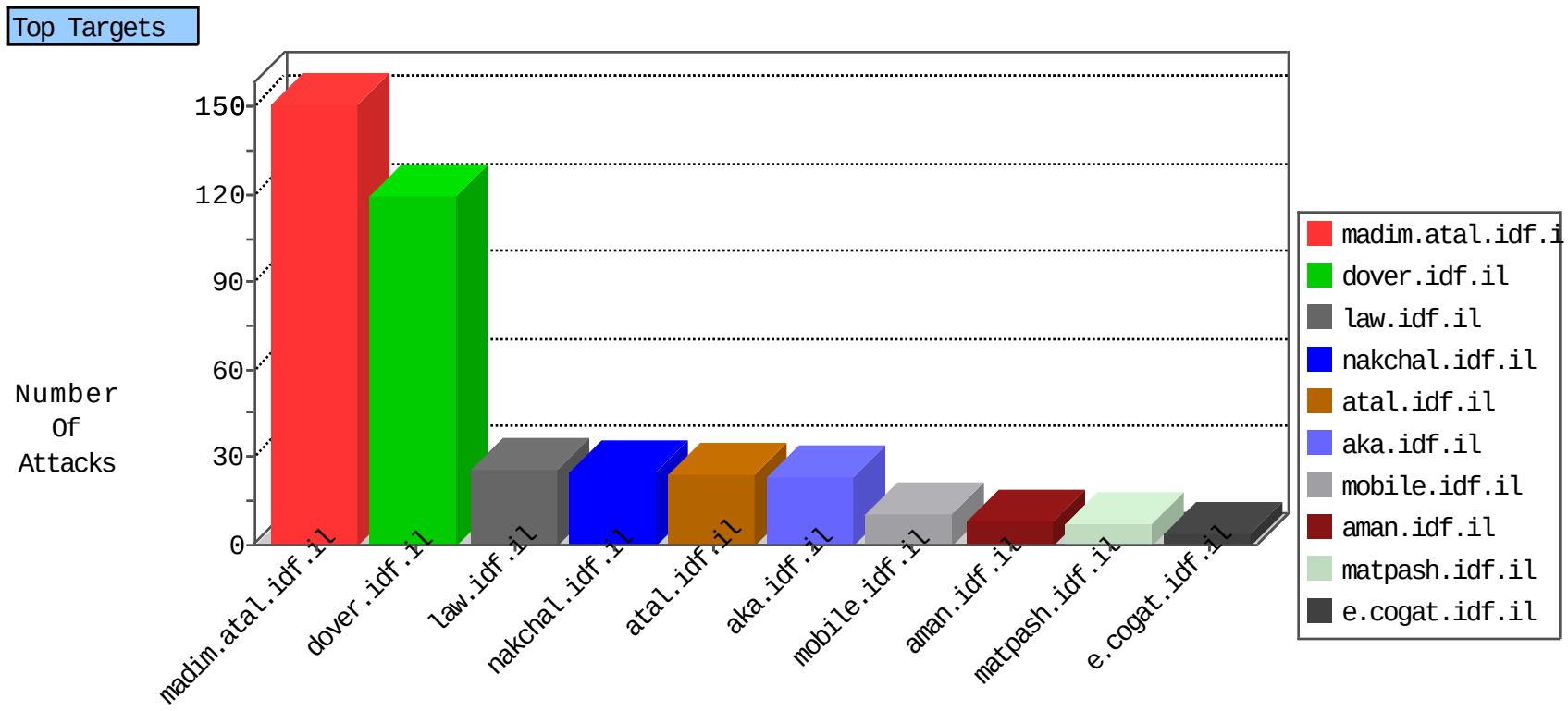
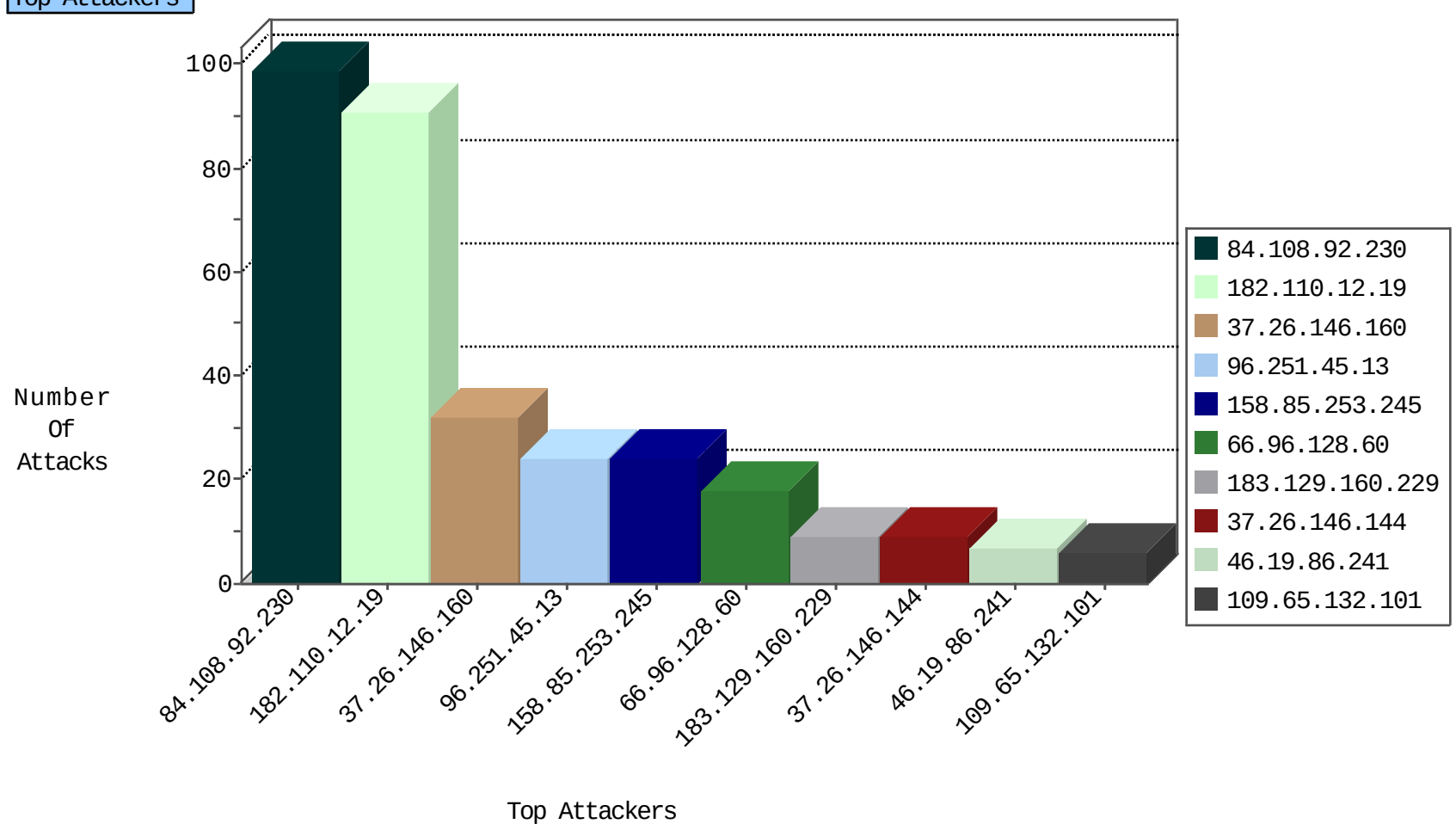
08-18-2016-19:04:04 to 08-18-2016-20:04:04

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



08-18-2016-19:04:04 to 08-18-2016-20:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 151.80.108.148 | France | 147.237.76.38 | e.e.meitav.idf.il | Black List | drop | 1 |

08-18-2016-19:04:04 to 08-18-2016-20:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 96.251.45.13 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 3 |
| 51.255.51.7 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 212.47.231.31 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 106.120.188.69 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

08-18-2016-19:04:04 to 08-18-2016-20:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 96.251.45.13 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 18 |
| 182.110.12.19 | 147.237.77.216 | China | dover.idf.il | LOCAL_RULES - Request with the string install.php in it | 2 |
| 80.246.130.95 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 218.204.153.227 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.172.71.251 | 147.237.0.35 | Ukraine | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 213.57.161.221 | 147.237.72.166 | Israel | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 180.97.106.37 | 147.237.72.217 | China | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 178.220.147.151 | 147.237.76.38 | | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 88.249.106.23 | 147.237.8.50 | Turkey | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 221.226.31.210 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -f -sS | 1 |
| 66.249.66.169 | 147.237.76.30 | United States | himush.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 221.6.32.82 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -f -sS | 1 |
| 58.218.204.245 | 147.237.76.148 | China | gqcenter.aka.idf.i | ET SCAN Potential SSH Scan | 1 |
| 218.204.153.227 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 1 |
| 198.20.69.74 | 147.237.76.44 | United States | e.refuah.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 180.97.106.37 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 178.220.147.151 | 147.237.76.38 | | e.e.meitav.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 124.216.184.111 | 147.237.76.30 | Korea, Republic of | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.125.184.101 | 147.237.77.74 | United Kingdom | law.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 221.226.31.210 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 221.6.32.82 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 62.219.119.92 | 147.237.76.42 | Israel | refuah.idf.il | ET SCAN NMAP -sA (2) | 1 |

08-18-2016-19:04:04 to 08-18-2016-20:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 158.85.253.245 | United States | 147.237.76.31 | nakchal.idf.il | drop | SAM rule | drop | 24 |
| 66.96.128.60 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 18 |
| 109.65.132.101 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 6 |
| 155.178.180.11 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 188.247.78.103 | Jordan | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 5.102.124.138 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 2 |
| 2.55.49.2 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 216.243.31.2 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 1 |
| 176.13.238.213 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 1 |
| 61.90.48.136 | Thailand | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.77.178 | e.matpash.idf.il | drop | SAM rule | drop | 1 |
| 141.212.122.80 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.0.35 | akaws.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.179 | e.mazi.idf.il | drop | SAM rule | drop | 1 |
| 141.212.122.95 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 191.96.249.18 | Chile | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.8.28 | e.mobile-ks.idf.il | drop | SAM rule | drop | 1 |
| 66.240.192.138 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.205 | prisha.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 1 |
| 79.177.183.186 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.108.92.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 99 |
| 182.110.12.19 | China | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 44 |
| 182.110.12.19 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 182.110.12.19 | Block | 43 |
| 37.26.146.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 32 |
| 37.26.146.144 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 8 |
| 46.19.86.241 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 172.89.91.185 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx | Block | 4 |
| 2.53.29.123 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 87.69.36.223 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.229.104 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.116.22.97 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 2 |
| 157.55.39.131 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.204.104.31 | Lebanon | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp | Block | 2 |
| 46.116.22.97 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/ | Block | 2 |
| 79.180.231.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 77.138.109.38 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/ | Block | 2 |
| 104.128.144.131 | Canada | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to 147.237.72.156/redirect.php | Block | 1 |
| 77.138.243.23 | France | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/salah.stm" target="_blank | Block | 1 |
| 5.29.181.69 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 84.109.2.122 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 68.180.228.185 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx | Block | 1 |
| 37.46.34.192 | Israel | 147.237.77.243 | mobile.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 104.128.144.131 | Canada | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to 147.237.76.147/redirect.php | Block | 1 |
| 77.139.5.142 | France | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/favicon.ico | Block | 1 |
| 31.154.81.7 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/ | Block | 1 |
| 85.55.112.138 | Spain | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 68.180.230.158 | United States | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 182.110.12.19 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/11m.php | Block | 1 |
| 37.142.70.103 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/219-he/patzar.aspx | Block | 1 |
| 109.67.128.70 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.102.9.95 | 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 |
| 217.132.12.62 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx | Block | 1 |
| 37.26.146.144 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.13.7.38 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 87.68.43.213 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 193.150.8.113 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 1 |
| 37.142.251.135 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 109.67.211.187 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 80.246.133.52 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 66.249.65.182 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css | Block | 1 |
| 182.110.12.19 | China | 147.237.77.216 | dover.idf.il | Admin Blocking | Block | 1 |
| 77.138.135.45 | France | 147.237.76.42 | refuah.idf.il | Unauthorized Method POST for 147.237.76.42/ | Block | 1 |
| 207.46.13.9 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 2.53.148.38 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.79.174 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/robots.txt | Block | 1 |

08-18-2016-19:04:04 to 08-18-2016-20:04:04