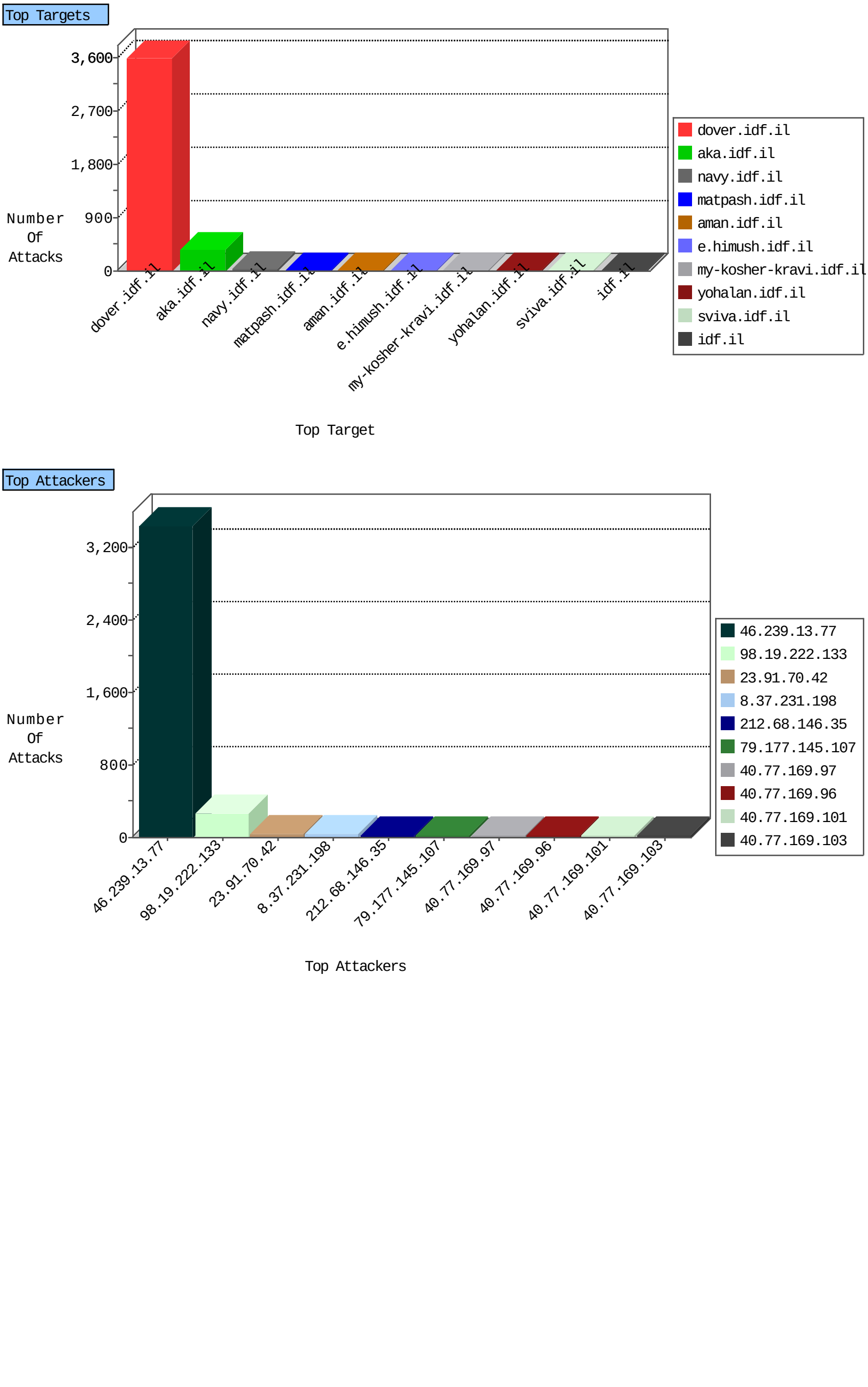
08-27-2016-10:04:03 to 08-27-2016-11:04:03

# IDF Under Attack Daily Report



08-27-2016-10:04:03 to 08-27-2016-11:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 8.37.231.198 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 66.249.66.180 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 222.186.34.151 | China | 147.237.76.202 | e.halag.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.196 | e.sviva.idf.il | Black List | drop | 1 |
| 37.230.210.161 | Russian Federation | 147.237.76.197 | e.himush.idf.il | Black List | drop | 1 |
| 222.186.34.151 | China | 147.237.76.197 | e.himush.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 222.186.34.151 | China | 147.237.76.202 | e.halag.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |

08-27-2016-10:04:03 to 08-27-2016-11:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 98.19.222.133 | United States | 147.237.72.166 | aka.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 53 |
| 98.19.222.133 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 19 |
| 23.91.70.42 | United States | 147.237.72.166 | aka.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 12 |
| 23.91.70.42 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 212.68.146.35 | Israel | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 85.94.76.17 | Croatia | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |

08-27-2016-10:04:03 to 08-27-2016-11:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 98.19.222.133 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 195 |
| 79.177.145.107 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 24 |
| 23.91.70.42 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 20 |
| 212.68.146.35 | 147.237.72.166 | Israel | aka.idf.il | SQL Injection - Select From | 18 |
| 85.94.76.17 | 147.237.72.166 | Croatia | aka.idf.il | SQL Injection - Select From | 8 |
| 146.200.158.162 | 147.237.77.216 | United Kingdom | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 185.110.132.201 | 147.237.76.176 | Ukraine | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.76.42 | Ukraine | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.203.215.242 | 147.237.76.177 | Canada | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.110.132.201 | 147.237.8.46 | Ukraine | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.0.35 | Ukraine | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.0.33 | Ukraine | idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 163.172.169.150 | 147.237.77.235 | United Kingdom | sviva.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.110.132.201 | 147.237.77.235 | Ukraine | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.77.179 | Ukraine | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.249.106.23 | 147.237.77.121 | Turkey | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.110.132.201 | 147.237.76.44 | Ukraine | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.76.30 | Ukraine | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.8.28 | Ukraine | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.0.34 | Ukraine | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.178.42.242 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.110.132.201 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.227.67.172 | 147.237.76.42 | Sweden | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.197 | United Kingdom | e.himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 5.255.90.133 | 147.237.76.176 | Netherlands | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 137.117.168.203 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.110.132.201 | 147.237.77.226 | Ukraine | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.195 | 147.237.77.235 | Netherlands | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-27-2016-10:04:03 to 08-27-2016-11:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.239.13.77 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3188 |
| 46.239.13.77 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | | drop | 250 |
| 8.37.231.198 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 21 |
| 40.77.169.96 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 19 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 18 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 12 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 40.77.169.103 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 94.64.167.134 | Greece | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 77.138.41.152 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 184.105.247.204 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 222.186.34.151 | China | 147.237.76.30 | himush.idf.il | drop | SAM rule | drop | 1 |
| 178.238.229.218 | Germany | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 222.186.34.151 | China | 147.237.76.39 | mobile.meitav.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.8.24 | e.lifestyle.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.72.167 | ishurim.aka.idf.il | drop | SAM rule | drop | 1 |
| 222.186.34.151 | China | 147.237.0.16 | my-kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 141.212.122.69 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 222.186.34.151 | China | 147.237.76.147 | chinuch.aka.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.8.46 | e.chinuch.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 222.186.34.151 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 141.212.122.70 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 184.105.139.112 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 1 |
| 222.186.34.151 | China | 147.237.0.33 | idf.il | drop | SAM rule | drop | 1 |
| 178.238.229.218 | Germany | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |

08-27-2016-10:04:03 to 08-27-2016-11:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 5 |
| 131.253.27.134 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 109.186.90.255 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 31.13.102.120 | Ireland | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 1 |
| 79.177.4.152 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 46.19.86.249 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL http/1.1 | Block | 1 |
| 66.249.76.85 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/eitan/pratim/pirteyerua/ | Block | 1 |
| 40.77.169.100 | United States | 147.237.77.176 | matpash.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 94.64.167.134 | Greece | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 46.19.86.249 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method oller/jquery.jcarousel.css?SiteVersion=1.05 in URL www.idf.ilhttp/1.1 | Block | 1 |
| 157.55.39.138 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to www.maarachot.idf.il/pdf/files/×'×™ ×œ×™××• ××ª | Block | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.106 | Block | 1 |
| 109.186.81.220 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 46.229.164.102 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 178.255.87.242 | United Kingdom | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to 147.237.0.16/robots.txt | Block | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/70685.pdf | Block | 1 |
| 46.19.86.249 | Israel | 147.237.77.216 | dover.idf.il | Abnormally Long Request method | Block | 1 |
| 66.102.9.21 | 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 |
| 207.46.13.161 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 68.180.228.87 | United States | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מא יר שחמו|.aspx | Block | 1 |
| 46.19.86.249 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version | Block | 1 |
| 109.253.211.114 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |

08-27-2016-10:04:03 to 08-27-2016-11:04:03