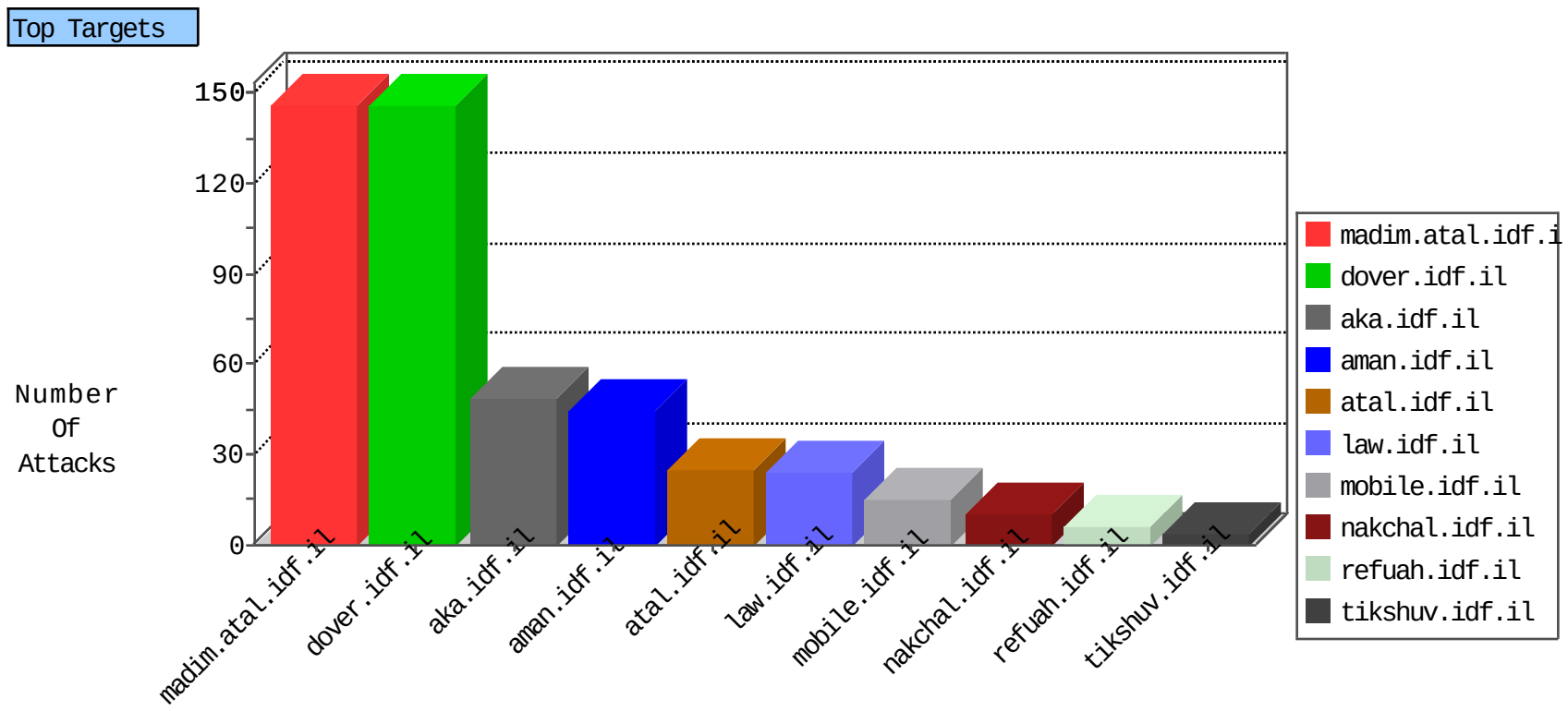
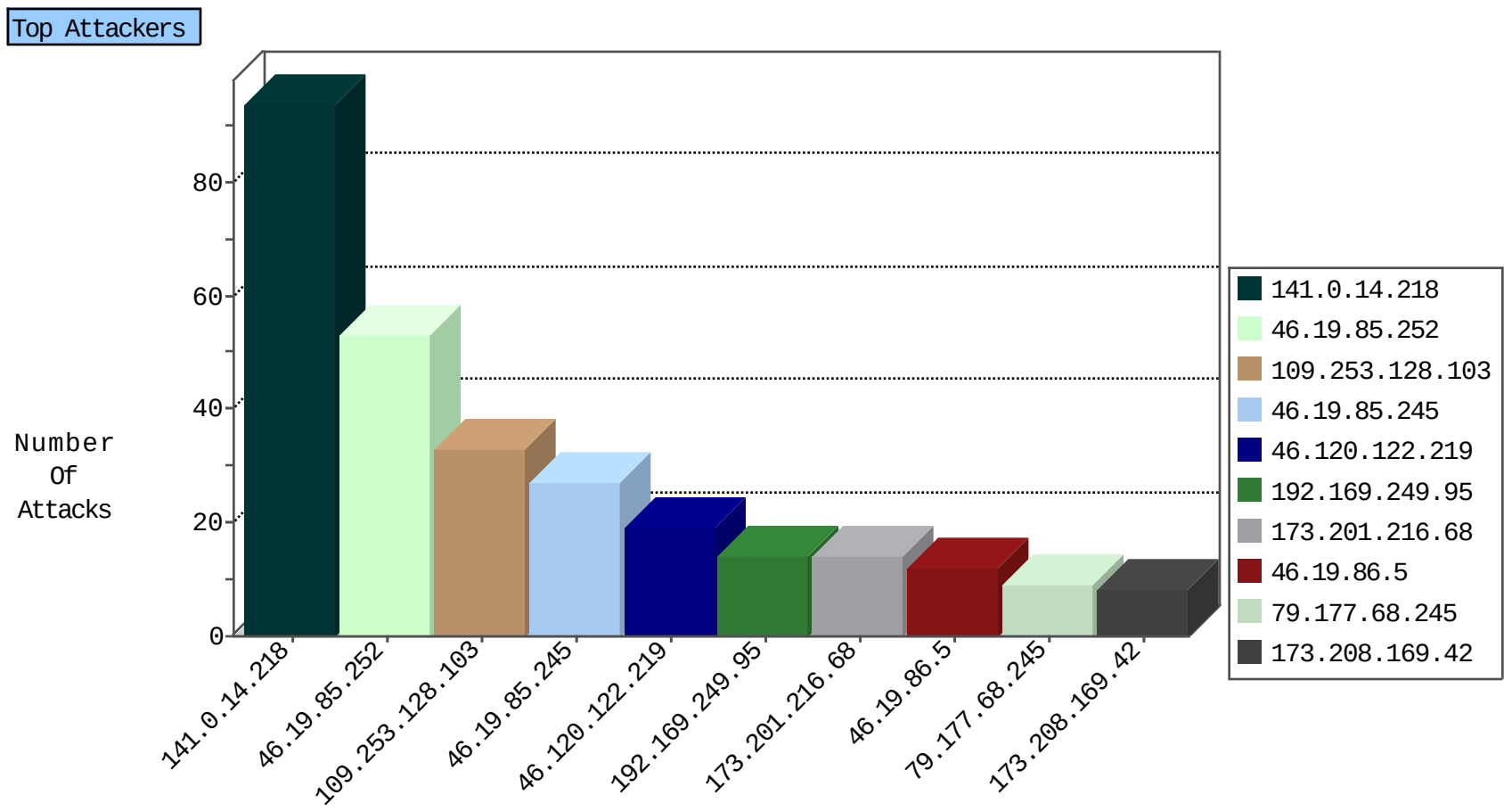
08-29-2016-18:04:01 to 08-29-2016-19:04:01

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-29-2016-18:04:01 to 08-29-2016-19:04:01

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 217.132.111.177 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 6 |
| 209.126.136.2 | United States | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |
| 123.151.42.61 | China | 147.237.76.198 | e.yohalan.idf.il | JLM_Purple_Con_Limit_Udp | drop | 1 |
| 123.151.42.61 | China | 147.237.76.198 | e.yohalan.idf.il | JLM_Under_Attack_Con_Udp | drop | 1 |
| 178.239.62.201 | Netherlands | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 5.79.65.180 | Netherlands | 147.237.76.201 | e.atal.idf.il | Black List | drop | 1 |

08-29-2016-18:04:01 to 08-29-2016-19:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 173.208.169.42 | United States | 147.237.77.233 | atal.idf.i | C1000125: HTTP: Block admin login to gov.il sites ?q=user | Permit | 8 |
| 192.169.249.95 | United States | 147.237.77.233 | atal.idf.i | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 173.201.216.68 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |

08-29-2016-18:04:01 to 08-29-2016-19:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 192.169.249.95 | 147.237.77.233 | United States | atal.idf.il | SQL Injection - Select From | 8 |
| 173.201.216.68 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 8 |
| 154.16.199.49 | 147.237.76.86 | United States | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.199.49 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.236.194.161 | 147.237.77.235 | Czech Republic | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 192.3.177.195 | 147.237.76.177 | United States | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.200.192.50 | 147.237.76.199 | Brazil | e.nakchal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 154.16.199.49 | 147.237.77.216 | United States | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.199.49 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.199.49 | 147.237.76.196 | United States | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.199.49 | 147.237.72.167 | United States | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.195 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 192.3.177.195 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.236.194.161 | 147.237.0.34 | Czech Republic | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 192.3.177.195 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.200.192.50 | 147.237.76.199 | Brazil | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.147 | United Kingdom | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 154.16.199.49 | 147.237.77.74 | United States | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.199.49 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |

08-29-2016-18:04:01 to 08-29-2016-19:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 141.0.14.218 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 94 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 82.166.42.184 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 6 |
| 46.19.85.112 | Israel | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 213.99.33.186 | Spain | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.120.122.219 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 46.120.122.219 | Israel | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 4 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 84.95.208.198 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.120.180.21 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 93.172.205.14 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.251.35 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.201.9 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.120.122.219 | Israel | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 176.13.14.182 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 46.120.122.219 | Israel | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 176.13.15.59 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 46.120.122.219 | Israel | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 176.13.228.69 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 141.212.121.180 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 46.120.122.219 | Israel | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 176.13.244.86 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.135.172 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 54.169.197.38 | Singapore | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 148.75.91.245 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |

08-29-2016-18:04:01 to 08-29-2016-19:04:01

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 53 |
| 109.253.128.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 33 |
| 46.19.85.245 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 27 |
| 46.19.86.5 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 77.139.84.133 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 7 |
| 109.64.82.24 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 80.246.136.188 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 207.46.13.64 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 6 |
| 213.57.59.50 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 80.246.133.147 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 79.177.68.245 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 5 |
| 46.120.38.133 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 79.177.68.245 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 4 |
| 213.151.32.163 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 87.71.29.74 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 77.124.5.23 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 213.57.128.141 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.5 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 3 |
| 2.55.144.165 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.140.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.102.195.129 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.53.179.230 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 82.80.53.190 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation FreeText in www.law.idf.il/421-he/patzar.aspx | Block | 2 |
| 62.219.92.25 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.142.191.197 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 77.138.177.110 | France | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 2 |
| 176.13.11.22 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 32.97.110.60 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 2 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 2 |
| 217.132.124.110 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.139.196 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 148.75.91.245 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 79.177.43.186 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 185.3.147.169 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |
| 79.180.208.2 | Israel | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 1 |
| 5.102.242.3 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 157.55.39.119 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 89.138.102.119 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/news/news.asp | Block | 1 |
| 46.117.226.32 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/layout.css | 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 |
| 2.55.24.226 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 109.66.150.31 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 82.80.53.190 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/724-4738-he/patzar.aspx | Block | 1 |
| 66.102.6.21 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 1 |
| 79.180.208.2 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/wp-login.php | Block | 1 |
| 24.207.173.56 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayallsoldiers.asp | Block | 1 |
| 77.139.89.70 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 66.249.79.16 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/robots.txt | Block | 1 |

08-29-2016-18:04:01 to 08-29-2016-19:04:01