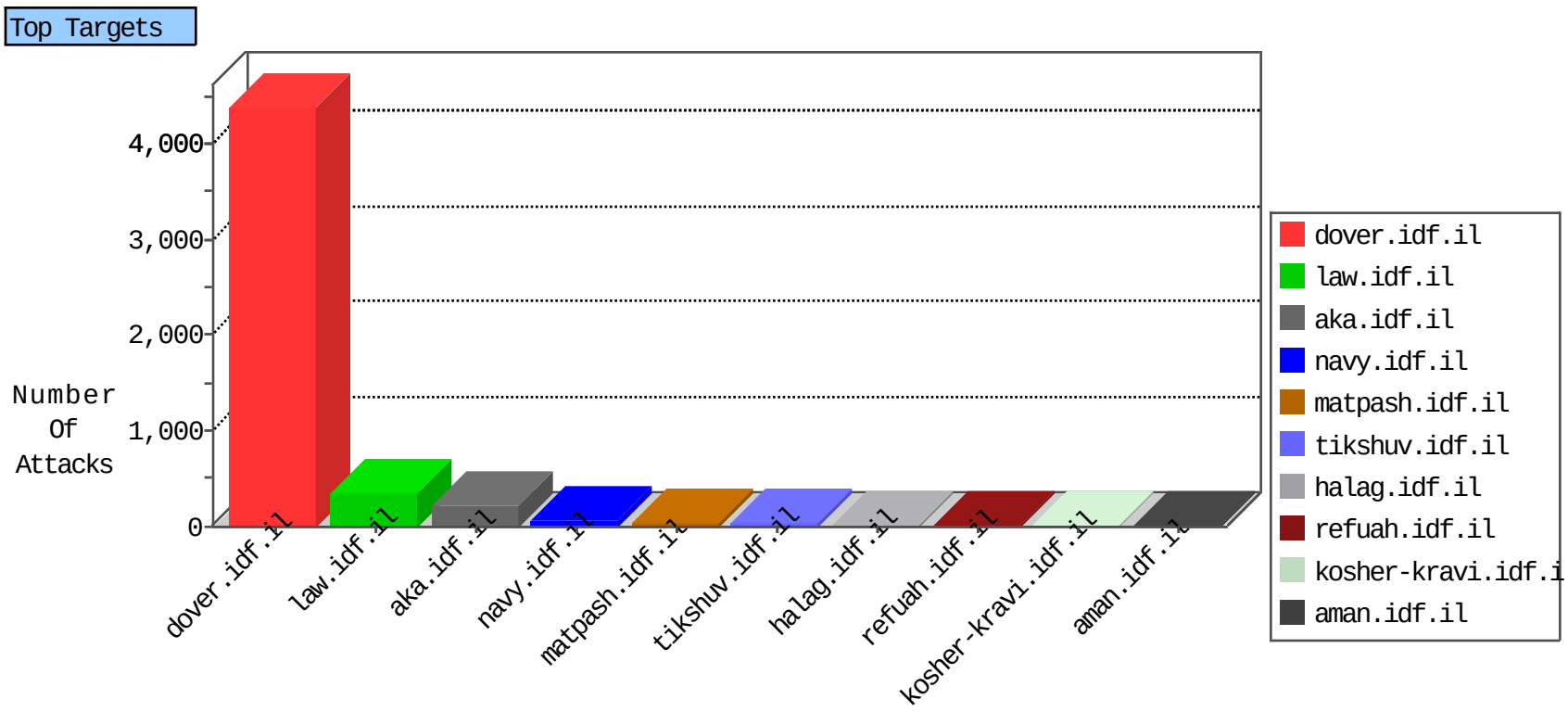
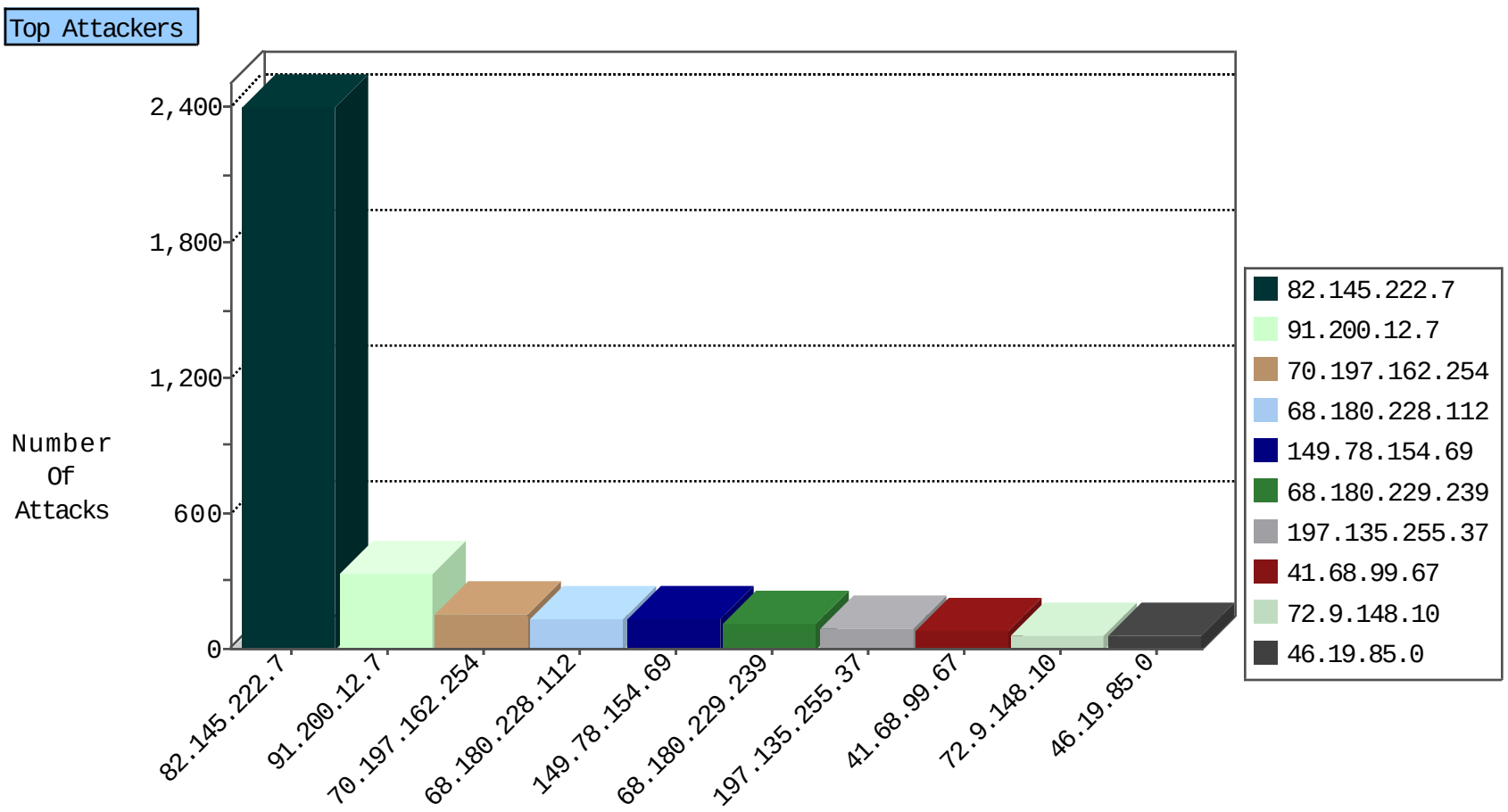
10-22-2015-02:04:02 to 10-22-2015-03:04:02

# IDF Under Attack Daily Report



10-22-2015-02:04:02 to 10-22-2015-03:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 220.181.108.177 | China | 147.237.76.86 | navy.idf.il | TCP handshake violation, first packet not syn | drop | 265 |
| 62.219.254.22 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 68.116.5.134 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

10-22-2015-02:04:02 to 10-22-2015-03:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

10-22-2015-02:04:02 to 10-22-2015-03:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 5 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.84.166 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 187.163.144.167 | 147.237.0.34 | Mexico | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 182.48.105.216 | 147.237.8.24 | China | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 173.193.252.242 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 158.85.158.198 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 111.93.198.54 | 147.237.77.61 | India | e.cogat.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 220.181.108.92 | 147.237.77.216 | China | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 182.48.105.216 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 173.193.252.242 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 169.229.3.91 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 139.162.144.227 | 147.237.0.15 | Netherlands | kosher-kravi.idf.i | ET SCAN Potential SSH Scan | 1 |
| 111.93.198.54 | 147.237.77.61 | India | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.151.55.40 | 147.237.76.147 | Ukraine | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 14.175.102.244 | 147.237.76.42 | Vietnam | refuah.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 201.127.176.159 | 147.237.76.30 | Mexico | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

10-22-2015-02:04:02 to 10-22-2015-03:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 82.145.222.7 | Europe | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 2407 |
| 70.197.162.254 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 148 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 128 |
| 197.135.255.37 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 89 |
| 41.68.99.67 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 84 |
| 95.86.90.29 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 54 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 53 |
| 176.13.5.73 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 38 |
| 185.26.180.207 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 34 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 33 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 31 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 29 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 29 |
| 23.126.102.45 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 28 |
| 24.130.48.144 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 198.58.102.117 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 132.72.233.223 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 25 |
| 86.108.95.192 | Jordan | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 25 |
| 68.196.94.231 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 25 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 207.46.13.178 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 19 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 19 |
| 66.102.8.178 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 18 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 17 |
| 66.102.7.226 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 17 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | SAM rule | drop | 16 |
| 68.4.124.213 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 16 |
| 64.233.172.155 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 15 |
| 93.172.184.58 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |
| 66.249.88.101 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 41.234.80.204 | Egypt | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 199.30.24.219 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 104.131.199.242 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 109.64.200.226 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 109.66.194.3 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 100.40.147.162 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 79.179.144.235 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 37.142.64.48 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 157.55.39.237 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 24.130.241.190 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 207.46.13.178 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 68.189.187.121 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |

10-22-2015-02:04:02 to 10-22-2015-03:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.200.12.7 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 168 |
| 91.200.12.7 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 91.200.12.7 | Block | 154 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 84 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 84 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 56 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 178.255.215.87 | Block | 28 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx | Block | 28 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 28 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal | Block | 14 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 14 |
| 46.19.85.0 | Israel | 147.237.77.216 | dover.idf.il | Abnormally Long Request request version | Block | 14 |
| 194.187.168.19 | Poland | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 66.249.67.65 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.67.65 | Block | 14 |
| 208.115.113.82 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx | Block | 14 |
| 178.255.87.242 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 14 |
| 66.249.78.248 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/robots.txt | Block | 14 |
| 46.19.85.0 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version __atuvc=1%7C42; __atuvs=56281c54676303d9000; _pk_id.20.8afc=860fc0a3fb072567.1445469270.1.1445469270.1445469270.; _pk_ses.20.8afc=* | Block | 14 |
| 207.46.13.39 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx | Block | 14 |
| 66.249.78.102 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx | Block | 14 |
| 212.34.11.4 | Jordan | 147.237.77.176 | matpash.idf.il | Distributed Illegal HTTP Version | Block | 14 |
| 46.19.85.0 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL vvvvvvv=d752a4b9vvvvvvv_d752a4b9; | Block | 14 |
| 207.46.13.46 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 14 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 14 |
| 212.34.11.4 | Jordan | 147.237.77.176 | matpash.idf.il | Distributed Malformed URL | Block | 14 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp | Block | 14 |
| 46.19.85.0 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method .NET_SessionId=wuw01k550to2dnmflba4sm2o; in URL vvvvvvv=d752a4b9vvvvvvv_d752a4b9 | Block | 14 |
| 207.46.13.119 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 14 |
| 91.200.12.7 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/592-4071-en/index.php | Block | 14 |
| 212.34.11.4 | Jordan | 147.237.77.176 | matpash.idf.il | Distributed Unknown HTTP Request Method | Block | 14 |
| 184.154.174.162 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/wp-admin/ | Block | 14 |
| 46.117.63.121 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 14 |
| 208.115.113.82 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in tikshuv.idf.il/site/story.aspx | Block | 14 |

10-22-2015-02:04:02 to 10-22-2015-03:04:02