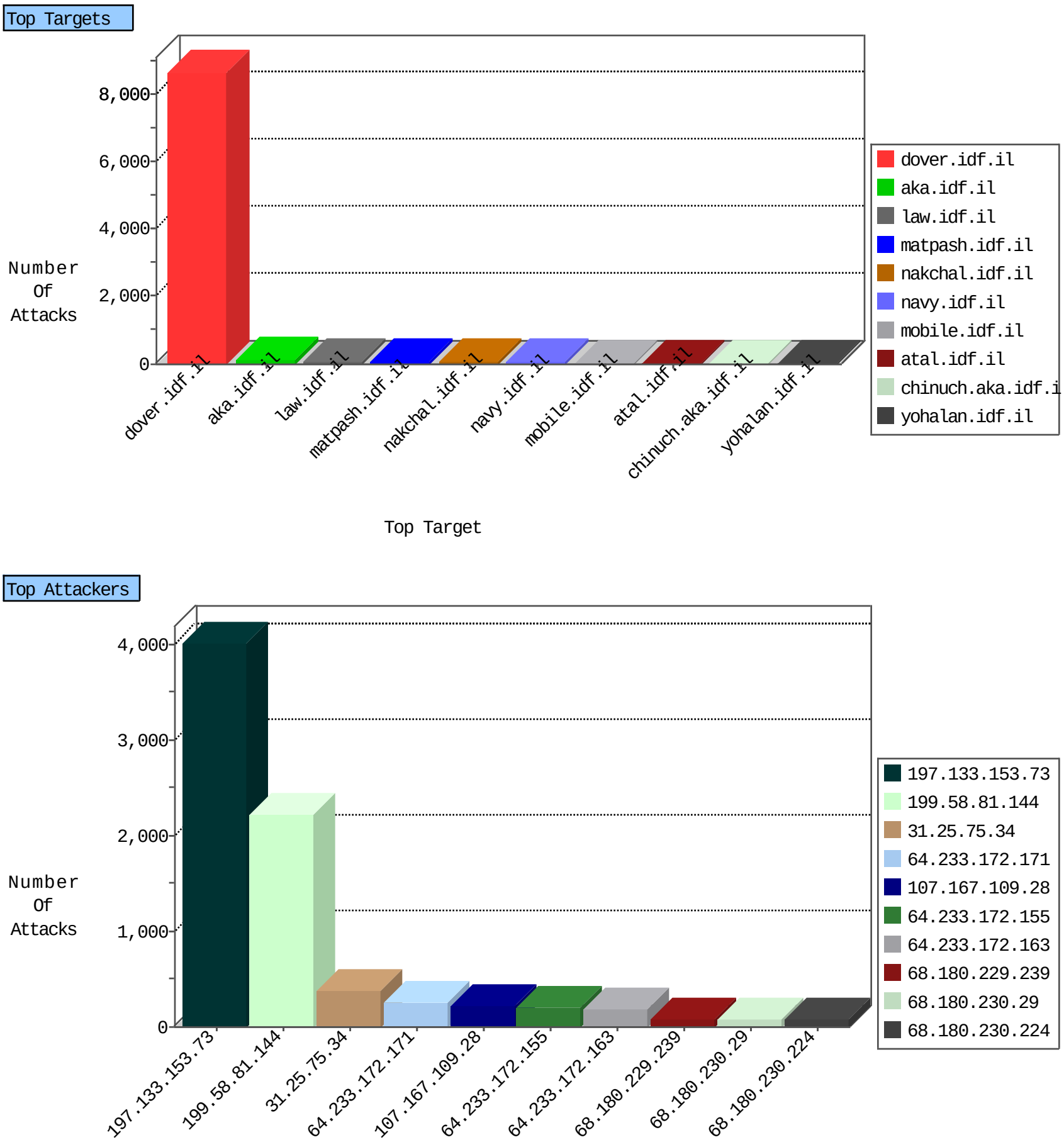
10-22-2015-05:04:03 to 10-22-2015-06:04:03

# IDF Under Attack Daily Report



10-22-2015-05:04:03 to 10-22-2015-06:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.213.152.192 | United States | 147.237.76.30 | himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 162.213.152.192 | United States | 147.237.76.196 | e.sviva.idf.il | Block_Ntp_All_Net | drop | 1 |
| 197.133.153.73 | Egypt | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 1 |

10-22-2015-05:04:03 to 10-22-2015-06:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 199.58.81.144 | Canada | 147.237.77.216 | dover.idf.il | C014: HTTP: Fuck in url | Block | 133 |

10-22-2015-05:04:03 to 10-22-2015-06:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 177.44.189.40 | 147.237.0.16 | Brazil | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 177.44.189.40 | 147.237.0.200 | Brazil | m4u.idf.il | ET SCAN Potential SSH Scan | 2 |
| 177.44.189.40 | 147.237.72.156 | Brazil | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.8.28 | Brazil | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.20.69.98 | 147.237.77.243 | United States | mobile.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 177.44.189.40 | 147.237.0.19 | Brazil | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.68.62.253 | 147.237.77.74 | United Kingdom | law.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.124.35.115 | 147.237.0.19 | Nicaragua | madim.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 177.44.189.40 | 147.237.77.121 | Brazil | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.76.201 | Brazil | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.76.38 | Brazil | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.72.167 | Brazil | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.72.14 | Brazil | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 195.68.62.253 | 147.237.77.176 | United Kingdom | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.44.189.40 | 147.237.0.17 | Brazil | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.242.138.19 | 147.237.0.35 | Portugal | akaws.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 190.124.35.115 | 147.237.0.19 | Nicaragua | madim.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 177.44.189.40 | 147.237.77.74 | Brazil | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.76.176 | Brazil | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.44.189.40 | 147.237.76.34 | Brazil | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |

10-22-2015-05:04:03 to 10-22-2015-06:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.133.153.73 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 3766 |
| 31.25.75.34 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 378 |
| 199.58.81.144 | Canada | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 347 |
| 64.233.172.171 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 259 |
| 107.167.109.28 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 225 |
| 64.233.172.155 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 201 |
| 64.233.172.163 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 192 |
| 197.133.153.73 | Egypt | 147.237.77.216 | dover.idf.i | drop | | drop | 187 |
| 199.58.81.144 | Canada | 147.237.77.216 | dover.idf.i | Block HTTP Non Compliant | Response out of state | monitor | 118 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 81 |
| 105.182.224.13 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 69 |
| 58.172.72.53 | Australia | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 54 |
| 197.133.153.73 | Egypt | 147.237.77.216 | dover.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 52 |
| 99.132.72.114 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 39 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 32 |
| 37.26.146.243 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 31 |
| 85.65.244.190 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 31 |
| 17.142.152.68 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 27 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 24 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 22 |
| 99.132.72.114 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 21 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 54.224.21.23 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 18 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | SAM rule | drop | 17 |
| 176.12.142.30 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 16 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 16 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 16 |
| 17.142.152.85 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 15 |
| 180.166.23.5 | China | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 183.79.219.142 | Japan | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 128.204.23.21 | Russian Federation | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 17.142.152.89 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 13 |
| 32.42.15.123 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 13 |
| 198.58.96.215 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 89.138.226.39 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 162.243.199.26 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 17.142.145.3 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 17.142.152.72 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 66.152.117.140 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 93.172.184.58 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 197.133.153.73 | Egypt | 147.237.77.216 | dover.idf.i | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 17.142.152.111 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 66.152.117.140 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 17.142.152.94 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |

10-22-2015-05:04:03 to 10-22-2015-06:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 199.58.81.144 | Canada | 147.237.77.216 | dover.idf.il | Multiple Unknown HTTP Request Method from 199.58.81.144 | Block | 1611 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx | Block | 84 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx | Block | 84 |
| 68.180.230.224 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx | Block | 84 |
| 72.9.148.10 | 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 | 56 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx | Block | 42 |
| 157.55.39.101 | United States | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 28 |
| 91.200.12.9 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 28 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 28 |
| 199.58.81.144 | Canada | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method fuck in URL | Block | 14 |
| 157.55.39.13 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 184.105.247.196 | United States | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to 147.237.77.243/ | Block | 14 |
| 91.200.12.9 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 91.200.12.9 | Block | 14 |
| 31.193.51.78 | France | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 207.46.13.178 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/news/main | Block | 14 |
| 188.143.232.10 | Russian Federation | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx | Block | 14 |
| 66.249.67.27 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 14 |
| 178.255.87.242 | United Kingdom | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to 147.237.77.243/robots.txt | Block | 14 |
| 188.143.232.22 | Russian Federation | 147.237.72.166 | aka.idf.il | Suspicious Response Code_Custom_Temporary | Block | 14 |
| 91.200.12.9 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/307.pdf/xmlrpc.php | Block | 14 |
| 66.249.67.46 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 14 |
| 180.76.15.145 | China | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to atal.idf.il/shared/clientscripts/{1} | Block | 14 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 183.79.219.142 | Japan | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |

10-22-2015-05:04:03 to 10-22-2015-06:04:03