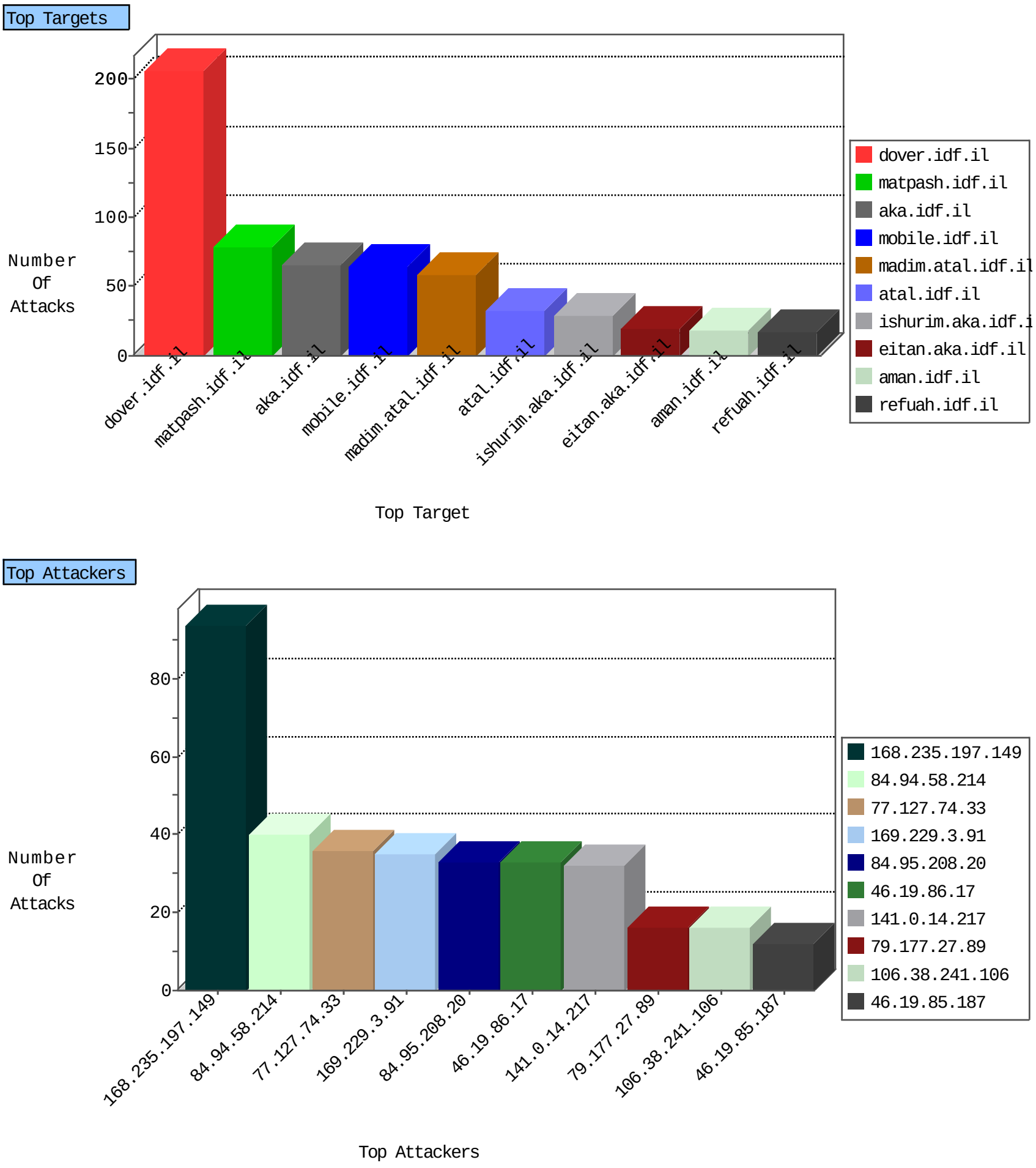
10-01-2016-13:04:02 to 10-01-2016-14:04:02

# IDF Under Attack
# Daily Report



10-01-2016-13:04:02 to 10-01-2016-14:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 168.235.197.149 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 168.235.197.149 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 85.250.214.228 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 123.151.42.61 | China | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets_Con_Limit | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 66.240.192.138 | United States | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 218.93.206.21 | China | 147.237.77.234 | halag.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 168.235.197.149 | United States | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |

10-01-2016-13:04:02 to 10-01-2016-14:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 220.181.125.23 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 9 |
| 108.59.8.80 | United States | 147.237.77.234 | halag.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 5.9.111.70 | Germany | 147.237.76.200 | eitan.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

10-01-2016-13:04:02 to 10-01-2016-14:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 202.112.38.190 | 147.237.76.197 | China | e.himush.idf.il | GPL SCAN nmap TCP | 2 |
| 58.214.232.91 | 147.237.72.156 | China | aman.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 2 |
| 46.120.122.219 | 147.237.76.200 | Israel | eitan.aka.idf.il | Xenu Link Sleuth User Agent | 2 |
| 146.200.148.0 | 147.237.77.216 | United Kingdom | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 62.210.243.100 | 147.237.0.200 | France | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.220.2.5 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 54.198.176.57 | 147.237.77.216 | United States | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 1 |
| 217.23.1.12 | 147.237.76.199 | Netherlands | e.nakchal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 217.23.1.12 | 147.237.76.199 | Netherlands | e.nakchal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 209.95.50.84 | 147.237.77.74 | United States | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.23.48.64 | 147.237.8.27 | Vietnam | e.madim.atal.idf.i | ET SCAN NMAP -sS window 4096 | 1 |
| 62.210.243.100 | 147.237.8.46 | France | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.220.2.5 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 217.23.1.12 | 147.237.77.205 | Netherlands | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 217.23.1.12 | 147.237.76.199 | Netherlands | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 217.23.1.12 | 147.237.76.148 | Netherlands | gqcenter.aka.idf.i | ET SCAN NMAP -sS window 3072 | 1 |
| 208.100.26.228 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.23.48.64 | 147.237.8.27 | Vietnam | e.madim.atal.idf.i | ET SCAN NMAP -sS window 1024 | 1 |

10-01-2016-13:04:02 to 10-01-2016-14:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.197.149 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 84 |
| 77.127.74.33 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 141.0.14.217 | Europe | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 32 |
| 79.177.27.89 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 16 |
| 46.19.86.17 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 85.65.201.15 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.86.17 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 46.19.86.17 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 6 |
| 46.19.85.187 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 66.249.79.6 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.187 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 132.66.235.87 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 106.38.241.106 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 6 |
| 109.253.139.182 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 168.235.197.149 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.86.190 | Israel | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 217.132.3.63 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.116.139.25 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 213.57.97.233 | Israel | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 84.95.33.244 | Israel | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.17 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 46.19.85.214 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.65.10 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 213.8.204.64 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.18 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 213.57.140.216 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.253.139.182 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 3 |
| 46.19.85.32 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.154.49.81 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 77.126.14.141 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.17 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 41.46.177.177 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.247.130 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 37.26.147.173 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 80.246.139.175 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 85.64.199.220 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 109.253.139.182 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 87.68.243.174 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 176.13.242.217 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 2.55.18.111 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 27.34.84.89 | Nepal | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 46.19.86.76 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.85.123 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 46.19.86.125 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 77.138.237.88 | France | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |

10-01-2016-13:04:02 to 10-01-2016-14:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.94.58.214 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 39 |
| 46.117.161.48 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 7 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 4 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 3 |
| 46.19.85.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 104.145.239.82 | Canada | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/ | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 109.64.51.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 189.236.218.53 | Mexico | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 2 |
| 213.8.204.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 89.237.69.75 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx | Block | 2 |
| 213.8.204.64 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 77.139.75.232 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | Multiple Unknown HTTP Request Method from 169.229.3.91 | Block | 1 |
| 5.22.134.156 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/ | Block | 1 |
| 204.79.180.217 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main/ | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Multiple Abnormally Long Request from 169.229.3.91 | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | Distributed Malformed URL | Block | 1 |
| 46.120.113.100 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/robots.txt | Block | 1 |
| 220.181.125.23 | China | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | Multiple Abnormally Long Request from 169.229.3.91 | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | NULL Character in Method OÕ[[#0]]ewJÍ§)û[[#16]]£°*ÿškB | Block | 1 |
| 87.69.40.21 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.233 | atal.idf.il | Multiple Abnormally Long Request from 169.229.3.91 | Block | 1 |
| 77.237.138.202 | Czech Republic | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to / | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Abnormally Long Request method | Block | 1 |
| 31.154.81.63 | Israel | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 1 |
| 207.46.13.11 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 147.237.76.86/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Multiple Illegal Byte Code Character in Header Name from 169.229.3.91 | Block | 1 |
| 84.108.122.44 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx | None | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 46.120.122.219 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx | None | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | Multiple Illegal Byte Code Character in Header Name from 169.229.3.91 | Block | 1 |
| 87.69.222.132 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.233 | atal.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Illegal Byte Code Character in Method P¼"[[#6]]•(ÈHÌ>[ ¯Ckù£¿É"¤ÖMû/Û"„V | Block | 1 |
| 79.180.116.132 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/null | Block | 1 |
| 109.66.105.19 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 31.154.81.63 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 84.108.127.51 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 68.180.228.238 | United States | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |

10-01-2016-13:04:02 to 10-01-2016-14:04:02