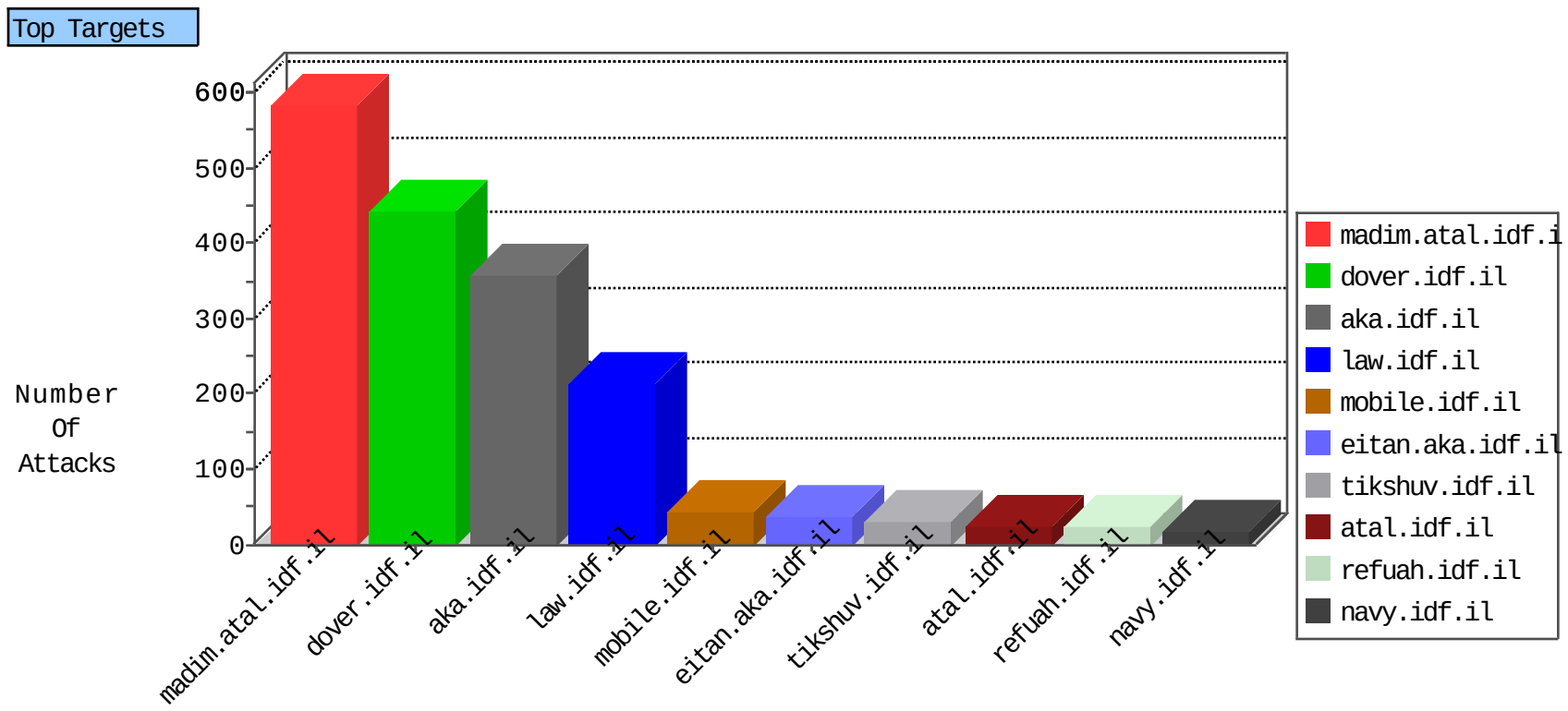
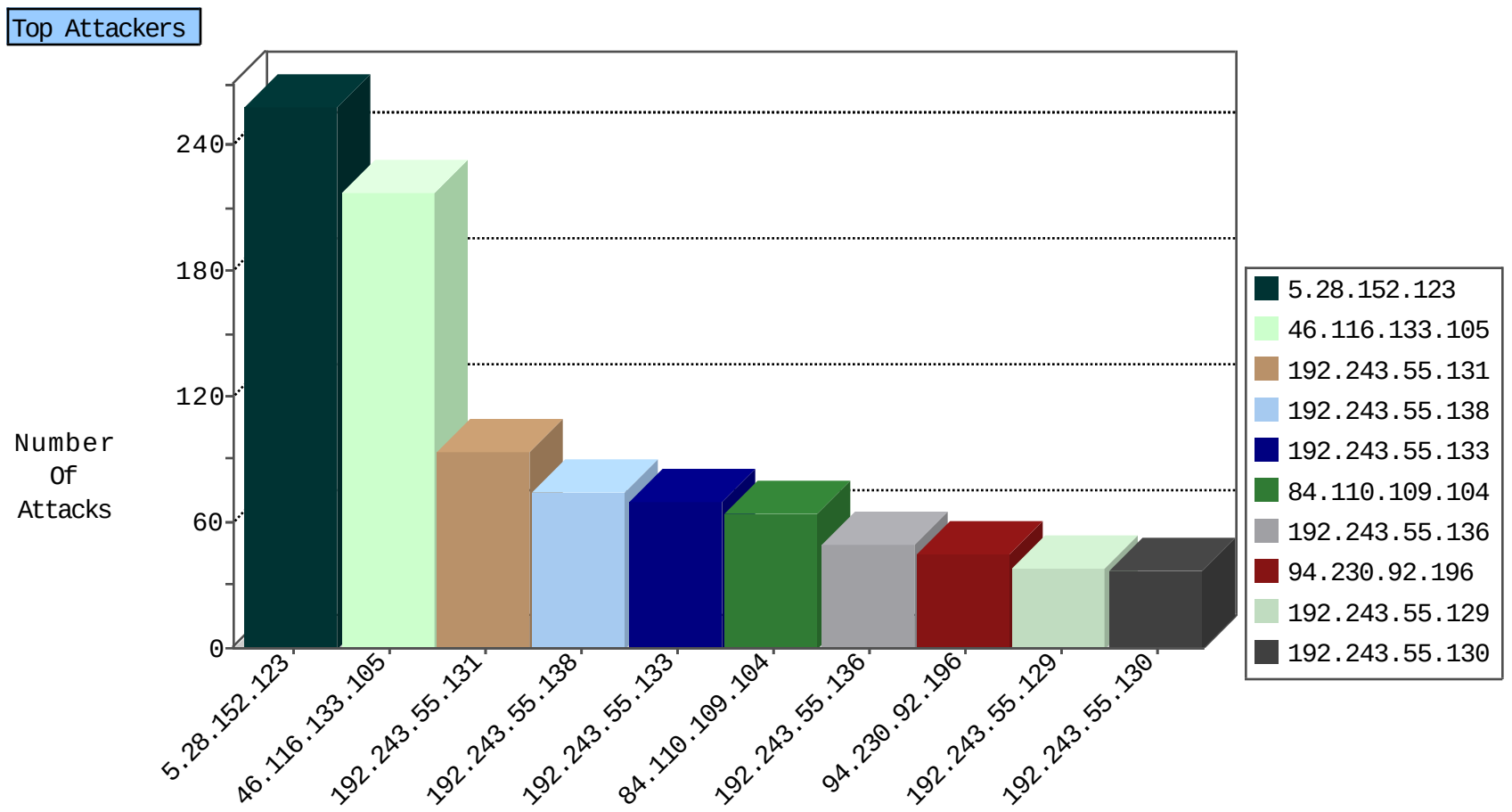
02-20-2016-19:04:02 to 02-20-2016-20:04:02

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



02-20-2016-19:04:02 to 02-20-2016-20:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.132.229.15 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 119.142.236.243 | China | 147.237.76.86 | navy.idf.il | Block_Udp_All_Nets | drop | 2 |
| 115.239.228.10 | China | 147.237.76.86 | navy.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 80.93.126.203 | Ukraine | 147.237.76.148 | gqcenter.aka.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 66.249.78.160 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 80.93.126.203 | Ukraine | 147.237.76.198 | e.yohalan.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 80.93.126.203 | Ukraine | 147.237.8.14 | e.orchot.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 80.93.126.203 | Ukraine | 147.237.76.39 | mobile.meitav.idf.il | L4 Source or Dest Port Zero | drop | 1 |

02-20-2016-19:04:02 to 02-20-2016-20:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 64.251.25.176 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 64.251.25.176 | United States | 147.237.77.216 | dover.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 69.30.213.18 | United States | 147.237.72.166 | aka.idf.il | C1000106: HTTP: majestic bot | Block | 2 |
| 69.30.213.18 | United States | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 2 |
| 84.111.159.126 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000212: HTTP: prefix 1.01 in the URL | Block | 2 |
| 31.168.144.34 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000212: HTTP: prefix 1.01 in the URL | Block | 2 |
| 109.64.190.192 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000212: HTTP: prefix 1.01 in the URL | Block | 1 |
| 46.117.156.218 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |
| 123.126.68.115 | China | 147.237.77.216 | dover.idf.il | C1000103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 151.80.31.117 | Italy | 147.237.0.15 | kosher-kravi.idf.il | C1000228: HTTP:  AhrefBot crawler | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.187 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000212: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000103: HTTP: User Agent Sogou+web+spider | Block | 1 |

02-20-2016-19:04:02 to 02-20-2016-20:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 64.251.25.176 | 147.237.77.216 | United States | dover.idf.il | SQL Injection - Select From | 12 |
| 64.251.25.176 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 9 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 45.32.84.108 | 147.237.8.45 | | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 212.199.151.146 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 45.32.84.108 | 147.237.0.19 | | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 40.117.40.240 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.61.109.189 | 147.237.76.86 | China | navy.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 125.227.64.115 | 147.237.0.15 | Taiwan | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.44.133.108 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 81.169.245.171 | 147.237.0.19 | Germany | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 45.32.84.108 | 147.237.76.38 | | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 45.32.84.108 | 147.237.0.33 | | idf.il | ET SCAN Potential SSH Scan | 1 |
| 208.80.155.217 | 147.237.77.216 | United States | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 45.32.84.108 | 147.237.0.16 | | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.61.109.189 | 147.237.76.86 | China | navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 31.210.188.10 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.88.138.225 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.44.133.108 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 87.106.248.49 | 147.237.76.44 | Germany | e.refuah.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 45.32.84.108 | 147.237.76.148 | | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |

02-20-2016-19:04:02 to 02-20-2016-20:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 25 |
| 185.3.144.46 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 89.139.233.108 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 107.167.106.22 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 19 |
| 85.130.141.48 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 18 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 46.116.133.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 15 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.19.85.210 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 13 |
| 46.19.85.84 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 192.243.55.136 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 192.243.55.132 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 84.228.95.138 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 109.65.174.4 | Israel | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 109.64.18.186 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.177.20.193 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 91.135.102.191 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 84.108.58.128 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 91.135.102.191 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 192.243.55.136 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.129 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 79.182.96.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.132 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 2.52.22.32 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.178.70.215 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.199.218.50 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 84.108.42.69 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 188.120.154.51 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 192.243.55.130 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 79.180.112.238 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.28.152.123 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 135 |
| 46.116.133.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 106 |
| 5.28.152.123 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 104 |
| 46.116.133.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 93 |
| 84.110.109.104 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 27 |
| 84.110.109.104 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 19 |
| 84.110.109.104 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 18 |
| 79.180.52.194 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 5.28.152.123 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 17 |
| 109.186.181.86 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 109.186.181.86 | Block | 14 |
| 176.13.4.109 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 176.13.4.109 | None | 11 |
| 46.19.85.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 2.52.144.249 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.116.133.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 4 |
| 5.29.43.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.177.218.68 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.133.192 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 5.28.152.123 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 3 |
| 109.65.174.4 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 109.65.174.4 | Block | 2 |
| 5.29.160.112 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 17.138.56.26 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.138.56.26 | Block | 2 |
| 213.8.204.65 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Multiple Unauthorized URL Access from 213.8.204.65 | Block | 2 |
| 46.99.125.164 | Albania | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Abnormally Long Header Line request header name | Block | 1 |
| 2.54.151.197 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx | Block | 1 |
| 104.131.211.161 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/14-he | Block | 1 |
| 80.246.136.39 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 78.154.170.2 | Ukraine | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp | None | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Multiple NULL Character in Header Name from 94.230.92.196 | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Malformed HTTP Header Line 4 | Block | 1 |
| 46.117.109.75 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/error/styles/ | Block | 1 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/iraq/english/info07.asp | Block | 1 |
| 85.65.207.247 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx | Block | 1 |
| 149.254.56.57 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Unknown HTTP Request Method 'ÂµÃ¼[[#17]]Ã»%Ã¯Ã‡Â?,o5[[#25]]Ã“[[#4]]wÃƒÂ, in URL ydh×?[[#0]]ÃŠqn(Ö¸=Ö³uÃ?93nÂ»gÂ¶Â¦×˜nnÃ»0×“^0[[#22]]Â?â€¦3b×?Ã·Â?×•cÃž[[#12]]ËœÂ¯ÂŒ×€/Ö°h7â„¢Â?Ã·"â€ž}×©â€¹Ö½Ã¼w}×?(Â¶kvpb×°Æ'@d[[#7]]â€Ž | Block | 1 |
| 79.183.7.21 | Israel | 147.237.77.233 | atal.idf.il | Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Header Value from 94.230.92.196 | Block | 1 |
| 65.55.210.193 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 199.73.63.142 | Jamaica | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.99.125.164 | Albania | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 185.72.217.89 |  | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Abnormally Long Request method | Block | 1 |
| 84.108.42.69 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 94.230.92.196 | Block | 1 |
| 94.230.92.196 | Israel | 147.237.72.166 | aka.idf.il | Malformed URL ydh×?[[#0]]ÃŠqn(Ö¸=Ö³uÃ?93nÂ»gÂ¶Â¦×˜nnÃ»0×“^0[[#22]]Â?â€¦3b×?Ã·Â?×•cÃž[[#12]]ËœÂ¯ÂŒ×€/Ö°h7â„¢Â?Ã·"â€ž}×©â€¹Ö½Ã¼w}×?(Â¶kvpb×°Æ'@d[[#7]]â€Ž | Block | 1 |
| 46.120.73.203 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/https:/mobile.idf.il/ | Block | 1 |
| 195.154.146.225 | France | 147.237.77.74 | law.idf.il | Illegal HTTP Version HTTP/ | Block | 1 |
| 86.97.148.123 | United Arab Emirates | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 149.254.56.57 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |