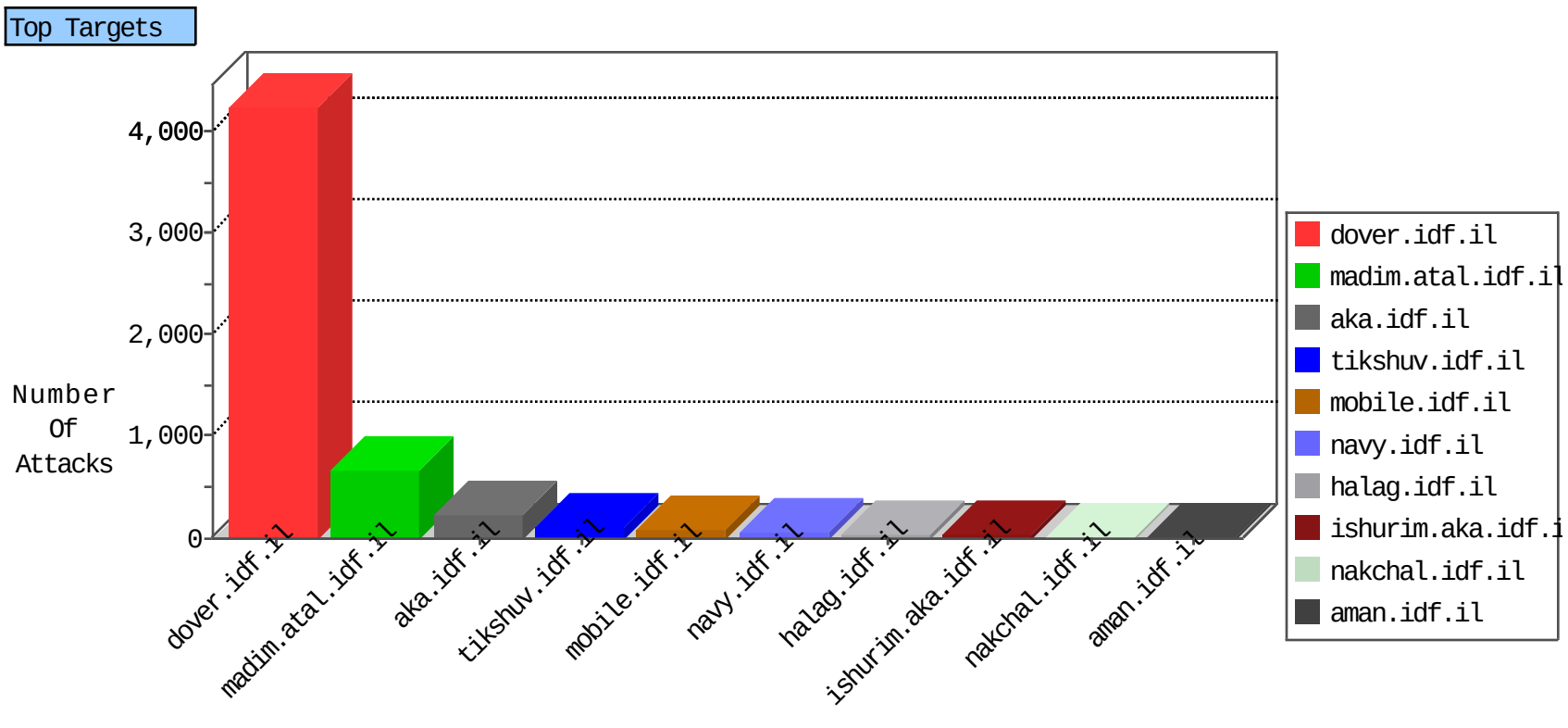
04-13-2016-19:04:01 to 04-13-2016-20:04:01

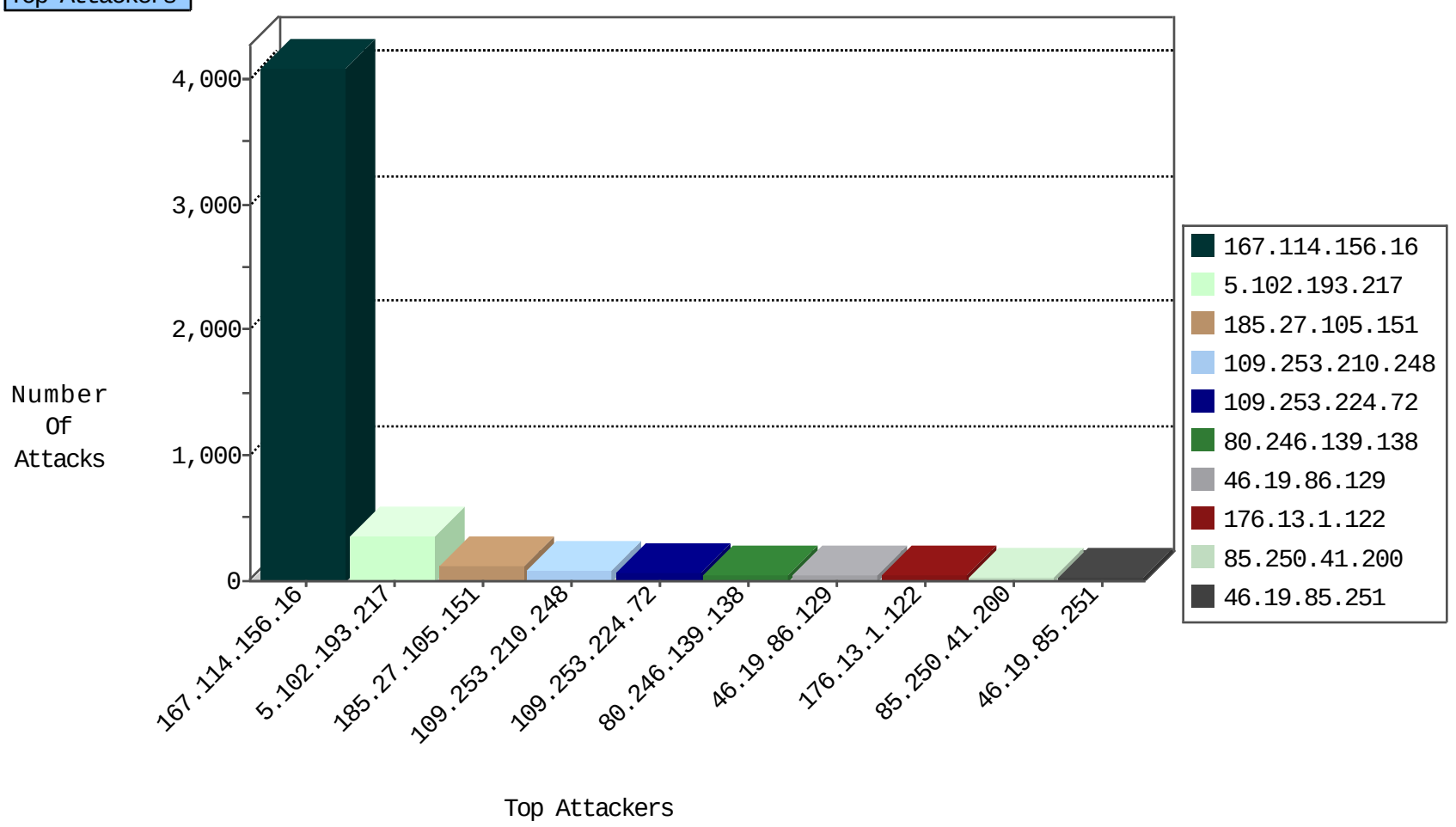
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

04-13-2016-19:04:01 to 04-13-2016-20:04:01

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 4074 |
| 79.181.215.254 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 79.181.215.254 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 37.26.146.156 | Israel | 147.237.72.166 | aka.idf.il | Invalid TCP Flags | drop | 3 |
| 66.240.219.146 | United States | 147.237.77.179 | e.mazi.idf.il | Block_Udp_All_Nets | drop | 1 |
| 37.28.152.58 | Poland | 147.237.77.121 | e.navy.idf.il | Block_Ntp_All_Net | drop | 1 |
| 41.102.211.208 | Algeria | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Url | dest-reset | 1 |

04-13-2016-19:04:01 to 04-13-2016-20:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.58.71 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 89.138.105.47 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 46.19.85.145 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 66.249.66.158 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 41.102.211.208 | Algeria | 147.237.77.216 | dover.idf.il | 0361: HTTP: Protected File Access (/etc/passwd) | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.154 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |

04-13-2016-19:04:01 to 04-13-2016-20:04:01

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 | 9 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 62.219.115.215 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.216.176.244 | 147.237.8.28 | Latvia | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 13.92.100.128 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 185.3.147.111 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.55.22.49 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.216.57 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 107.158.255.194 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 107.158.255.194 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 104.171.122.176 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 99.95.129.139 | 147.237.76.30 | United States | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 220.231.195.122 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 84.200.15.174 | 147.237.77.235 | Germany | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.216.176.244 | 147.237.8.45 | Latvia | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.22.130.251 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 152.97.175.251 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 107.158.255.194 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 107.158.255.194 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -f -sS | 1 |
| 104.171.122.176 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 104.171.122.176 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -f -sS | 1 |
| 84.200.15.174 | 147.237.77.235 | Germany | sviva.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 202.67.237.220 | 147.237.8.28 | Hong Kong | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |

04-13-2016-19:04:01 to 04-13-2016-20:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.253.224.72 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 69 |
| 46.19.86.129 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 85.250.41.200 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 33 |
| 176.13.1.122 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 109.253.224.73 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 176.13.12.163 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 87.70.52.243 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.53.160.46 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.13.7.232 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 85.250.50.254 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 11 |
| 46.19.86.229 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 77.127.30.59 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 46.19.85.251 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.80 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 176.13.10.231 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.4 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 176.13.15.13 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.1.122 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 82.81.209.165 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.251 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.80 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.251 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.80 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.80 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 176.13.7.232 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.4 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.251 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.85.4 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 185.106.92.47 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | drop | SAM rule | drop | 5 |
| 46.19.85.4 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 5.22.130.246 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 85.130.183.32 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.86.18 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 4 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 80.178.204.62 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 41.102.211.208 | Algeria | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 46.19.86.18 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 4 |
| 149.88.37.22 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.53.55.41 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.96.177 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.27.105.151 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.242.24 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 176.13.1.122 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 5.22.131.9 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 82.81.77.251 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-13-2016-19:04:01 to 04-13-2016-20:04:01

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.102.193.217 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 358 |
| 185.27.105.151 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 108 |
| 109.253.210.248 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 82 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 32 |
| 46.19.86.46 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 16 |
| 46.19.86.2 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 176.13.22.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 46.19.86.129 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 6 |
| 157.55.39.217 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 46.19.85.63 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.175.192 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 91.200.12.79 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 3 |
| 46.19.86.150 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.146.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.55.129.183 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.88 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.16.199 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.183.96.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 134.134.139.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 91.200.12.79 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 91.200.12.79 | Block | 2 |
| 46.19.86.140 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.200.90 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.186.41.242 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 134.134.137.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 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 | 2 |
| 65.55.213.30 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 77.75.77.101 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/page/34/ | Block | 1 |
| 187.115.163.250 | Brazil | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wp-login.php | Block | 1 |
| 170.140.105.70 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 185.3.144.33 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png | Block | 1 |
| 66.249.69.26 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 134.134.139.82 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.127.30.59 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 176.13.7.232 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 84.109.176.26 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 157.55.39.54 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 91.200.12.79 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/wp-login.php | Block | 1 |
| 77.237.138.202 | Czech Republic | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to / | Block | 1 |
| 46.19.86.229 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.13.10.231 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 110.86.186.223 | China | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 1 |
| 41.102.211.208 | Algeria | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he/dover.aspx' | Block | 1 |
| 85.250.41.200 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 185.32.179.182 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/smalim/resources/styles/showbigstyle.css | Block | 1 |
| 157.55.39.199 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 2.55.168.6 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 79.177.100.152 | Israel | 147.237.76.86 | navy.idf.il | Cookie Tampering on cookie __atrfs: Expected ab/ | None | 1 |

04-13-2016-19:04:01 to 04-13-2016-20:04:01