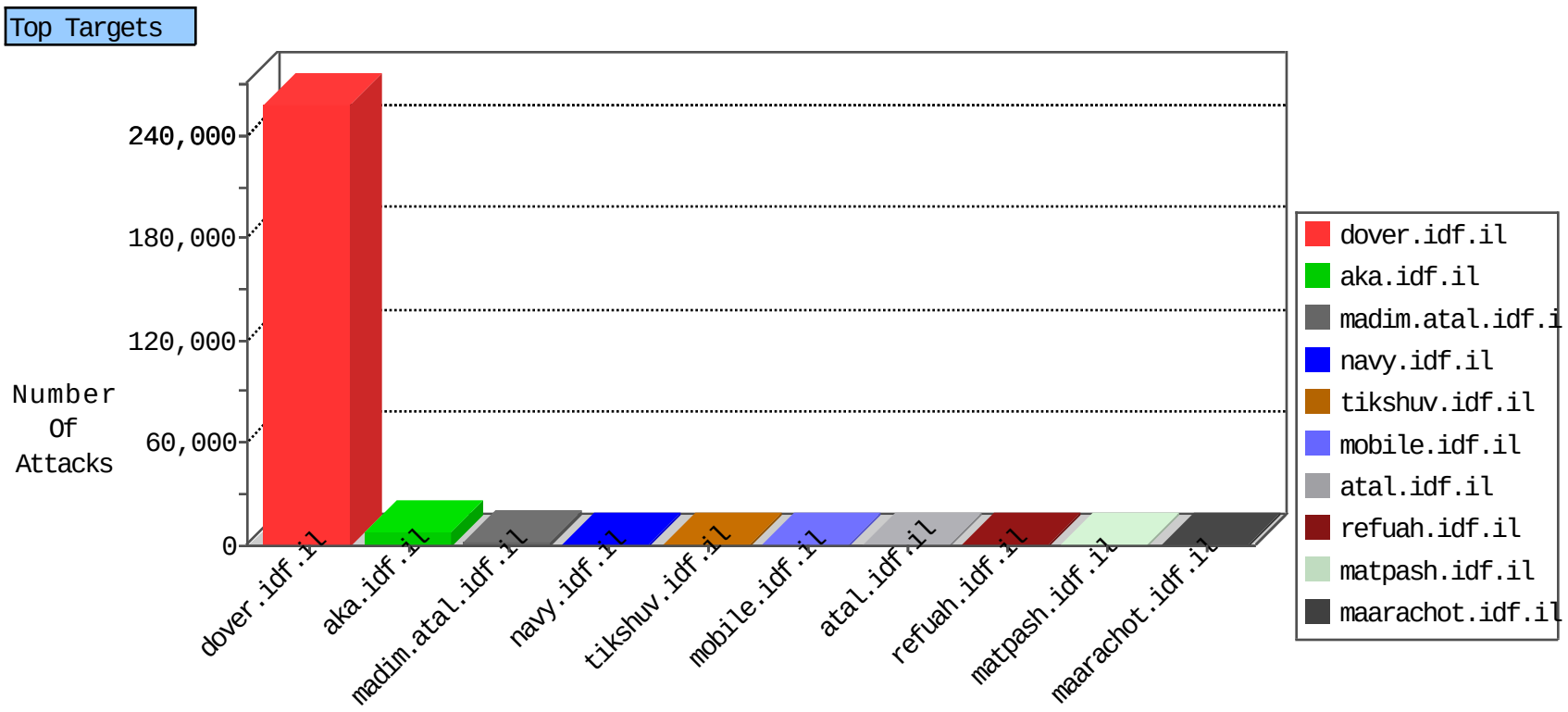
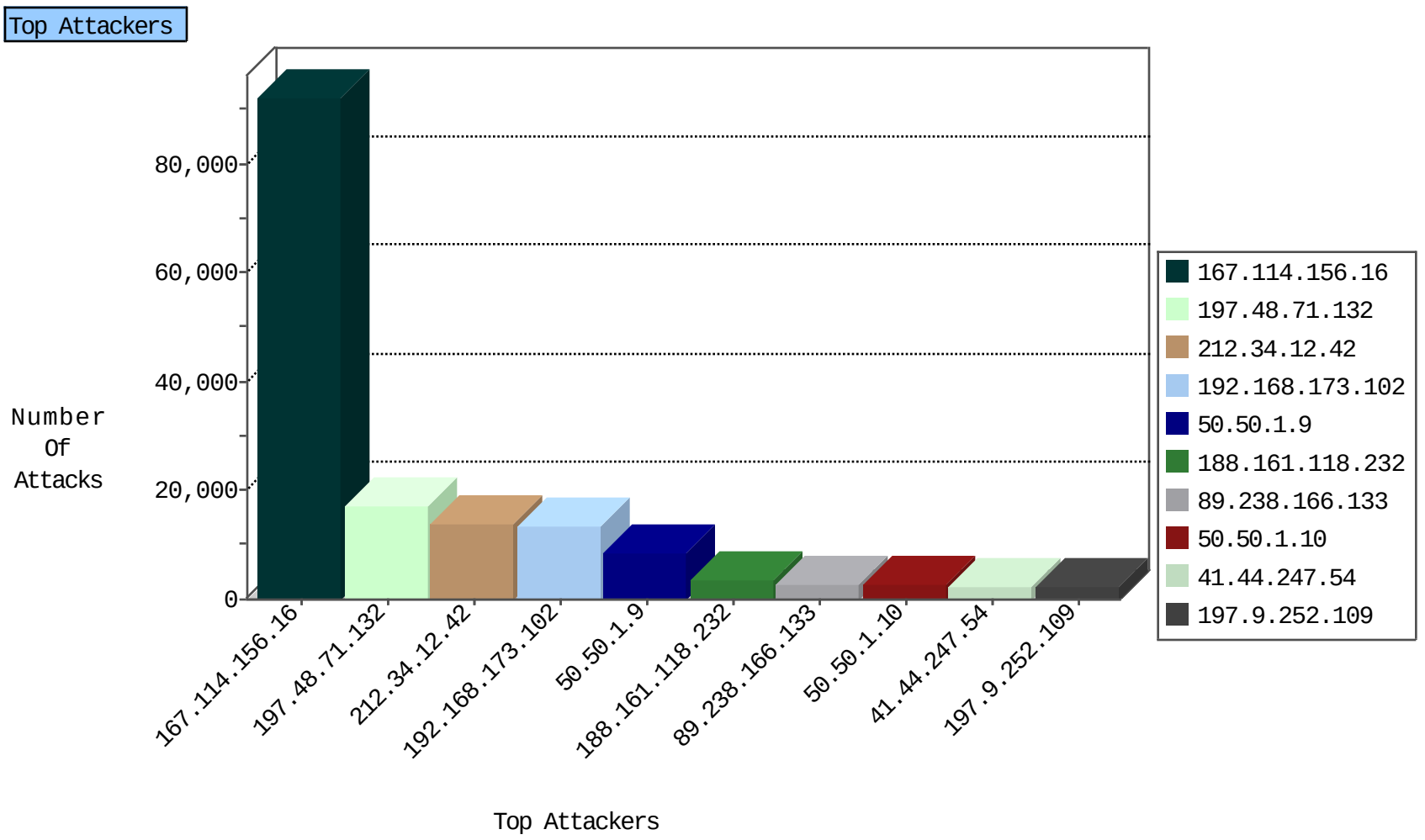
04-08-2016 to 04-09-2016

# IDF Under Attack Daily Report

Top Targets




Top Attackers



04-08-2016 to 04-09-2016

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.60.147.79 | Switzerland | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 98981 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 92268 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 25486 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 6736 |
| 188.55.204.168 | Saudi Arabia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 5171 |
| 130.211.134.65 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4579 |
| 173.77.16.91 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4123 |
| 2.53.10.182 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3161 |
| 134.35.172.113 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3150 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3033 |
| 52.23.215.54 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2944 |
| 89.238.166.133 | United Kingdom | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 2609 |
| 201.92.15.72 | Brazil | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 2388 |
| 199.47.125.84 | Canada | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2158 |
| 106.186.115.90 | Japan | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2002 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1968 |
| 37.26.146.238 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1408 |
| 89.238.166.133 | United Kingdom | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1362 |
| 87.69.195.171 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1145 |
| 172.56.13.206 | United States | 147.237.0.34 | tikshuv.idf.il | TCP handshake violation, first packet not syn | drop | 1106 |
| 46.43.126.188 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | HTTP-MISC-DoS-GoodBye-30 | dest-reset | 1101 |
| 54.94.252.114 | Brazil | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1010 |
| 213.229.73.244 | United Kingdom | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 934 |
| 37.76.221.20 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 800 |
| 176.2.134.161 | Germany | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 766 |
| 212.34.12.42 | Jordan | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 694 |
| 104.197.101.166 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 568 |
| 156.205.17.252 | Egypt | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 545 |
| 89.238.143.70 | United Kingdom | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 525 |
| 108.59.83.170 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 520 |
| 188.161.118.232 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 502 |
| 191.239.6.183 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 499 |
| 191.239.218.221 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 330 |
| 212.126.112.37 | Iraq | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 269 |
| 79.177.236.12 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 252 |
| 149.78.169.36 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 171 |
| 128.199.144.177 | Singapore | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 153 |
| 52.17.98.103 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 137 |
| 54.76.190.11 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 117 |
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 91 |
| 79.177.181.5 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 85 |
| 52.32.129.70 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 62 |
| 79.183.149.64 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 62 |
| 46.32.121.115 | Jordan | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 58 |
| 41.44.247.54 | Egypt | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 56 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 51 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 51 |
| 52.29.55.227 | Germany | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 41 |
| 212.34.12.42 | Jordan | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 34 |
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 29 |

04-08-2016 to 04-09-2016

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 24 |
| 85.64.249.42 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 16 |
| 46.120.2.93 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 14 |
| 123.126.113.109 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 11 |
| 213.8.204.29 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 11 |
| 46.121.115.4 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 11 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 10 |
| 106.38.241.150 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 10 |
| 149.50.122.164 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 10 |
| 109.64.223.223 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 9 |
| 132.66.237.92 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 9 |
| 207.46.13.45 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 9 |
| 5.28.187.52 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 79.177.235.221 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 79.178.178.180 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 109.65.1.251 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 84.228.245.181 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 5.102.242.160 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 84.228.248.18 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 149.78.42.56 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 2.53.15.51 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 109.253.128.85 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 208.83.7.157 | United States | 147.237.77.216 | dover.idf.il | 12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack) | Block | 6 |
| 162.213.152.176 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 40.76.83.187 | United States | 147.237.76.30 | himush.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 162.213.152.216 | United States | 147.237.0.19 | madim.atal.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 162.213.152.176 | United States | 147.237.0.19 | madim.atal.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 162.213.152.176 | United States | 147.237.0.15 | kosher-kravi.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 162.213.152.216 | United States | 147.237.0.15 | kosher-kravi.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 46.117.20.148 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 87.69.19.30 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 109.253.136.216 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 213.8.204.32 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 46.120.36.93 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 79.183.149.64 | Israel | 147.237.77.216 | dover.idf.il | 12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack) | Block | 4 |
| 66.249.78.134 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 151.80.44.115 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 4 |
| 213.8.204.34 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 185.120.125.47 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 91.198.143.123 | Ukraine | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Block | 4 |
| 84.108.205.84 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 66.249.66.59 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 163.172.15.135 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 3 |
| 69.30.234.2 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 176.228.201.184 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 151.80.44.115 | France | 147.237.76.147 | chinuch.aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 195.154.187.115 | France | 147.237.72.167 | ishurim.aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 37.26.148.134 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 136.243.152.18 | Germany | 147.237.76.42 | refuah.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 66.249.78.120 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |

04-08-2016 to 04-09-2016

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.66.12 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 276 |
| 202.191.64.166 | 147.237.77.216 | India | dover.idf.il | ET WEB_SERVER UA WordPress, probable DDOS-Attack | 144 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 92 |
| 93.172.187.50 | 147.237.76.86 | Israel | navy.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 66 |
| 93.172.187.50 | 147.237.77.216 | Israel | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 14 |
| 66.249.69.34 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 12 |
| 66.249.66.15 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 6 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 213.151.60.89 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 132.74.95.21 | 147.237.77.170 | Israel | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 87.118.118.207 | 147.237.77.216 | Germany | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 192.116.108.18 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 192.169.188.231 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 66.249.64.165 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 217.55.71.27 | 147.237.77.216 | Egypt | dover.idf.il | SQL Injection - Select From | 2 |
| 109.253.207.193 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 66.102.8.243 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 195.216.176.244 | 147.237.8.46 | Latvia | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 31.210.188.20 | 147.237.77.216 | Israel | dover.idf.il | GPL SCAN myscan | 2 |
| 192.169.188.231 | 147.237.77.19 | United States | law-forum.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 80.246.133.61 | 147.237.77.170 | Israel | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 66.249.66.20 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 217.55.71.27 | 147.237.77.216 | Egypt | dover.idf.il | GPL WEB_SERVER /etc/passwd | 2 |
| 85.250.87.19 | 147.237.72.166 | Israel | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 192.169.188.231 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 192.169.188.231 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 80.82.78.38 | 147.237.76.202 | Netherlands | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.79.109 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 31.210.188.20 | 147.237.77.216 | Israel | dover.idf.il | INDICATOR-SCAN myscan | 2 |
| 192.169.188.231 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 66.249.69.93 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 195.216.176.244 | 147.237.8.14 | Latvia | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 208.100.26.228 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 79.177.179.182 | 147.237.72.166 | Israel | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.66.114 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 192.169.188.231 | 147.237.76.86 | United States | navy.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 88.204.187.90 | 147.237.76.86 | Kazakstan | navy.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 208.100.26.228 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.67 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 128.199.222.66 | 147.237.77.216 | Singapore | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 94.255.224.2 | 147.237.77.226 | Sweden | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 67.211.217.180 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 195.154.54.169 | 147.237.76.200 | France | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 23.102.168.255 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 179.43.144.37 | 147.237.77.243 | Switzerland | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 114.199.230.194 | 147.237.77.234 | Korea, Republic of | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 122.172.34.79 | 147.237.8.28 | India | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 89.248.167.131 | 147.237.77.74 | Netherlands | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 210.44.52.150 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

04-08-2016 to 04-09-2016

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.i | Bad TCP sequence | | monitor | 10263 |
| 192.168.173.102 | | 147.237.77.216 | dover.idf.i | Geo-location enforcement | Geo-location inbound enforcement | monitor | 8555 |
| 50.50.1.9 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8294 |
| 212.34.12.42 | Jordan | 147.237.77.216 | dover.idf.i | Bad TCP sequence | | monitor | 7562 |
| 192.168.173.102 | | 147.237.72.166 | aka.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 4657 |
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.i | Bad TCP sequence | Invalid ACK number | alert | 4046 |
| 212.34.12.42 | Jordan | 147.237.77.216 | dover.idf.i | Bad TCP sequence | Invalid ACK number | alert | 3237 |
| 188.161.118.232 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 2775 |
| 212.34.12.42 | Jordan | 147.237.77.216 | dover.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2666 |
| 50.50.1.10 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 2528 |
| 41.44.247.54 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 2129 |
| 212.126.112.38 | Iraq | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 1715 |
| 197.9.252.109 | Tunisia | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 1598 |
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 1267 |
| 194.9.28.11 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 1180 |
| 199.21.115.134 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 1041 |
| 98.158.190.196 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 992 |
| 106.186.123.25 | Japan | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 988 |
| 197.48.71.132 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 964 |
| 74.120.15.74 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 889 |
| 209.160.24.14 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 774 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | SAM rule | drop | 766 |
| 151.236.48.204 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 758 |
| 66.155.75.222 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 756 |
| 23.236.48.8 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 749 |
| 23.251.156.240 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 731 |
| 23.97.58.45 | Singapore | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 698 |
| 106.187.51.76 | Japan | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 696 |
| 46.43.126.188 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 686 |
| 162.212.56.149 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 671 |
| 130.211.158.164 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 661 |
| 130.211.172.63 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 615 |
| 146.148.35.16 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 602 |
| 183.82.51.188 | India | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 597 |
| 37.76.221.20 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 579 |
| 199.223.233.140 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 573 |
| 104.197.119.48 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 564 |
| 146.148.119.116 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 562 |
| 104.155.83.50 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 557 |
| 193.107.252.143 | Czech Republic | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 547 |
| 213.171.205.177 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 541 |
| 62.249.169.200 | Norway | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 521 |
| 146.148.61.21 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 521 |
| 108.59.83.170 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 518 |
| 88.208.192.244 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 513 |
| 74.120.15.102 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 505 |
| 106.187.93.83 | Japan | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 501 |
| 197.9.252.109 | Tunisia | 147.237.77.216 | dover.idf.i | drop | | drop | 500 |
| 104.197.1.208 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 486 |
| 130.211.133.99 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 486 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 149.78.35.248 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 161 |
| 46.19.85.239 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 124 |
| 176.13.3.169 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 110 |
| 149.88.63.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 104 |
| 46.19.85.72 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 85 |
| 2.54.175.16 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 70 |
| 46.19.86.134 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 70 |
| 80.246.139.248 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 65 |
| 109.66.29.87 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 56 |
| 5.102.199.57 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 5.102.199.57 | Block | 50 |
| 109.186.188.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 49 |
| 176.13.12.178 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 47 |
| 46.19.85.137 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 47 |
| 2.53.8.169 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 43 |
| 46.19.86.83 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 41 |
| 176.13.0.11 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 40 |
| 185.120.125.32 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 38 |
| 5.189.190.212 | Germany | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 35 |
| 84.108.131.180 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 176.13.14.25 | Israel | 147.237.0.19 | madim.atal.idf.i | Suspicious Response Code | Block | 29 |
| 37.26.149.134 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 113.67.189.221 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 113.67.189.221 | Block | 27 |
| 109.253.133.246 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 21 |
| 79.180.161.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 21 |
| 149.50.82.87 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 149.50.82.87 | Block | 17 |
| 2.53.56.75 | Israel | 147.237.0.19 | madim.atal.idf.i | Suspicious Response Code | Block | 17 |
| 37.46.38.22 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 15 |
| 84.94.33.189 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 15 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 13 |
| 208.115.111.72 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 13 |
| 212.179.159.253 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 212.179.159.253 | Block | 13 |
| 208.115.111.72 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.111.72 | Block | 12 |
| 79.177.206.55 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 12 |
| 46.19.85.142 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 11 |
| 37.26.149.190 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 9 |
| 217.55.71.27 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 217.55.71.27 | Block | 9 |
| 197.15.245.65 | Tunisia | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 197.15.245.65 | Block | 7 |
| 157.55.39.205 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 7 |
| 105.110.23.24 | Algeria | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 7 |
| 199.30.25.110 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 7 |
| 93.173.223.98 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 93.173.223.98 | Block | 6 |
| 185.14.140.99 | United Kingdom | 147.237.77.74 | law.idf.il | Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx | Block | 6 |
| 149.202.239.135 | France | 147.237.77.216 | dover.idf.il | Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum | Block | 6 |
| 164.138.118.38 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 46.19.86.245 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 109.253.136.235 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 185.3.144.13 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 185.3.144.13 | Block | 6 |
| 46.120.23.172 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 213.251.182.103 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 6 |
| 149.202.239.135 | France | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx | Block | 6 |

04-08-2016 to 04-09-2016