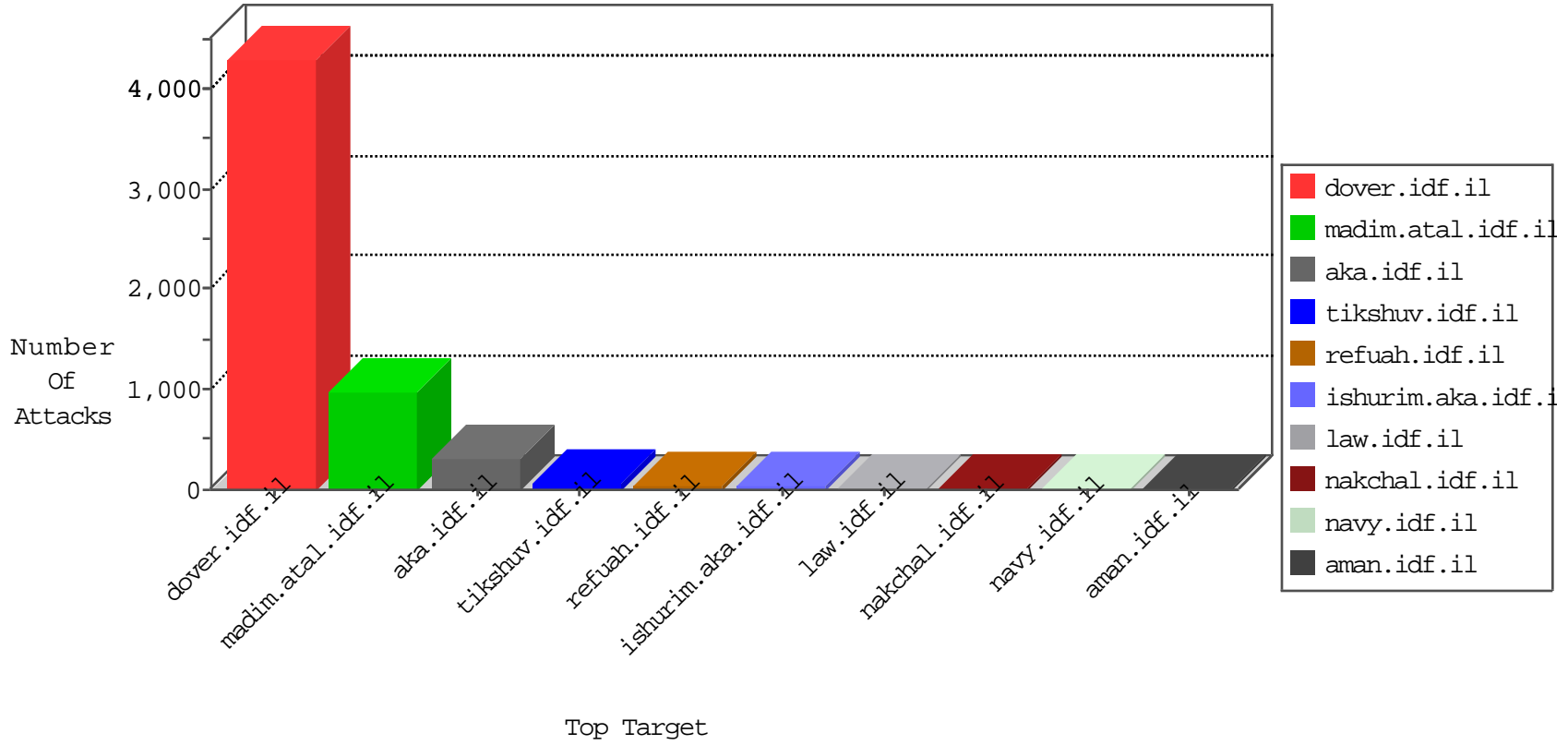


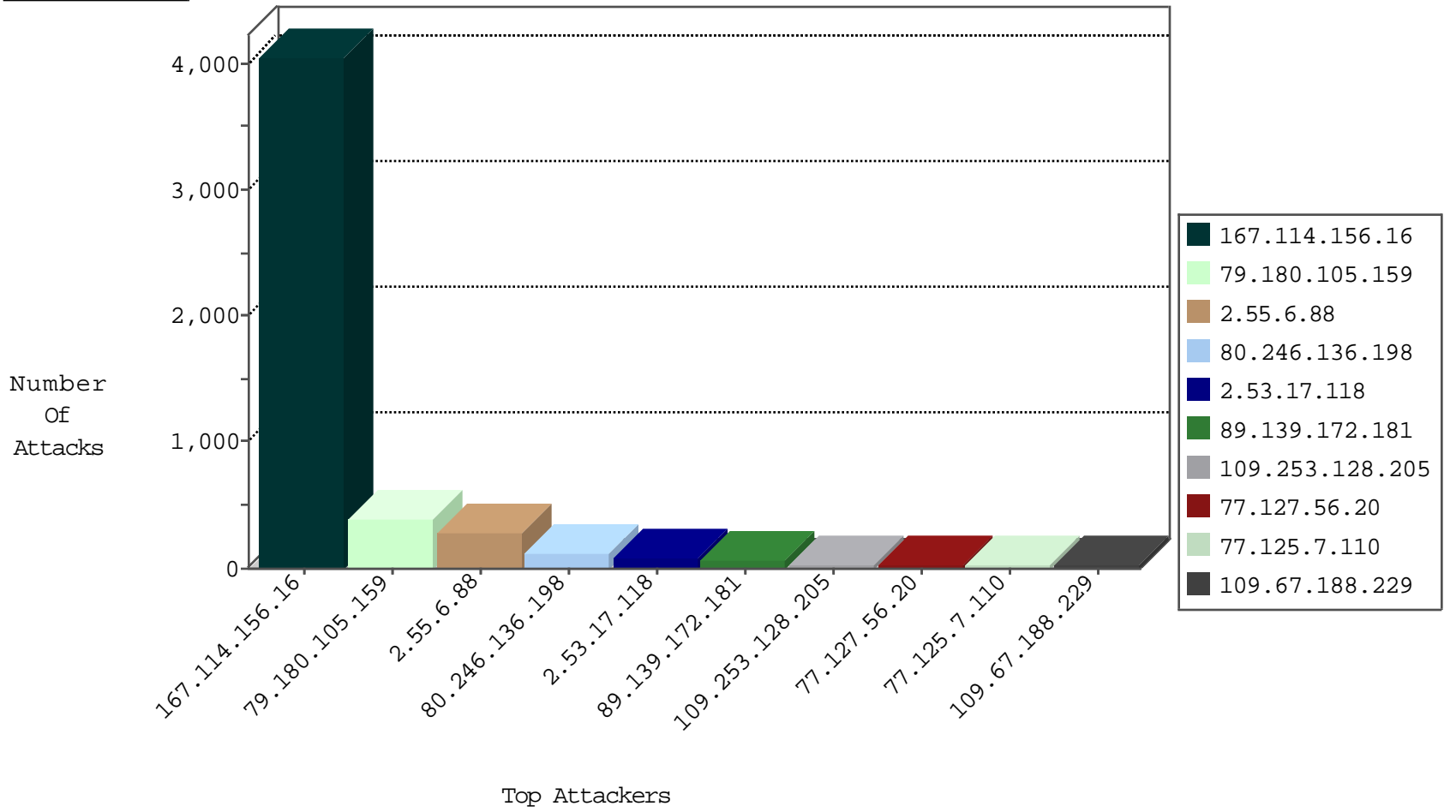
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | 4045 |
| 95.86.112.173 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 212.199.244.112 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 168.235.207.176 | United States | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 168.235.207.176 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 113.190.20.222 | Vietnam | 147.237.77.227 | e.hamaz.idf.il | Block_Udp_All_Nets | drop | 1 |
| 176.31.60.249 | France | 147.237.76.176 | test.noore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 5.189.167.216 | Germany | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 1 |
| 113.190.20.222 | Vietnam | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 222.186.31.188 | China | 147.237.0.16 | my-kosher-kravi.idf.il | JLM_Under_Attack_Con_Tcp | drop | 1 |
| 113.190.20.222 | Vietnam | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------|---|---------------|-------|
| 213.57.231.142 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 11 |
| 79.176.88.182 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 80.246.130.122 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 31.210.187.34 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 37.46.39.23 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 85.64.234.103 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 144.76.4.148 | Germany | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 151.80.31.177 | France | 147.237.77.170 | maarachot.idf.il | C1000146: HTTP: AhrefBot crawler | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 80.246.133.87 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 52.1.90.117 | United States | 147.237.72.166 | aka.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|----------------|------------------------------------|-------|
| 84.94.192.223 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.179.204.251 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.89.99 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 217.132.60.107 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.117.104.113 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.76.121.189 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.28.233 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 199.101.186.221 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 176.13.17.230 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.50.32.26 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.153.13 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.199.238 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.178.5.204 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.117.104.187 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.199.94.201 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.22.135.115 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.3.144.75 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.10.206 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.67.198.43 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|--------------------|----------------|--------------------|--|---|---------------|-------|
| 77.127.56.20 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 33 |
| 77.125.7.110 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 28 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 46.19.86.217 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 21 |
| 109.67.188.229 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 212.235.98.139 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 19 |
| 5.47.194.53 | Turkey | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 82.166.190.11 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 109.253.213.147 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 81.218.171.27 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 2.53.28.168 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.147.199 | Israel | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 2.53.33.49 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.28.171.26 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.146.6.2 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.127 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 89.139.147.36 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.47.194.53 | Turkey | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.147 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 82.166.239.115 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.147 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 80.246.130.35 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 5 |
| 31.210.186.74 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 212.235.98.139 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 31.184.238.195 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 46.19.85.56 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 94.249.26.99 | Jordan | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 37.46.39.23 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 87.69.162.85 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 41.33.231.82 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 3 |
| 192.116.240.8 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.3.200 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.143.159.98 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.218.62 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 157.55.39.234 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.144.128 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.178.109.80 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.131.119 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 82.80.154.90 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.200 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.198.109 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 188.254.60.29 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.56 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 109.67.188.229 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.168.24.33 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|------------|--|---|---------------|-------|
| 5.28.190.107 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 82.81.104.52 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.53.163.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|--------------------|----------------|------------------------|---|---------------|-------|
| 79.180.105.159 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 388 |
| 2.55.6.88 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 272 |
| 80.246.136.198 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 120 |
| 2.53.17.118 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 75 |
| 89.139.172.181 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 63 |
| 109.253.128.205 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 33 |
| 80.179.122.50 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 80.179.122.50 | Block | 17 |
| 79.180.105.159 | Israel | 147.237.0.19 | madim.atal.idf.il | Automated Vulnerability Scanning V1 | Block | 10 |
| 80.178.28.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 199.30.24.164 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 199.30.25.57 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 65.55.210.157 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 109.186.191.80 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 109.186.191.80 | Block | 3 |
| 62.219.99.130 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 157.55.2.180 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 134.191.232.71 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 157.55.39.65 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 80.246.136.188 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 199.30.25.6 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 46.116.21.190 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 194.114.146.227 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 194.114.146.227 | Block | 2 |
| 77.125.126.8 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 157.55.2.175 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 79.179.135.182 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 2 |
| 157.55.2.178 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 109.253.128.205 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ct100\$ContentPlaceholder1\$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx | Block | 2 |
| 2.55.182.192 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.186.191.80 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx | Block | 2 |
| 80.246.133.120 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.16.189 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 207.46.13.72 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 46.19.85.76 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 1 |
| 5.255.253.51 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/ | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 54.67.54.15 | United States | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to 147.237.77.19/ | Block | 1 |
| 213.8.39.241 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https://www.idf.il/ | Block | 1 |
| 80.246.133.243 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.19.85.56 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Abnormally Long Request | Block | 1 |
| 131.253.25.231 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.65.223 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx | Block | 1 |
| 46.19.86.19 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 208.115.125.36 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 94.188.161.145 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 1 |
| 31.168.13.78 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 194.90.254.244 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 77.125.7.110 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 149.88.41.194 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$emailUpdate\$hiddenUpdate Email in www.aka.idf.il/main/giyus/faq.aspx | None | 1 |
| 54.172.110.245 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 1 |
| 109.186.191.80 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx | Block | 1 |