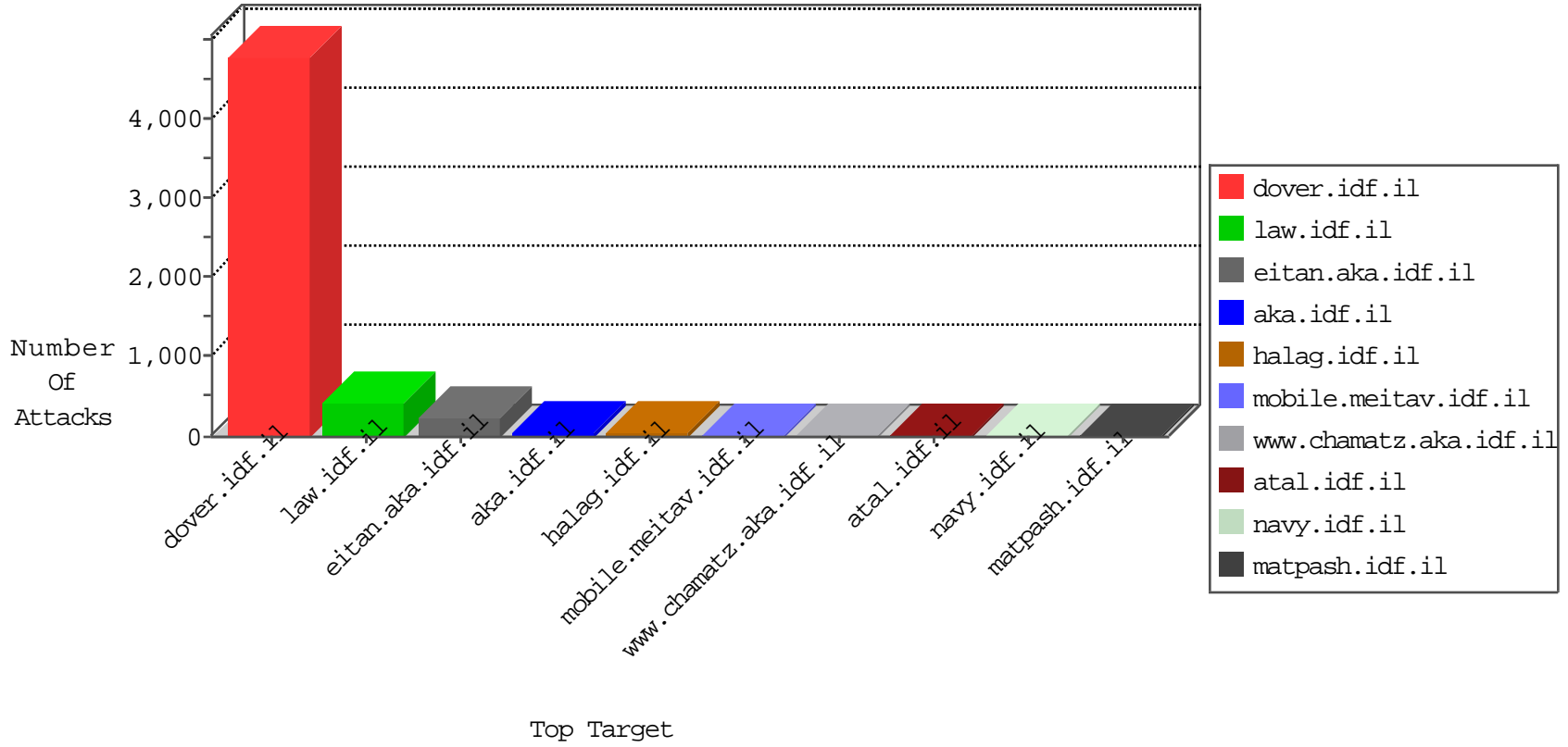


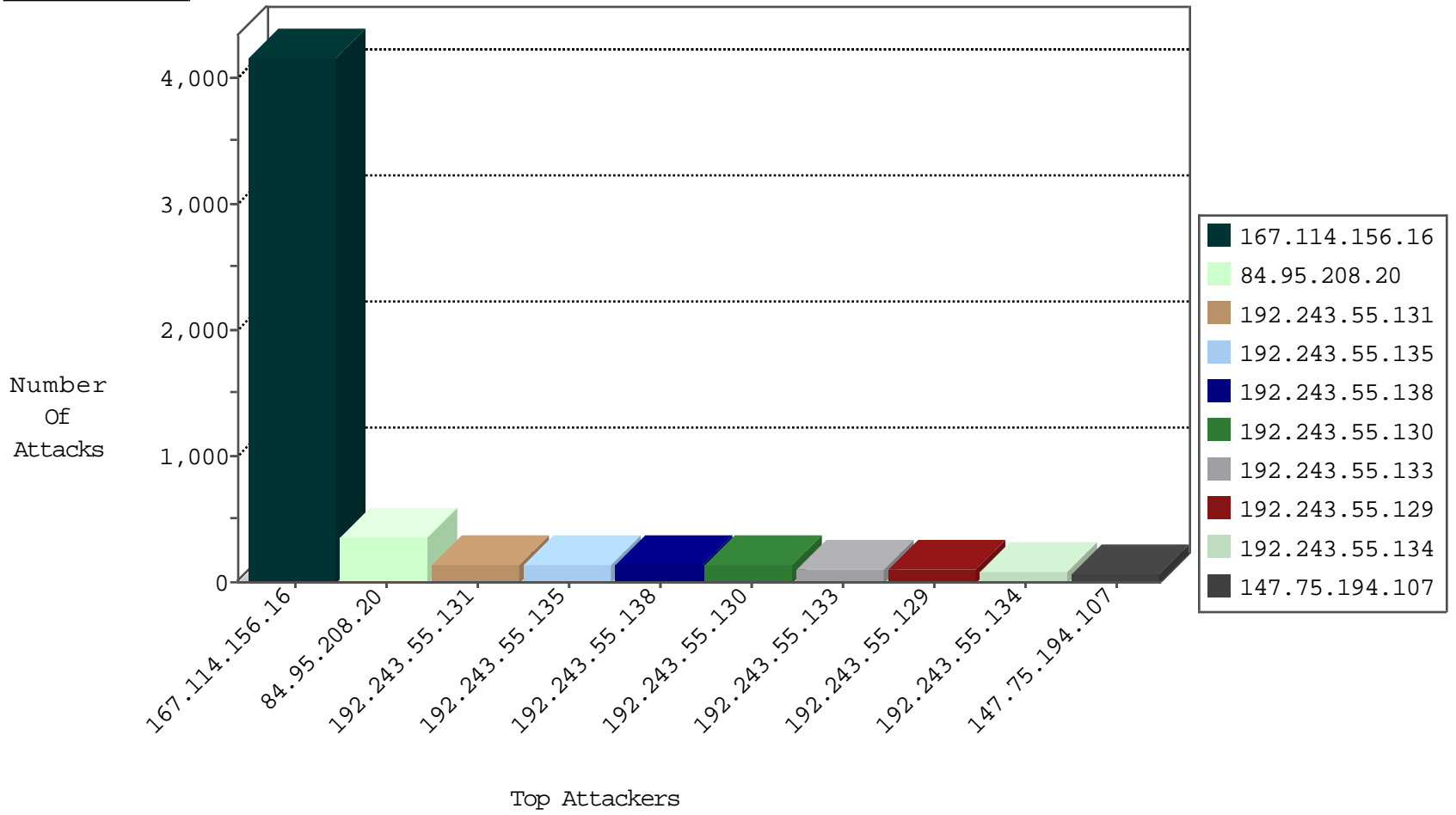
IDF Under Attack Daily Report



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 | 4140 |
| 147.75.194.107 | United States | 147.237.77.234 | halag.idf.il | block-sp-trafl | forward | 30 |
| 147.75.194.107 | United States | 147.237.76.39 | mobile.meitav.idf.il | block-sp-trafl | forward | 22 |
| 147.75.194.107 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-trafl | forward | 2 |
| 80.82.78.38 | Netherlands | 147.237.77.233 | atal.idf.il | block-sp-trafl | forward | 2 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 147.75.194.107 | United States | 147.237.72.156 | aman.idf.il | block-sp-trafl | forward | 2 |
| 80.82.78.38 | Netherlands | 147.237.77.216 | dover.idf.il | block-sp-trafl | forward | 2 |
| 216.218.206.75 | United States | 147.237.72.217 | e.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 |
| 184.105.247.238 | United States | 147.237.8.46 | e.chinuch.idf.il | Block_Udp_All_Nets | drop | 1 |
| 71.6.135.131 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 82.145.208.78 | Europe | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 1 |
| 71.6.167.142 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 149.56.110.175 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 61.135.189.122 | China | 147.237.76.31 | nakchal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

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 | 10 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 89.163.212.37 | 147.237.76.177 | Germany | ncore.idf.il | ET SCAN Potential SSH Scan | 2 |
| 89.163.212.37 | 147.237.76.31 | Germany | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 89.163.212.37 | 147.237.77.19 | Germany | law-forum.idf.il | ET SCAN Potential SSH Scan | 2 |
| 199.101.186.221 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.163.212.37 | 147.237.76.196 | Germany | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.245.78.52 | 147.237.76.34 | Mexico | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 89.163.212.37 | 147.237.76.44 | Germany | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 101.200.181.38 | 147.237.72.217 | China | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.163.212.37 | 147.237.76.34 | Germany | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 98.119.105.221 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.78.38 | 147.237.77.227 | Netherlands | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.163.212.37 | 147.237.77.233 | Germany | atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 13.82.25.94 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.163.212.37 | 147.237.77.176 | Germany | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 13.82.25.94 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 89.163.212.37 | 147.237.77.74 | Germany | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.73.18.162 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.163.212.37 | 147.237.76.200 | Germany | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 199.101.186.221 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 89.163.212.37 | 147.237.76.197 | Germany | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 128.199.34.35 | 147.237.77.170 | Netherlands | maarachot.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 89.163.212.37 | 147.237.76.38 | Germany | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 98.119.105.221 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 89.163.212.37 | 147.237.77.234 | Germany | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.163.212.37 | 147.237.77.212 | Germany | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 13.82.25.94 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 89.163.212.37 | 147.237.77.170 | Germany | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 13.82.25.94 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.100.26.228 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.163.212.37 | 147.237.76.199 | Germany | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|------------------|--|---|---------------|-------|
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 159 |
| 192.243.55.130 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 25 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 22 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 20 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 18 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 16 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 192.243.55.130 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 15 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 14 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 14 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 13 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 13 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 12 |
| 192.243.55.130 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 12 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 192.243.55.135 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.135 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 10 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 192.243.55.130 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.135 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------------|---|---------------|-------|
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 78 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 69 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 15 |
| 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 | 5 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 3 |
| 65.55.210.150 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.24.236 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 157.55.2.177 | 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 |
| 199.30.24.38 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.25.32 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 65.55.210.232 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.24.63 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.25.40 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 65.55.210.246 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.24.144 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.25.111 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 65.55.210.146 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 199.30.24.235 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 149.202.239.135 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 31.210.176.80 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 31.210.176.80 | Block | 1 |
| 207.46.13.171 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 66.249.78.246 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 192.243.55.131 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/en | Block | 1 |
| 108.227.98.31 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 1 |
| 66.249.64.143 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/resources/styles/sachar.css | Block | 1 |
| 38.99.96.166 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1589-en/dover.aspx | Block | 1 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/ | Block | 1 |
| 65.55.210.153 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 114.97.195.129 | China | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 114.97.195.129 | Block | 1 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 176.9.127.69 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 1 |
| 38.111.147.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-he | Block | 1 |
| 219.74.180.185 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.75.76.164 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/page/32/ | Block | 1 |
| 119.73.253.5 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 192.243.55.130 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.130 | Block | 1 |
| 54.153.33.233 | United States | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to 147.237.76.200/ | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 1 |
| 80.82.78.38 | Netherlands | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 66.249.65.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx | Block | 1 |
| 192.243.55.130 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy. | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 1 |
| 80.82.78.38 | Netherlands | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |