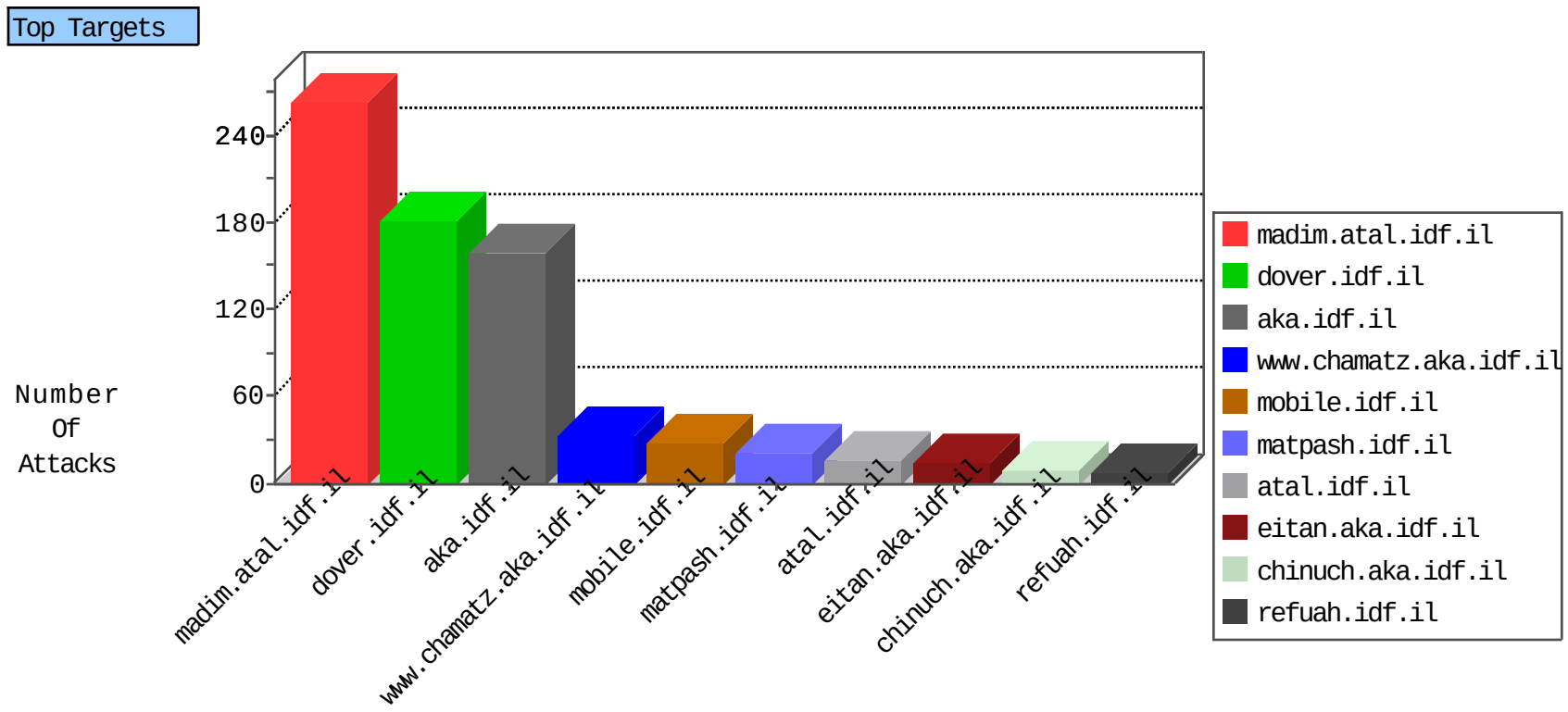
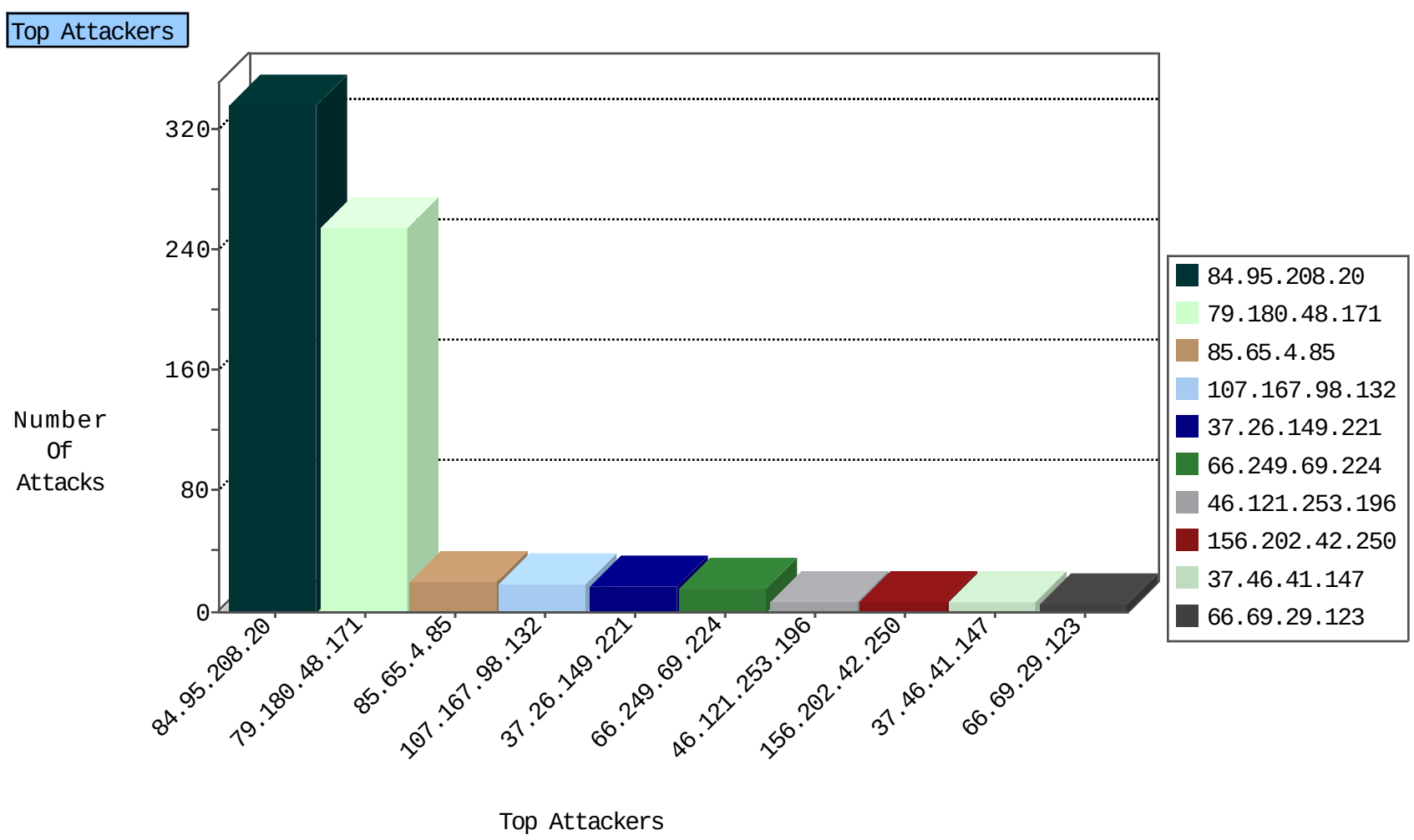
09-24-2016-09:04:09 to 09-24-2016-10:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-24-2016-09:04:09 to 09-24-2016-10:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 208.110.84.68 | United States | 147.237.76.200 | eitan.aka.idf.il | block-sp-traf1 | forward | 2 |
| 63.141.242.198 | United States | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | forward | 2 |
| 198.204.224.234 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 204.42.253.132 | United States | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 69.30.193.252 | United States | 147.237.72.166 | aka.idf.il | block-sp-traf1 | forward | 1 |
| 142.54.174.86 | United States | 147.237.77.235 | sviva.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.242.196 | United States | 147.237.77.74 | law.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.226.220 | United States | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | forward | 1 |
| 191.96.249.37 | Chile | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 69.30.226.221 | United States | 147.237.72.156 | aman.idf.il | block-sp-traf1 | forward | 1 |
| 45.63.53.164 | United States | 147.237.76.39 | mobile.meitav.idf.il | Black List | drop | 1 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 63.141.231.210 | United States | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | forward | 1 |

09-24-2016-09:04:09 to 09-24-2016-10:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.9.62.130 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 2 |

09-24-2016-09:04:09 to 09-24-2016-10:04:09

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 185.153.198.10 | 147.237.77.243 | | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 107.191.55.97 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.155 | 147.237.8.50 | Ukraine | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 88.249.106.23 | 147.237.0.200 | Turkey | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 40.121.139.43 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 14.148.170.77 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 216.81.230.167 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.153.198.10 | 147.237.77.19 | | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 107.191.55.97 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.249.106.23 | 147.237.8.50 | Turkey | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 74.82.47.8 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 37.8.21.91 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |

09-24-2016-09:04:09 to 09-24-2016-10:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 85.65.4.85 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 107.167.98.132 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 19 |
| 37.26.149.221 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 17 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.69.29.123 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 156.202.42.250 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.53.139.211 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 128.232.110.28 | United Kingdom | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 87.69.222.132 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 87.69.222.132 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 46.121.253.196 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 2.53.167.211 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 37.46.38.1 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 103.48.194.78 | Vietnam | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Command Injection | command injection detected in URL: 'replace' | monitor | 1 |
| 77.138.18.178 | France | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 156.202.42.250 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 46.121.253.196 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 5.22.134.220 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 85.65.160.49 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.20.5.157 | United Kingdom | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 1 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 146.115.132.147 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 45.30.245.31 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 103.48.194.78 | Vietnam | 147.237.76.147 | chinuch.aka.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 1 |
| 84.108.119.30 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 216.218.206.74 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 82.221.105.6 | Iceland | 147.237.77.212 | e.dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 176.13.9.157 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.121.253.196 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 139.162.37.147 | United States | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.22.134.231 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | SQL Injection | SQL injection detected in URL: 'concat' | monitor | 1 |
| 185.20.5.157 | United Kingdom | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.85.181 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 84.108.119.30 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 216.218.206.98 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 176.13.11.136 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 46.121.253.196 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.59 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 31.210.187.82 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.20.5.157 | United Kingdom | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 156.202.42.250 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.85.181 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.48.171 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 255 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 135 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 94 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 22 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 13 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.69.224 | Block | 12 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Distributed PHP Attempt | Block | 10 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 8 |
| 37.46.41.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 5 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 5 |
| 84.95.208.20 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 85.65.10.198 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 4 |
| 84.95.208.20 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 3 |
| 84.95.208.20 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 109.253.246.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 66.249.69.232 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.69.232 | Block | 2 |
| 66.249.69.228 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.69.228 | Block | 2 |
| 46.121.253.196 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 66.249.69.228 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php | Block | 1 |
| 84.95.208.20 | Israel | 147.237.72.156 | aman.idf.il | PHP Attempt | Block | 1 |
| 66.249.75.32 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-22777-ar/dover.aspx | Block | 1 |
| 66.102.9.5 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 84.95.208.20 | Israel | 147.237.0.15 | kosher-kravi.idf.il | PHP Attempt | Block | 1 |
| 176.13.243.88 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 68.180.230.216 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx | Block | 1 |
| 66.102.9.8 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 1 |
| 176.228.175.10 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 1 |
| 66.249.69.232 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/international_training/course_photos.asp | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.234 | halag.idf.il | PHP Attempt | Block | 1 |
| 84.95.208.20 | Israel | 147.237.0.34 | tikshuv.idf.il | PHP Attempt | Block | 1 |
| 213.8.204.67 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 213.8.204.67 | Block | 1 |
| 66.249.75.4 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9004-he/refuah.aspx | Block | 1 |
| 37.142.2.145 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 37.142.2.145 | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item | Block | 1 |
| 79.181.21.49 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 84.95.208.20 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 1 |
| 213.8.204.67 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 66.249.75.12 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3274.jpg | Block | 1 |