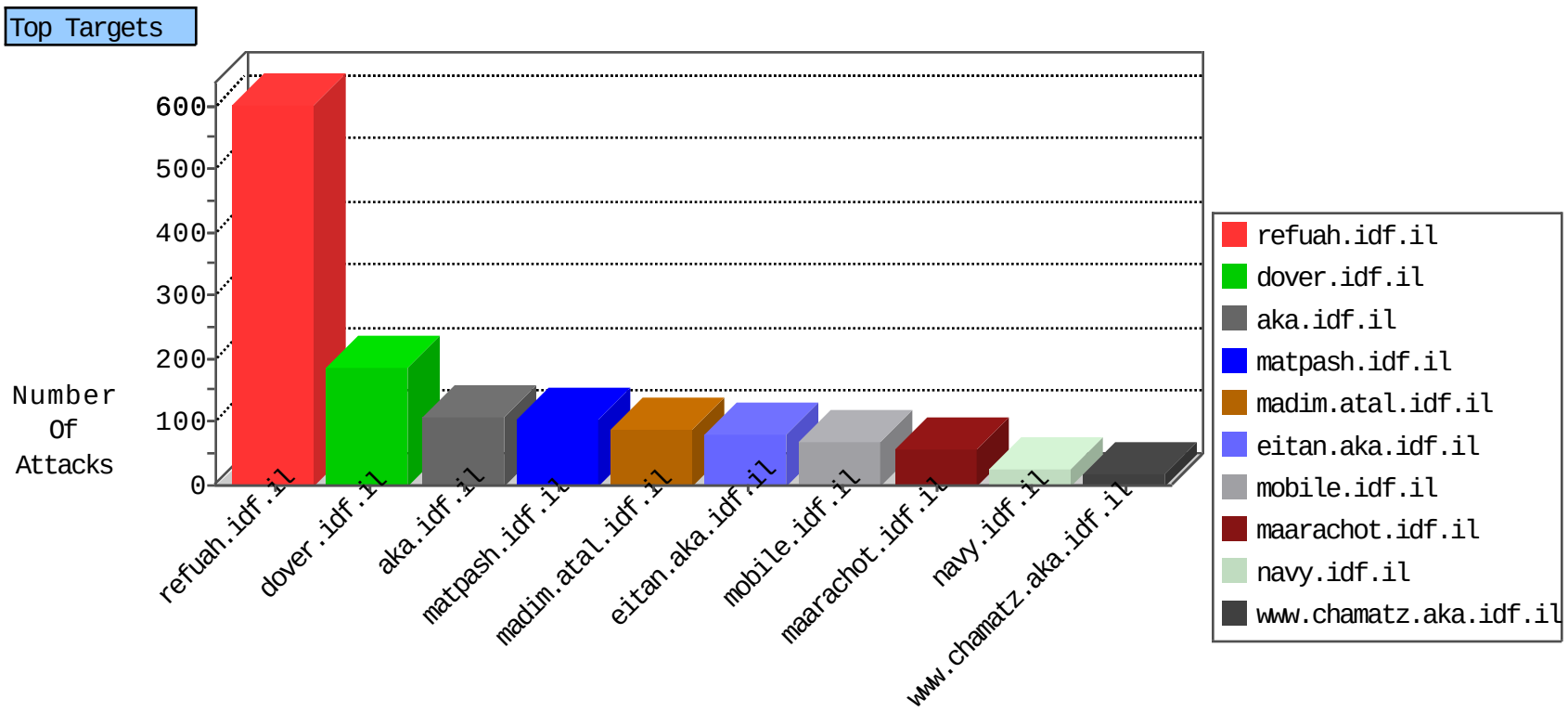
10-02-2016-11:04:10 to 10-02-2016-12:04:10

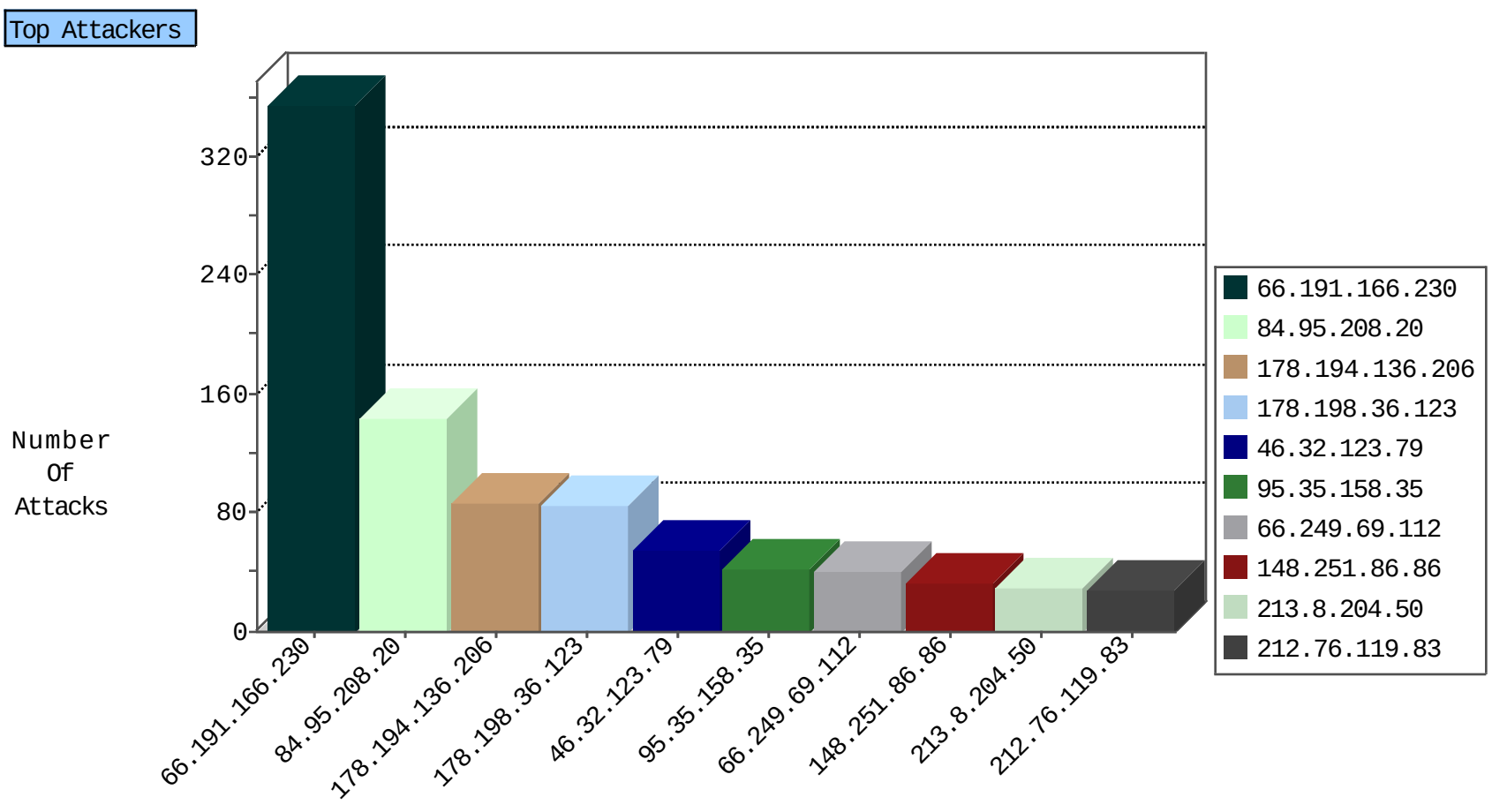
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

10-02-2016-11:04:10 to 10-02-2016-12:04:10

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.121.238.128 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 7 |
| 69.30.226.221 | United States | 147.237.76.86 | navy.idf.il | block-sp-traf1 | forward | 2 |
| 198.204.247.219 | United States | 147.237.76.30 | himush.idf.il | block-sp-traf1 | forward | 2 |
| 192.187.118.21 | United States | 147.237.76.31 | nakchal.idf.il | block-sp-traf1 | forward | 2 |
| 69.30.226.222 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 2 |
| 198.204.247.220 | United States | 147.237.76.200 | eitan.aka.idf.il | block-sp-traf1 | forward | 2 |
| 63.141.242.198 | United States | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | forward | 2 |
| 192.187.118.69 | United States | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | forward | 1 |
| 142.54.174.84 | United States | 147.237.77.74 | law.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.231.213 | United States | 147.237.72.166 | aka.idf.il | block-sp-traf1 | forward | 1 |
| 198.204.255.78 | United States | 147.237.77.216 | dover.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.207.130 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.226.221 | United States | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | forward | 1 |
| 192.187.118.70 | United States | 147.237.77.233 | atal.idf.il | block-sp-traf1 | forward | 1 |
| 142.54.174.85 | United States | 147.237.0.34 | tikshuv.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.242.194 | United States | 147.237.77.234 | halag.idf.il | block-sp-traf1 | forward | 1 |
| 204.12.217.6 | United States | 147.237.72.156 | aman.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.213.195 | United States | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.150.116 | United States | 147.237.0.19 | madim.atal.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.242.196 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 204.12.217.6 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | forward | 1 |
| 63.141.231.211 | United States | 147.237.77.235 | sviva.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.198.10 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | block-sp-traf1 | forward | 1 |

10-02-2016-11:04:10 to 10-02-2016-12:04:10

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 108.59.8.70 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 5.9.88.103 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 1 |

10-02-2016-11:04:10 to 10-02-2016-12:04:10

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.69.112 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sA (2) | 41 |
| 79.180.43.40 | 147.237.72.166 | Israel | aka.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 62.210.113.183 | 147.237.72.166 | France | aka.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 50.84.213.146 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 42.112.28.187 | 147.237.8.27 | Vietnam | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.80.245.167 | 147.237.77.235 | Vietnam | sviva.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 5.255.90.133 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.177 | United Kingdom | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 124.243.134.208 | 147.237.77.179 | Australia | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 106.75.9.82 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 75.99.111.10 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 66.249.64.103 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 50.116.123.33 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.84.213.146 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.100.26.228 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.255.90.133 | 147.237.76.86 | Netherlands | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.77.216 | United Kingdom | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.148 | United Kingdom | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.59.173.17 | 147.237.77.227 | China | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

10-02-2016-11:04:10 to 10-02-2016-12:04:10

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.191.166.230 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 346 |
| 213.8.204.50 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 46.32.123.79 | Jordan | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 26 |
| 107.167.104.28 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 23 |
| 212.14.228.210 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 22 |
| 178.194.136.206 | Switzerland | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 178.198.36.123 | Switzerland | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 178.198.36.123 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 18 |
| 178.194.136.206 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 17 |
| 178.198.36.123 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 17 |
| 178.194.136.206 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 17 |
| 178.194.136.206 | Switzerland | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 17 |
| 178.198.36.123 | Switzerland | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 16 |
| 178.194.136.206 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 178.198.36.123 | Switzerland | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 46.32.123.79 | Jordan | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.32.123.79 | Jordan | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.19.85.111 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.32.123.79 | Jordan | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 13 |
| 46.19.86.194 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 13 |
| 2.53.48.195 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.110.108.165 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 52.3.127.144 | United States | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 11 |
| 141.226.162.86 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 141.226.162.86 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 93.173.104.14 | Israel | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 9 |
| 176.13.0.49 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.86.12 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 46.19.85.152 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 84.109.114.12 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 184.204.182.76 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 7 |
| 46.19.85.111 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 87.71.31.217 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 184.204.182.76 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 6 |
| 46.19.85.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.53.159.154 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 148.251.86.86 | Germany | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 5 |
| 184.204.182.76 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 148.251.86.86 | Germany | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 46.19.85.32 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.116.192.23 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 148.251.86.86 | Germany | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 5 |
| 46.19.85.32 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | | monitor | 4 |
| 148.251.86.86 | Germany | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 4 |
| 176.13.228.123 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.86.12 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 46.19.86.59 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.73 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.86.12 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |

## 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 | 54 |
| 95.35.158.35 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 42 |
| 212.76.119.83 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 27 |
| 2.53.61.238 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 79.177.170.47 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized HTTP Method | Block | 4 |
| 176.13.7.206 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 46.117.31.84 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 3 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 46.117.31.84 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 46.117.31.84 | Block | 2 |
| 2.53.157.234 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.177.170.47 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 2 |
| 77.138.131.128 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/ | Block | 1 |
| 66.249.64.56 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Multiple Illegal Byte Code Character in Header Name from 169.229.3.91 | Block | 1 |
| 84.229.17.117 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx | Block | 1 |
| 17.78.122.211 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 1 |
| 79.182.63.17 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.65.188 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8822-he/refuah.aspx | Block | 1 |
| 157.55.39.145 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx | Block | 1 |
| 46.117.31.84 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-18481-he/ | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 77.139.223.105 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 1 |
| 66.249.64.58 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 84.229.17.117 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 31.154.19.5 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/images/1.he/error.png | Block | 1 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 1 |
| 207.46.13.108 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/robots.txt | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.77 | Block | 1 |
| 52.16.137.212 | Ireland | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to / | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal Byte Code Character in URL D¹0t]]72#[[Š²k•§o¬qx› | Block | 1 |
| 2.53.48.195 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.65.24 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-20329-he/dover.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Multiple Malformed URL from 169.229.3.91 | Block | 1 |
| 90.27.172.5 | France | 147.237.76.42 | refuah.idf.il | Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx | Block | 1 |
| 46.19.86.39 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 66.249.76.79 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 61.216.2.15 | Taiwan | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Illegal HTTP Version | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Parameter Type Violation aspxerrorpath in www.idf.il/error.htm | Block | 1 |
| 79.177.170.47 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 79.177.170.47 | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Multiple Unknown HTTP Request Method from 169.229.3.91 | Block | 1 |
| 66.249.65.51 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.51 | Block | 1 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 220.181.108.106 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.76.108 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/valtam | Block | 1 |
| 66.102.9.22 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/home/default.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | Multiple Abnormally Long Request from 169.229.3.91 | Block | 1 |