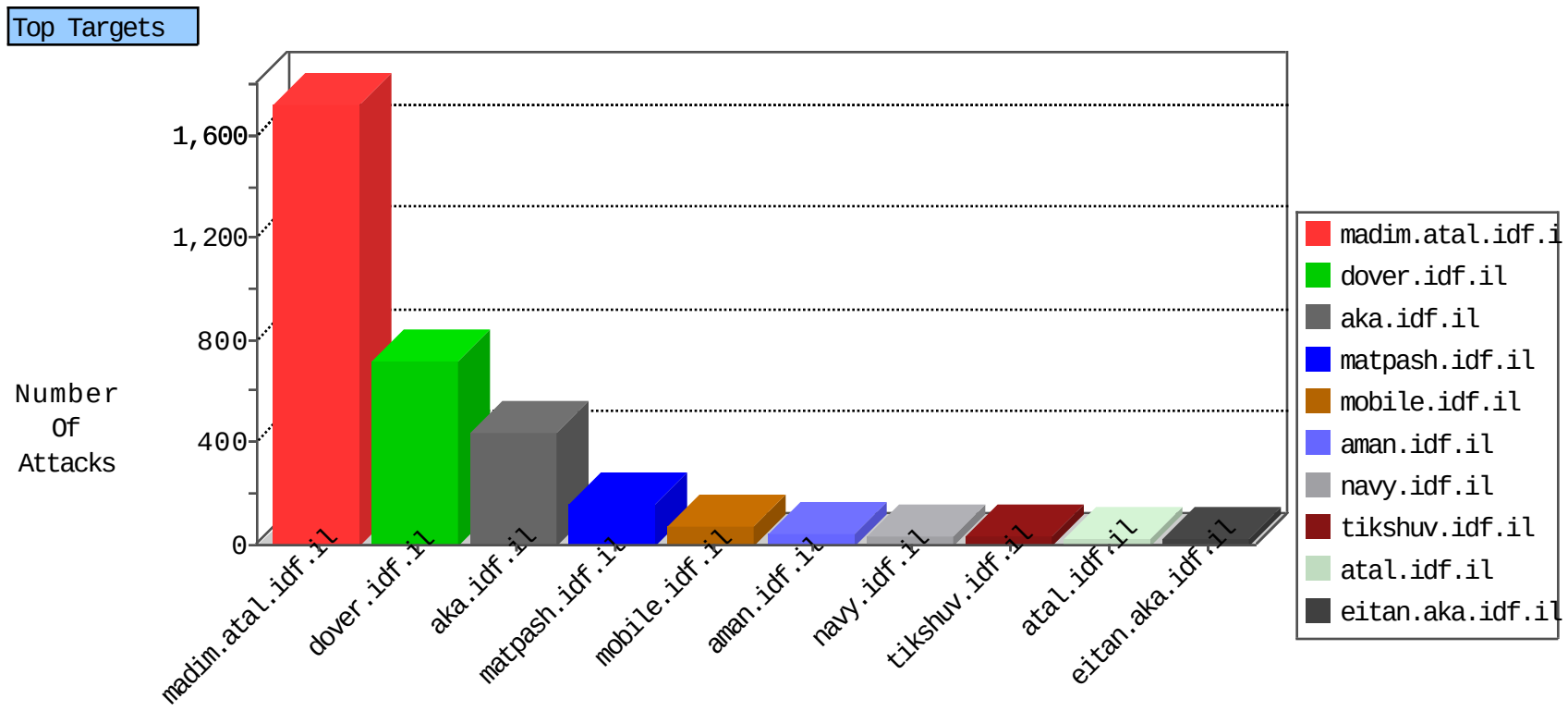
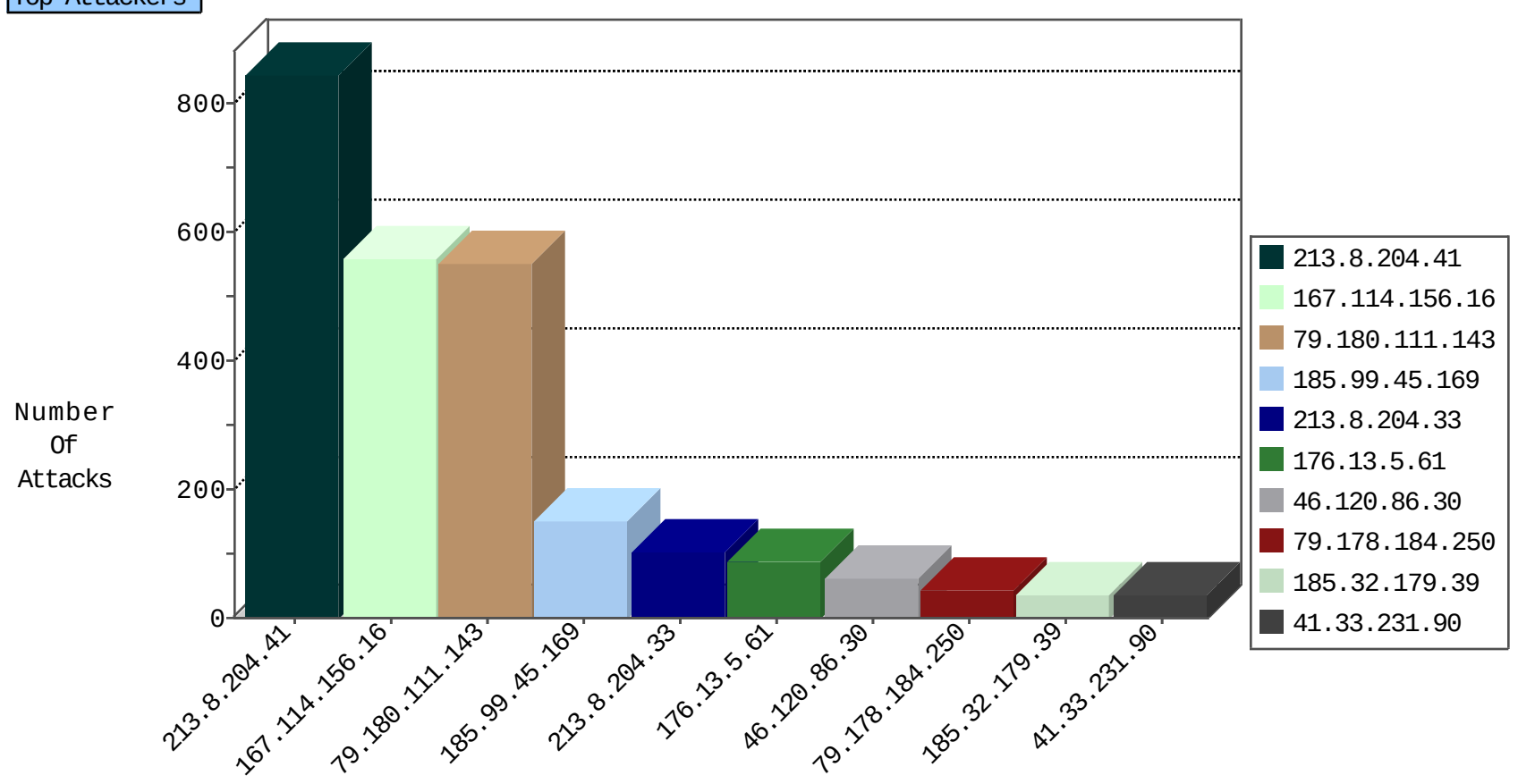
01-09-2016-20:04:03 to 01-09-2016-21:04:03

# IDF Under Attack Daily Report

Top Targets




Top Attackers



01-09-2016-20:04:03 to 01-09-2016-21:04:03

## 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 | DOS-Tool-SwitchbladG | dest-reset | 3566 |
| 85.64.71.65 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 66.249.78.153 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |

01-09-2016-20:04:03 to 01-09-2016-21:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 188.165.15.119 | France | 147.237.77.233 | atal.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 188.165.15.203 | France | 147.237.72.167 | ishurim.aka.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |

01-09-2016-20:04:03 to 01-09-2016-21:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 213.8.204.41 | 147.237.0.19 | Israel | madim.atal.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 15 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.78.151 | 147.237.76.39 | United States | mobile.meitav.idf.i | ET SCAN NMAP -sA (2) | 2 |
| 37.143.82.50 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN NMAP -f -sS | 1 |
| 183.61.109.189 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 132.74.95.21 | 147.237.77.170 | Israel | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 131.109.15.15 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 106.75.199.201 | 147.237.8.45 | China | e.eitan.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 218.77.79.38 | 147.237.77.212 | China | e.dover.idf.il | ET SCAN Rapid POP3 Connections - Possible Brute Force Attack | 1 |
| 88.249.106.23 | 147.237.77.243 | Turkey | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 199.191.56.187 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 66.249.66.61 | 147.237.72.166 | United States | aka.idf.il | WEB-CGI redirect access | 1 |
| 199.191.56.187 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 37.143.82.50 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN NMAP -sS window 2048 | 1 |
| 185.130.5.247 | 147.237.77.212 |  | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.61.109.189 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 131.109.15.15 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 131.109.15.15 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN NMAP -f -sS | 1 |
| 93.174.93.203 | 147.237.76.86 | Netherlands | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 199.191.56.187 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 46.19.85.135 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 198.20.69.74 | 147.237.77.205 | United States | prisha.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 37.143.82.50 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN NMAP -sS window 3072 | 1 |
| 189.203.240.181 | 147.237.0.33 | Mexico | idf.il | ET SCAN Potential SSH Scan | 1 |

01-09-2016-20:04:03 to 01-09-2016-21:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.99.45.169 | | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 133 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 34 |
| 37.26.149.171 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 84.228.78.60 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 15 |
| 5.102.254.174 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 185.99.45.169 | | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 13 |
| 37.142.231.35 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 37.26.146.167 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 217.132.84.32 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 46.19.85.64 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 10 |
| 66.249.78.37 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 109.64.133.209 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 109.67.48.74 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 87.68.19.83 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.180.205.69 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 46.19.85.228 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 79.182.226.3 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 8 |
| 5.29.1.195 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 5.29.1.195 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 8 |
| 85.64.66.2 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.19.85.135 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 212.68.153.26 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 89.138.55.167 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 89.138.55.167 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 208.115.113.92 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 85.65.138.212 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 5.28.154.26 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.65.138.212 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.135 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 79.183.226.214 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.64.212.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 82.80.146.24 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.217 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 5.29.1.195 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.86.58 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 197.165.156.240 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 79.177.31.160 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.228 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 46.19.86.217 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.85.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 5 |
| 5.29.1.195 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 94.230.86.153 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.102.254.174 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.117.9.195 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 5.29.1.195 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 91.200.12.143 | Ukraine | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 4 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 213.8.204.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 441 |
| 79.180.111.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 315 |
| 213.8.204.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 213.8.204.41 | Block | 232 |
| 79.180.111.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 133 |
| 79.180.111.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 104 |
| 213.8.204.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 104 |
| 213.8.204.33 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 101 |
| 46.120.86.30 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 60 |
| 176.13.5.61 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 60 |
| 213.8.204.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 213.8.204.41 | Block | 55 |
| 79.178.184.250 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 44 |
| 185.32.179.39 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 37 |
| 79.180.109.238 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 32 |
| 176.13.5.61 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 24 |
| 85.250.174.66 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 13 |
| 46.19.86.182 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 109.186.168.47 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 109.186.168.47 | Block | 6 |
| 109.226.48.121 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 5 |
| 5.29.33.241 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 5.29.33.241 | Block | 4 |
| 109.253.206.196 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 192.243.55.131 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.131 | Block | 3 |
| 85.65.122.216 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/ | Block | 3 |
| 46.117.96.44 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 46.117.96.44 | Block | 3 |
| 77.127.78.98 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 77.127.78.98 | None | 3 |
| 46.117.96.44 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 3 |
| 46.19.85.102 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.64.133.209 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.142.231.35 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 82.166.240.203 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 2 |
| 109.64.133.209 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1538 | Block | 2 |
| 149.78.231.192 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 213.57.241.39 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 213.57.241.39 | Block | 2 |
| 2.54.158.242 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 2.54.158.242 | Block | 2 |
| 109.253.130.76 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.63 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.186.168.47 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 2 |
| 77.127.78.98 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in m.my-kosher-kravi.idf.il/templates/login.aspx | Block | 2 |
| 2.54.189.24 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 82.81.28.10 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/aman | Block | 1 |
| 213.8.204.33 | Israel | 147.237.0.19 | madim.atal.idf.il | Multiple Untraceable SSL Sessions from 213.8.204.33 (Open Mode) | None | 1 |
| 47.53.167.242 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman | Block | 1 |
| 79.176.198.28 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 195.154.194.111 | France | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/wp-login.php | Block | 1 |
| 37.142.64.112 | Israel | 147.237.72.166 | aka.idf.il | Malformed URL | Block | 1 |
| 77.125.147.96 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.66.31 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-13115-en/dover | Block | 1 |
| 149.78.93.80 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 1 |
| 24.61.185.177 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Unsupported Cipher | None | 1 |
| 84.228.78.60 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 101 cookies | Block | 1 |
| 2.54.14.95 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |