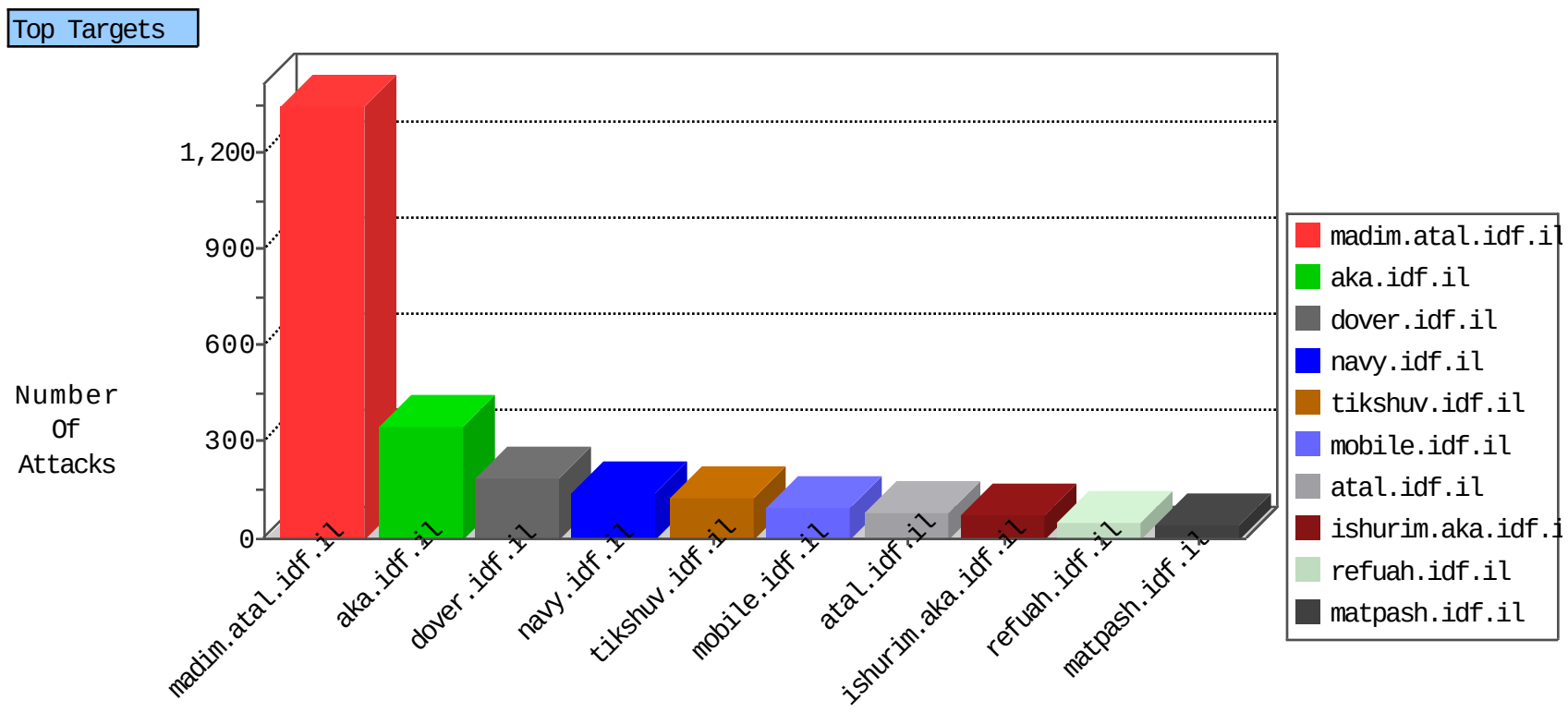
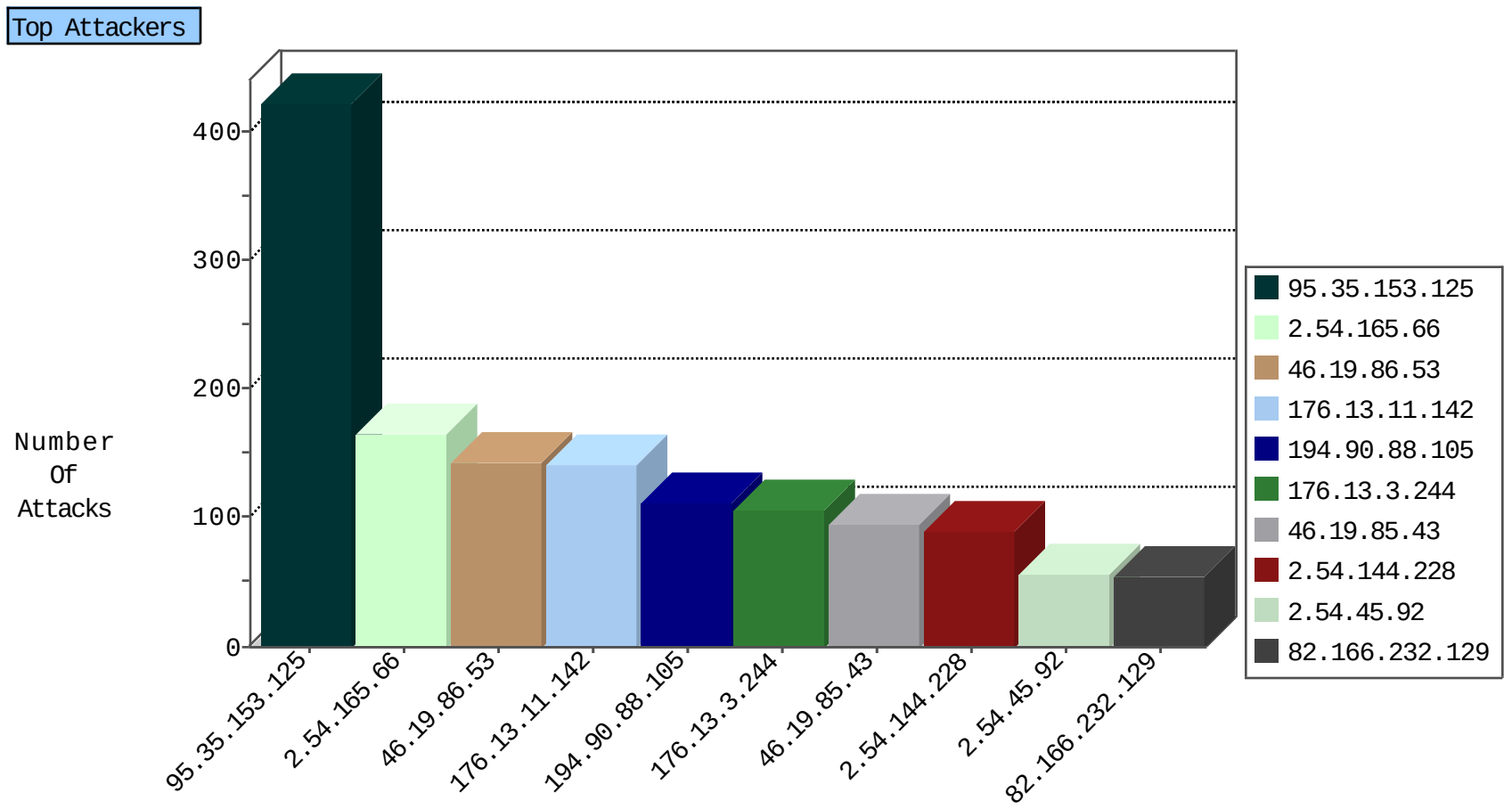
01-26-2016-10:04:00 to 01-26-2016-11:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



01-26-2016-10:04:00 to 01-26-2016-11:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 93 |
| 81.218.206.82 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 204.42.253.130 | United States | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 2 |
| 207.104.161.245 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 2 |
| 204.42.253.130 | United States | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 74.91.28.61 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | drop | 1 |
| 142.54.169.162 | United States | 147.237.77.205 | prisha.idf.il | block-sp-traf1 | drop | 1 |
| 74.91.28.61 | United States | 147.237.77.234 | halag.idf.il | block-sp-traf1 | drop | 1 |
| 142.54.169.164 | United States | 147.237.77.19 | law-forum.idf.il | block-sp-traf1 | drop | 1 |

01-26-2016-10:04:00 to 01-26-2016-11:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

01-26-2016-10:04:00 to 01-26-2016-11:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 94.76.10.253 | 147.237.77.226 | Bahrain | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.78.9 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 176.13.20.131 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.86.25 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 172.98.200.238 | 147.237.77.205 | | prisha.idf.il | ET SCAN NMAP -f -sS | 1 |
| 46.19.85.58 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 151.11.201.3 | 147.237.77.235 | Italy | sviva.idf.il | ET SCAN NMAP -f -sS | 1 |
| 132.67.250.31 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.76.10.253 | 147.237.76.198 | Bahrain | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.139.135.200 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 218.246.0.97 | 147.237.77.216 | China | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.102.168.82 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.160.242.40 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 172.98.200.238 | 147.237.77.205 | | prisha.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 46.19.86.15 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 151.11.201.3 | 147.237.77.235 | Italy | sviva.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 37.26.148.244 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.68.164.42 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.76.10.253 | 147.237.77.234 | Bahrain | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.76.10.253 | 147.237.77.216 | Bahrain | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.76.10.253 | 147.237.77.216 | Bahrain | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.76.10.253 | 147.237.76.196 | Bahrain | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.117.208.243 | 147.237.76.147 | | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 213.8.204.47 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.183.224.53 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

01-26-2016-10:04:00 to 01-26-2016-11:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 82.166.232.129 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 54 |
| 46.19.85.239 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 43 |
| 213.8.98.153 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 37 |
| 194.254.107.68 | France | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 30 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 28 |
| 2.54.144.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 185.89.217.230 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 20 |
| 176.13.2.79 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 17 |
| 84.111.125.6 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 185.89.217.235 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 16 |
| 2.54.140.60 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 185.89.217.229 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 15 |
| 185.89.217.225 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 14 |
| 185.89.217.231 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 13 |
| 2.52.7.106 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 13 |
| 109.253.218.178 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.89.217.232 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 12 |
| 176.13.5.63 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.89.217.227 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 185.89.217.233 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 185.89.217.226 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.194 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 185.89.217.228 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 7 |
| 46.19.85.242 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 185.89.217.234 | | 147.237.76.86 | navy.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 7 |
| 37.26.149.132 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 37.26.148.219 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.54.171.87 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 82.80.28.123 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.141 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 212.143.136.134 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.164.82 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.148.219 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 77.125.141.255 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.130.252.37 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.67.28.89 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 31.154.8.70 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.141 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.52.165.164 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.239 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.102 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 85.130.252.37 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.102 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.194 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.41 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.185 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.218 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 84.228.127.141 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.185 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |

01-26-2016-10:04:00 to 01-26-2016-11:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 95.35.153.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 241 |
| 2.54.165.66 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 145 |
| 46.19.86.53 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 135 |
| 95.35.153.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 122 |
| 194.90.88.105 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 112 |
| 176.13.3.244 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 106 |
| 46.19.85.43 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 84 |
| 176.13.11.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 82 |
| 2.54.144.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 68 |
| 176.13.11.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 59 |
| 95.35.153.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 95.35.153.125 | Block | 59 |
| 2.54.45.92 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 56 |
| 185.32.179.173 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 47 |
| 2.54.165.66 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 20 |
| 80.246.136.69 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 15 |
| 2.54.9.248 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 15 |
| 46.19.85.43 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 11 |
| 46.19.86.53 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 7 |
| 2.54.12.169 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 37.26.148.179 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 37.26.148.183 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 176.13.5.63 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.43.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.21.189 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.2.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.9.202 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.88 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.120 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 212.179.21.194 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg | Block | 3 |
| 109.253.221.126 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 212.179.50.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 3 |
| 109.65.108.211 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 212.179.50.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/style/shared/ | Block | 3 |
| 46.19.86.81 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.2.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.218.178 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302 | Block | 2 |
| 46.19.86.124 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 5.28.137.100 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 2 |
| 79.181.199.46 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 2 |
| 77.127.77.37 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 8.37.70.248 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1397-en/dover.aspx&usg=alkjrhix3y85kzfje5gev10yvcdwojb9mg | Block | 1 |
| 95.35.75.35 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.4 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/robots.txt | Block | 1 |
| 192.118.10.10 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 192.118.10.10 | Block | 1 |
| 5.29.51.180 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 81.218.6.122 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 46.19.86.74 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 169.229.3.91 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 79.182.96.48 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 79.182.96.48 | Block | 1 |

01-26-2016-10:04:00 to 01-26-2016-11:04:00