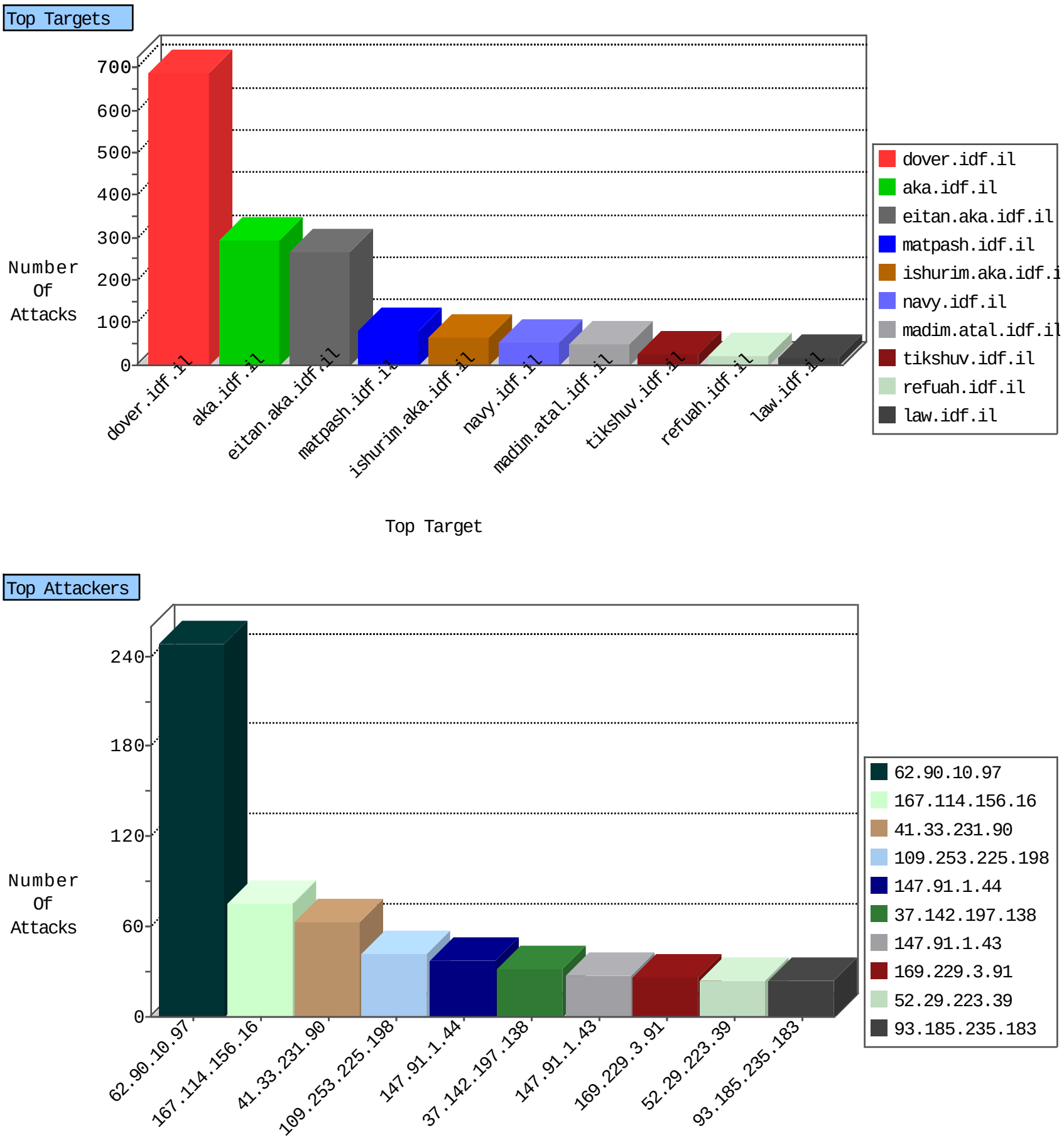
04-21-2016-14:04:04 to 04-21-2016-15:04:04

# IDF Under Attack
# Daily Report



04-21-2016-14:04:04 to 04-21-2016-15:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 2955 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 2848 |
| 134.191.232.72 | Israel | 147.237.76.42 | refuah.idf.il | JLM_Purple_Con_Limit_Http | drop | 29 |
| 104.148.71.133 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-traf1 | forward | 5 |
| 79.179.64.204 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3 |
| 104.148.71.133 | United States | 147.237.0.19 | madim.atal.idf.il | block-sp-traf1 | forward | 1 |
| 188.138.25.228 | France | 147.237.0.16 | my-kosher-kravi.idf.il | Frk_Under_Attack_Con_Tcp | drop | 1 |
| 212.235.20.201 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 104.148.71.133 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |

04-21-2016-14:04:04 to 04-21-2016-15:04:04

## Top Attackers In IPS

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

04-21-2016-14:04:04 to 04-21-2016-15:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 188.138.25.228 | 147.237.0.17 | France | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 82.81.106.102 | 147.237.77.216 | Israel | dover.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 58.218.211.11 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.116.63.50 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.138.25.228 | 147.237.0.35 | France | akaws.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.19.86.200 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.138.25.228 | 147.237.0.19 | France | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.130.5.99 | 147.237.0.15 | Lithuania | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 125.212.247.129 | 147.237.77.170 | Vietnam | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.67.119.31 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.94.199.118 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.82.78.38 | 147.237.76.34 | Netherlands | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 217.66.243.251 | 147.237.77.176 | Palestinian Territory, Occupied | matpash.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 58.218.211.11 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.114.187.3 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.45.137.76 | 147.237.0.200 | Turkey | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.138.25.228 | 147.237.0.33 | France | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 2.53.132.189 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 109.160.150.111 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.71.54.154 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

04-21-2016-14:04:04 to 04-21-2016-15:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 62.90.10.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 249 |
| 37.142.197.138 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 32 |
| 147.91.1.44 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 147.91.1.43 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 93.185.235.183 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 66.249.65.211 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 139.162.216.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 212.179.21.194 | Israel | 147.237.76.197 | e.himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 13 |
| 2.53.162.66 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 62.212.73.211 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 37.26.148.223 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 194.90.15.61 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 162.243.116.152 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 198.58.102.95 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 207.46.13.28 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 40.77.167.25 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 40.77.167.69 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 213.57.95.254 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 212.235.20.201 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 213.57.95.254 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 212.199.34.114 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 146.185.28.59 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 79.176.101.57 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 85.65.223.15 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 79.183.18.231 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 6 |
| 213.57.95.254 | Israel | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 6 |
| 66.249.69.93 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.65.241.217 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 109.253.203.77 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 5.29.69.57 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 147.91.1.41 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.250 | Israel | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 109.253.225.198 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |

04-21-2016-14:04:04 to 04-21-2016-15:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.10.118 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 2.53.167.6 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 217.132.41.33 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 217.132.41.33 | Block | 9 |
| 147.91.1.44 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 8 |
| 46.19.85.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 134.191.232.69 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 134.191.232.70 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 192.115.99.130 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113625.pdf | Block | 4 |
| 46.117.217.15 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Unauthorized HTTP Method | Block | 4 |
| 193.43.245.250 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 87.68.9.131 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 4 |
| 147.91.1.41 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 2.55.159.135 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 147.91.1.42 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 134.191.232.71 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 147.91.1.43 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 2.55.158.178 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 104.148.71.133 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Malformed URL | Block | 2 |
| 82.81.106.102 | Israel | 147.237.77.216 | dover.idf.il | Multiple Untraceable SSL Sessions from 82.81.106.102 (Protocol violation (SSL_CONN_CLIENT_HELLO)) | None | 2 |
| 87.81.227.9 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 2 |
| 2.55.159.135 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 2 |
| 134.191.232.72 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 147.91.1.45 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 66.249.73.243 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/default.asp | Block | 1 |
| 185.27.105.141 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx | Block | 1 |
| 104.148.71.133 | United States | 147.237.0.19 | madim.atal.idf.il | NULL Character in Header Name at | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | Unknown HTTP Request Method …Çj¨5wÃT0[[#5]]+jz8ÎWÔ-?æ[[#5]]ñ´^ÿ6š>[[#5]]N3V•cP[[#11]]z²†äï¬9Î”Í«[[#18]]Iên€9*E in URL | Block | 1 |
| 5.22.135.246 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Malformed URL | Block | 1 |
| 87.71.195.56 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx | None | 1 |
| 79.181.103.84 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 194.90.15.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 62.210.254.52 | France | 147.237.72.166 | aka.idf.il | Unknown Parameter &bc in www.aka.idf.il/main/giyus/captcha.ashx | None | 1 |
| 169.229.3.91 | United States | 147.237.77.235 | sviva.idf.il | Multiple Malformed URL from 169.229.3.91 | Block | 1 |
| 109.64.89.224 | Israel | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.nakhal.idf.il/1119-he/nakhal.aspx | Block | 1 |
| 5.22.135.246 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | Abnormally Long Request method | Block | 1 |
| 213.254.241.7 | France | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx | None | 1 |
| 5.22.135.246 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Distributed Illegal Byte Code Character in Header Name | Block | 1 |
| 157.55.39.223 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 68.180.230.108 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx | Block | 1 |
| 46.19.85.151 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.200 | eitan.aka.idf.il | Abnormally Long Request method | Block | 1 |
| 104.148.71.133 | United States | 147.237.0.19 | madim.atal.idf.il | NULL Character in Method €˜[[#1]][[#3]][[#1]][[#0]]o[[#0]][[#0]][[#0]] | Block | 1 |
| 5.22.135.246 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Illegal Byte Code Character in Header Value | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Multiple Abnormally Long Request from 169.229.3.91 | Block | 1 |
| 79.183.244.184 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 194.114.146.227 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 194.114.146.227 | Block | 1 |
| 66.249.65.211 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.65.211 | Block | 1 |

04-21-2016-14:04:04 to 04-21-2016-15:04:04