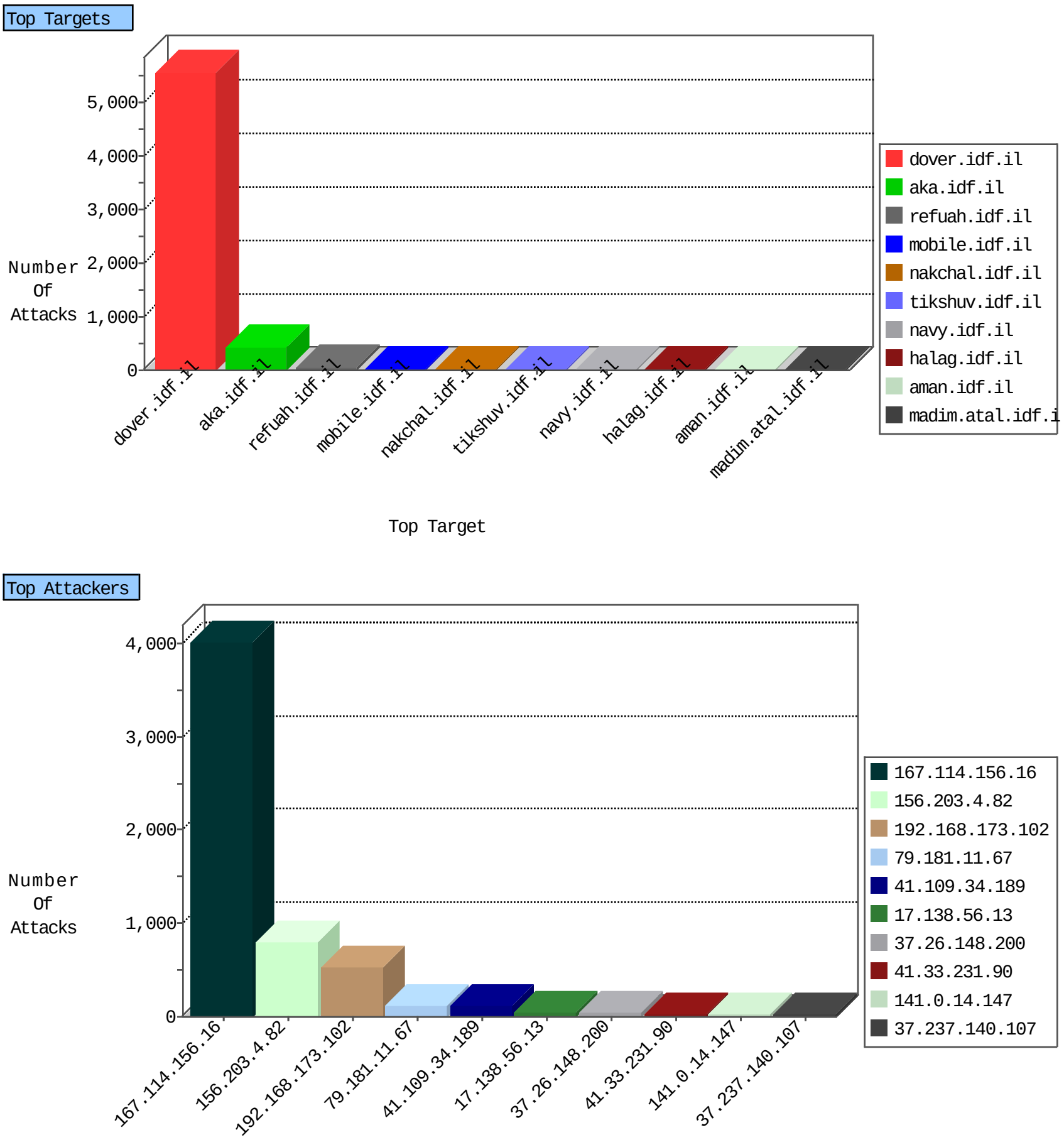
04-09-2016-17:04:06 to 04-09-2016-18:04:06

# IDF Under Attack Daily Report



04-09-2016-17:04:06 to 04-09-2016-18:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 6644 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 4019 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1144 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 155 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 54 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | DOS-LOIC-TCP-80-cat | dest-reset | 18 |
| 37.237.140.107 | Iraq | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 4 |
| 141.0.14.147 | Europe | 147.237.76.42 | refuah.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 141.0.14.147 | Europe | 147.237.76.42 | refuah.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 71.6.165.200 | United States | 147.237.77.121 | e.navy.idf.il | Block_Udp_All_Nets | drop | 1 |
| 41.109.54.44 | Algeria | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 176.31.60.249 | France | 147.237.8.28 | e.mobile-ks.idf.il | Block_Ntp_All_Net | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

04-09-2016-17:04:06 to 04-09-2016-18:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 207.232.46.209 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 12 |
| 84.111.234.25 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 78.46.50.246 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 5.9.151.22 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 69.30.234.2 | United States | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 149.78.57.114 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 5.9.151.22 | Germany | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 78.46.50.246 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 66.249.78.120 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 66.249.78.127 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 66.249.78.134 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

04-09-2016-17:04:06 to 04-09-2016-18:04:06

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 | 4 |
| 82.166.118.226 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 208.100.26.228 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 156.203.4.82 | 147.237.77.216 | Egypt | dover.idf.il | ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string | 1 |
| 93.183.201.2 | 147.237.8.45 | Ukraine | e.eitan.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 80.82.78.38 | 147.237.8.14 | Netherlands | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.100.26.228 | 147.237.72.167 | United States | ishurim.aka.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 101.200.181.38 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 88.249.106.23 | 147.237.77.216 | Turkey | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.78.38 | 147.237.72.167 | Netherlands | ishurim.aka.idf.i | ET SCAN NMAP -sS window 1024 | 1 |

04-09-2016-17:04:06 to 04-09-2016-18:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 517 |
| 192.168.173.102 | | 147.237.77.216 | dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 358 |
| 192.168.173.102 | | 147.237.72.166 | aka.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 168 |
| 79.181.11.67 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 120 |
| 17.138.56.13 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 53 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 141.0.14.147 | Europe | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 24 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 31.154.148.147 | Israel | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 16 |
| 37.26.148.200 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 37.26.148.200 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 11 |
| 37.26.148.200 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 11 |
| 37.26.148.200 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 41.102.26.221 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 37.237.140.107 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 5.102.254.234 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 37.237.140.107 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 37.237.140.107 | Iraq | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 7 |
| 5.102.195.77 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 109.64.143.180 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 37.26.148.175 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.178.194.127 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 77.127.167.153 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.28.171.208 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.148.141 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.102.195.77 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 87.70.84.200 | Israel | 147.237.76.200 | eitan.aka.idf.. | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.67.228.35 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 37.46.39.59 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 4 |
| 178.59.131.21 | Greece | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Response out of state | monitor | 4 |
| 62.90.161.134 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.223 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.154.156.123 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.33.243 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.239.26 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.22.135.15 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.154.157.84 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.154.203 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.2.25.117 | Turkey | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 94.230.86.216 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 41.96.149.228 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 46.19.85.16 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 5.28.184.189 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.167.112 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 79.180.167.112 | Block | 12 |
| 79.180.167.112 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized HTTP Method | Block | 10 |
| 37.187.131.127 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 37.187.131.127 | Block | 5 |
| 149.78.23.55 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 149.78.23.55 | Block | 4 |
| 109.67.106.115 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 93.173.20.172 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 3 |
| 87.69.225.75 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 37.142.72.86 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 66.249.65.217 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.74 | law.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 41.74.65.183 | Libyan Arab Jamahiriya | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 46.19.86.213 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 217.69.133.247 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/afhyrim | Block | 1 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 104.131.147.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/iraq/english/media.stm, | Block | 1 |
| 173.252.115.84 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 41.96.149.228 | Algeria | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 149.78.251.134 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 79.183.152.110 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 46.121.17.114 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 1 |
| 217.69.133.247 | Russian Federation | 147.237.72.166 | aka.idf.il | Unknown Parameter 55594cf0 in aka.idf.il/giyus/ | None | 1 |
| 157.55.39.194 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/chamatz/klali/default.asp | None | 1 |
| 37.237.140.107 | Iraq | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 109.65.114.10 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 68.180.229.226 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/ | Block | 1 |
| 178.59.131.21 | Greece | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 41.109.34.189 | Algeria | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 5.29.95.54 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Abnormally Long Request from 156.203.4.82 | Block | 1 |
| 84.108.69.118 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 54.153.33.233 | United States | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to 147.237.76.200/ | Block | 1 |
| 169.229.3.90 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/ts.php | Block | 1 |
| 40.77.167.25 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/robots.txt | Block | 1 |
| 77.124.21.158 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 1 |
| 196.218.59.224 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 41.230.14.223 | Tunisia | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/hinuch | Block | 1 |
| 37.26.148.175 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Malformed URL from 156.203.4.82 | Block | 1 |
| 65.55.210.119 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 169.229.3.90 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ts.php | Block | 1 |
| 41.42.199.194 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 109.173.145.70 | Poland | 147.237.77.176 | matpash.idf.il | Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx | Block | 1 |
| 46.19.85.115 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 207.46.13.169 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 156.203.4.82 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Unknown HTTP Request Method from 156.203.4.82 | Block | 1 |

04-09-2016-17:04:06 to 04-09-2016-18:04:06