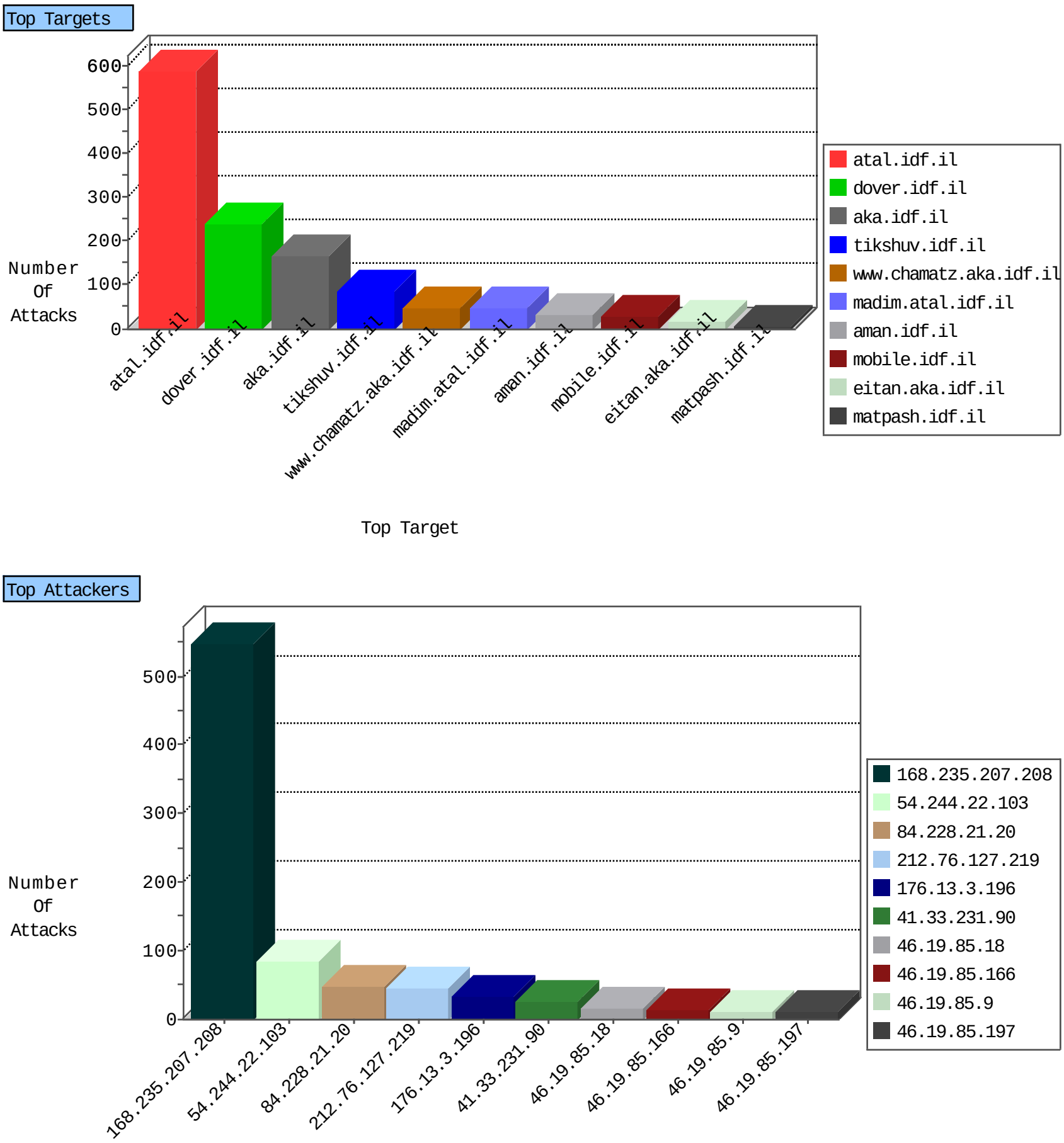
02-04-2016-00:04:05 to 02-04-2016-01:04:05

# IDF Under Attack Daily Report



02-04-2016-00:04:05 to 02-04-2016-01:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 168.235.207.208 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 191 |
| 168.235.207.208 | United States | 147.237.77.233 | atal.idf.il | Frk_Purple_Con_Limit_Http | drop | 3 |
| 168.235.207.208 | United States | 147.237.77.233 | atal.idf.il | Frk_Under_Attack_Con_Http | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 54.67.38.74 | United States | 147.237.77.74 | law.idf.il | DOS-httpdx-hreadrequest-FS | dest-reset | 1 |
| 74.91.28.59 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | drop | 1 |
| 185.130.5.224 | | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 52.32.210.122 | United States | 147.237.77.176 | matpash.idf.il | 22280: HTTP: Joomla Object Injection Vulnerability | Block | 1 |
| 93.114.64.76 | Romania | 147.237.77.176 | matpash.idf.il | 19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability | Block | 1 |
| 52.26.202.58 | United States | 147.237.77.216 | dover.idf.il | 22280: HTTP: Joomla Object Injection Vulnerability | Block | 1 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 10 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 64.233.172.155 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.78.254 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 46.148.22.26 | 147.237.77.176 | Lithuania | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.182.17.13 | 147.237.0.200 | China | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.77.212 | China | e.dover.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.240.144.65 | 147.237.77.121 | China | e.navy.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.240.144.65 | 147.237.72.217 | China | e.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.240.144.65 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 162.222.185.165 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.148.22.26 | 147.237.0.19 | Lithuania | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.76.38 | United States | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.29.81.30 | 147.237.76.30 | Israel | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 162.222.185.165 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.77.234 | China | halag.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.240.144.65 | 147.237.77.212 | China | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.240.144.65 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Potential VNC Scan 5800-5820 | 1 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.207.208 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 541 |
| 54.244.22.103 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 78 |
| 212.76.127.219 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 45 |
| 84.228.21.20 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 46.19.85.236 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 84.108.129.165 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 37.46.38.200 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 188.120.148.182 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 84.228.21.20 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 93.173.253.15 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.19.85.197 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.54.39.185 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 185.32.179.36 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.211 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 54.244.22.103 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.20 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.211 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.96 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.54.145.130 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.9 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.178.196.224 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.20 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.96 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.9 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 95.86.85.6 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.197 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 84.110.210.71 | 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 | 5 |
| 84.228.21.20 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 149.78.63.21 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.27 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 199.30.24.43 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 84.228.21.20 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | | monitor | 4 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.127 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.46.38.75 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.29.0.55 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 37.46.38.121 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 62.219.161.150 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.171.203 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.21.20 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 109.64.57.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.78.254 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.3.196 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 32 |
| 46.19.85.156 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 4 |
| 149.88.79.201 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 2 |
| 2.54.29.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 2 |
| 192.243.55.130 | Dominica | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 46.121.80.243 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 109.253.197.201 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 31.168.149.152 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 79.178.199.59 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 66.249.78.4 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx | Block | 1 |
| 192.243.55.135 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/kadatz | Block | 1 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version __atuvs=56b27e456826b332000; __atssc=facebook%3B9 | Block | 1 |
| 87.69.54.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 45.56.21.173 |  | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 2.54.39.212 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 192.243.55.130 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/news | Block | 1 |
| 46.121.80.243 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 149.78.4.149 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$90 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 37.26.147.247 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$75 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 84.108.20.180 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.78.95 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-13286-he/dover.aspx | Block | 1 |
| 192.243.55.136 | Dominica | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112435.pdf). | Block | 1 |
| 176.13.9.227 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 46.19.86.37 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 91.230.236.155 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 1 |
| 2.54.133.31 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 79.176.101.112 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 192.243.55.132 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx?catid=59027 | Block | 1 |
| 46.121.80.243 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 46.19.85.166 | Israel | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 1 |
| 37.26.148.179 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 84.108.129.165 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 66.249.78.109 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx | Block | 1 |
| 213.8.204.9 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 180.76.15.151 | China | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/list6.htm | Block | 1 |
| 46.19.86.239 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 95.86.85.6 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.19.85.18 | Israel | 147.237.77.216 | dover.idf.il | Distributed Illegal HTTP Version | Block | 1 |
| 2.54.133.31 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 79.176.101.112 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 192.243.55.134 | Dominica | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper | Block | 1 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05

| Attacker Address | Attacker Country | Target Address | **Site** | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 60.214.152.78 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | Unauthorized URL Access to 147.237.0.17/login!check.do | Block | 1 |
| 149.88.97.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$85 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 85.65.244.157 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |

02-04-2016-00:04:05 to 02-04-2016-01:04:05