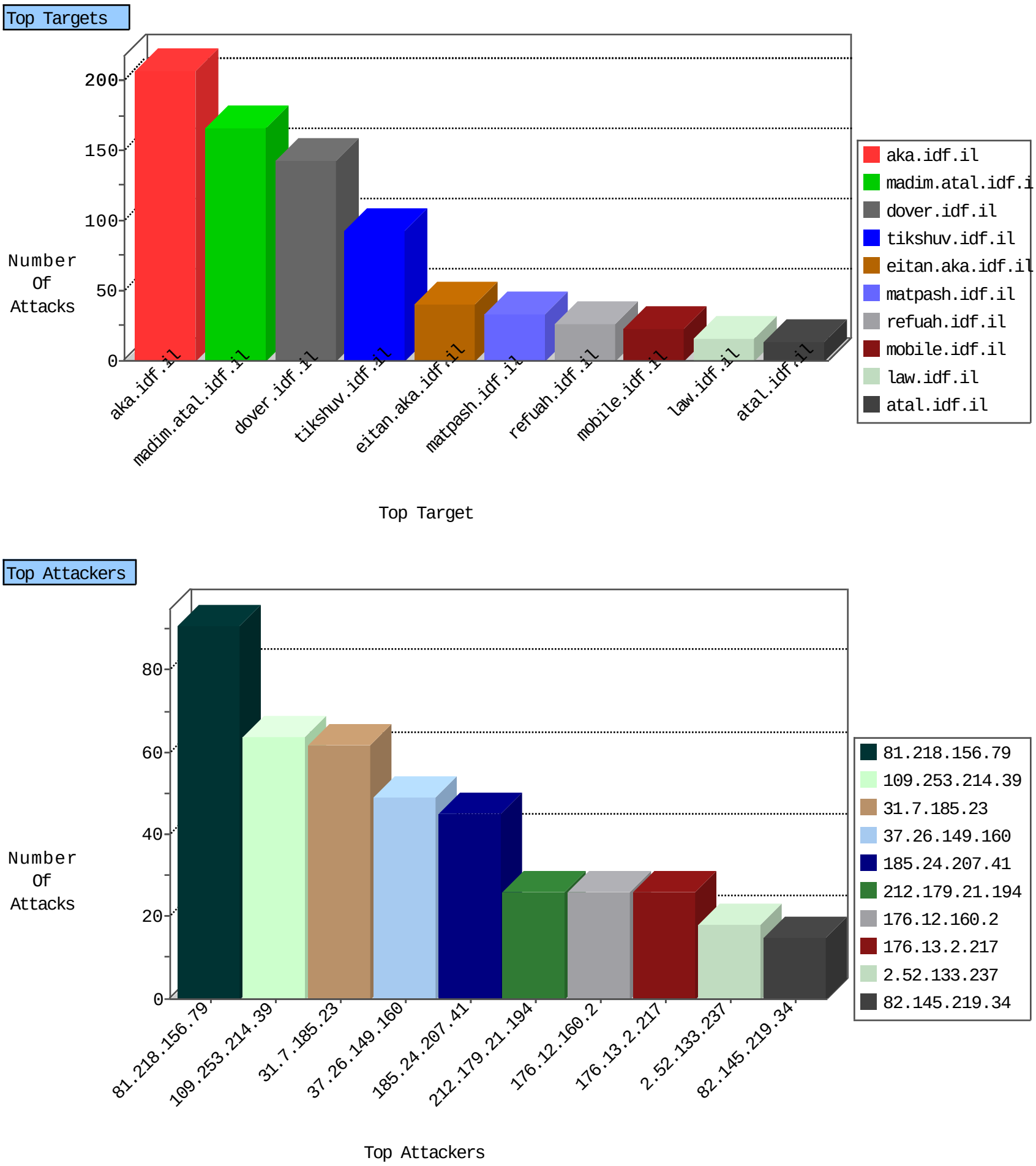
03-09-2016-14:04:03 to 03-09-2016-15:04:03

# IDF Under Attack
# Daily Report



03-09-2016-14:04:03 to 03-09-2016-15:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.145.219.34 | Europe | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 15 |
| 81.218.8.34 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.130.5.201 | | 147.237.76.30 | himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 188.138.102.50 | Germany | 147.237.77.212 | e.dover.idf.il | Block_Udp_All_Nets | drop | 1 |

03-09-2016-14:04:03 to 03-09-2016-15:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 51.254.97.22 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 92.236.71.145 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 176.13.11.73 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.120.173.102 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 198.20.69.74 | United States | 147.237.76.177 | ncore.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

03-09-2016-14:04:03 to 03-09-2016-15:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 31.7.185.23 | 147.237.76.39 | Germany | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 79.182.141.66 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 37.26.149.196 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 209.126.116.147 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 31.168.6.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 199.203.35.238 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.162.104 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.76.50.6 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.200.228 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.108.32.83 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 81.218.97.114 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 217.194.207.185 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.75.231 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 210.73.74.224 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.107.94.86 | 147.237.77.216 | Hungary | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 210.73.74.224 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.26.149.191 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 199.203.173.198 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 118.165.79.90 | 147.237.76.39 | Taiwan | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.232.98.38 | 147.237.77.170 |  | maarachot.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 82.81.4.86 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 210.73.74.224 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.72.202.214 | 147.237.77.216 | Netherlands | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 210.73.74.224 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |

03-09-2016-14:04:03 to 03-09-2016-15:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.24.207.41 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 26 |
| 2.52.133.237 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 46.19.85.114 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 10 |
| 185.32.179.4 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 176.12.160.2 | Israel | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 9 |
| 176.12.160.2 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 185.24.207.41 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 213.151.61.1 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 85.65.176.188 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 212.199.151.119 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 109.253.129.56 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 147.236.238.40 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 81.218.126.219 | Israel | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 141.8.132.112 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 31.7.185.23 | Germany | 147.237.76.34 | yohalan.idf.il | drop | First packet isn't SYN | drop | 6 |
| 79.180.219.64 | 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 |
| 141.0.14.58 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 185.24.207.41 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 2.52.32.21 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 31.7.185.23 | Germany | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 4 |
| 185.24.207.41 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 109.253.218.144 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 31.7.185.23 | Germany | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 4 |
| 46.19.85.38 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 31.7.185.23 | Germany | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 4 |
| 46.19.85.42 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.121.233.46 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 176.12.160.2 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 5.28.163.173 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.154.162.195 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.7.185.23 | Germany | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 3 |
| 31.7.185.23 | Germany | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.253.218.144 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 2.54.133.157 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.95.186 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 80.246.139.84 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 79.177.200.114 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.146.177 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 64.134.243.238 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.181.104.31 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 147.235.8.31 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 87.71.114.145 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.148.238 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.147.165 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 37.26.149.191 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.7.185.23 | Germany | 147.237.76.199 | e.nakchal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 3 |
| 77.126.165.39 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 130.193.51.91 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

03-09-2016-14:04:03 to 03-09-2016-15:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 81.218.156.79 | Israel | 147.237.0.34 | tikshuv.idf.il | Automated Vulnerability Scanning V1 | Block | 91 |
| 109.253.214.39 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 64 |
| 37.26.149.160 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 49 |
| 176.13.2.217 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 26 |
| 147.235.8.31 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 5 |
| 217.160.155.145 | Germany | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 217.160.155.145 | Block | 5 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.233 | Block | 3 |
| 213.151.38.66 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 213.151.38.66 | Block | 3 |
| 2.54.2.150 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.122 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.157.175 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.19.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.23.192 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 37.26.149.154 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 131.253.25.173 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.151.38.66 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 213.151.38.66 | Block | 2 |
| 46.19.86.31 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 87.71.114.145 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 2 |
| 37.46.39.72 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 185.32.179.4 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1599 | Block | 2 |
| 46.19.85.100 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 213.151.61.1 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 84.229.38.75 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 190.42.125.133 | Peru | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.180.150.131 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl91 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 66.249.64.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx | Block | 1 |
| 94.230.93.61 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 37.26.146.192 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 81.218.89.58 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 213.113.25.210 | Sweden | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png | Block | 1 |
| 79.180.150.131 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 130.193.51.92 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp | Block | 1 |
| 46.19.85.230 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.52.171.56 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 213.254.241.7 | United Kingdom | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx | None | 1 |
| 87.70.48.31 | Israel | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 194.90.99.129 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/1.he/960.css | Block | 1 |
| 79.183.169.121 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 147.236.238.40 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 94.230.93.109 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx | Block | 1 |
| 81.218.97.114 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 185.32.179.4 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.180.150.131 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 46.19.85.230 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 87.70.48.31 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation SortDir in www.idf.il/1065-en/dover.aspx | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 157.55.39.65 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 109.7.69.34 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/ | Block | 1 |
| 185.32.179.4 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 185.32.179.4 | Block | 1 |

03-09-2016-14:04:03 to 03-09-2016-15:04:03