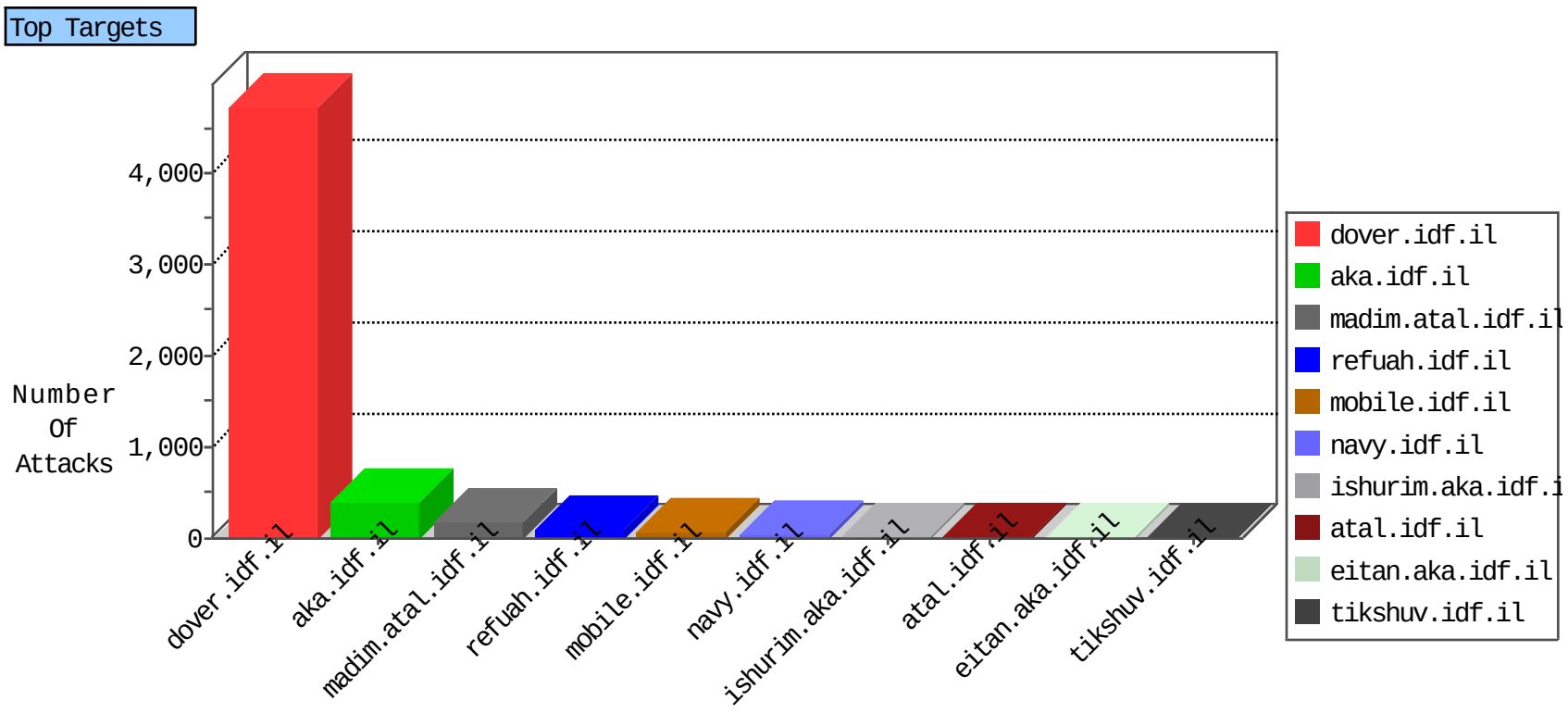
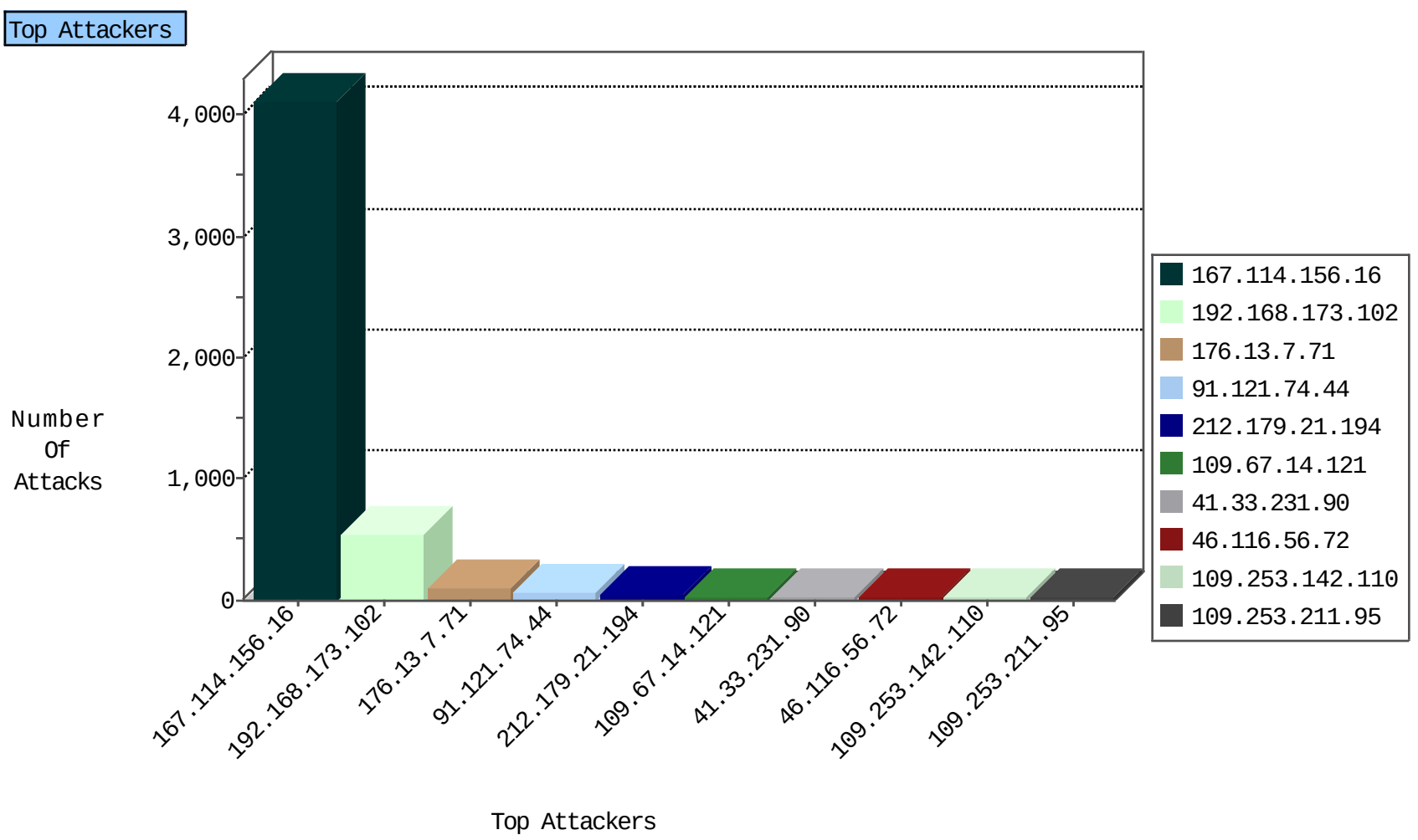
04-10-2016-08:04:06 to 04-10-2016-09:04:06

# IDF Under Attack Daily Report

Top Targets




Top Attackers



04-10-2016-08:04:06 to 04-10-2016-09:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 4120 |
| 79.177.194.237 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 80.246.138.51 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 81.218.165.186 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Block_Udp_All_Nets | drop | 5 |
| 81.218.165.186 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 125.65.46.143 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | forward | 2 |
| 209.126.127.17 | United States | 147.237.77.121 | e.navy.idf.il | Block_Udp_All_Nets | drop | 2 |
| 77.126.253.17 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 209.126.127.17 | United States | 147.237.77.205 | prisha.idf.il | Block_Udp_All_Nets | drop | 2 |
| 209.126.127.17 | United States | 147.237.77.170 | maarachot.idf.il | Block_Udp_All_Nets | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.227 | e.hamaz.idf.il | Block_Udp_All_Nets | drop | 1 |
| 192.3.220.210 | United States | 147.237.8.27 | e.madim.atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.235 | sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.74 | law.idf.il | Block_Udp_All_Nets | drop | 1 |
| 111.85.191.131 | China | 147.237.76.38 | e.e.meitav.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.178 | e.matpash.idf.il | Block_Udp_All_Nets | drop | 1 |
| 176.31.60.249 | France | 147.237.8.14 | e.orchot.idf.il | Block_Ntp_All_Net | drop | 1 |
| 209.126.127.17 | United States | 147.237.77.243 | mobile.idf.il | Block_Udp_All_Nets | drop | 1 |
| 111.85.191.131 | China | 147.237.76.198 | e.yohalan.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 176.31.60.249 | France | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 1 |

04-10-2016-08:04:06 to 04-10-2016-09:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 131.253.25.153 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 62.210.143.245 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 108.59.8.70 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 61.135.189.122 | China | 147.237.76.31 | nakchal.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 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 5.8.45.251 | Chile | 147.237.77.216 | dover.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |

04-10-2016-08:04:06 to 04-10-2016-09:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 5.8.45.251 | 147.237.77.216 | Chile | dover.idf.il | SQL Injection - Select From | 5 |
| 199.203.84.80 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 4 |
| 5.29.177.172 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.227.225.218 | 147.237.76.198 | United States | e.yohalan.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 108.46.33.175 | 147.237.77.216 | United States | 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 |
| 66.240.213.93 | 147.237.8.46 | United States | e.chinuch.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.85.216 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 218.108.132.58 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 179.184.176.50 | 147.237.76.44 | Brazil | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.204.187.90 | 147.237.76.34 | Kazakstan | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.180.192.236 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.219.232.76 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.28 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

04-10-2016-08:04:06 to 04-10-2016-09:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 192.168.173.102 | | 147.237.77.216 | dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 350 |
| 192.168.173.102 | | 147.237.72.166 | aka.idf.il | Geo-location enforcement | Geo-location inbound enforcement | monitor | 184 |
| 91.121.74.44 | France | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 57 |
| 109.67.14.121 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 34 |
| 109.253.211.95 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 2.54.177.238 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 2.54.169.4 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 212.199.251.227 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 12 |
| 46.116.56.72 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 46.19.85.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 46.116.56.72 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 46.19.85.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 79.177.194.237 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 46.116.56.72 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 80.246.139.150 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 80.246.137.166 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 109.253.3.191 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.54.131.226 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 62.90.45.107 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.52.162.226 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 80.246.139.170 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 109.253.144.39 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 82.80.29.186 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 91.228.248.251 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 212.199.142.90 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.62 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 106.38.241.149 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 2.52.161.186 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 80.246.136.182 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 207.241.229.223 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 80.246.136.182 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 207.241.229.225 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 94.230.86.208 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.181 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 4 |
| 109.253.144.39 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 91.200.12.114 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 46.19.85.209 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 176.13.7.85 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 62.219.52.35 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 80.179.9.7 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 95.35.146.233 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.126.29.118 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.196.22 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.13.80 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.28.161.12 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.97.7 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 147.236.38.2 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-10-2016-08:04:06 to 04-10-2016-09:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.7.71 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 96 |
| 109.253.142.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 31 |
| 212.179.21.194 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 212.179.21.194 | Block | 24 |
| 2.53.34.242 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 19 |
| 5.28.143.155 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 15 |
| 212.179.21.194 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 212.179.21.194 | Block | 11 |
| 46.19.86.159 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.12.236 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 200.187.64.91 | Brazil | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 200.187.64.91 | Block | 3 |
| 2.52.149.208 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.67.59.95 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/120203 | Block | 2 |
| 2.54.169.4 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 212.179.21.194 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/images/shared/side_line_bg.gif" | Block | 1 |
| 31.168.187.238 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 1 |
| 66.249.66.123 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2368.jpg | Block | 1 |
| 91.121.74.44 | France | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 91.121.74.44 | Block | 1 |
| 37.26.148.160 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 216.218.206.68 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 66.249.66.125 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2372.jpg | Block | 1 |
| 46.116.165.63 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 5.8.45.251 | Chile | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 91.121.74.44 | France | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.224 | Block | 1 |
| 41.42.3.214 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 109.253.206.38 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx | None | 1 |
| 79.176.51.205 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 54.153.33.145 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 147.237.77.226/ | Block | 1 |
| 5.8.45.251 | Chile | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/interface/ipsconnect/ipsconnect.php | Block | 1 |
| 92.126.5.174 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi'a=0 | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/en | Block | 1 |
| 46.19.85.132 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 125.65.46.143 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idlethumbs.net/wp-admin/admin-ajax.php | Block | 1 |
| 82.166.190.11 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg | Block | 1 |
| 66.249.65.12 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.65.12 | Block | 1 |
| 93.115.135.7 | Romania | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp | Block | 1 |
| 66.249.66.121 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2277.jpg | Block | 1 |
| 46.19.85.148 | Israel | 147.237.77.243 | mobile.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 84.95.207.127 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 66.249.65.217 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx | Block | 1 |

04-10-2016-08:04:06 to 04-10-2016-09:04:06