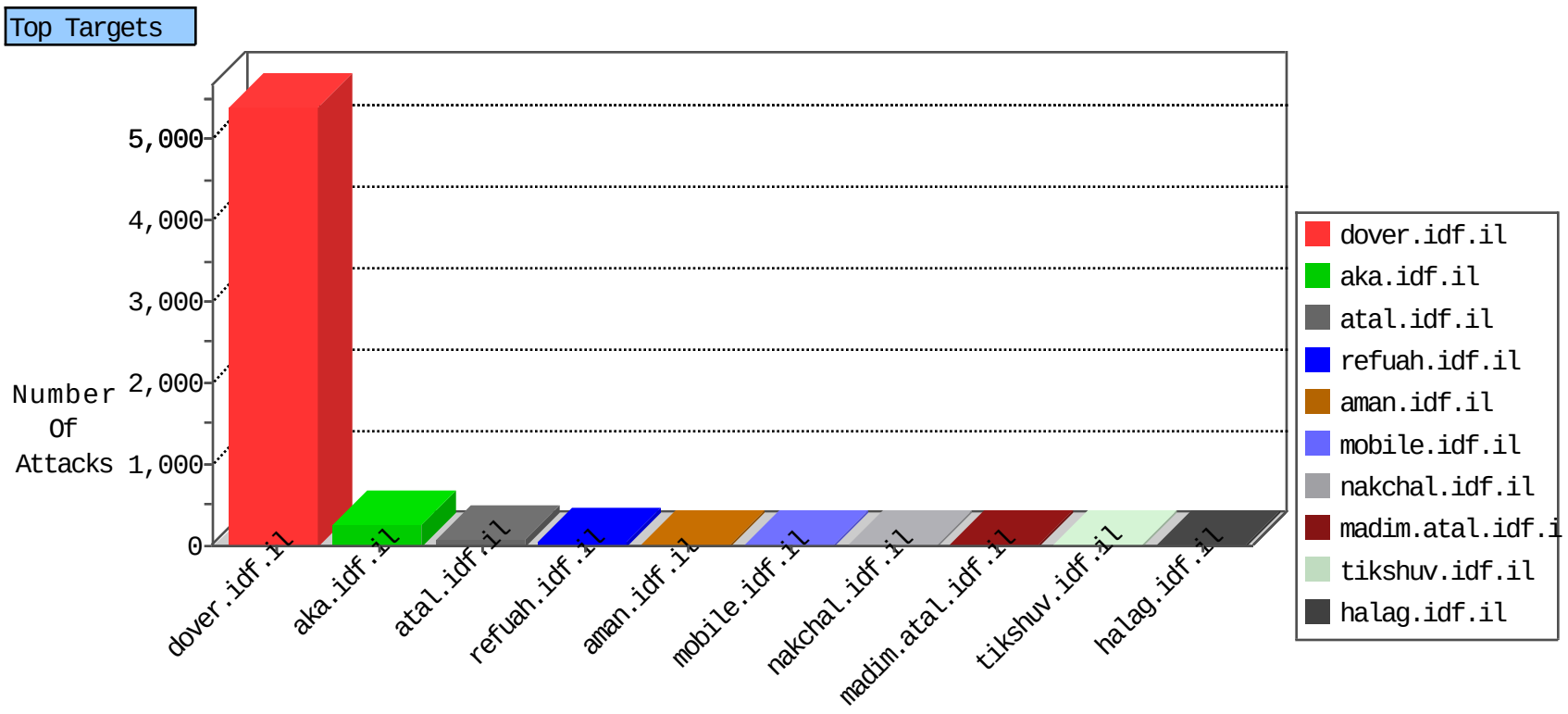
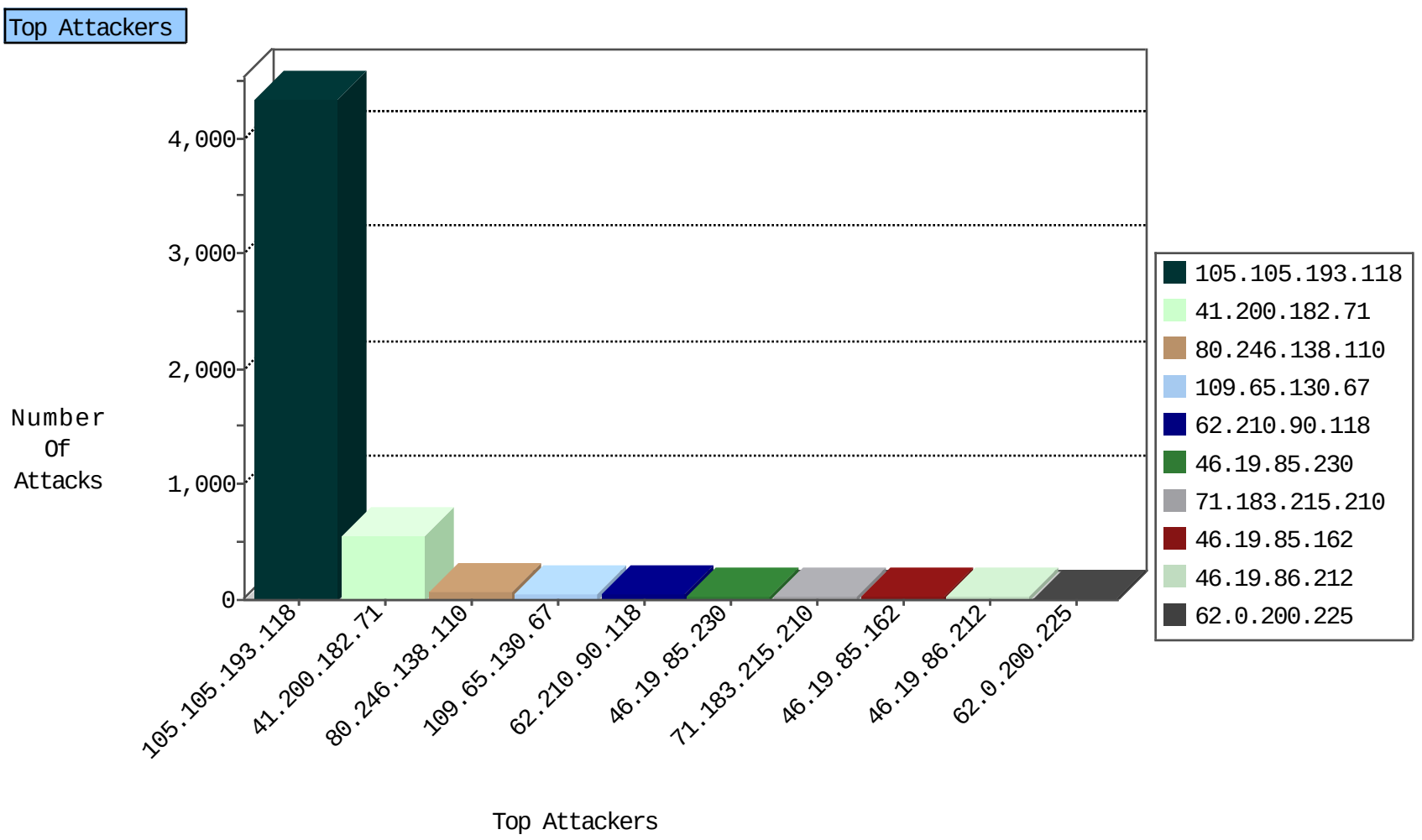
09-26-2016-19:04:09 to 09-26-2016-20:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-26-2016-19:04:09 to 09-26-2016-20:04:09

## 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 Page Flood Attack | forward | 9091 |
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 9049 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 6654 |
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 3526 |
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 714 |
| 217.148.45.113 | United Kingdom | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 3 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 93.174.94.235 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Black List | drop | 1 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 1 |
| 197.45.132.217 | Egypt | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 1 |
| 61.147.110.17 | China | 147.237.76.31 | nakchal.idf.il | JLM_Under_Attack_Con_Tcp | drop | 1 |

09-26-2016-19:04:09 to 09-26-2016-20:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 62.210.90.118 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 36 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | C1000076: HTTP: Trying to locate existing FCKeditor | Permit | 2 |
| 62.210.90.118 | France | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 51.254.129.90 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 62.210.90.118 | France | 147.237.72.156 | aman.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 62.210.90.118 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 199.58.86.206 | United States | 147.237.72.156 | aman.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 62.210.90.118 | France | 147.237.76.42 | refuah.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | 0360: HTTP: Protected Directory Access (~root) | Block | 1 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | 0863: HTTP: fpadmcgi.exe Access | Block | 1 |
| 104.192.169.238 | United States | 147.237.72.166 | aka.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | 1185: HTTP: IIS admcgi CGI Access | Block | 1 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | C1000064: HTTP: Access to - admin.asp | Permit | 1 |

09-26-2016-19:04:09 to 09-26-2016-20:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 105.105.193.118 | 147.237.77.216 | Algeria | dover.idf.il | SERVER-WEBAPP backup access | 3 |
| 93.174.89.146 | 147.237.0.17 | Netherlands | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 91.201.236.158 | 147.237.77.179 | Ukraine | e.mazi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 58.220.2.5 | 147.237.8.28 | China | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.0.17 | United Kingdom | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 106.38.241.106 | 147.237.76.86 | China | navy.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 50.245.143.138 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 105.105.193.118 | 147.237.77.216 | Algeria | dover.idf.il | Tehila defacement attempt (-Hacked By- sent to Web Server) | 1 |
| 50.245.143.138 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 104.218.120.204 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 93.174.89.146 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 93.174.89.146 | 147.237.0.16 | Netherlands | my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 91.201.236.158 | 147.237.72.156 | Ukraine | aman.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 211.149.244.79 | 147.237.77.212 | China | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 139.162.13.205 | 147.237.76.42 | Singapore | refuah.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 58.218.200.137 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 105.105.193.118 | 147.237.77.216 | Algeria | dover.idf.il | WEB-CGI finger access | 1 |
| 50.245.143.138 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 105.105.193.118 | 147.237.77.216 | Algeria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 41.200.182.71 | 147.237.77.216 | Algeria | dover.idf.il | ET WEB_SERVER Poison Null Byte | 1 |
| 105.105.193.118 | 147.237.77.216 | Algeria | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.89.146 | 147.237.76.30 | Netherlands | himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

09-26-2016-19:04:09 to 09-26-2016-20:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 581 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 52 |
| 109.65.130.67 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 30 |
| 71.183.215.210 | United States | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 25 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 19 |
| 62.0.200.225 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 46.19.85.230 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 109.65.130.67 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 15 |
| 46.19.85.230 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 14 |
| 46.19.85.233 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 14 |
| 185.32.179.215 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 13 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 109.253.215.161 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.212 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.160 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 85.64.124.34 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 46.19.85.162 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.55.144.30 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.234.118 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 95.86.94.101 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.5.74 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 80.246.138.110 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 6 |
| 46.19.85.162 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.86.212 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 77.127.53.132 | Israel | 147.237.77.243 | mobile.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 |
| 46.19.85.162 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 217.132.37.126 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 176.13.5.74 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 217.132.37.126 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.85.162 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.212 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 46.19.86.33 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.86.24 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 85.65.186.62 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 185.120.126.13 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.85.184 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 77.138.88.53 | France | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.86.24 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 85.65.186.62 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 46.19.86.13 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.110.176.46 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 160.39.82.247 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 37.26.149.248 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 185.3.147.225 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 176.13.245.178 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |

09-26-2016-19:04:09 to 09-26-2016-20:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 105.105.193.118 | Block | 1261 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 41.200.182.71 | Block | 474 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 18 |
| 2.53.133.70 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 79.179.162.67 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Unauthorized HTTP Method | Block | 5 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 41.200.182.71 | Block | 5 |
| 83.22.248.194 | Poland | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 3 |
| 37.26.149.241 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.33.57 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.178.33.57 | Block | 3 |
| 46.19.85.92 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 194.242.168.39 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/sachar | Block | 3 |
| 46.19.86.87 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.158.143 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 109.253.144.119 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/ | Block | 2 |
| 212.25.102.63 | Israel | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 2 |
| 77.138.109.4 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 2 |
| 109.64.87.214 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Unauthorized HTTP Method | Block | 2 |
| 109.64.87.214 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/1/ | Block | 2 |
| 79.177.32.115 | Israel | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 79.177.32.115 | Block | 1 |
| 204.79.180.66 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main/ | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.234 | halag.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.249.66.179 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 105.105.193.118 | Algeria | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/uniscan965/ | Block | 1 |
| 46.19.86.182 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 212.76.122.94 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman/site/default.asp | Block | 1 |
| 71.183.215.210 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/favicon.ico | Block | 1 |
| 185.89.217.230 | Netherlands | 147.237.76.42 | refuah.idf.il | URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png | Block | 1 |
| 66.249.64.85 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in www.eitan.aka.idf.il/1028-en/eitan.aspx | None | 1 |
| 46.19.85.210 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version _pk_ses.20.8afc=* | Block | 1 |
| 79.177.32.115 | Israel | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 1 |
| 2.55.144.30 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 164.138.126.28 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/hashal/default.aspx | Block | 1 |
| 66.249.69.228 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 46.121.112.160 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 106.38.241.106 | China | 147.237.76.86 | navy.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 41.200.182.71 | Algeria | 147.237.77.216 | dover.idf.il | NULL Character in URL /[[#0]] | Block | 1 |
| 213.57.46.70 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 190.142.222.59 | Venezuela | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.64.166 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1710 | Block | 1 |
| 109.253.144.119 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 109.253.144.119 | Block | 1 |
| 84.109.36.149 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 46.19.85.210 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL _pk_id.20.8afc=151efa73691d5696.1469720625.9.1474906331.1474906331.; | Block | 1 |
| 31.168.1.202 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 212.25.102.63 | Israel | 147.237.77.216 | dover.idf.il | Distributed Illegal HTTP Version | Block | 1 |
| 79.177.95.252 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Request Content Type text/ping | Block | 1 |
| 165.225.86.55 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp | Block | 1 |
| 66.249.76.30 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1711 | Block | 1 |
| 62.90.49.25 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2017 | Block | 1 |
| 79.179.162.67 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 79.179.162.67 | Block | 1 |
| 77.138.167.111 | France | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |

09-26-2016-19:04:09 to 09-26-2016-20:04:09