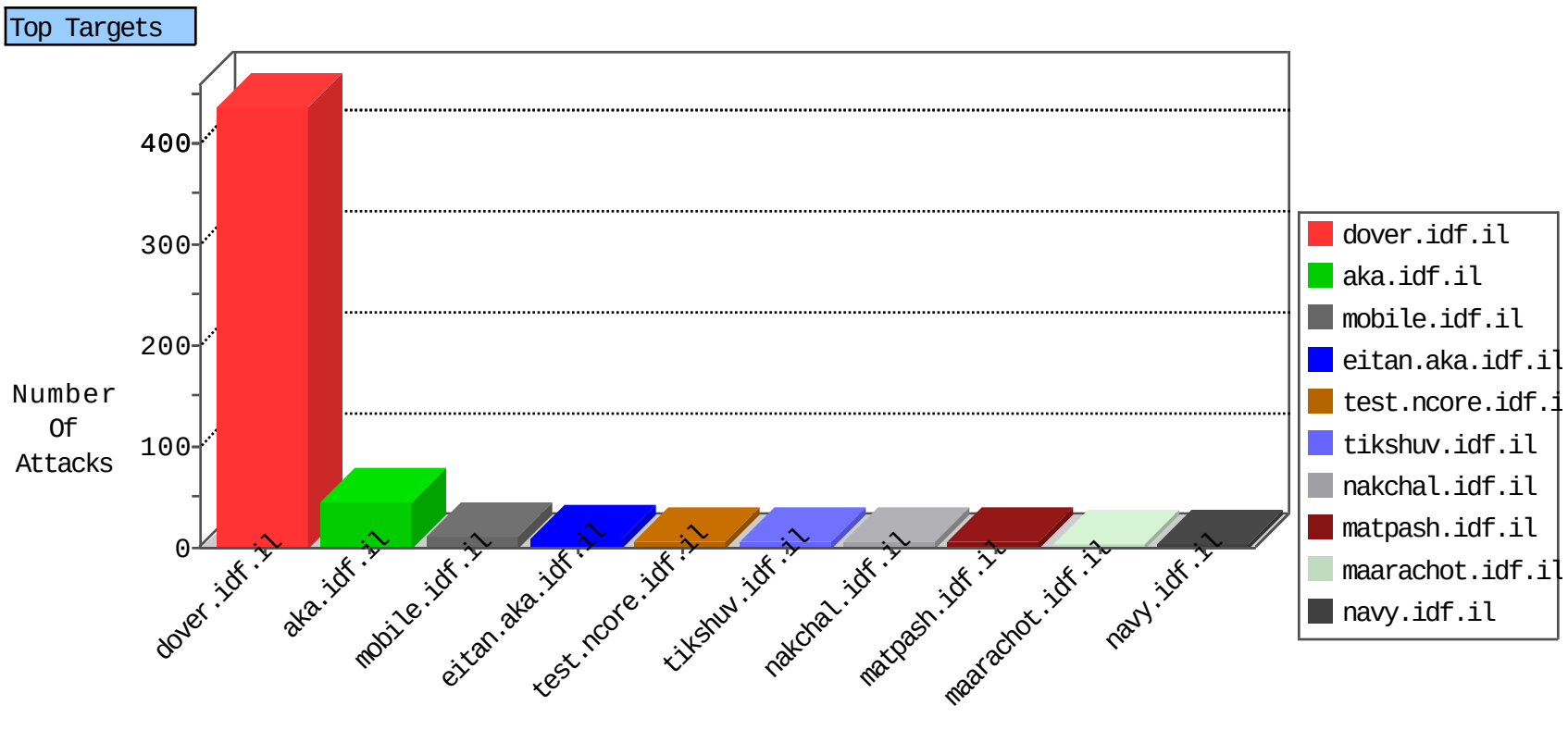
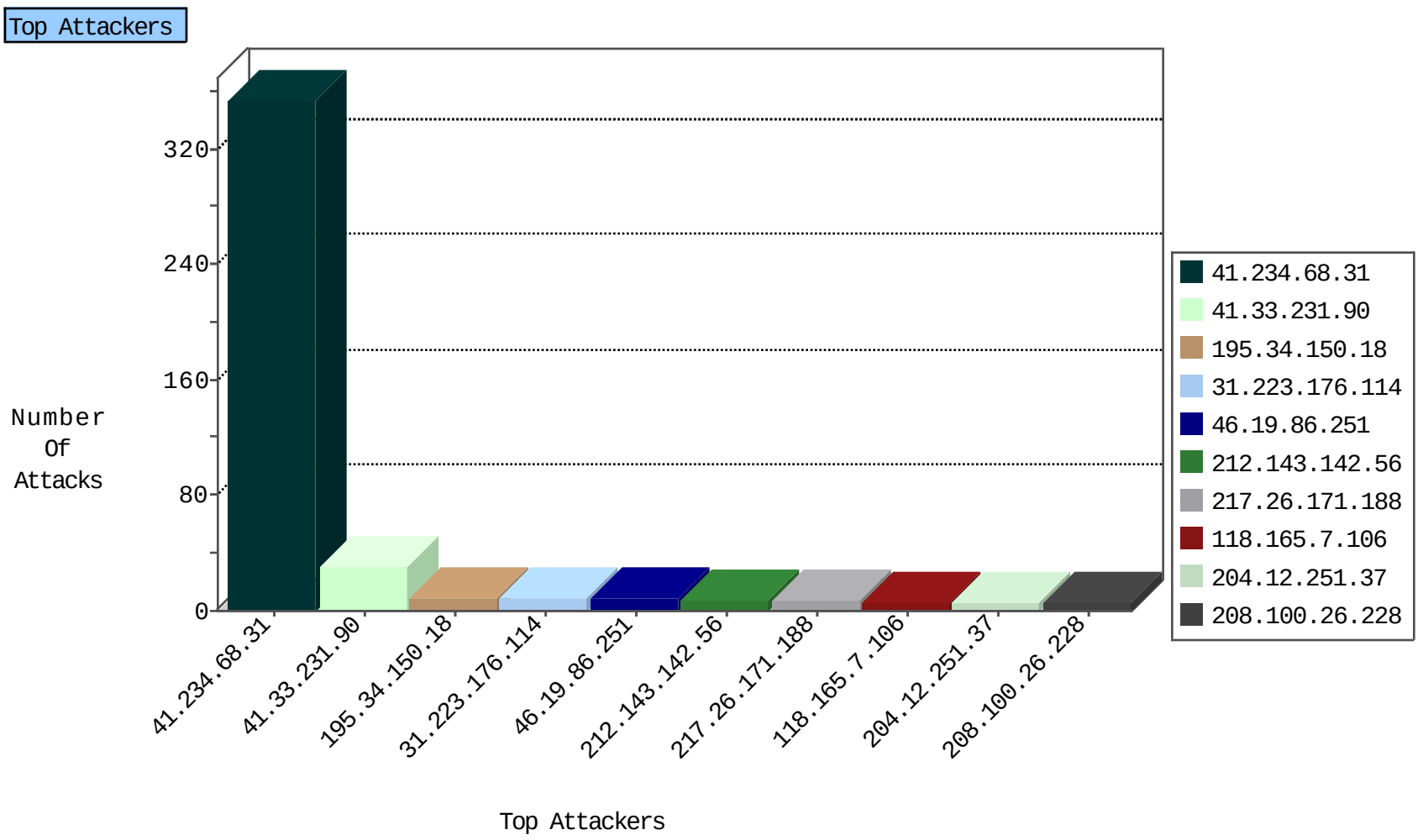
02-26-2016-01:09:42 to 02-26-2016-02:09:42

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-26-2016-01:09:42 to 02-26-2016-02:09:42

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.234.68.31 | Egypt | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 2147 |
| 41.234.68.31 | Egypt | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 5 |
| 217.26.171.188 | Moldova, Republic of | 147.237.76.176 | test.ncore.idf.il | L4 Source or Dest Port Zero | drop | 4 |
| 217.26.171.188 | Moldova, Republic of | 147.237.77.176 | matpash.idf.il | L4 Source or Dest Port Zero | drop | 3 |
| 163.44.112.118 | Japan | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 208.100.26.228 | United States | 147.237.77.205 | prisha.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.94.111.1 | | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 208.100.26.228 | United States | 147.237.77.235 | sviva.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 |
| 208.100.26.228 | United States | 147.237.77.61 | e.cogat.idf.il | Block_Ntp_All_Net | drop | 1 |
| 208.100.26.228 | United States | 147.237.77.243 | mobile.idf.il | Block_Ntp_All_Net | drop | 1 |
| 59.29.207.55 | Korea, Republic of | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 208.100.26.228 | United States | 147.237.77.74 | law.idf.il | Block_Ntp_All_Net | drop | 1 |

02-26-2016-01:09:42 to 02-26-2016-02:09:42

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 61.135.189.103 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 4 |
| 108.59.8.80 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 51.255.65.31 | United Kingdom | 147.237.77.170 | maarachot.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 151.80.31.151 | Italy | 147.237.72.166 | aka.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.43 | United Kingdom | 147.237.77.170 | maarachot.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 151.80.31.151 | Italy | 147.237.76.42 | refuah.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.47 | United Kingdom | 147.237.77.170 | maarachot.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 157.55.39.92 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 207.46.13.145 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 51.255.65.27 | United Kingdom | 147.237.77.170 | maarachot.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

02-26-2016-01:09:42 to 02-26-2016-02:09:42

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 |
| 218.246.0.97 | 147.237.72.217 | China | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.204.188.142 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 204.101.135.203 | 147.237.0.16 | Canada | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 38.105.146.70 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 118.165.7.106 | 147.237.76.38 | Taiwan | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.76.30 | Taiwan | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.0.19 | Taiwan | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.44.133.108 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 104.44.133.108 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -f -sS | 1 |
| 50.204.188.142 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 204.101.135.203 | 147.237.76.201 | Canada | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 41.234.68.31 | 147.237.77.216 | Egypt | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.82.164.152 | 147.237.0.33 | Poland | idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.58.76.88 | 147.237.0.33 | Ukraine | idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.76.177 | Taiwan | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.76.31 | Taiwan | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.0.34 | Taiwan | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.182.17.13 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.44.133.108 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 88.249.106.23 | 147.237.72.167 | Turkey | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

02-26-2016-01:09:42 to 02-26-2016-02:09:42

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.234.68.31 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 34 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 204.12.251.37 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.251 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 31.223.176.114 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 103.239.103.231 | Hong Kong | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 41.234.68.31 | Egypt | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 79.176.55.222 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.68.240.57 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.146.190 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 217.132.20.139 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.107.113 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.222.1 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.137.9 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.78.216 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.168.178 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.223.176.114 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 5.22.129.82 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 188.120.154.49 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 204.79.180.103 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 165.215.209.15 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 84.228.146.70 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 93.174.91.29 | Netherlands | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.199 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.146 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.65 | United States | 147.237.76.176 | test.ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 204.79.180.126 | United States | 147.237.76.200 | eitan.aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 141.212.122.194 | United States | 147.237.76.198 | e.yohalan.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 52.53.253.180 | United States | 147.237.77.176 | matpash.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |
| 141.212.122.128 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 118.98.92.109 | Indonesia | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 198.20.69.74 | United States | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 159.226.95.66 | China | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 79.176.232.127 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.147 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.72 | United States | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 188.165.15.148 | France | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 5.22.129.82 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 89.138.182.231 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 141.212.122.195 | United States | 147.237.76.38 | e.e.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 54.183.204.102 | United States | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |
| 141.212.122.128 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 123.125.71.108 | China | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 100.127.132.39 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

02-26-2016-01:09:42 to 02-26-2016-02:09:42

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 186.202.150.247 | Brazil | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 186.202.150.247 | Block | 3 |
| 186.202.150.247 | Brazil | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/wp-admin/ | Block | 1 |
| 91.196.50.33 | Poland | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php | Block | 1 |
| 46.19.86.251 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn | Block | 1 |
| 89.248.174.4 | Netherlands | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to 147.237.77.19/ | Block | 1 |
| 5.29.95.197 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 189.144.206.93 | Mexico | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 91.196.50.33 | Poland | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php | Block | 1 |
| 66.249.69.81 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/925-he/atal.aspx | Block | 1 |
| 157.55.39.37 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 89.248.174.4 | Netherlands | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 40.77.167.29 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 207.46.13.143 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |
| 109.65.152.145 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 66.249.69.89 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/927-he/atal.aspx | Block | 1 |
| 185.82.203.241 |  | 147.237.77.216 | dover.idf.il | Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx | Block | 1 |
| 89.248.174.4 | Netherlands | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 147.237.77.226/ | Block | 1 |
| 40.77.167.37 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter c in www.aka.idf.il/miluim/templates/inner.asp | None | 1 |
| 113.76.90.196 | China | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 66.249.69.97 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/926-he/atal.aspx | Block | 1 |
| 2.54.11.30 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 91.196.50.33 | Poland | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php | Block | 1 |
| 41.234.68.31 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to / | Block | 1 |
| 141.212.122.145 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SSL Untraceable Connection - Unknown Server Certificate | None | 1 |
| 84.112.185.114 | Austria | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp | Block | 1 |
| 2.54.187.96 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |

02-26-2016-01:09:42 to 02-26-2016-02:09:42