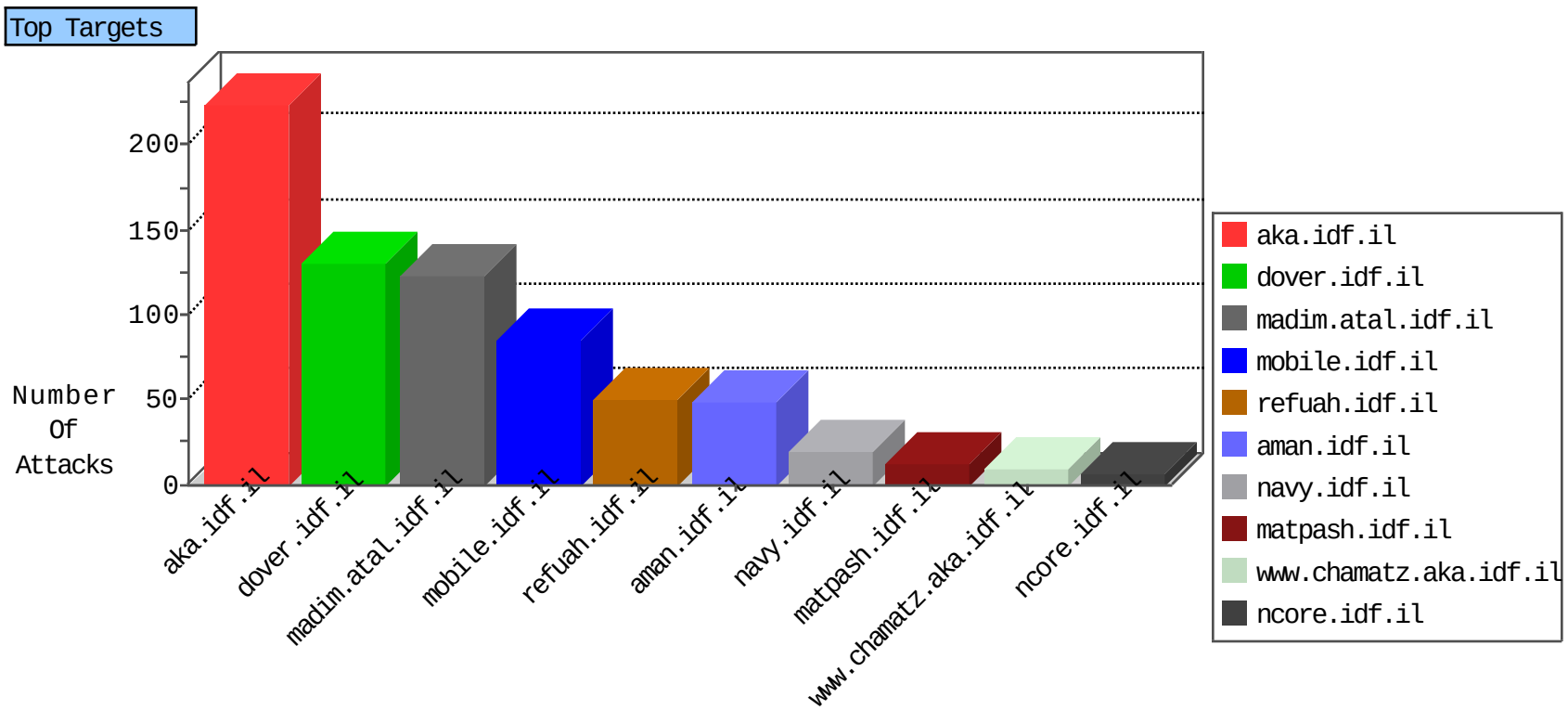
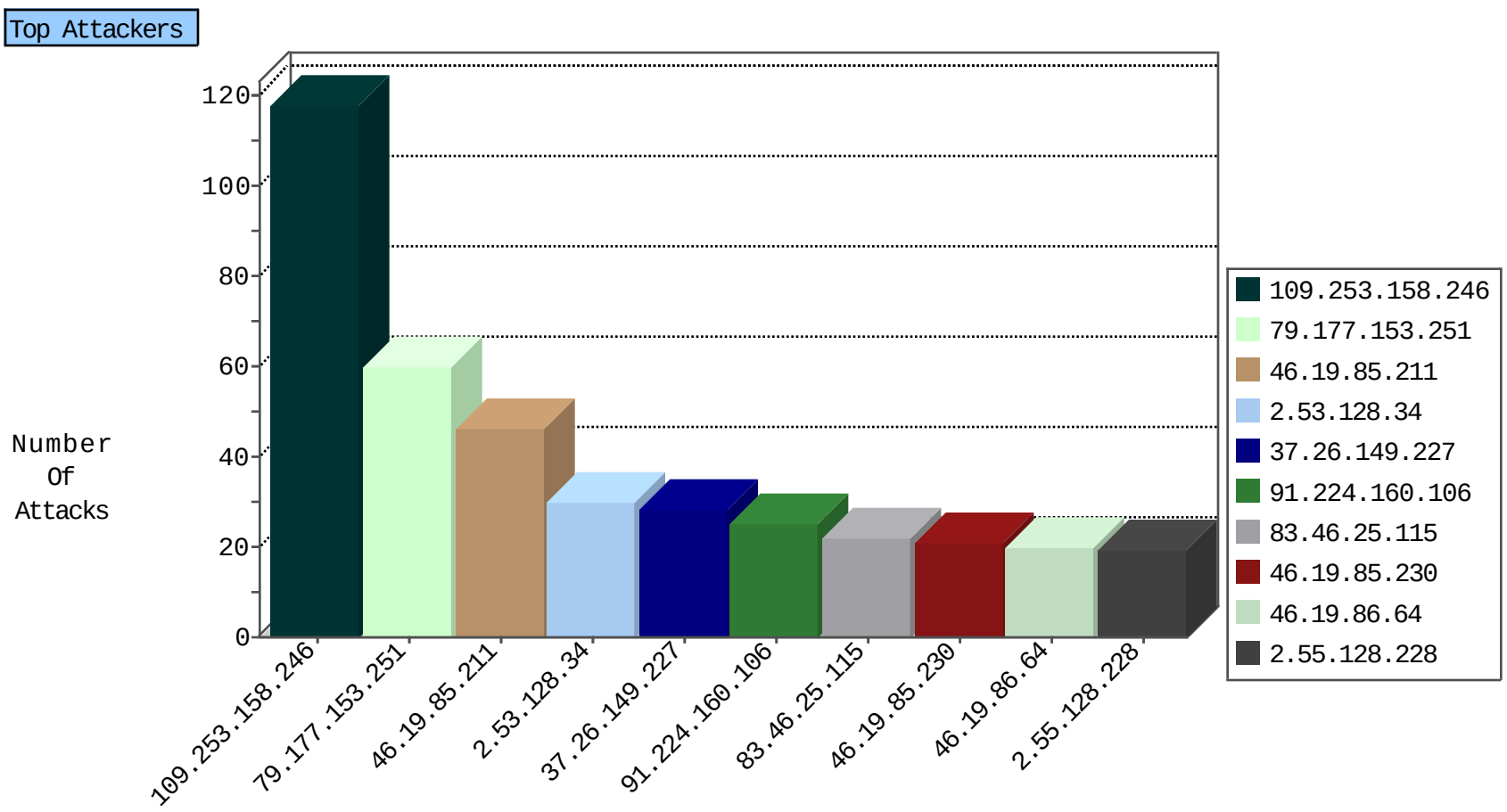
09-15-2016-21:04:06 to 09-15-2016-22:04:06

# IDF Under Attack Daily Report




Top Attackers

09-15-2016-21:04:06 to 09-15-2016-22:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 198.133.224.147 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 139.78.141.243 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 198.82.160.238 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.10.120.193 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 2 |
| 195.113.161.82 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 200.19.159.35 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 216.48.80.12 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 156.56.250.227 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 134.197.113.3 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.42.142.45 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 143.225.229.236 | Italy | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 130.195.4.69 | New Zealand | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 164.107.127.12 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 200.19.159.34 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 153.90.1.34 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 131.247.2.241 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 141.22.213.34 | Germany | 147.237.72.167 | ishurim.aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.93.229.138 | United States | 147.237.72.167 | ishurim.aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 153.90.1.35 | United States | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 134.117.226.180 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.8.126.111 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 141.212.113.178 | United States | 147.237.72.156 | aman.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.93.229.139 | United States | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |

09-15-2016-21:04:06 to 09-15-2016-22:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 69.30.198.178 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 123.126.113.17 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

09-15-2016-21:04:06 to 09-15-2016-22:04:06

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 6 |
| 91.224.160.106 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.224.160.106 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.224.160.106 | 147.237.77.205 | Netherlands | prisha.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.224.160.106 | 147.237.76.177 | Netherlands | ncore.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.224.160.106 | 147.237.76.34 | Netherlands | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.72.156 | Netherlands | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.77.234 | Netherlands | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.8.28 | Netherlands | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.77.216 | Netherlands | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.17 | Netherlands | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.77.178 | Netherlands | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 64.137.168.128 | 147.237.0.35 | Canada | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.201.225.73 | 147.237.77.234 | Ukraine | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.201.225.73 | 147.237.77.205 | Ukraine | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.73 | 147.237.77.170 | Ukraine | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.81.216.190 | 147.237.76.30 | United States | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.162 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.72.166 | Netherlands | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 133.208.21.66 | 147.237.77.227 | Japan | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.8.46 | Netherlands | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.77.226 | Netherlands | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 202.155.58.28 | 147.237.77.61 | Indonesia | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.77.170 | Netherlands | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.227.67.158 | 147.237.76.176 | Sweden | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.73 | 147.237.77.227 | Ukraine | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.224.160.106 | 147.237.76.202 | Netherlands | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.201.225.73 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.76.197 | Netherlands | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.23.181.171 | 147.237.76.177 | Ukraine | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.32.179.128 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

09-15-2016-21:04:06 to 09-15-2016-22:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.177.153.251 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 60 |
| 2.53.128.34 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 37.26.149.227 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 46.19.85.230 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 46.19.85.211 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 14 |
| 46.19.85.211 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 100.92.96.84 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.86.64 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 46.19.86.64 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 83.46.25.115 | Spain | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 46.19.85.211 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 87.71.50.7 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.211 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 2.55.128.228 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.98 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 87.71.50.7 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 46.19.85.73 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 109.66.110.11 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 46.19.86.243 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 185.24.207.120 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 83.46.25.115 | Spain | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.243 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 109.66.110.11 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 2.53.141.78 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 185.24.207.120 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 2.55.128.228 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 93.208.90.45 | Germany | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 46.19.86.250 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 185.24.207.120 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 2.55.128.228 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 79.177.242.250 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 2.53.128.132 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 46.19.85.244 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 2.53.128.132 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 46.19.85.244 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.110.11 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 185.3.147.89 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 2.53.128.132 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 213.8.204.29 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 3 |
| 83.46.25.115 | Spain | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 109.64.9.155 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 46.19.85.98 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 2 |
| 66.249.93.87 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 84.109.1.137 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 109.253.130.131 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 46.19.85.158 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 93.172.151.116 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 2.53.128.132 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |

09-15-2016-21:04:06 to 09-15-2016-22:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.253.158.246 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 118 |
| 213.8.204.19 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 37.26.149.227 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 46.116.64.54 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.116.64.54 | Block | 4 |
| 2.53.37.97 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.28.185.76 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx | Block | 2 |
| 109.65.46.195 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 2 |
| 31.154.49.145 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 2 |
| 2.53.167.61 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 83.46.25.115 | Spain | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 159.220.74.2 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/patzar/news/default.asp | Block | 1 |
| 77.139.75.72 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main | Block | 1 |
| 66.102.9.22 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/home/default.aspx | Block | 1 |
| 217.132.49.220 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx | None | 1 |
| 77.138.128.113 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 46.116.64.54 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/ | Block | 1 |
| 185.32.179.28 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 77.237.146.28 | Czech Republic | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to / | Block | 1 |
| 66.249.64.128 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg | Block | 1 |
| 77.138.162.100 | France | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 1 |
| 46.121.253.6 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 199.195.156.135 | United States | 147.237.72.156 | aman.idf.il | PHP Attempt | Block | 1 |
| 79.180.236.134 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/guyus | Block | 1 |
| 66.249.64.134 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 31.154.81.1 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/.main/giyus/ | Block | 1 |
| 120.27.35.11 | China | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 77.138.191.22 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 66.102.9.2 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 199.195.156.135 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/wp-login.php | Block | 1 |
| 68.180.228.171 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx | Block | 1 |
| 120.27.35.11 | China | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wp-login.php | Block | 1 |
| 77.139.69.124 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx | Block | 1 |
| 66.102.9.5 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 2.53.184.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 87.71.50.7 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 77.138.21.143 | France | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 1 |

09-15-2016-21:04:06 to 09-15-2016-22:04:06