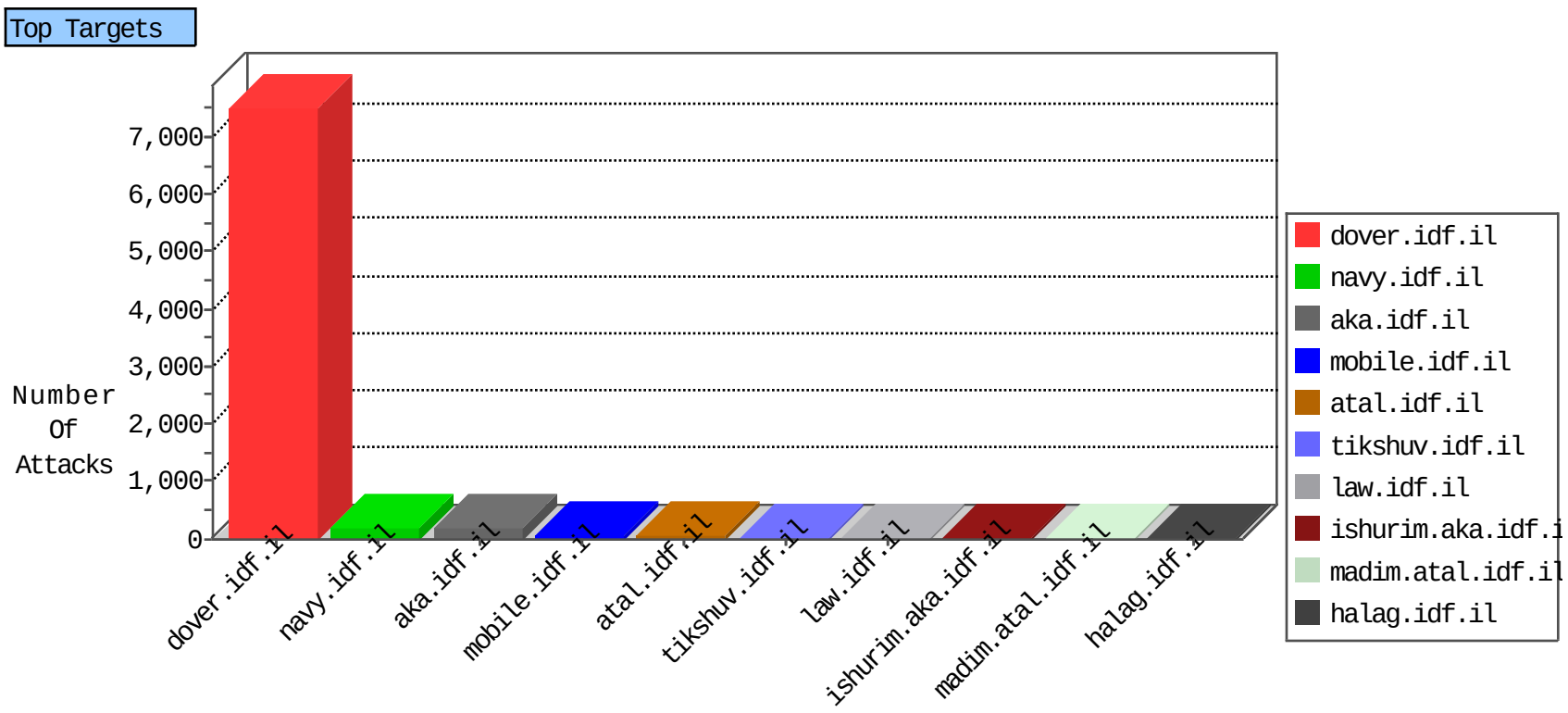
09-06-2016-22:04:06 to 09-06-2016-23:04:06

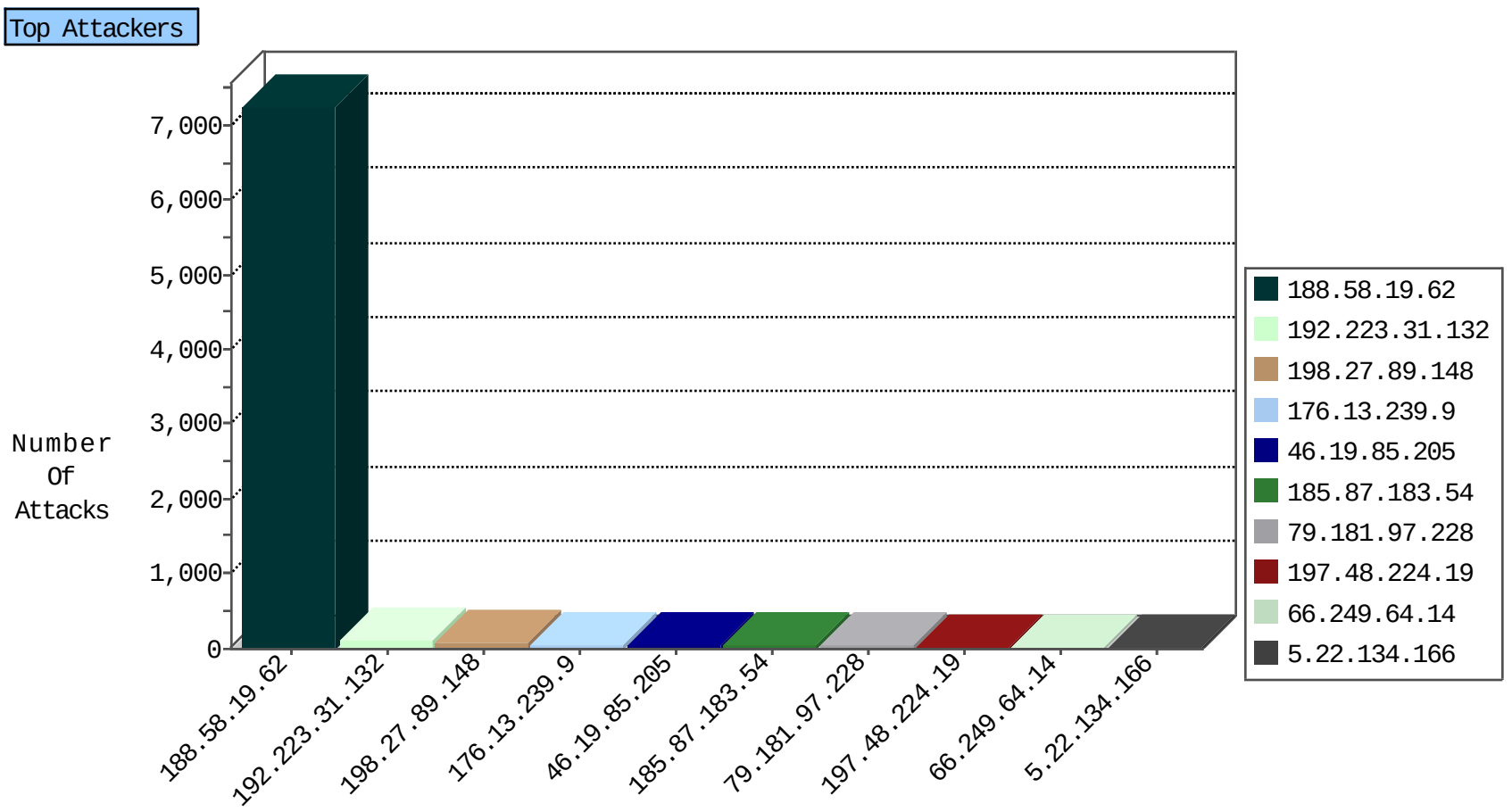
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

09-06-2016-22:04:06 to 09-06-2016-23:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.181.161.77 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 2 |
| 177.222.227.56 | Brazil | 147.237.76.148 | gqcenter.aka.idf.il | JLM_Under_Attack_Con_Tcp | drop | 1 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 185.128.40.162 | Switzerland | 147.237.76.34 | yohalan.idf.il | Black List | drop | 1 |
| 185.128.40.162 | Switzerland | 147.237.76.44 | e.refuah.idf.il | Black List | drop | 1 |

09-06-2016-22:04:06 to 09-06-2016-23:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.200.12.47 | Ukraine | 147.237.77.233 | atal.idf.il | C1000016: HTTP: administrator in URI | Permit | 8 |
| 199.58.86.209 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 94.154.239.69 | Ukraine | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.100 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 123.125.125.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

09-06-2016-22:04:06 to 09-06-2016-23:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.64.14 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 23 |
| 188.58.19.62 | 147.237.77.216 | Turkey | dover.idf.il | ET WEB_SERVER LOIC Javascript DDoS Inbound | 2 |
| 62.210.113.183 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 62.210.38.242 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 94.102.48.195 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.77.235 | Ukraine | sviva.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 177.200.192.50 | 147.237.8.50 | Brazil | e.tikshuv.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 64.137.171.55 | 147.237.76.42 | Canada | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.13.14.195 | 147.237.77.216 | Israel | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 117.21.248.87 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.77.226 | China | www.chamatz.aka.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 117.21.248.87 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 109.60.153.178 | 147.237.77.19 | Russian Federation | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.205.151.198 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 61.240.144.65 | 147.237.0.33 | China | idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 106.120.209.153 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 208.100.26.228 | 147.237.77.212 | United States | e.dover.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.172.71.251 | 147.237.76.34 | Ukraine | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.52.71 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.100.26.228 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 5.255.90.133 | 147.237.76.39 | Netherlands | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.77.235 | Ukraine | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.200.192.50 | 147.237.8.50 | Brazil | e.tikshuv.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 177.200.192.50 | 147.237.8.50 | Brazil | e.tikshuv.idf.il | ET SCAN NMAP -f -sS | 1 |
| 64.137.171.55 | 147.237.0.19 | Canada | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.21.248.87 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.21.248.87 | 147.237.76.30 | China | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 117.21.248.87 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.72.156 | China | aman.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 106.120.209.153 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 218.205.151.198 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 46.172.71.251 | 147.237.76.202 | Ukraine | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.167.6.84 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.100.26.228 | 147.237.77.212 | United States | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.255.90.133 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

09-06-2016-22:04:06 to 09-06-2016-23:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 188.58.19.62 | Turkey | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 6894 |
| 188.58.19.62 | Turkey | 147.237.77.216 | dover.idf.il | drop | | drop | 333 |
| 192.223.31.132 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 63 |
| 79.181.97.228 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 32 |
| 176.13.239.9 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 22 |
| 5.22.134.166 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 18 |
| 188.58.19.62 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 109.64.99.62 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 109.65.181.168 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 176.13.239.9 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 13 |
| 176.13.239.9 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 13 |
| 46.19.85.164 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 192.223.31.132 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 12 |
| 192.223.31.132 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 12 |
| 79.182.111.167 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 11 |
| 185.87.183.54 | Iran, Islamic Republic of | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 10 |
| 185.87.183.54 | Iran, Islamic Republic of | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 2.53.163.18 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 213.151.53.48 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 37.26.147.181 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.241 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 207.46.13.68 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 185.87.183.54 | Iran, Islamic Republic of | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 9 |
| 197.48.224.19 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 197.48.224.19 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.241 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 185.87.183.54 | Iran, Islamic Republic of | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 79.178.169.246 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 46.19.86.204 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 192.223.31.132 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.47 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.10 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.76.73 | United States | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 95.35.95.46 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.86.67 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 198.27.89.148 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 197.48.224.19 | Egypt | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 192.223.31.132 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 198.27.89.148 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 197.48.224.19 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 198.27.89.148 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 198.27.89.148 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.86.67 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 198.27.89.148 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 198.27.89.148 | United States | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |

09-06-2016-22:04:06 to 09-06-2016-23:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 199.243.180.70 | Canada | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/giyus/qanda/default.asp | Block | 9 |
| 46.19.86.56 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 46.19.85.254 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 85.65.42.202 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 80.246.137.138 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 4 |
| 213.57.59.50 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 4 |
| 79.180.167.174 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/ | Block | 3 |
| 37.26.147.181 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.151 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 80.246.138.98 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 3 |
| 84.108.25.59 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 64.62.219.167 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 46.19.85.164 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.53.163.18 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 89.139.185.249 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 2 |
| 64.62.219.148 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 77.138.107.34 | France | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 79.180.167.174 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.180.167.174 | Block | 2 |
| 66.249.69.246 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp | Block | 1 |
| 109.65.167.53 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 46.121.228.3 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 5.28.174.106 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx | None | 1 |
| 73.22.155.10 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/ | Block | 1 |
| 89.237.101.124 | France | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 64.62.219.163 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.138.255.16 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |
| 66.249.69.250 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 141.226.218.113 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 85.65.117.89 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 64.62.219.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 79.181.97.228 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 207.46.13.111 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/main/smalim/showbig.aspx | None | 1 |
| 77.138.36.226 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim | Block | 1 |
| 91.200.12.47 | Ukraine | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 1 |
| 79.178.169.246 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 148.251.2.180 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 87.70.61.82 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |
| 64.62.219.76 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 79.182.111.167 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 77.138.107.34 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |
| 66.102.9.3 | 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 |
| 91.200.12.47 | Ukraine | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to atal.idf.il/wp-login.php | Block | 1 |
| 46.19.86.214 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 82.81.22.185 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/ | Block | 1 |
| 79.179.114.159 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 157.55.39.115 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.19.85.179 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.182.111.167 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il./favicon.ico | Block | 1 |

09-06-2016-22:04:06 to 09-06-2016-23:04:06