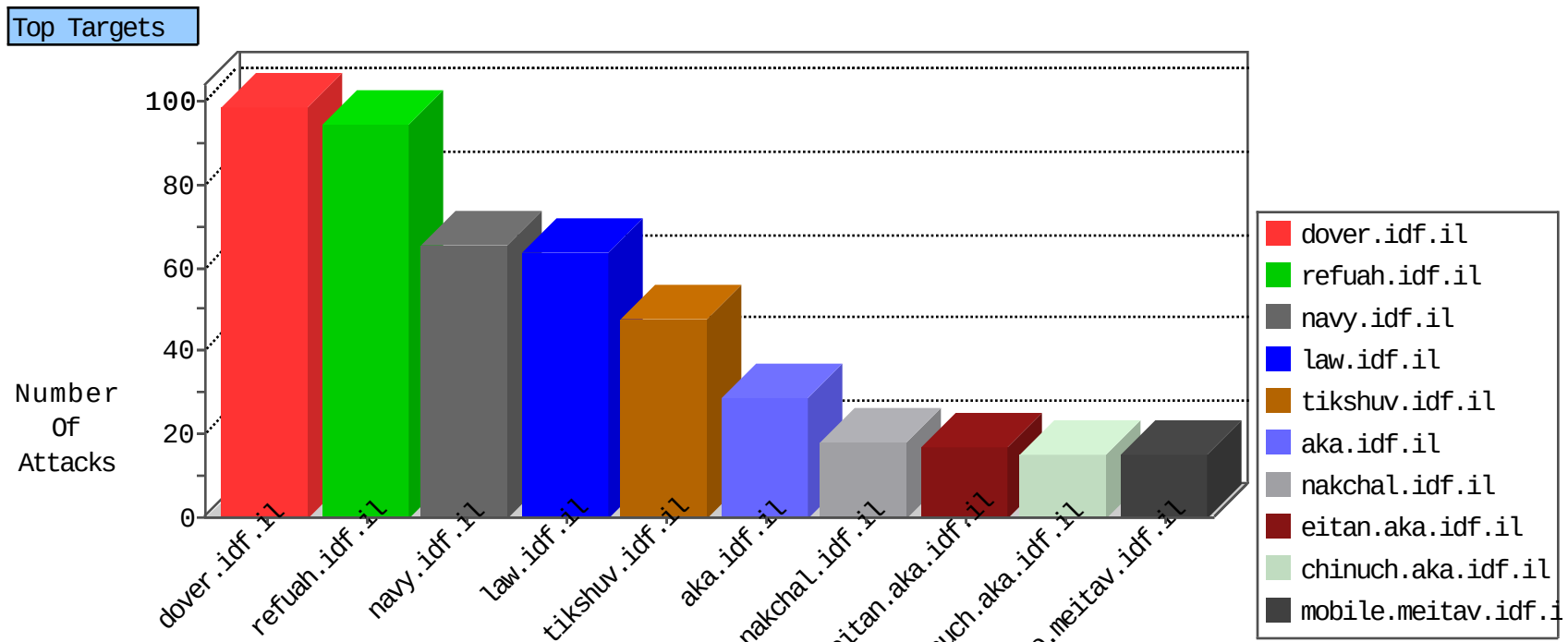
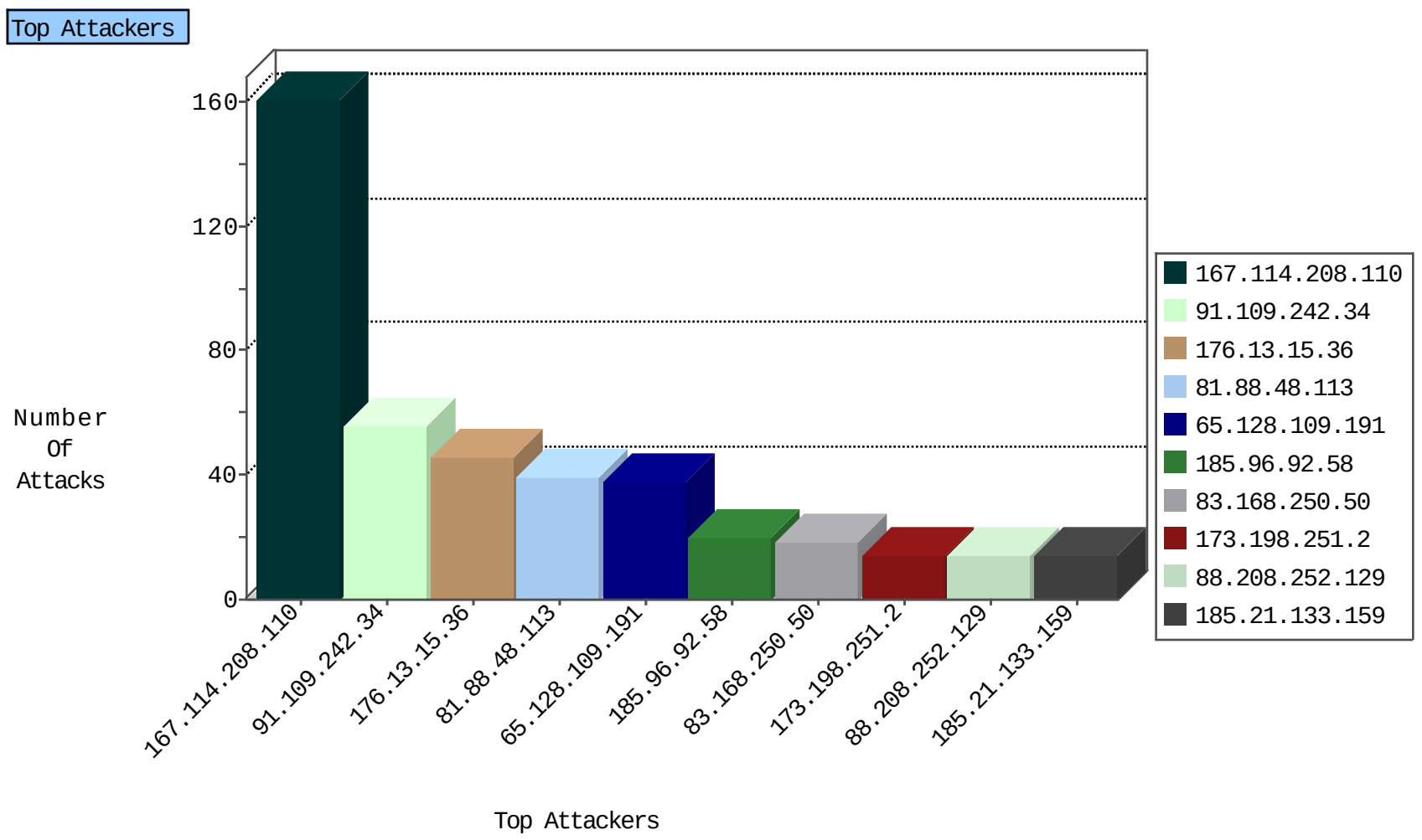
09-01-2016-04:04:00 to 09-01-2016-05:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-01-2016-04:04:00 to 09-01-2016-05:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.94.111.1 | Russian Federation | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |

09-01-2016-04:04:00 to 09-01-2016-05:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.109.242.34 | United Kingdom | 147.237.76.42 | refuah.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 12 |
| 81.88.48.113 | Italy | 147.237.0.34 | tikshuv.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 12 |
| 217.37.125.121 | United Kingdom | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 91.109.242.34 | United Kingdom | 147.237.76.42 | refuah.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 81.88.48.113 | Italy | 147.237.0.34 | tikshuv.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 173.198.251.2 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 185.21.133.159 | United Kingdom | 147.237.77.216 | dover.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 88.208.252.129 | United Kingdom | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 185.96.92.58 | United Kingdom | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 158.85.253.245 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 91.109.242.34 | United Kingdom | 147.237.76.42 | refuah.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 5 |
| 162.210.196.130 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 91.109.242.34 | United Kingdom | 147.237.76.42 | refuah.idf.il | 9785: HTTP: SQL Injection (Referer Header) | Block | 1 |
| 137.117.80.189 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |

09-01-2016-04:04:00 to 09-01-2016-05:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.109.242.34 | 147.237.76.42 | United Kingdom | refuah.idf.il | SQL Injection - Select From | 32 |
| 81.88.48.113 | 147.237.0.34 | Italy | tikshuv.idf.il | SQL Injection - Select From | 21 |
| 185.96.92.58 | 147.237.77.74 | United Kingdom | law.idf.il | SQL Injection - Select From | 14 |
| 88.208.252.129 | 147.237.77.74 | United Kingdom | law.idf.il | SQL Injection - Select From | 8 |
| 173.198.251.2 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 8 |
| 185.21.133.159 | 147.237.77.216 | United Kingdom | dover.idf.il | SQL Injection - Select From | 8 |
| 217.37.125.121 | 147.237.77.74 | United Kingdom | law.idf.il | SQL Injection - Select From | 5 |
| 158.85.253.245 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 4 |
| 138.128.221.194 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 208.100.26.232 | 147.237.76.177 | United States | ncore.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 2 |
| 89.216.119.94 | 147.237.77.235 | | sviva.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 138.128.221.194 | 147.237.8.28 | United States | e.mobile-ks.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 138.128.221.194 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 211.63.33.239 | 147.237.76.38 | Korea, Republic of | e.e.meitav.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 138.128.221.194 | 147.237.0.33 | United States | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 208.100.26.232 | 147.237.76.177 | United States | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 138.128.221.194 | 147.237.0.15 | United States | kosher-kravi.idf.i | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 193.201.225.149 | 147.237.76.196 | Ukraine | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 103.207.39.82 | 147.237.76.197 | Vietnam | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.76.177 | Ukraine | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.216.119.94 | 147.237.77.235 | | sviva.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 138.128.221.194 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 89.216.119.94 | 147.237.77.235 | | sviva.idf.il | ET SCAN NMAP -f -sS | 1 |
| 138.128.221.194 | 147.237.8.45 | United States | e.eitan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 138.128.221.194 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 138.128.221.194 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 138.128.221.194 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 208.100.26.228 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 121.55.147.130 | 147.237.0.34 | Korea, Republic of | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 193.201.225.149 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.50 | 147.237.76.177 | Ukraine | ncore.idf.il | ET SCAN NMAP -sS window 4096 | 1 |

09-01-2016-04:04:00 to 09-01-2016-05:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 83.168.250.50 | Sweden | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 18 |
| 167.114.208.110 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 167.114.208.110 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 167.114.208.110 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.208.110 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.208.110 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.208.110 | Canada | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 167.114.208.110 | Canada | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 167.114.208.110 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 65.128.109.191 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 65.128.109.191 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 8 |
| 65.128.109.191 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 8 |
| 65.128.109.191 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 65.128.109.191 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 7 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |
| 89.139.151.92 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 176.13.15.36 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 167.114.208.110 | Canada | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 167.114.208.110 | Canada | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 46.19.85.205 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 167.114.208.110 | Canada | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 79.177.221.194 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.233.19 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 2 |
| 167.114.208.110 | Canada | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 84.109.115.177 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 54.78.205.14 | Ireland | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 141.212.122.39 | United States | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 201.46.55.34 | Brazil | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 54.78.205.14 | Ireland | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 95.163.144.203 | Russian Federation | 147.237.76.201 | e.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 169.229.3.91 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | drop | First packet isn't SYN | drop | 1 |
| 201.46.55.34 | Brazil | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 76.122.133.226 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 1 |

09-01-2016-04:04:00 to 09-01-2016-05:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 69.159.14.152 | Canada | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 5 |
| 180.97.106.37 | China | 147.237.77.226 | www.chamatz.aka.idf.il | NULL Character in Method | Block | 1 |
| 66.249.76.116 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx | Block | 1 |
| 213.151.62.217 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/894-he | Block | 1 |
| 180.97.106.37 | China | 147.237.77.74 | law.idf.il | NULL Character in Method | Block | 1 |
| 66.249.76.30 | Israel | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 1 |
| 180.97.106.162 | China | 147.237.76.31 | nakchal.idf.il | Distributed Illegal Byte Code Character in Method | Block | 1 |
| 180.97.106.37 | China | 147.237.77.176 | matpash.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 66.249.76.73 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/ghlxchbg.html | Block | 1 |
| 180.97.106.162 | China | 147.237.76.31 | nakchal.idf.il | Distributed NULL Character in Method | Block | 1 |
| 180.97.106.37 | China | 147.237.0.19 | madim.atal.idf.il | Distributed Illegal Byte Code Character in Method | Block | 1 |
| 180.97.106.37 | China | 147.237.77.176 | matpash.idf.il | NULL Character in Method | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 180.97.106.162 | China | 147.237.77.234 | halag.idf.il | Distributed Illegal Byte Code Character in Method | Block | 1 |
| 180.97.106.37 | China | 147.237.0.19 | madim.atal.idf.il | Distributed NULL Character in Method | Block | 1 |
| 66.249.64.59 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/robots.txt | Block | 1 |
| 180.97.106.37 | China | 147.237.77.226 | www.chamatz.aka.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 66.249.76.79 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp | Block | 1 |
| 180.97.106.162 | China | 147.237.77.234 | halag.idf.il | Distributed NULL Character in Method | Block | 1 |
| 180.97.106.37 | China | 147.237.77.74 | law.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 66.249.66.177 | Israel | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1086-he/dover.aspx | Block | 1 |

09-01-2016-04:04:00 to 09-01-2016-05:04:00