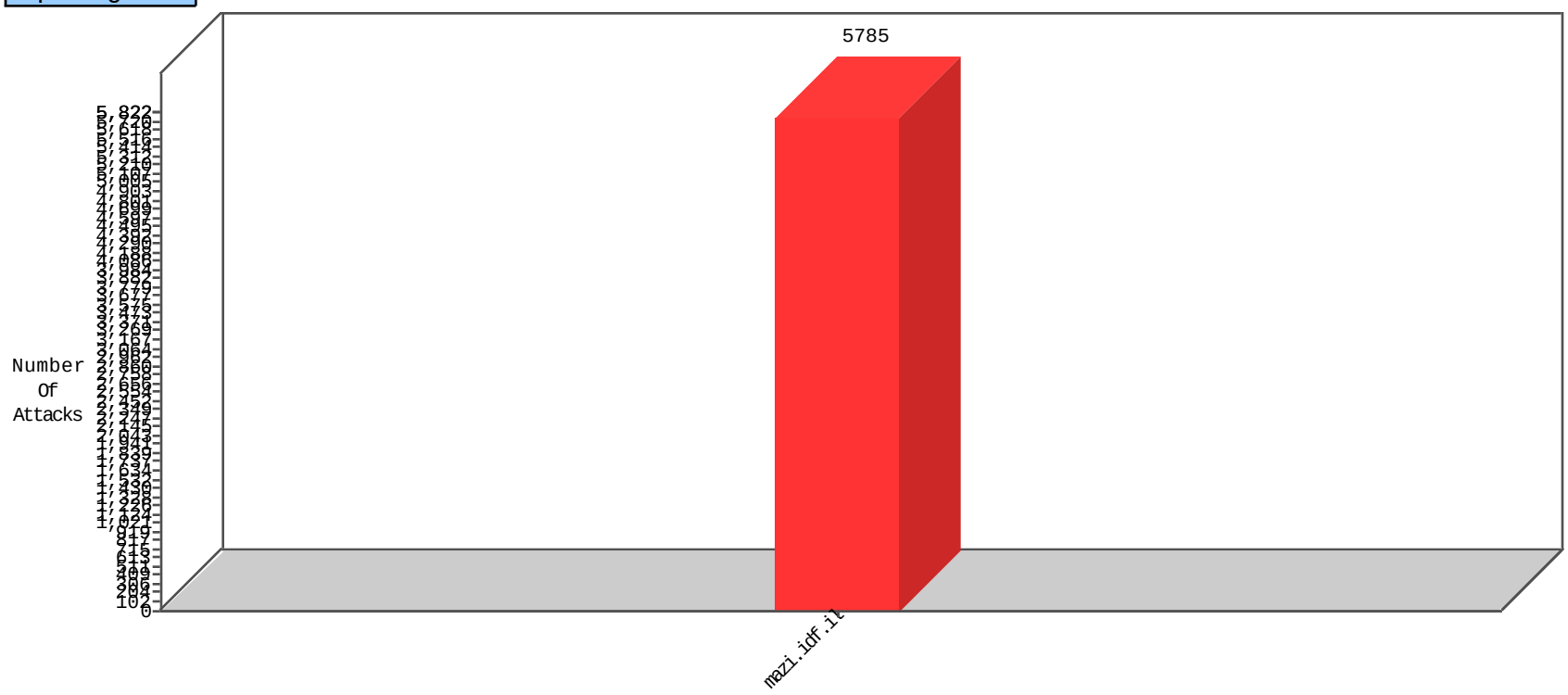
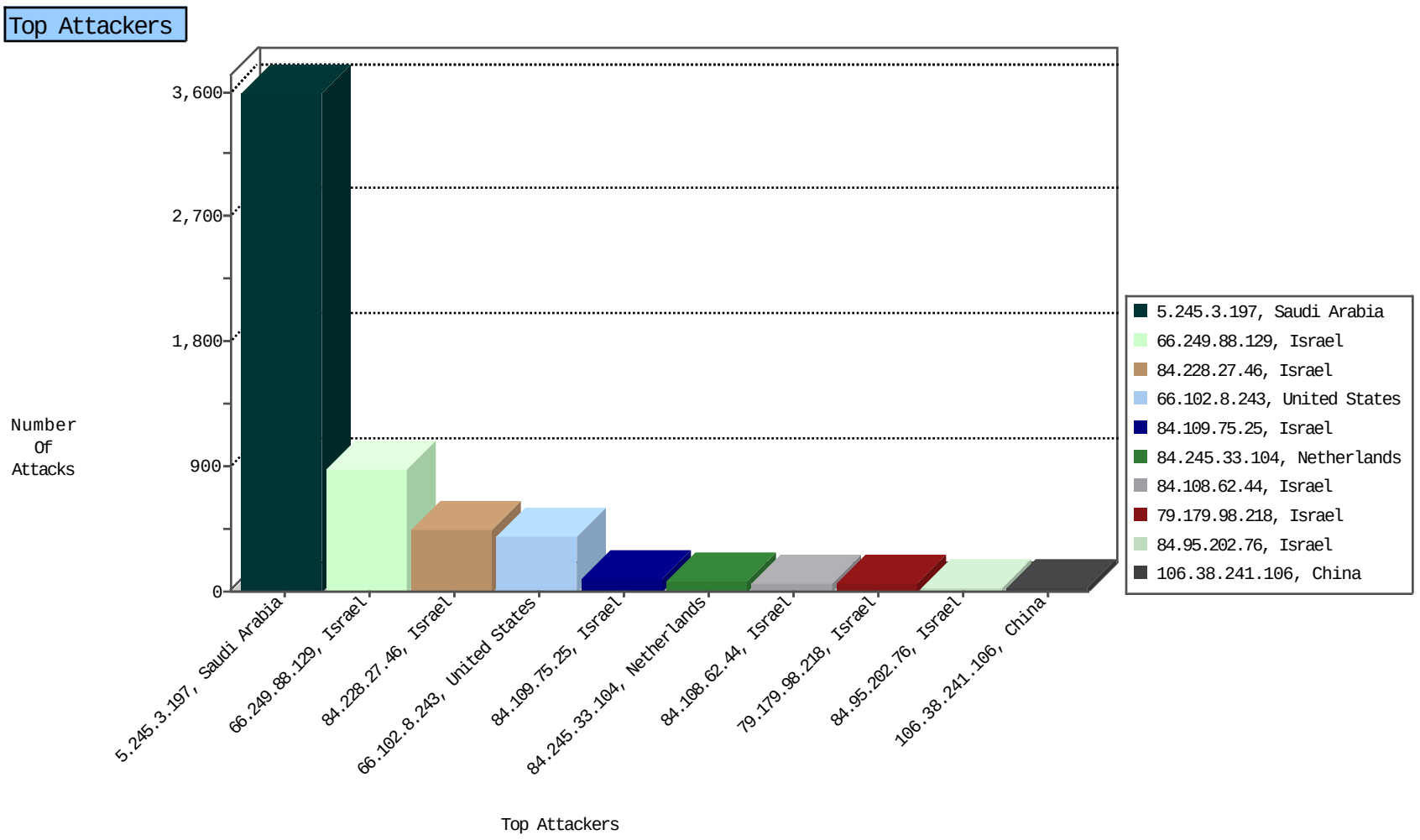
02-22-2016 to 02-23-2016

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



02-22-2016 to 02-23-2016

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|---|---|---|---|---|---|---|---|
| 5.245.3.197 | Saudi Arabia | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 3596 |
| 66.249.88.129 | Israel | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 884 |
| 66.102.8.243 | United States | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 400 |
| 31.168.133.226 | Israel | 147.237.77.17 | mazi.idf.il | Block_Udp_All_Nets | drop | BBL-Israel | 3 |
| 66.102.9.101 | United States | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 2 |
| 94.228.34.248 | United Kingdom | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |
| 96.233.85.239 | United States | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |
| 66.102.9.111 | United States | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |
| 66.249.79.127 | Israel | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |
| 66.249.79.246 | Israel | 147.237.77.17 | mazi.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |

02-22-2016 to 02-23-2016

## Top Attackers In IPS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.228.27.46 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 442 |
| 84.109.75.25 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 92 |
| 79.179.98.218 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 50 |
| 84.108.62.44 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 50 |
| 84.245.33.104 | Netherlands | 147.237.77.17 | mazi.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 43 |
| 84.95.202.76 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 26 |
| 106.38.241.106 | China | 147.237.77.17 | mazi.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 25 |
| 66.249.66.181 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 15 |
| 84.245.33.104 | Netherlands | 147.237.77.17 | mazi.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 11 |
| 46.19.86.164 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 185.120.126.42 |  | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 5 |
| 177.185.194.138 | Brazil | 147.237.77.17 | mazi.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 94.245.88.217 | United Kingdom | 147.237.77.17 | mazi.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 3 |
| 66.249.66.184 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 66.249.79.232 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 5.245.3.197 | Saudi Arabia | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 157.55.2.148 | United States | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 94.245.88.217 | United Kingdom | 147.237.77.17 | mazi.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 2 |
| 79.183.108.60 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 185.3.144.42 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 66.249.79.246 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 37.142.68.29 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 109.64.16.57 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 109.65.217.91 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 79.179.155.146 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 157.55.39.2 | United States | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 157.55.39.176 | United States | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 94.245.88.250 | United Kingdom | 147.237.77.17 | mazi.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 1 |
| 66.249.66.187 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 188.165.15.75 | France | 147.237.77.17 | mazi.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 62.219.119.44 | Israel | 147.237.77.17 | mazi.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 94.245.88.250 | United Kingdom | 147.237.77.17 | mazi.idf.il | 9785: HTTP: SQL Injection (Referer Header) | Block | 1 |

02-22-2016 to 02-23-2016

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 84.245.33.104 | Netherlands | 147.237.77.17 | mazi.idf.il | SQL Injection - Select From | 18 |
| 177.185.194.138 | Brazil | 147.237.77.17 | mazi.idf.il | SQL Injection - Select From | 14 |
| 94.245.88.217 | United Kingdom | 147.237.77.17 | mazi.idf.il | SQL Injection - Select From | 8 |
| 94.245.88.250 | United Kingdom | 147.237.77.17 | mazi.idf.il | SQL Injection - Select From | 6 |
| 66.249.66.181 | United States | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 98.119.105.221 | United States | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 98.119.105.221 | United States | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 120.55.90.163 | China | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 59.45.79.117 | China | 147.237.77.17 | mazi.idf.il | ET SCAN Potential SSH Scan | 1 |

02-22-2016 to 02-23-2016

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.3.144.42 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 155 |
| 212.76.127.44 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 81 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 50 |
| 212.76.127.10 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 36 |
| 62.219.119.44 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 36 |
| 46.19.85.98 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 25 |
| 46.19.85.98 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 25 |
| 212.76.127.111 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 25 |
| 185.3.144.42 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 20 |
| 31.210.188.121 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | | reject | 13 |
| 46.188.23.215 | Russian Federation | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 46.188.23.215 | Russian Federation | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 13 |
| 109.65.230.31 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 46.188.23.215 | Russian Federation | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.19.85.81 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 195.239.16.53 | Russian Federation | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 157.55.39.159 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 46.19.85.81 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 79.179.14.70 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 157.55.39.159 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 79.179.14.70 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 157.55.39.159 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 79.179.172.190 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 2.52.35.199 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 195.239.16.40 | Russian Federation | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 212.76.127.219 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 109.64.131.174 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid sequence number | monitor | 7 |
| 217.194.199.151 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 5 |
| 79.181.170.242 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 208.115.113.91 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 79.127.43.252 | Iran, Islamic Republic of | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 213.8.204.16 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.108.62.44 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 209.255.170.213 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | | monitor | 4 |
| 109.66.51.150 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 77.154.204.9 | France | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.154.18 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 212.143.161.240 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 208.115.113.91 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 79.180.38.7 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 68.115.81.162 | United States | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 73.209.197.171 | United States | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 209.255.170.213 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | | alert | 4 |
| 2.54.154.18 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 84.111.115.235 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 209.255.170.213 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 2.52.0.137 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 209.255.170.213 | United States | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 3 |

02-22-2016 to 02-23-2016

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.66.181 | Israel | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 66.249.66.181 | Block | 3 |
| 207.46.13.151 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/robots.txt | Block | 2 |
| 79.179.62.186 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx | Block | 2 |
| 169.229.3.91 | United States | 147.237.77.17 | mazi.idf.i | Illegal Byte Code Character in URL | Block | 2 |
| 148.251.21.227 | Germany | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 148.251.21.227 | Block | 2 |
| 212.76.98.189 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/647-he/mazi.aspx&sa=u&ved=0ahukewjavdau4ivlahvcfswkhu6hbciqfggpmae&usg=afqjcnecg60jwz920kawomo-sav7zcm-jw | Block | 2 |
| 169.229.3.91 | United States | 147.237.77.17 | mazi.idf.i | Unknown HTTP Request Method * in URL | Block | 2 |
| 148.251.21.227 | Germany | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/14-4980-he | Block | 2 |
| 68.180.228.160 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/14-8331-he | Block | 2 |
| 207.46.13.129 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to www.mazi.idf.il/14-8330-he | Block | 2 |
| 66.249.66.185 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/robots.txt | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/4070-11595-he/ובקרה| תכנון מחלקת.aspx | Block | 1 |
| 217.69.133.226 | Russian Federation | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/14-7708-he | Block | 1 |
| 66.249.66.185 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/robots.txt | Block | 1 |
| 157.55.39.2 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/5551-11516-he/×ž×©×œ×‘×™ ×§×”×™×œ×”.aspx | Block | 1 |
| 79.180.38.7 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx | Block | 1 |
| 66.249.66.181 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/14-7711-he | Block | 1 |
| 212.76.104.60 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/6368-9590-he/igf.aspx&sa=u&ved=0ahukewjz2jpfiyzlahwgehikhqawbg0qfggvmay&usg=afqjcneszjx8skubdb0bxb299cofjnnmha | Block | 1 |
| 157.55.39.2 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/5551-11516-he/משלבים קהילה.aspx | Block | 1 |
| 84.108.149.17 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx | Block | 1 |
| 66.249.66.182 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/4070-11595-he/×ž×—×œ×§×ª ×ª×›× ×•× ×•×‘×§×¨×”.aspx | Block | 1 |
| 68.180.228.160 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/sip_storage/files | Block | 1 |
| 31.168.114.31 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg | Block | 1 |
| 217.69.133.220 | Russian Federation | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/sip_storage/files | Block | 1 |
| 157.55.39.159 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to www.mazi.idf.il/14-8330-he | Block | 1 |
| 87.70.36.189 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx | Block | 1 |

02-22-2016 to 02-23-2016