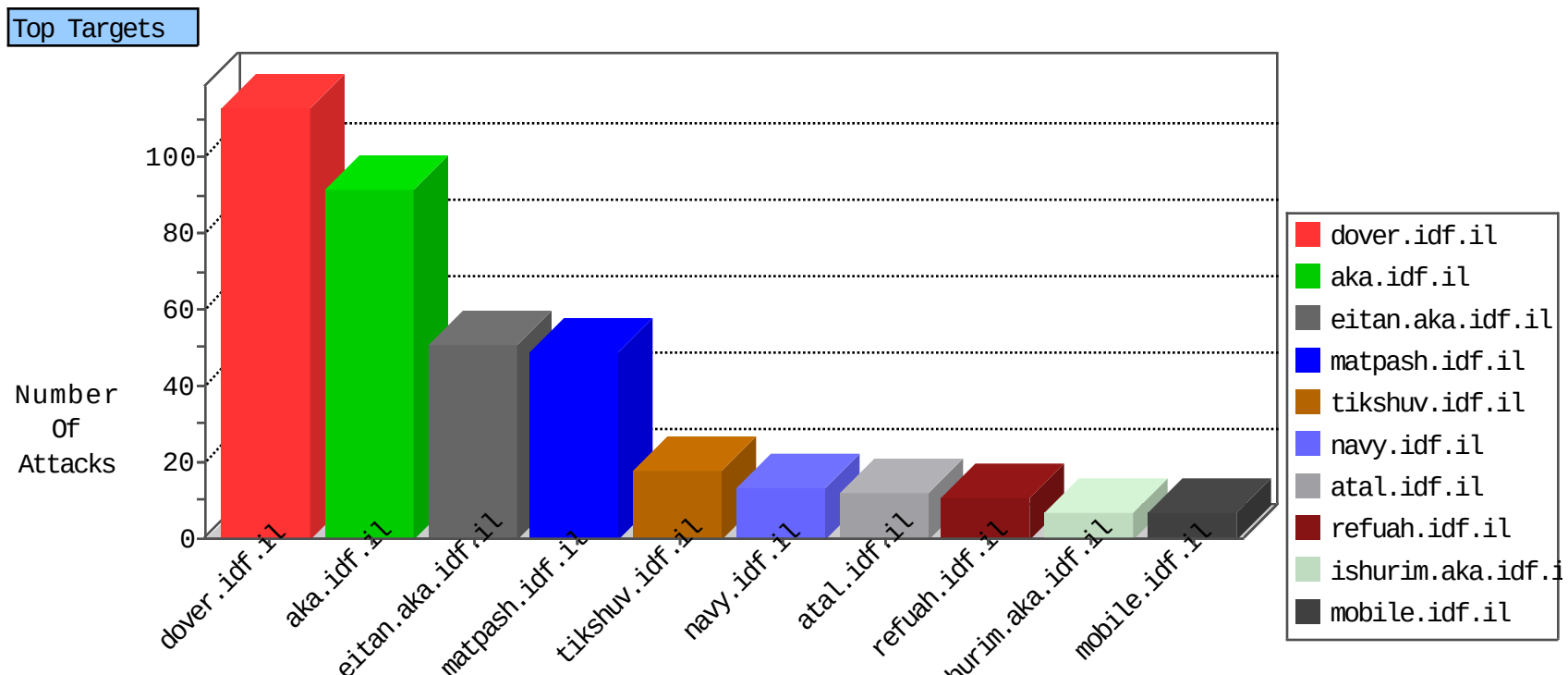
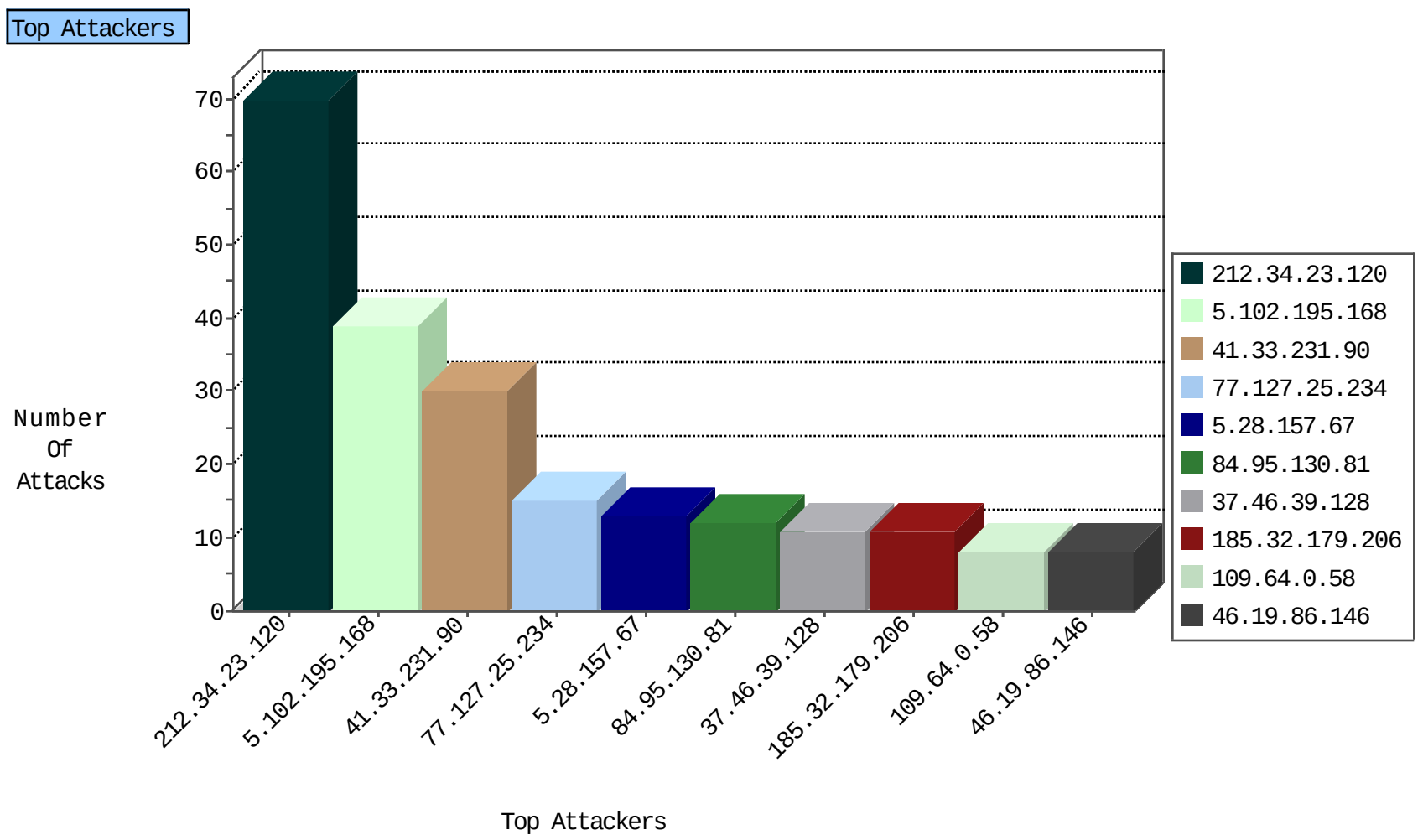
02-28-2016-01:04:29 to 02-28-2016-02:04:29

# IDF Under Attack
# Daily Report



02-28-2016-01:04:29 to 02-28-2016-02:04:29

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 134.147.203.115 | Germany | 147.237.76.177 | ncore.idf.il | Block_Ntp_All_Net | drop | 2 |
| 179.43.144.33 | Switzerland | 147.237.8.45 | e.eitan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 77.81.191.126 | Romania | 147.237.0.15 | kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.33.223.46 | Taiwan | 147.237.77.170 | maarachot.idf.il | Block_Udp_All_Nets | drop | 1 |
| 179.43.144.33 | Switzerland | 147.237.8.46 | e.chinuch.idf.il | Block_Ntp_All_Net | drop | 1 |
| 77.81.191.126 | Romania | 147.237.8.46 | e.chinuch.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.33.223.46 | Taiwan | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 205.209.185.11 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 77.81.191.126 | Romania | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 1 |
| 205.209.185.11 | United States | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 1 |
| 77.81.191.126 | Romania | 147.237.77.216 | dover.idf.il | Block_Ntp_All_Net | drop | 1 |

02-28-2016-01:04:29 to 02-28-2016-02:04:29

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.28.157.67 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 13 |
| 61.135.189.121 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 4 |
| 79.182.71.168 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 93.219.116.162 | Germany | 147.237.72.156 | aman.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 46.165.197.142 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 162.210.196.97 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 66.249.64.190 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 51.255.65.58 | United Kingdom | 147.237.77.233 | atal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 134.249.53.96 | Ukraine | 147.237.76.200 | eitan.aka.idf.il | C1000016: HTTP: administrator in URI | Block | 1 |
| 51.255.65.89 | United Kingdom | 147.237.77.233 | atal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.95 | United Kingdom | 147.237.77.233 | atal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 51.255.65.33 | United Kingdom | 147.237.77.233 | atal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 51.255.65.34 | United Kingdom | 147.237.77.233 | atal.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

02-28-2016-01:04:29 to 02-28-2016-02:04:29

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 |
| 66.249.66.33 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 50.204.188.142 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.114 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.204.188.142 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 50.204.188.142 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -f -sS | 1 |

02-28-2016-01:04:29 to 02-28-2016-02:04:29

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 33 |
| 5.102.195.168 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 32 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 77.127.25.234 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 84.95.130.81 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.32.179.206 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 109.64.0.58 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 37.46.39.128 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.86.146 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 110.142.218.4 | Australia | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 91.200.12.141 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 37.46.39.128 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 5.102.195.168 | Israel | 147.237.76.200 | eitan.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 75.126.221.55 | United States | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 2.52.37.33 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.128.160 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.195.168 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 77.125.123.231 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.145.25 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.205.117 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.126.92.236 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 79.179.102.206 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 84.228.6.192 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.126.162.187 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.110.149 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.120.126.199 |  | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.36.93 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.86.146 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 149.78.167.172 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 149.78.167.172 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 73.204.112.34 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 149.78.167.172 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 75.126.221.55 | United States | 147.237.77.74 | law.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 176.13.10.236 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 123.125.71.81 | China | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 31.210.187.203 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 85.130.128.51 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 79.177.141.217 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 71.6.167.142 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 180.76.15.20 | China | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.225 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 5.28.132.87 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |

02-28-2016-01:04:29 to 02-28-2016-02:04:29

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | Multiple Malformed URL from 212.34.23.120 | Block | 4 |
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | Multiple Illegal HTTP Version from 212.34.23.120 | Block | 4 |
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | Multiple Unknown HTTP Request Method from 212.34.23.120 | Block | 4 |
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | Multiple Malformed URL from 212.34.23.120 | Block | 4 |
| 66.249.79.75 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.75 | Block | 4 |
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | Multiple Unknown HTTP Request Method from 212.34.23.120 | Block | 4 |
| 212.34.23.120 | Jordan | 147.237.77.216 | dover.idf.il | Multiple Illegal HTTP Version from 212.34.23.120 | Block | 2 |
| 31.13.102.104 | Ireland | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 148.251.21.227 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx) | Block | 1 |
| 66.249.66.33 | United States | 147.237.77.74 | law.idf.il | Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx | None | 1 |
| 64.41.200.107 | United States | 147.237.77.216 | dover.idf.il | Multiple Untraceable SSL Sessions from 64.41.200.107 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)) | None | 1 |
| 93.160.60.22 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1503-en/dover.aspx. | Block | 1 |
| 66.102.7.240 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 31.13.102.121 | Ireland | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 195.91.212.123 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi | Block | 1 |
| 66.249.66.33 | United States | 147.237.77.74 | law.idf.il | Multiple Illegal Parameter Encoding from 66.249.66.33 | None | 1 |
| 64.41.200.107 | United States | 147.237.77.216 | dover.idf.il | Multiple Untraceable SSL Sessions from 64.41.200.107 (Unsupported Cipher) | None | 1 |
| 113.76.90.154 | China | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to 147.237.76.147/ | Block | 1 |
| 66.249.64.229 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1241-he/atal.aspx | Block | 1 |
| 213.151.32.163 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 31.13.112.120 | Ireland | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 198.20.69.74 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to 147.237.0.16/ | Block | 1 |
| 64.41.200.107 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE) | None | 1 |
| 134.249.53.96 | Ukraine | 147.237.76.200 | eitan.aka.idf.il | PHP Attempt | Block | 1 |
| 66.249.64.234 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx | Block | 1 |
| 217.132.109.235 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 37.26.146.210 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 207.46.13.185 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SSL Untraceable Connection - Unknown Server Certificate | None | 1 |
| 79.177.148.181 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 64.41.200.107 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Unsupported Cipher | None | 1 |
| 134.249.53.96 | Ukraine | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php | Block | 1 |
| 66.249.64.239 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1249-he/atal.aspx | Block | 1 |
| 46.19.85.252 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 212.34.23.120 | Jordan | 147.237.77.176 | matpash.idf.il | Multiple Abnormally Long Request from 212.34.23.120 | Block | 1 |
| 79.178.6.96 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 1 |
| 64.41.200.107 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |

02-28-2016-01:04:29 to 02-28-2016-02:04:29