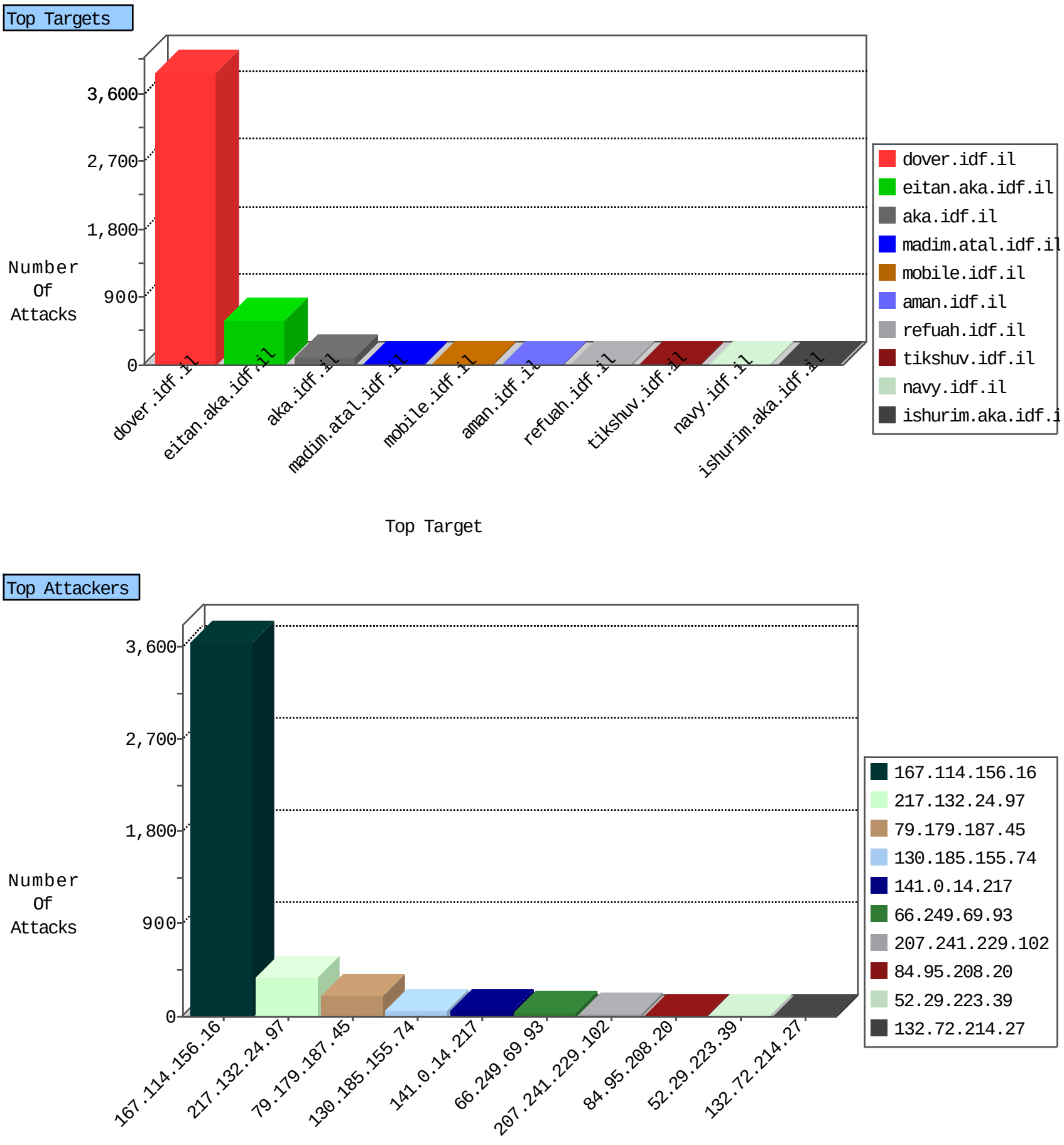
04-21-2016-01:06:26 to 04-21-2016-02:06:26

# IDF Under Attack Daily Report



04-21-2016-01:06:26 to 04-21-2016-02:06:26

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 13121 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 2558 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 336 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-MISC-Slowloris-DOS-Var1 | dest-reset | 7 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 3 |
| 173.208.197.250 | United States | 147.237.76.30 | himush.idf.il | block-sp-traf1 | forward | 2 |
| 74.91.23.109 | United States | 147.237.76.31 | nakchal.idf.il | block-sp-traf1 | forward | 2 |
| 69.30.226.98 | United States | 147.237.76.86 | navy.idf.il | block-sp-traf1 | forward | 2 |
| 69.30.226.99 | United States | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | forward | 2 |
| 74.91.17.182 | United States | 147.237.77.74 | law.idf.il | block-sp-traf1 | drop | 1 |
| 69.30.202.227 | United States | 147.237.77.74 | law.idf.il | block-sp-traf1 | drop | 1 |
| 69.30.226.220 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 173.208.197.252 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | drop | 1 |
| 69.30.226.221 | United States | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | drop | 1 |
| 69.30.198.146 | United States | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | drop | 1 |
| 89.248.160.138 | Netherlands | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 69.30.226.221 | United States | 147.237.77.235 | sviva.idf.il | block-sp-traf1 | drop | 1 |
| 69.30.202.226 | United States | 147.237.72.156 | aman.idf.il | block-sp-traf1 | drop | 1 |
| 89.248.160.138 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 69.30.226.102 | United States | 147.237.77.19 | law-forum.idf.il | block-sp-traf1 | drop | 1 |

04-21-2016-01:06:26 to 04-21-2016-02:06:26

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

04-21-2016-01:06:26 to 04-21-2016-02:06:26

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 |
| 217.78.54.61 | 147.237.77.176 | Palestinian Territory, Occupied | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 113.57.128.212 | 147.237.77.233 | China | atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.57.128.212 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 112.196.49.101 | 147.237.76.147 | India | chinuch.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 107.158.255.194 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 93.180.66.29 | 147.237.8.28 | Netherlands | e.mobile-ks.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 67.130.39.67 | 147.237.0.33 | United States | idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 146.0.79.176 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.57.128.212 | 147.237.77.227 | China | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.57.128.212 | 147.237.77.179 | China | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 112.196.49.101 | 147.237.76.147 | India | chinuch.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 107.158.255.194 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.180.66.29 | 147.237.8.27 | Netherlands | e.madim.atal.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 220.231.195.122 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 65.181.123.161 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 200.163.107.93 | 147.237.0.33 | Brazil | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 159.122.220.135 | 147.237.72.14 | United States | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |

04-21-2016-01:06:26 to 04-21-2016-02:06:26

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3392 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 369 |
| 79.179.187.45 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 201 |
| 141.0.14.217 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 130.185.155.74 | Sweden | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 66.249.69.93 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 207.241.229.102 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 19 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 87.69.255.212 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 46.165.223.217 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 128.177.161.184 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 207.46.13.118 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 109.66.30.144 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 91.200.12.143 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 3 |
| 79.181.212.170 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.93.245 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.114 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 174.48.237.121 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 5.28.175.45 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.8.140 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 118.173.129.184 | Thailand | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.49 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.95.208.20 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.69.175 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.29.162.98 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 209.122.193.207 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 188.120.154.229 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 5.102.242.66 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.41 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 128.232.110.28 | United Kingdom | 147.237.8.28 | e.mobile-ks.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 37.9.122.203 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.120 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 128.232.110.28 | United Kingdom | 147.237.72.217 | e.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 37.26.146.150 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 2 |
| 91.200.12.143 | Ukraine | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.151 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.85.104 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 109.163.234.8 | Romania | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 185.3.147.232 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 169.229.3.91 | United States | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 79.176.113.168 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |

04-21-2016-01:06:26 to 04-21-2016-02:06:26

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 132.72.214.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 141.8.132.78 | Block | 3 |
| 176.13.18.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 17.138.55.96 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.138.55.96 | Block | 2 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/sip_storage/files/0/1850.jpg | Block | 2 |
| 17.138.55.96 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/ | Block | 2 |
| 199.30.24.160 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 37.26.149.228 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 37.26.149.228 | Block | 2 |
| 176.13.8.140 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.179.100.247 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized HTTP Method | Block | 2 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 217.132.24.97 | Block | 2 |
| 17.138.55.96 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 84.95.208.20 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx | Block | 1 |
| 68.180.228.37 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/ | Block | 1 |
| 141.8.183.16 | Russian Federation | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/901-9903- | Block | 1 |
| 74.91.23.109 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.app-softwares.com/ | Block | 1 |
| 41.66.208.88 | Ghana | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 198.58.102.95 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english | Block | 1 |
| 84.111.232.5 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx | Block | 1 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx | None | 1 |
| 157.55.39.41 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 79.179.100.247 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 79.179.100.247 | Block | 1 |
| 46.19.85.130 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 69.30.226.220 | United States | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to www.369bs.com/ | Block | 1 |
| 46.116.241.29 | Israel | 147.237.76.39 | mobile.meitav.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 73.251.79.97 | United States | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 37.26.149.228 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/mobile | Block | 1 |
| 176.13.8.140 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.179.100.247 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/4/ | Block | 1 |
| 66.249.75.18 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 217.132.24.97 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized Method POST for www.eitan.aka.idf.il/1093-he/eitan.aspx | None | 1 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi | Block | 1 |
| 73.251.79.97 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wp-login.php | Block | 1 |
| 41.66.208.88 | Ghana | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |

04-21-2016-01:06:26 to 04-21-2016-02:06:26