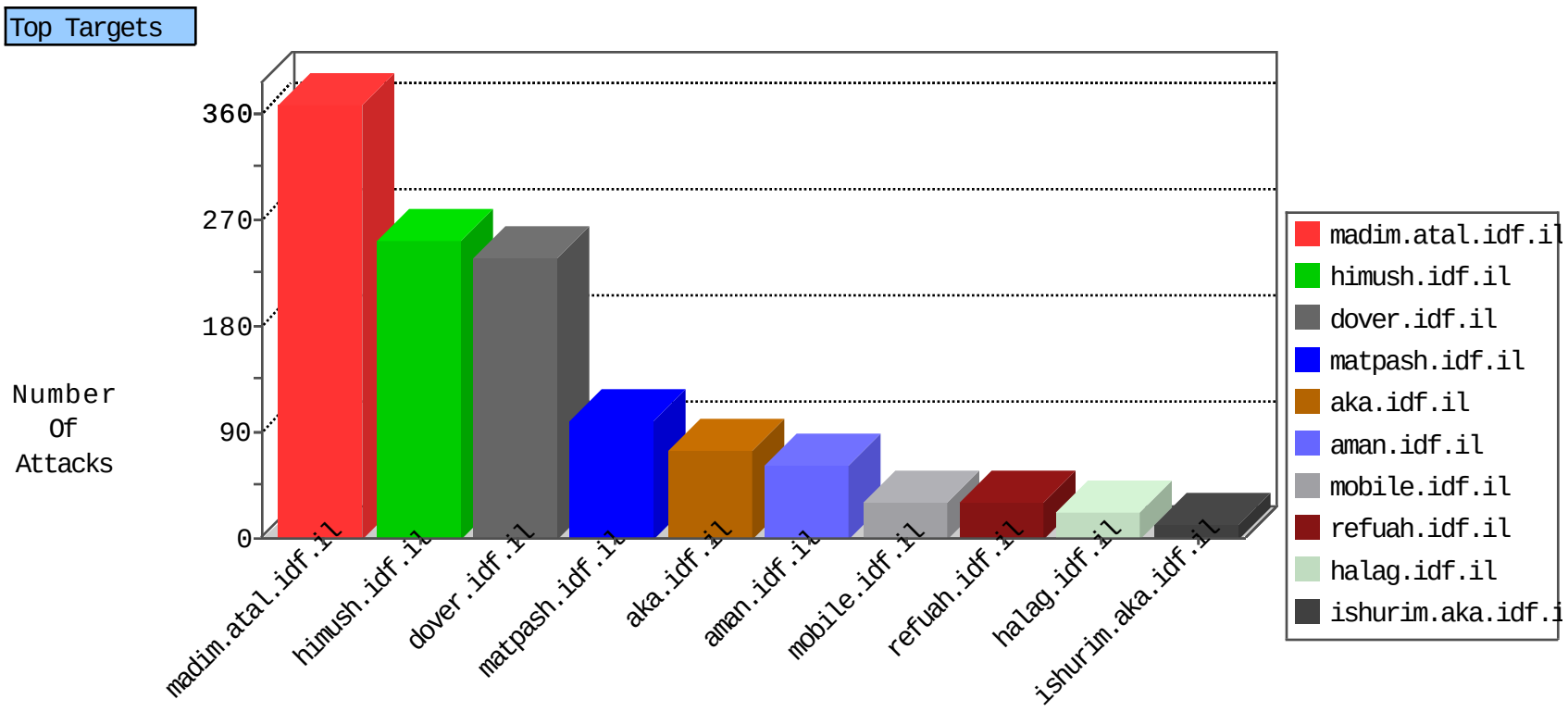
10-03-2016-16:04:00 to 10-03-2016-17:04:00

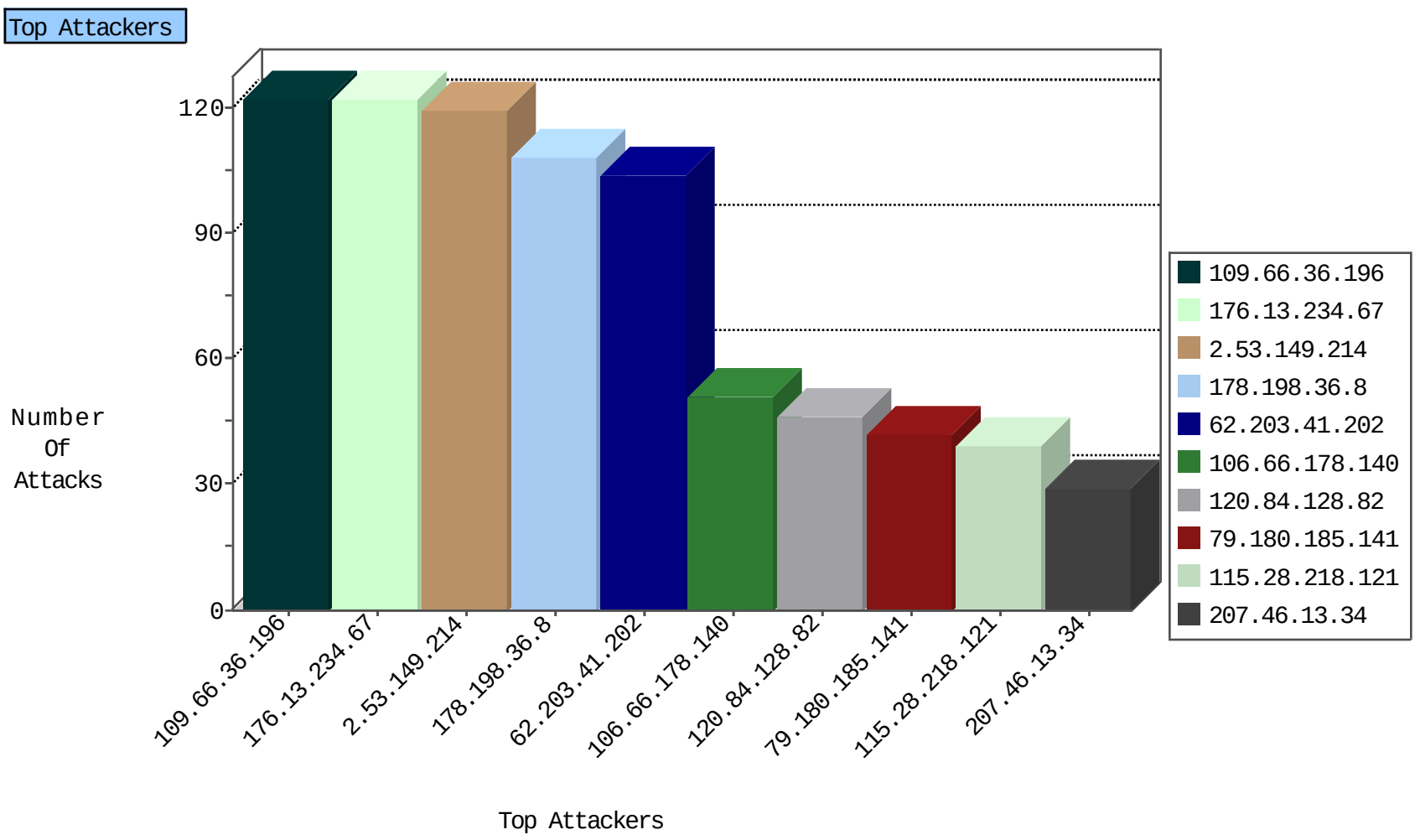
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

10-03-2016-16:04:00 to 10-03-2016-17:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 178.78.253.146 | Sweden | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 78.129.171.175 | United Kingdom | 147.237.76.86 | navy.idf.il | Black List | drop | 1 |
| 78.129.171.175 | United Kingdom | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 120.68.232.186 | China | 147.237.76.199 | e.nakchal.idf.il | Black List | drop | 1 |
| 71.6.146.185 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |

10-03-2016-16:04:00 to 10-03-2016-17:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 106.38.241.106 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 7 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

10-03-2016-16:04:00 to 10-03-2016-17:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 183.129.160.229 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.240.213.93 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.11.244 | 147.237.0.34 | United Kingdom | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.132.63.102 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 162.248.76.109 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 106.187.45.144 | 147.237.76.42 | Japan | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 105.107.99.2 | 147.237.77.216 | Algeria | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.224.161.69 | 147.237.76.38 | Netherlands | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.161.69 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.50 | 147.237.72.217 | Ukraine | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.129.38.2 | 147.237.8.50 | Romania | e.tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.201.236.50 | 147.237.72.217 | Ukraine | e.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 163.172.11.244 | 147.237.0.34 | United Kingdom | tikshuv.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 66.240.213.93 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 162.248.76.109 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 14.149.102.146 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 162.248.76.109 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN NMAP -f -sS | 1 |
| 106.38.241.106 | 147.237.76.86 | China | navy.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 91.224.161.69 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.161.69 | 147.237.76.31 | Netherlands | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.161.69 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.50 | 147.237.72.217 | Ukraine | e.idf.il | ET SCAN NMAP -sS window 3072 | 1 |

10-03-2016-16:04:00 to 10-03-2016-17:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 106.66.178.140 | India | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 27 |
| 207.46.13.34 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 27 |
| 185.26.180.151 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 25 |
| 178.198.36.8 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 24 |
| 66.249.65.53 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 24 |
| 213.6.74.138 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 24 |
| 62.203.41.202 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 22 |
| 178.198.36.8 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 21 |
| 62.203.41.202 | Switzerland | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 21 |
| 178.198.36.8 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 21 |
| 62.203.41.202 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 21 |
| 79.180.14.173 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 21 |
| 178.198.36.8 | Switzerland | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 21 |
| 178.198.36.8 | Switzerland | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 21 |
| 62.203.41.202 | Switzerland | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 20 |
| 62.203.41.202 | Switzerland | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 20 |
| 79.180.185.141 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 84.108.27.15 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 16 |
| 109.64.98.170 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 79.178.10.80 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 79.180.185.141 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.64.98.170 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 11 |
| 115.28.218.121 | China | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 115.28.218.121 | China | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 9 |
| 115.28.218.121 | China | 147.237.76.30 | himush.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 9 |
| 46.120.181.48 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 115.28.218.121 | China | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 37.142.197.14 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 106.66.178.140 | India | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 106.66.178.140 | India | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 109.253.144.233 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.115.202.57 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.53.190.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 176.13.244.188 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 66.249.83.221 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.216 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 66.102.6.21 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 176.13.20.219 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 79.180.185.141 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 79.177.103.99 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 85.250.67.204 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 185.110.108.165 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.86.221 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 106.66.178.140 | India | 147.237.77.176 | matpash.idf.il | SYN Attack | | monitor | 4 |
| 115.28.218.121 | China | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 46.31.103.69 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 4 |
| 79.180.185.141 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 79.176.129.136 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 109.67.53.40 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |

10-03-2016-16:04:00 to 10-03-2016-17:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.66.36.196 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 122 |
| 2.53.149.214 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 119 |
| 176.13.234.67 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 117 |
| 120.84.128.82 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 120.84.128.82 | Block | 18 |
| 120.84.128.82 | China | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 120.84.128.82 | Block | 15 |
| 120.84.128.82 | China | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 6 |
| 120.84.128.82 | China | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 6 |
| 109.67.61.22 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 5 |
| 95.35.169.252 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 80.246.139.138 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 79.178.10.80 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 151.37.74.228 | Italy | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 79.180.185.141 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 66.249.73.133 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx | Block | 1 |
| 130.193.51.51 | Russian Federation | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 109.66.9.49 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 178.78.253.146 | Sweden | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ english | Block | 1 |
| 40.77.167.92 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 84.108.137.89 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.76.109 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx | Block | 1 |
| 136.243.11.18 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 79.180.14.173 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 192.52.250.229 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 1 |
| 62.117.59.30 | Egypt | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage | Block | 1 |
| 120.84.128.82 | China | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/index.asp | Block | 1 |
| 85.64.131.192 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/html/profs.asp | Block | 1 |
| 68.180.229.234 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/patzar | Block | 1 |
| 66.102.6.4 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/sachar | Block | 1 |
| 68.180.231.57 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx | Block | 1 |
| 157.55.39.98 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/ | Block | 1 |
| 109.67.227.41 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 80.178.99.200 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 80.178.99.200 | Block | 1 |
| 66.249.64.124 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/1150-he/chinuch.aspx | Block | 1 |
| 109.65.184.191 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 77.138.206.92 | France | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 37.142.197.14 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |

10-03-2016-16:04:00 to 10-03-2016-17:04:00