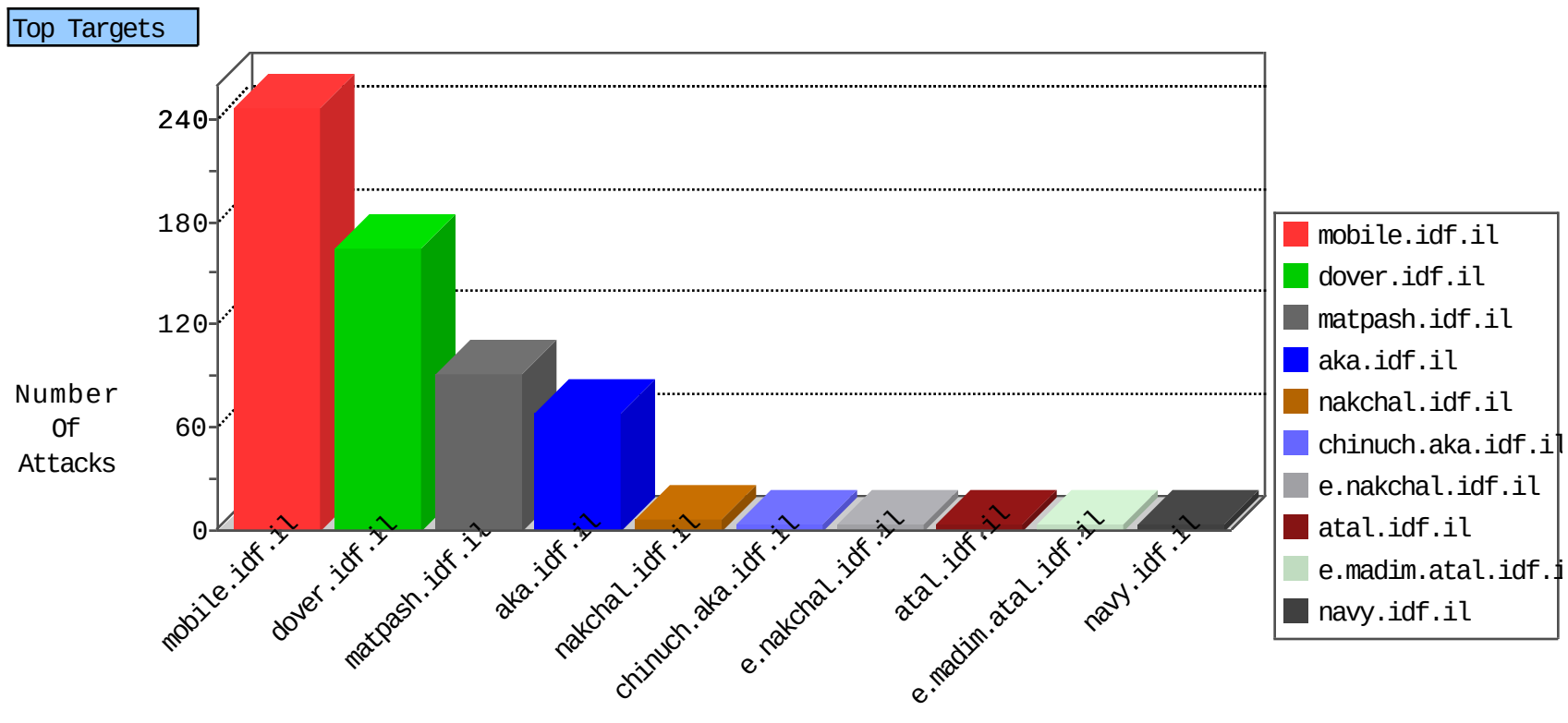
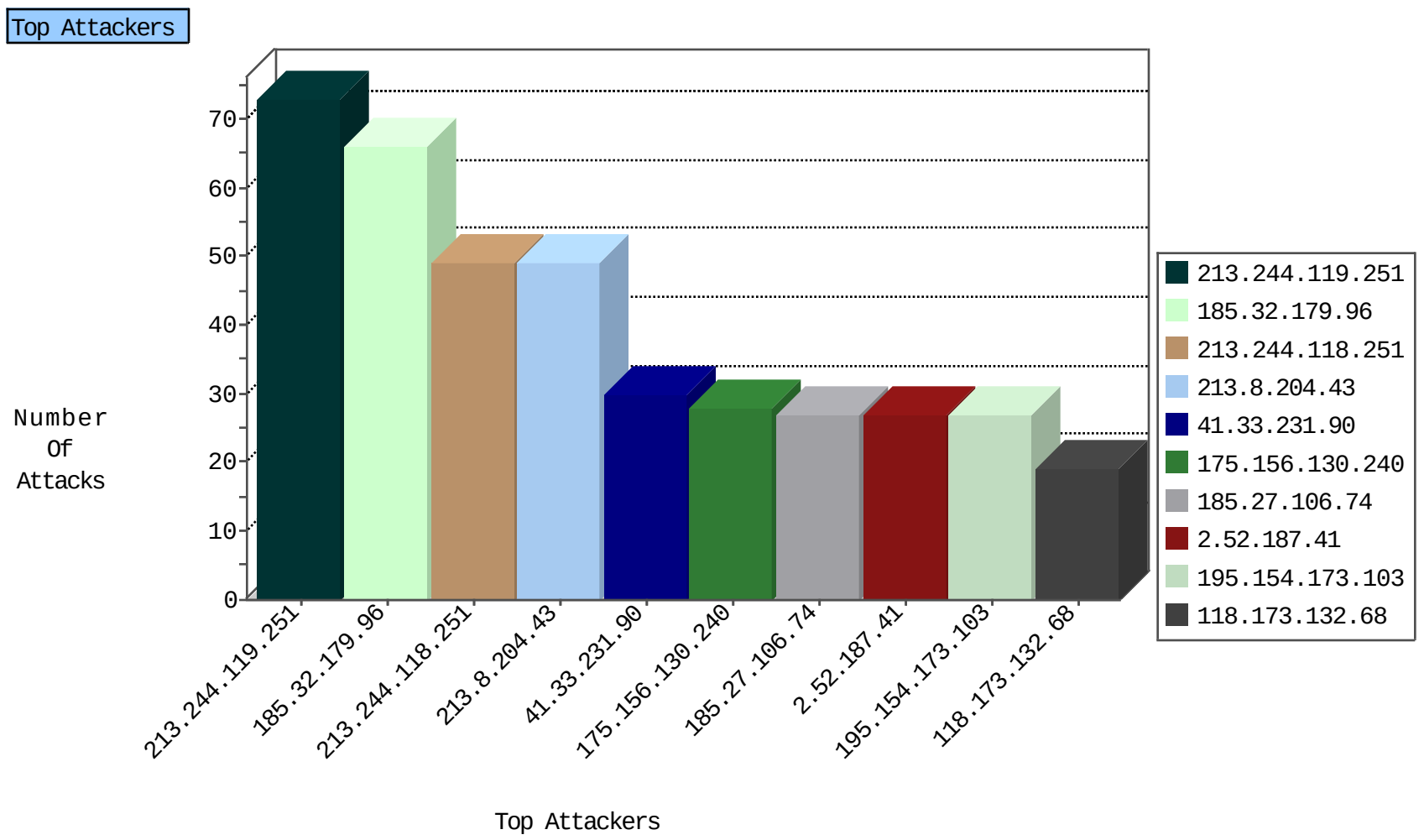
02-28-2016-02:04:05 to 02-28-2016-03:04:05

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-28-2016-02:04:05 to 02-28-2016-03:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 178.33.179.251 | France | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 179.43.144.33 | Switzerland | 147.237.72.14 | dover.idf.il(old) | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.201 | | 147.237.0.200 | m4u.idf.il | Block_Udp_All_Nets | drop | 1 |
| 204.42.253.2 | United States | 147.237.8.28 | e.mobile-ks.idf.il | Block_Udp_All_Nets | drop | 1 |

02-28-2016-02:04:05 to 02-28-2016-03:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 61.135.189.121 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 2 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.64.180 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 66.249.64.190 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |

02-28-2016-02:04:05 to 02-28-2016-03:04:05

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 |
| 118.165.7.106 | 147.237.76.39 | Taiwan | mobile.meitav.idf.i | ET SCAN Potential SSH Scan | 1 |
| 98.119.105.221 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 98.119.105.221 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 66.249.78.158 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 50.204.188.142 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 46.151.52.210 | 147.237.0.15 | Ukraine | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 118.165.7.106 | 147.237.76.199 | Taiwan | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.76.147 | Taiwan | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.165.7.106 | 147.237.0.15 | Taiwan | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 98.119.105.221 | 147.237.77.178 | United States | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 93.113.125.11 | 147.237.76.86 | Romania | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.204.188.142 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 50.204.188.142 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 218.246.0.97 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 41.251.23.150 | 147.237.76.34 | Morocco | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 185.106.92.112 | 147.237.77.170 | | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 118.165.7.106 | 147.237.76.196 | Taiwan | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |

02-28-2016-02:04:05 to 02-28-2016-03:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.32.179.96 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 54 |
| 213.8.204.43 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 39 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 195.154.173.103 | France | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 24 |
| 2.52.187.41 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 185.27.106.74 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 175.156.130.240 | Singapore | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 118.173.132.68 | Thailand | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 19 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 77.126.253.32 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 14 |
| 109.253.214.213 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 213.57.152.195 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 176.13.6.110 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 185.3.144.97 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.86.137 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 2.54.17.206 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 2.54.181.172 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 185.120.126.74 |  | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.49 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 195.154.173.103 | France | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 3 |
| 93.158.152.49 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 3 |
| 79.176.10.244 | 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 |
| 89.138.96.20 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 185.3.144.97 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence |  | monitor | 2 |
| 173.196.250.202 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 89.138.181.131 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 213.244.118.245 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 200.114.226.9 | Argentina | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 2 |
| 194.30.134.180 | Cyprus | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 70.199.84.154 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |

02-28-2016-02:04:05 to 02-28-2016-03:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.32.179.96 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 66.249.79.75 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.75 | Block | 9 |
| 175.156.130.240 | Singapore | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 2.52.187.41 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 213.8.204.43 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 185.27.106.74 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 213.8.204.43 | Israel | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 4 |
| 77.126.253.32 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.6.110 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 213.57.152.195 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.119.127.64 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi/ | Block | 3 |
| 66.249.64.239 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx | Block | 1 |
| 185.82.203.241 |  | 147.237.77.74 | law.idf.il | Parameter Type Violation PageNum in www.law.idf.il/163-en/patzar.aspx | Block | 1 |
| 157.55.39.37 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 66.249.79.119 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 38.111.147.88 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 86.84.150.18 | Netherlands | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 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 |
| 197.27.77.181 | Tunisia | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 197.27.77.181 | Block | 1 |
| 157.55.39.105 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1134-he/dover.aspx | Block | 1 |
| 40.77.167.28 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 178.33.179.251 | France | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 89.138.181.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 1 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wepdwullte5odk5nji2ntmpzbyczg9kfgjmd2qwagidd2qwbaihdw8wah4hvmlzawjszwhkzaild2qwbaibd2qwagibdxychgrocmvmbqxkzwzhdwx0lmfzchhkagupzbycagepfgiebxn0ewxlbqt3awr0ado5ntbwebyeagepfgiecwlubmvyahrtbauz16nxknec15xxqidxldeq16nxlder15xxqmqcag8wah8cbqt3awr0ado5ntbwegqyaquex19db250cm9sc1jlcxvpcmvqb3n0qmfja0tlev9ffgmffmn0bdawjgn0bdawjhjivghpc1npdguffmn0bdawjgn0bdawjhjiqwxsu2l0zxmffmn0bdawjgn0bdawjhjiqwxsu2l0zxm8eh5yubarwrcttqtsdbjv4srbosmtntap+hah2uc8vg== | Block | 1 |
| 197.27.77.181 | Tunisia | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/1966-he/cogat'.aspx | Block | 1 |
| 173.196.250.202 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 1 |
| 213.244.118.245 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 46.19.86.137 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 148.251.21.227 | Block | 1 |
| 66.249.78.158 | United States | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 197.27.77.181 | Tunisia | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/1145-he/atal'.aspx | Block | 1 |
| 174.119.153.235 | Canada | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 70.199.84.154 | United States | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 149.88.156.194 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |

02-28-2016-02:04:05 to 02-28-2016-03:04:05