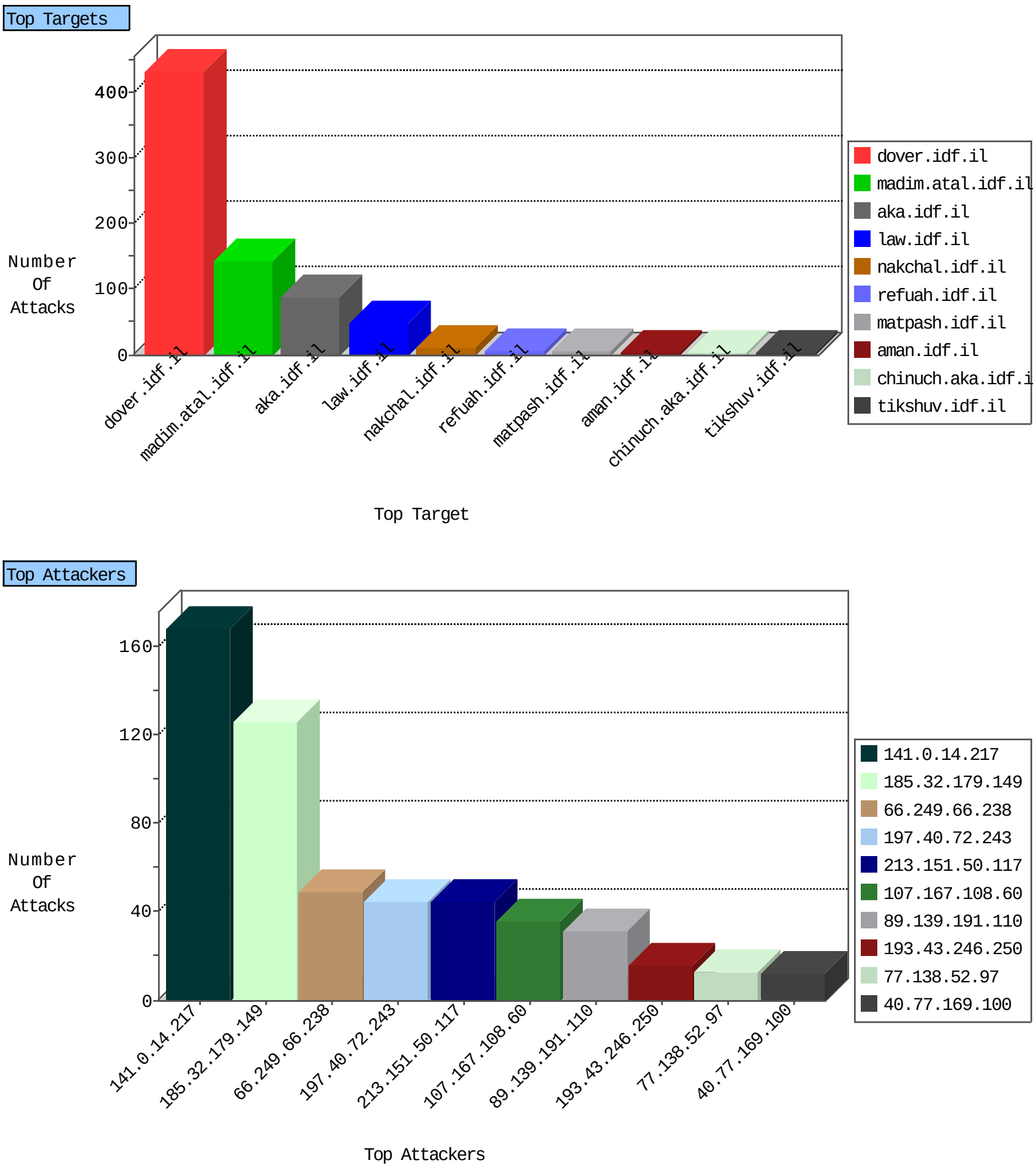
08-24-2016-20:04:05 to 08-24-2016-21:04:05

# IDF Under Attack Daily Report



08-24-2016-20:04:05 to 08-24-2016-21:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 168.235.207.185 | United States | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 62 |
| 82.80.78.2 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 6 |
| 93.223.204.11 | Germany | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 5 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 168.235.207.185 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 141.0.15.36 | Norway | 147.237.76.42 | refuah.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 141.0.15.36 | Norway | 147.237.76.42 | refuah.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 104.148.55.162 | United States | 147.237.76.197 | e.himush.idf.il | Black List | drop | 1 |
| 80.82.78.27 | Netherlands | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 217.160.204.6 | Germany | 147.237.76.196 | e.sviva.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |

08-24-2016-20:04:05 to 08-24-2016-21:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 71.6.146.185 | United States | 147.237.8.50 | e.tikshuv.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

08-24-2016-20:04:05 to 08-24-2016-21:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.66.238 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 49 |
| 202.155.58.28 | 147.237.76.38 | Indonesia | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.213.139 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 197.40.72.243 | 147.237.77.216 | Egypt | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 139.162.13.205 | 147.237.77.176 | Singapore | matpash.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 129.56.2.38 | 147.237.8.46 | Nigeria | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 129.56.2.38 | 147.237.8.24 | Nigeria | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.206.73.185 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 86.107.42.11 | 147.237.0.34 | United Kingdom | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 202.155.58.28 | 147.237.76.147 | Indonesia | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.213.139 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 202.155.58.28 | 147.237.76.31 | Indonesia | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.213.139 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 168.235.207.185 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 133.242.4.52 | 147.237.0.16 | Japan | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 129.56.2.38 | 147.237.8.28 | Nigeria | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.206.73.185 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 101.178.206.92 | 147.237.72.166 | Australia | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.65.82 | 147.237.77.216 | Netherlands | dover.idf.il | ET WEB_SERVER Poison Null Byte | 1 |
| 58.218.213.139 | 147.237.76.177 | China | ncore.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

08-24-2016-20:04:05 to 08-24-2016-21:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 141.0.14.217 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 168 |
| 107.167.108.60 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 89.139.191.110 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 197.40.72.243 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 197.40.72.243 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 15 |
| 37.142.95.73 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 46.19.86.225 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 197.40.72.243 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 40.77.169.98 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 6 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.83 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 2.53.165.158 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.13.17.122 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.241.117 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 3 |
| 66.102.9.171 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.86.172 | Israel | 147.237.76.147 | chinuch.aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 84.110.32.49 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 93.223.204.11 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 79.177.117.222 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 82.80.136.66 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.37 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 85.130.222.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 82.209.152.186 | Sweden | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.110 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | | drop | 2 |
| 84.94.60.58 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 217.160.204.6 | Germany | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 37.46.39.71 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 85.130.222.194 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 217.160.204.6 | Germany | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 204.79.180.42 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 77.40.0.13 | Russian Federation | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 134.35.83.178 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 217.160.204.6 | Germany | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 176.13.10.219 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 92.124.239.7 | Russian Federation | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

08-24-2016-20:04:05 to 08-24-2016-21:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.32.179.149 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 126 |
| 213.151.50.117 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 45 |
| 77.138.226.134 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/ | Block | 7 |
| 46.19.86.107 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.19.85.70 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 66.249.85.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 6 |
| 66.249.85.218 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 185.27.104.50 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 4 |
| 77.138.42.226 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/ | Block | 3 |
| 66.249.85.221 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 109.253.195.169 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.178.180.156 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 46.117.219.147 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx | Block | 2 |
| 185.27.104.50 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/ | Block | 2 |
| 199.30.24.38 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 139.162.13.205 | Singapore | 147.237.77.176 | matpash.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 2 |
| 5.22.132.8 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.120.49.16 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 109.66.51.3 | Israel | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 1 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 199.30.24.128 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.69.253 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |
| 157.55.39.100 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 5.28.189.86 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 80.179.118.96 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on www.logistics.atal.idf.il/1098 | Block | 1 |
| 68.180.230.171 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx | Block | 1 |
| 66.102.9.105 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx | Block | 1 |
| 185.97.132.15 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg | Block | 1 |
| 109.66.51.3 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/wp-login.php | Block | 1 |
| 40.77.169.103 | United States | 147.237.77.176 | matpash.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 77.139.66.201 | France | 147.237.76.42 | refuah.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx | Block | 1 |
| 213.8.204.73 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx | Block | 1 |
| 46.73.152.99 | Russian Federation | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 185.27.104.50 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 185.27.104.50 | Block | 1 |
| 37.142.246.5 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 84.108.44.142 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/page.asp | Block | 1 |
| 68.180.230.171 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/homefront | Block | 1 |
| 185.120.126.6 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 66.249.64.99 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112654.pdf | Block | 1 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 77.139.114.85 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx | Block | 1 |
| 46.116.221.162 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 85.64.215.39 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 192.116.175.102 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.66.75 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 1 |
| 136.243.16.208 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 2.53.10.59 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/1098 | Block | 1 |
| 87.68.43.107 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx | Block | 1 |

08-24-2016-20:04:05 to 08-24-2016-21:04:05