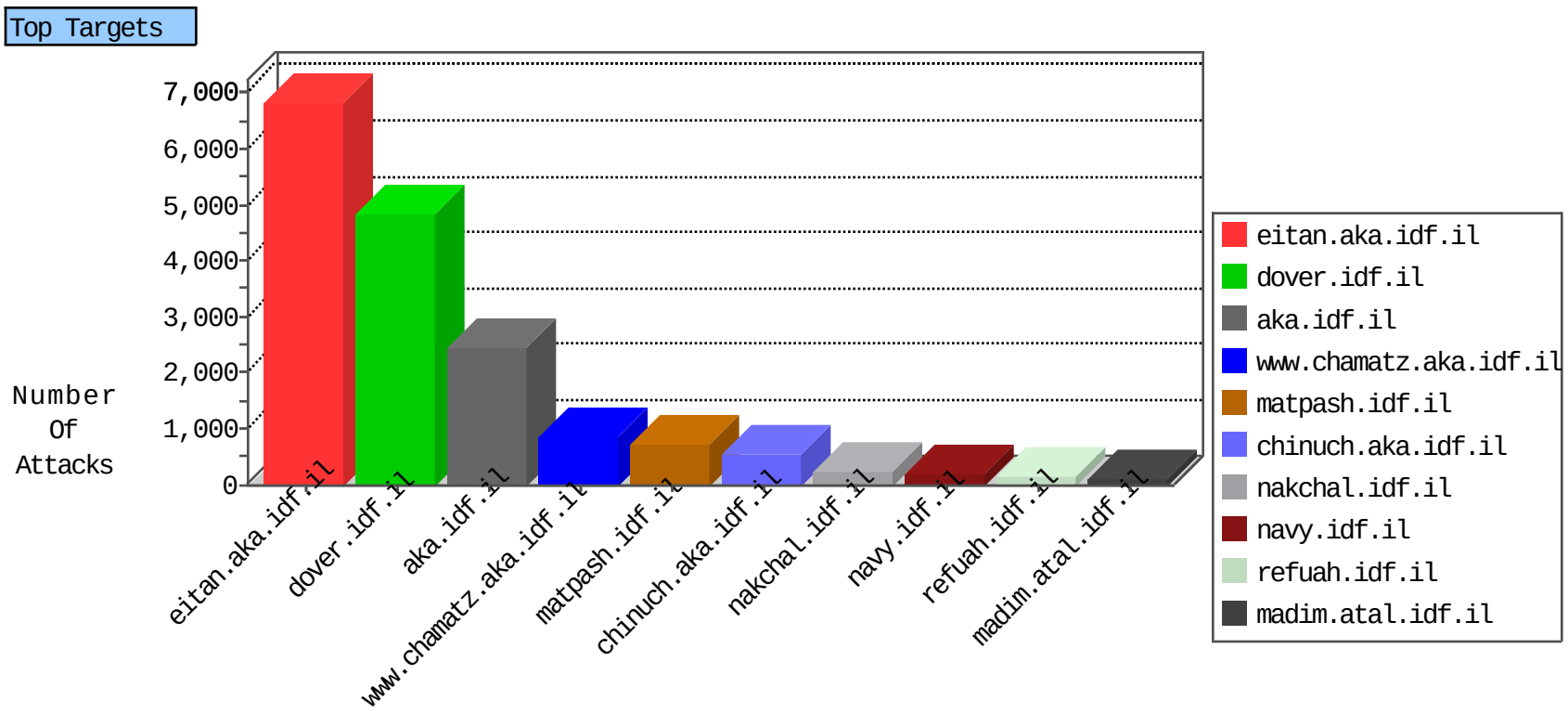
08-27-2016-20:04:02 to 08-27-2016-21:04:02

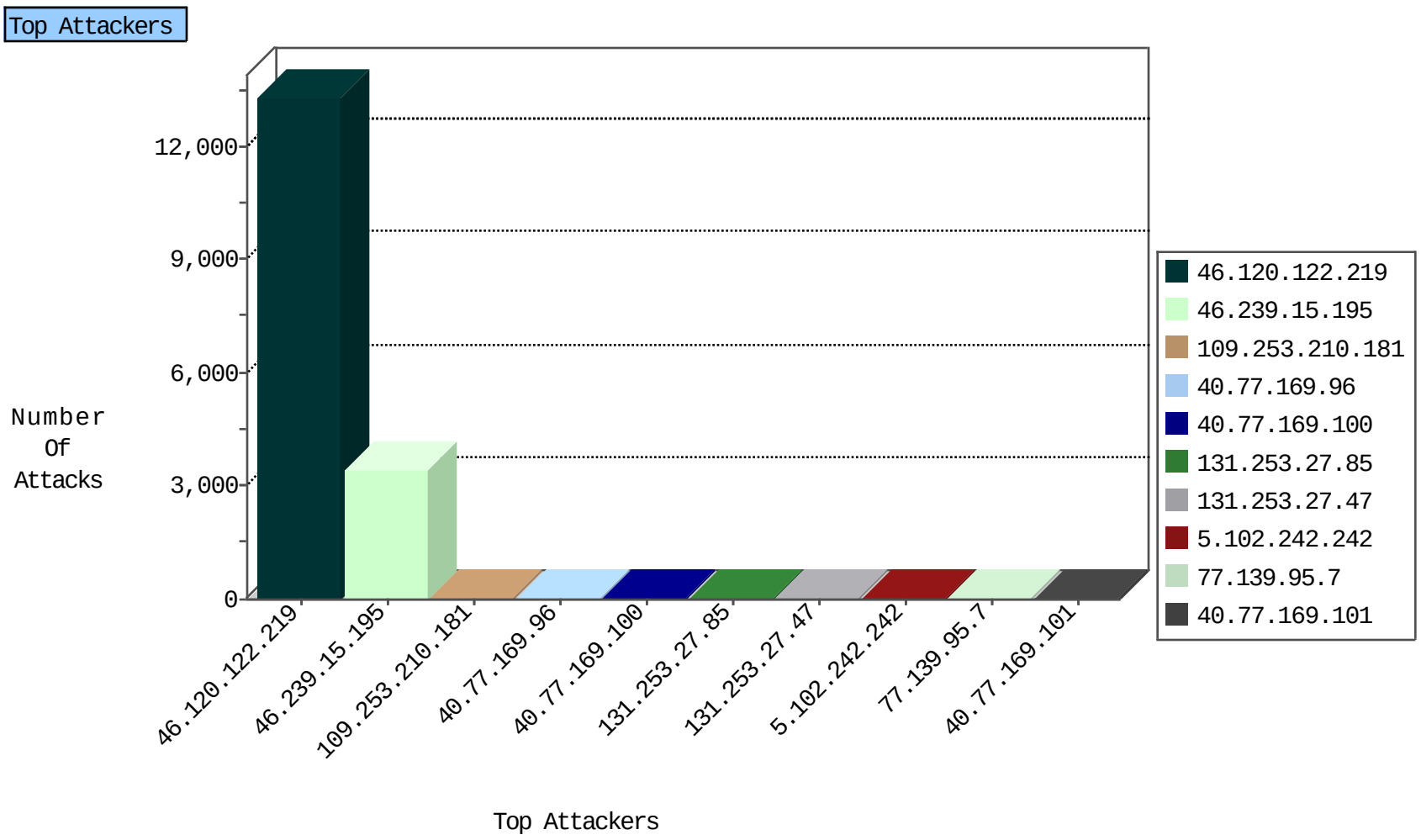
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

08-27-2016-20:04:02 to 08-27-2016-21:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.80.78.2 | Israel | 147.237.76.86 | navy.idf.il | Black List | drop | 2 |
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | Frk_Under_Attack_Con_Http | drop | 2 |
| 115.230.125.146 | China | 147.237.77.19 | law-forum.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |

08-27-2016-20:04:02 to 08-27-2016-21:04:02

## Top Attackers In IPS

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

08-27-2016-20:04:02 to 08-27-2016-21:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.120.122.219 | 147.237.76.200 | Israel | eitan.aka.idf.il | Xenu Link Sleuth User Agent | 6818 |
| 46.120.122.219 | 147.237.72.166 | Israel | aka.idf.il | Xenu Link Sleuth User Agent | 1591 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 1256 |
| 46.120.122.219 | 147.237.77.226 | Israel | www.chamatz.aka.idf.il | Xenu Link Sleuth User Agent | 859 |
| 46.120.122.219 | 147.237.77.176 | Israel | matpash.idf.il | Xenu Link Sleuth User Agent | 688 |
| 46.120.122.219 | 147.237.76.147 | Israel | chinuch.aka.idf.il | Xenu Link Sleuth User Agent | 555 |
| 46.120.122.219 | 147.237.76.31 | Israel | nakchal.idf.il | Xenu Link Sleuth User Agent | 248 |
| 46.120.122.219 | 147.237.76.86 | Israel | navy.idf.il | Xenu Link Sleuth User Agent | 201 |
| 46.120.122.219 | 147.237.76.42 | Israel | refuah.idf.il | Xenu Link Sleuth User Agent | 145 |
| 46.120.122.219 | 147.237.0.34 | Israel | tikshuv.idf.il | Xenu Link Sleuth User Agent | 58 |
| 46.120.122.219 | 147.237.77.233 | Israel | atal.idf.il | Xenu Link Sleuth User Agent | 10 |
| 46.120.122.219 | 147.237.77.170 | Israel | maarachot.idf.il | Xenu Link Sleuth User Agent | 9 |
| 46.120.122.219 | 147.237.72.167 | Israel | ishurim.aka.idf.il | Xenu Link Sleuth User Agent | 5 |
| 46.120.122.219 | 147.237.76.200 | Israel | eitan.aka.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 36.228.151.111 | 147.237.8.50 | Taiwan | e.tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.201.236.155 | 147.237.77.227 | Ukraine | e.hamaz.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 91.201.236.155 | 147.237.77.227 | Ukraine | e.hamaz.idf.il | ET SCAN NMAP -f -sS | 1 |
| 91.201.236.50 | 147.237.77.178 | Ukraine | e.matpash.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 66.203.215.242 | 147.237.0.34 | Canada | tikshuv.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 46.120.122.219 | 147.237.76.42 | Israel | refuah.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 58.218.204.245 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.218.204.245 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 163.172.169.150 | 147.237.76.148 | United Kingdom | gqcenter.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.120.122.219 | 147.237.0.15 | Israel | kosher-kravi.idf.il | Xenu Link Sleuth User Agent | 1 |
| 5.39.222.253 | 147.237.76.197 | Netherlands | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.155 | 147.237.77.227 | Ukraine | e.hamaz.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.50 | 147.237.77.178 | Ukraine | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.50 | 147.237.77.178 | Ukraine | e.matpash.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 66.203.215.242 | 147.237.0.34 | Canada | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.204.245 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.120.122.219 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.120.122.219 | 147.237.72.156 | Israel | aman.idf.il | Xenu Link Sleuth User Agent | 1 |
| 46.120.122.219 | 147.237.77.226 | Israel | www.chamatz.aka.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 46.120.122.219 | 147.237.0.17 | Israel | m.my-kosher-kravi.idf.il | Xenu Link Sleuth User Agent | 1 |

08-27-2016-20:04:02 to 08-27-2016-21:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3199 |
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | | drop | 200 |
| 40.77.169.96 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 27 |
| 40.77.169.99 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 11 |
| 40.77.169.96 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 11 |
| 40.77.169.101 | United States | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 10 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 40.77.169.101 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 7 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 7 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 109.66.172.82 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 106.38.241.105 | China | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 4 |
| 40.77.169.102 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 4 |
| 40.77.169.104 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 3 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 3 |
| 188.120.148.41 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 79.179.190.115 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.179.219.26 | Israel | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 2 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 185.120.126.17 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 109.253.210.181 | Israel | 147.237.0.19 | madim.atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.72.167 | ishurim.aka.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 117.215.169.251 | India | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 207.46.13.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 141.212.121.176 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 1 |
| 46.19.86.152 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.132.22 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.1.223 | Israel | 147.237.0.19 | madim.atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 1 |
| 109.253.157.207 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

08-27-2016-20:04:02 to 08-27-2016-21:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.120.122.219 | Block | 824 |
| 109.253.210.181 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 52 |
| 131.253.27.85 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 23 |
| 5.102.242.242 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 22 |
| 131.253.27.47 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 22 |
| 77.139.95.7 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 21 |
| 46.120.122.219 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 11 |
| 46.120.122.219 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 8 |
| 37.26.147.180 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 84.111.108.45 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 89.138.189.40 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 132.74.95.19 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112994.pdf | Block | 4 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 4 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 46.120.122.219 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 4 |
| 2.53.128.248 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 85.64.63.133 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.146 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 2 |
| 131.253.27.96 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 46.120.122.219 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 2 |
| 46.120.122.219 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/ | Block | 2 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in URL from 40.77.169.98 | Block | 2 |
| 46.120.122.219 | Israel | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 2 |
| 37.26.146.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.121.235.90 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 77.139.69.181 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 1 |
| 66.102.6.25 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 1 |
| 46.120.122.219 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 2.53.190.82 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 46.120.122.219 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 204.79.180.232 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/portalmiluim/templates/inner.asp | Block | 1 |
| 109.66.151.131 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 46.120.122.219 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 46.120.122.219 | Block | 1 |
| 40.77.169.98 | United States | 147.237.77.176 | matpash.idf.il | Multiple Illegal Byte Code Character in URL from 40.77.169.98 | Block | 1 |
| 66.249.64.45 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 46.120.122.219 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx | None | 1 |
| 89.237.65.76 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 89.237.65.76 | Block | 1 |
| 77.138.67.159 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/sachar | Block | 1 |
| 2.53.190.82 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 2.53.190.82 | Block | 1 |
| 213.57.97.170 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 84.94.174.209 | Israel | 147.237.77.216 | dover.idf.il | Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText | Block | 1 |
| 66.249.64.105 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx | Block | 1 |
| 46.120.122.219 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx | None | 1 |
| 89.237.65.76 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 77.138.74.21 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/recruitlane.aspx | Block | 1 |
| 213.151.57.119 | Israel | 147.237.77.216 | dover.idf.il | Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx | Block | 1 |
| 46.120.122.219 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx | Block | 1 |
| 131.253.27.41 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.19.85.66 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |

08-27-2016-20:04:02 to 08-27-2016-21:04:02