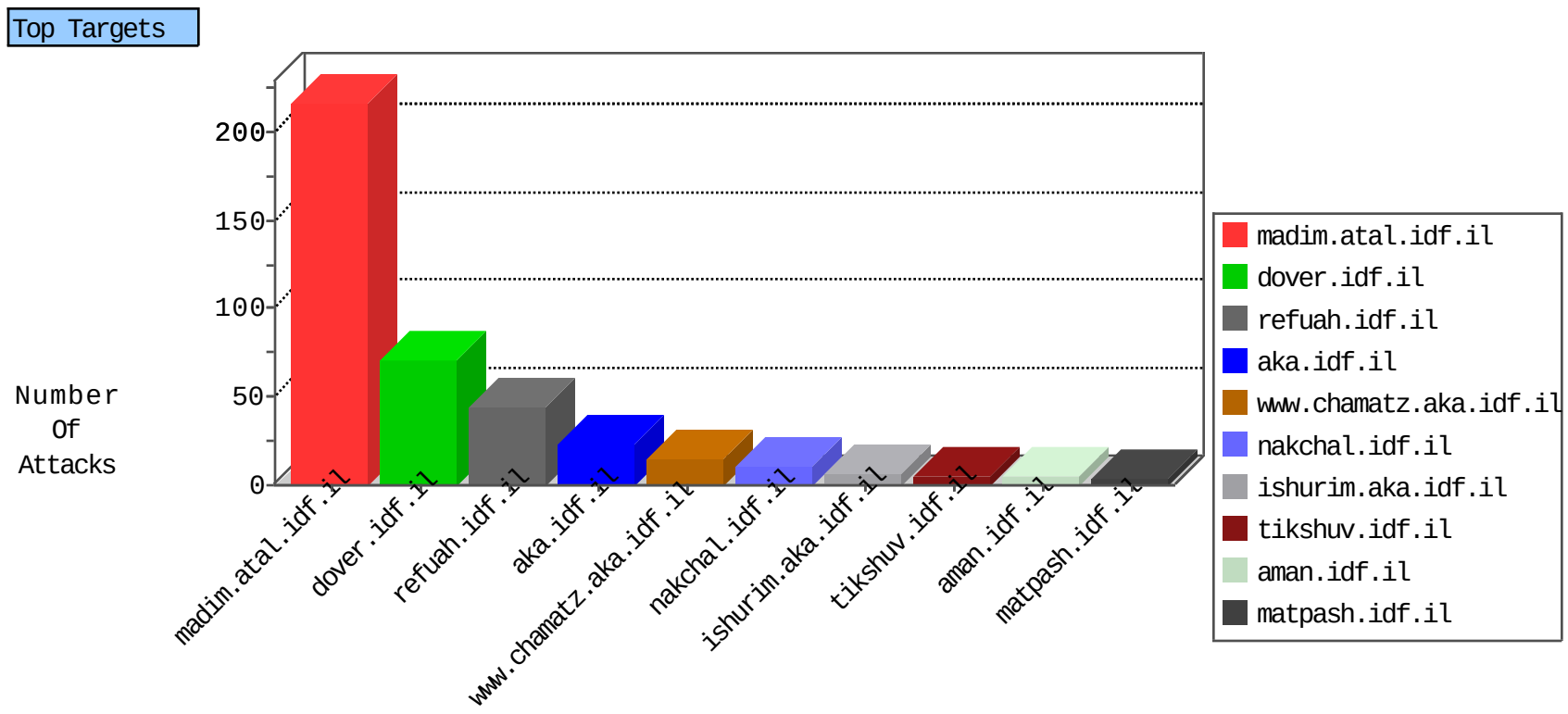
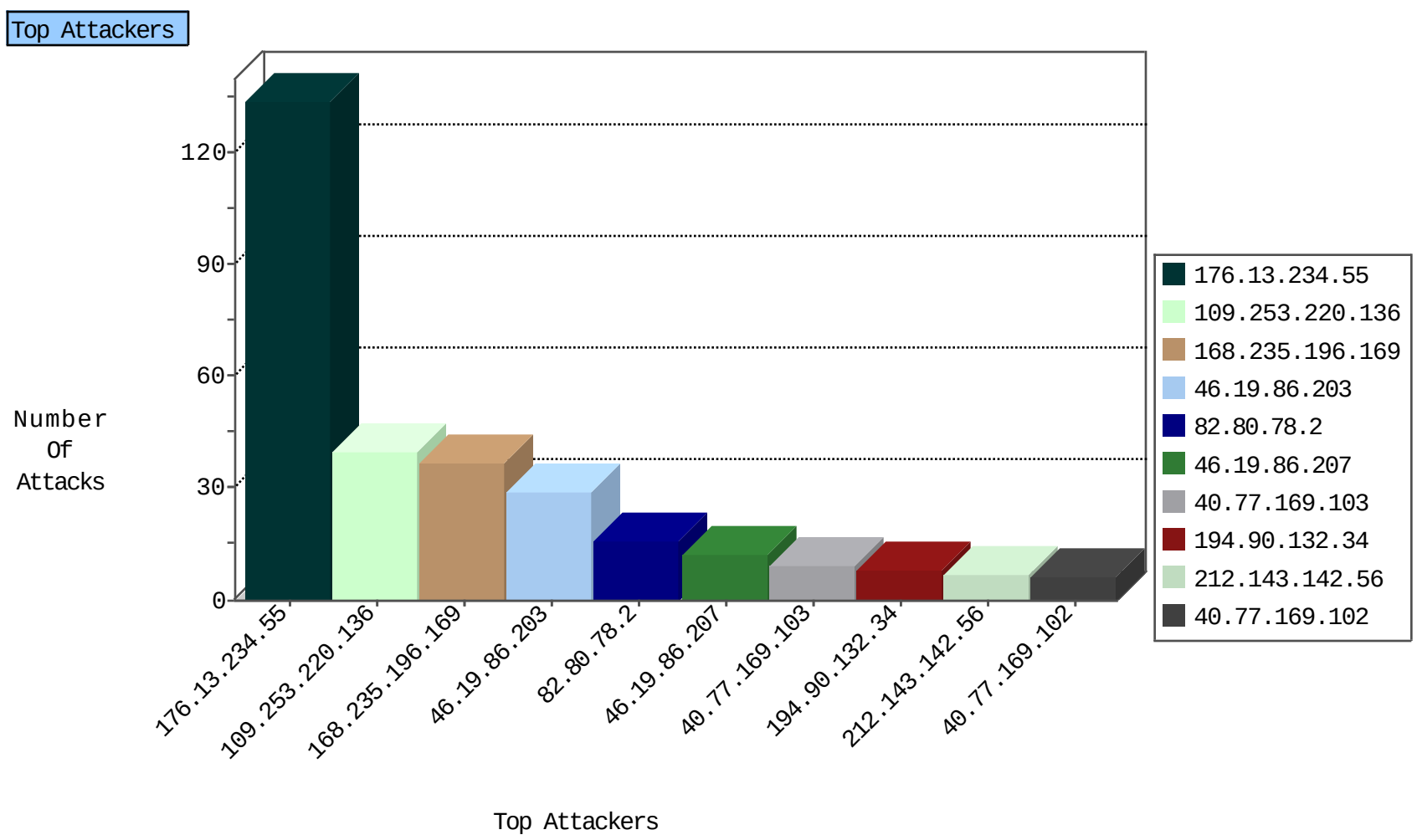
08-25-2016-10:04:06 to 08-25-2016-11:04:06

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-25-2016-10:04:06 to 08-25-2016-11:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.80.78.2 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Black List | drop | 15 |
| 168.235.196.169 | United States | 147.237.76.42 | refuah.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 209.126.136.2 | United States | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 1 |
| 168.235.196.169 | United States | 147.237.76.42 | refuah.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 185.128.40.162 | Switzerland | 147.237.76.34 | yohalan.idf.il | Black List | drop | 1 |
| 93.158.200.166 | Netherlands | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |
| 185.128.40.162 | Switzerland | 147.237.76.148 | ggcenter.aka.idf.il | Black List | drop | 1 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

08-25-2016-10:04:06 to 08-25-2016-11:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.9.10.227 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |

08-25-2016-10:04:06 to 08-25-2016-11:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 52.53.154.128 | 147.237.72.166 | United States | aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 82.166.247.138 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 8.26.94.207 | 147.237.77.233 | Canada | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 203.4.240.101 | 147.237.77.74 | Australia | law.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.178.147.43 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.225.149 | 147.237.0.17 | Ukraine | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.88.18 | 147.237.76.30 | United States | himush.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 185.110.132.201 | 147.237.77.212 | Ukraine | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 65.49.68.166 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.110.132.201 | 147.237.72.166 | Ukraine | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.219.125.238 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.110.132.201 | 147.237.0.17 | Ukraine | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.218.204.245 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 161.18.11.21 | 147.237.76.39 | Colombia | mobile.meitav.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.218.204.245 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 93.174.91.29 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.227.67.172 | 147.237.76.34 | Sweden | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.108.246.70 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 18.85.22.237 | 147.237.77.176 | United States | matpash.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 212.179.21.194 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.255.201 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.134.161 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 201.238.202.219 | 147.237.77.243 | Chile | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 74.91.23.106 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 186.114.39.29 | 147.237.76.31 | Colombia | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 66.203.215.242 | 147.237.8.28 | Canada | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 185.110.132.201 | 147.237.76.197 | Ukraine | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.219.138.24 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.110.132.201 | 147.237.8.14 | Ukraine | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.218.204.245 | 147.237.76.42 | China | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.13.21.147 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 58.218.204.245 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.253.242.205 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.169.200.194 | 147.237.77.19 | Russian Federation | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.56 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

08-25-2016-10:04:06 to 08-25-2016-11:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.196.169 | United States | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 33 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 6 |
| 46.19.85.72 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 82.166.93.161 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.110 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 4 |
| 37.26.146.167 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 178.222.213.170 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 212.143.142.44 | 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 |
| 196.205.150.141 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 62.219.153.137 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 80.178.67.231 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 209.88.157.240 | Israel | 147.237.76.148 | gqcenter.aka.idf.il | drop |  | drop | 1 |
| 109.253.197.16 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.219.53 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.19.85.247 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 195.81.184.242 | Italy | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 85.130.231.13 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.130.236 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 212.199.220.82 | Israel | 147.237.0.35 | akaws.idf.il | drop |  | drop | 1 |
| 209.88.157.240 | Israel | 147.237.76.34 | yohalan.idf.il | drop |  | drop | 1 |
| 109.253.159.93 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.218.206.76 | United States | 147.237.0.200 | m4u.idf.il | drop |  | drop | 1 |
| 176.13.13.204 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

08-25-2016-10:04:06 to 08-25-2016-11:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.234.55 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 134 |
| 109.253.220.136 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 40 |
| 46.19.86.203 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 46.19.86.207 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 12 |
| 194.90.132.34 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 194.90.132.34 | Block | 4 |
| 194.90.132.34 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 4 |
| 212.143.134.129 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 3 |
| 188.126.47.158 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/sachar | Block | 2 |
| 80.246.133.242 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 2 |
| 176.13.246.86 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 212.143.134.129 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/ href= | Block | 1 |
| 66.249.66.12 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113025.pdf | Block | 1 |
| 167.220.232.104 | Japan | 147.237.77.176 | matpash.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 207.46.13.155 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.34 | tikshuv.idf.il | Unknown HTTP Request Method {[[#5]][[#26]]/[[#4]]·Gdlžƒ#„úåÐ0[[#24]]ú»#012Q’ | Block | 1 |
| 217.69.133.28 | Russian Federation | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt | Block | 1 |
| 66.249.66.18 | Israel | 147.237.77.170 | maarachot.idf.il | Distributed Unauthorized URL Access on maarachot.idf.il/pdf/files/5/113025.pdf | Block | 1 |
| 194.90.66.15 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/text.css | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.34 | tikshuv.idf.il | Abnormally Long Request method | Block | 1 |
| 84.94.75.225 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 209.88.157.240 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 176.13.3.52 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 1 |
| 138.134.192.10 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 220.181.51.81 | China | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/robots.txt | Block | 1 |
| 66.249.76.70 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.34 | tikshuv.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 84.95.251.241 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 62.219.35.131 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 209.88.198.1 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 157.55.39.181 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_moreinfo.asp | Block | 1 |
| 77.138.178.56 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 1 |
| 40.77.167.66 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.34 | tikshuv.idf.il | Illegal Byte Code Character in Method {[[#5]][[#26]]/[[#4]]·Gdlžƒ#„úåÐ0[[#24]]ú»#012Q’ | Block | 1 |
| 85.64.38.169 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 66.102.9.43 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/drushim/ | Block | 1 |
| 157.55.39.229 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx | None | 1 |
| 78.37.72.142 | 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 |
| 46.19.86.60 | 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 |
| 194.153.113.35 | Germany | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.34 | tikshuv.idf.il | Malformed URL | Block | 1 |
| 109.253.144.73 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |

08-25-2016-10:04:06 to 08-25-2016-11:04:06