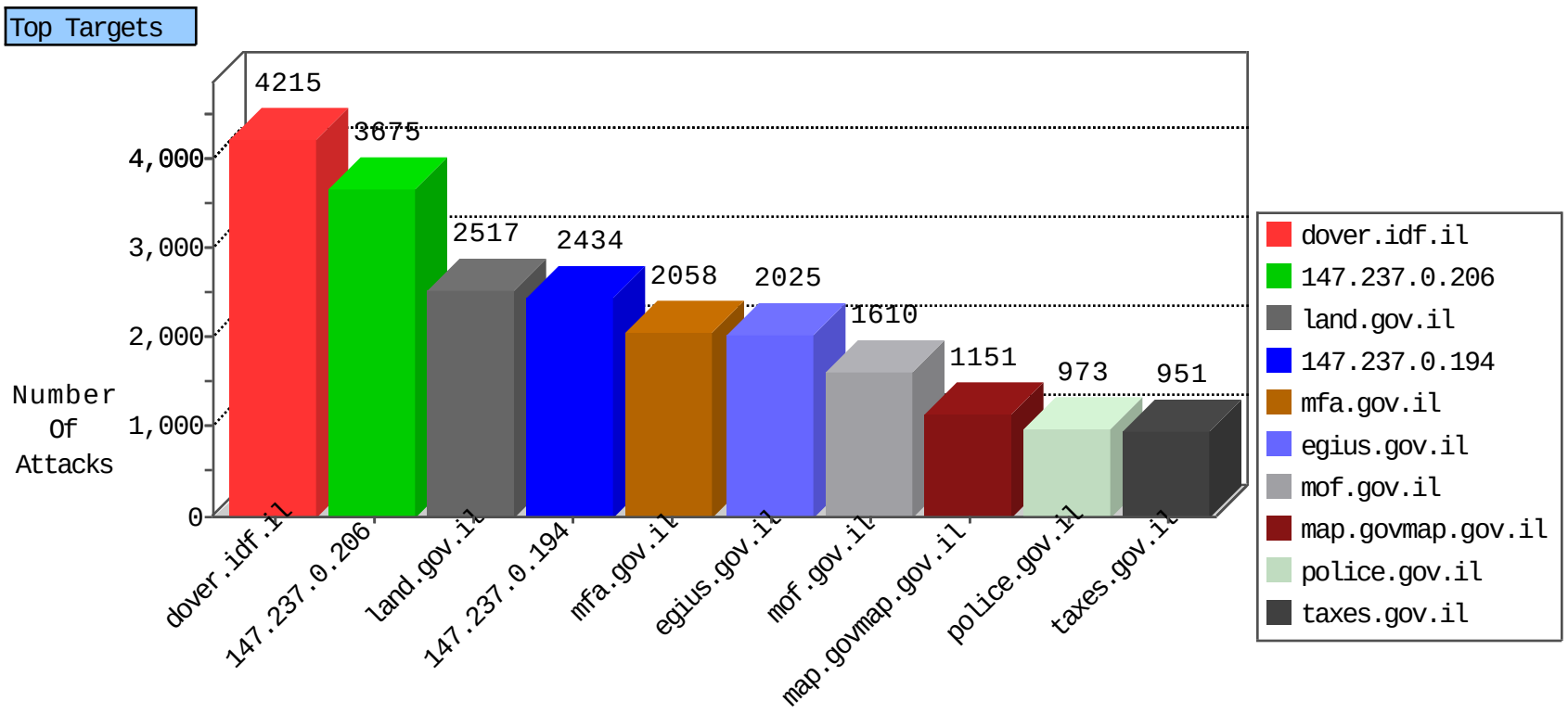
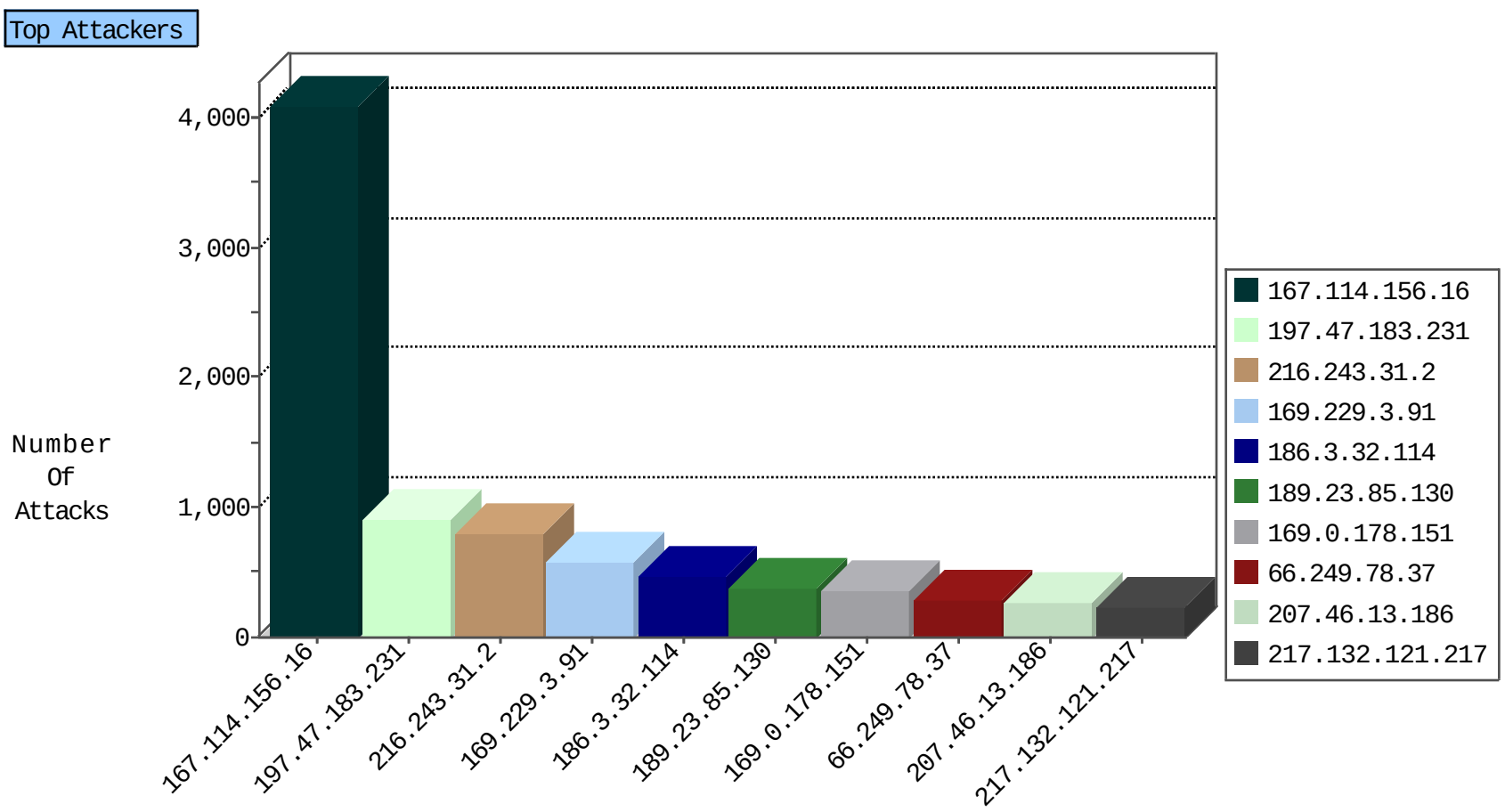
04-18-2016-19:02:08 to 04-18-2016-20:02:08

# Tehila Hosting Under Attack



04-18-2016-19:02:08 to 04-18-2016-20:02:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Signature | Device Action |
|---|---|---|---|---|
| 0.0.0.0 | 147.237.0.206 | | drop | 43 |
| 0.0.0.0 | 147.237.0.206 | | drop | 743 |
| 0.0.0.0 | 147.237.76.106 | | drop | 6 |
| 0.0.0.0 | 147.237.76.106 | | forward | 29 |
| 0.0.0.0 | 147.237.76.155 | | drop | 4 |
| 1.34.123.239 | 147.237.3.255 | Taiwan | drop | 1 |
| 2.26.11.175 | 147.237.76.106 | United Kingdom | drop | 6 |
| 2.53.9.195 | 147.237.0.206 | Israel | drop | 65 |
| 2.53.15.8 | 147.237.0.206 | Israel | drop | 2 |
| 2.53.15.100 | 147.237.0.206 | Israel | drop | 1 |
| 2.53.15.100 | 147.237.0.206 | Israel | drop | 1 |
| 2.53.42.124 | 147.237.0.206 | Israel | drop | 3 |
| 2.53.152.33 | 147.237.0.206 | Israel | drop | 1 |
| 2.53.181.160 | 147.237.0.206 | Israel | drop | 1 |
| 2.55.54.70 | 147.237.0.206 | Israel | drop | 7 |
| 2.55.54.70 | 147.237.0.206 | Israel | drop | 13 |
| 2.55.144.98 | 147.237.77.60 | Israel | dest-reset | 3 |
| 5.22.131.22 | 147.237.0.206 | Israel | drop | 1 |
| 5.22.131.22 | 147.237.0.206 | Israel | drop | 2 |
| 5.22.135.129 | 147.237.0.206 | Israel | drop | 1 |
| 5.22.135.129 | 147.237.0.206 | Israel | drop | 1 |
| 5.29.57.49 | 147.237.76.174 | Israel | drop | 3 |
| 5.29.73.205 | 147.237.76.43 | Israel | drop | 6 |
| 5.29.193.19 | 147.237.76.134 | Israel | drop | 3 |
| 5.29.193.19 | 147.237.76.172 | Israel | drop | 3 |
| 5.29.251.84 | 147.237.0.206 | Israel | drop | 1 |
| 10.0.0.1 | 147.237.0.206 | | drop | 6 |
| 10.0.0.2 | 147.237.0.206 | | drop | 3 |
| 23.106.166.235 | 147.237.76.155 | United States | drop | 2 |
| 27.140.164.228 | 147.237.9.12 | Japan | drop | 1 |
| 31.154.22.54 | 147.237.77.138 | Israel | dest-reset | 3 |
| 31.154.41.17 | 147.237.0.206 | Israel | drop | 1 |
| 31.168.179.203 | 147.237.77.77 | Israel | dest-reset | 2 |
| 31.210.186.48 | 147.237.0.206 | Israel | drop | 5 |
| 31.210.186.245 | 147.237.76.172 | Israel | drop | 6 |
| 37.26.147.222 | 147.237.0.206 | Israel | drop | 1 |
| 37.46.38.16 | 147.237.0.206 | Israel | drop | 5 |
| 37.46.41.121 | 147.237.0.206 | Israel | drop | 2 |
| 37.46.41.121 | 147.237.0.206 | Israel | drop | 9 |
| 37.142.64.19 | 147.237.0.206 | Israel | drop | 2 |
| 38.108.202.139 | 147.237.76.106 | United States | drop | 1 |
| 40.77.167.105 | 147.237.76.32 | United States | forward | 1 |
| 41.40.34.229 | 147.237.0.206 | Egypt | drop | 3 |
| 46.19.85.6 | 147.237.0.206 | Israel | drop | 15 |
| 46.19.85.27 | 147.237.0.206 | Israel | drop | 1 |
| 46.19.85.49 | 147.237.0.206 | Israel | drop | 4 |
| 46.19.85.51 | 147.237.0.206 | Israel | drop | 5 |
| 46.19.85.95 | 147.237.0.206 | Israel | drop | 1 |
| 46.19.85.134 | 147.237.0.206 | Israel | drop | 2 |
| 46.19.85.134 | 147.237.0.206 | Israel | drop | 2 |

04-18-2016-19:02:08 to 04-18-2016-20:02:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Name | Device Action | Count |
|---|---|---|---|---|---|
| 31.168.245.179 | 147.237.0.49 | Israel | 16471: HTTP: TeamViewer Communication Attempt | Block | 98 |
| 87.142.240.209 | 147.237.77.225 | Germany | 1633: HTTP: WebDAV Protocol PROPFIND Method | Block | 8 |
| 87.142.240.209 | 147.237.76.106 | Germany | 1633: HTTP: WebDAV Protocol PROPFIND Method | Block | 6 |
| 71.6.158.166 | 147.237.76.155 | United States | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 109.160.205.68 | 147.237.77.88 | Israel | 15323: HTTP: User-Agent (MRSPUTNIK) | Block | 1 |
| 195.230.3.17 | 147.237.0.206 | Bulgaria | 14170: HTTP: Blank User-Agent (descriptor but no string) | Block | 1 |
| 71.6.146.185 | 147.237.8.83 | United States | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 77.120.108.186 | 147.237.72.201 | Ukraine | 13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet | Permit | 1 |
| 142.54.167.98 | 147.237.77.88 | United States | 22280: HTTP: Joomla Object Injection Vulnerability | Block | 1 |

04-18-2016-19:02:08 to 04-18-2016-20:02:08

Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Name |
|---|---|---|---|
| 2.53.2.238 | 147.237.77.246 | Israel | 3 |
| 2.53.16.15 | 147.237.0.64 | Israel | 1 |
| 2.53.22.78 | 147.237.77.238 | Israel | 2 |
| 2.53.25.37 | 147.237.77.250 | Israel | 1 |
| 2.53.29.162 | 147.237.77.250 | Israel | 4 |
| 2.53.37.247 | 147.237.0.64 | Israel | 9 |
| 2.53.43.104 | 147.237.0.64 | Israel | 4 |
| 2.53.48.4 | 147.237.77.18 | Israel | 17 |
| 2.53.48.165 | 147.237.76.132 | Israel | 15 |
| 2.53.53.13 | 147.237.76.26 | Israel | 4 |
| 2.53.55.62 | 147.237.0.61 | Israel | 1 |
| 2.53.55.75 | 147.237.76.26 | Israel | 3 |
| 2.53.128.86 | 147.237.76.136 | Israel | 1 |
| 2.53.150.73 | 147.237.0.64 | Israel | 2 |
| 2.53.159.166 | 147.237.77.250 | Israel | 3 |
| 2.53.176.18 | 147.237.76.20 | Israel | 5 |
| 2.53.177.79 | 147.237.0.64 | Israel | 2 |
| 2.55.142.200 | 147.237.72.201 | Israel | 1 |
| 2.55.173.165 | 147.237.0.64 | Israel | 3 |
| 2.55.188.98 | 147.237.76.136 | Israel | 1 |
| 2.71.250.93 | 147.237.76.106 | Sweden | 9 |
| 2.216.192.89 | 147.237.76.20 | United Kingdom | 10 |
| 2.216.192.89 | 147.237.77.18 | United Kingdom | 3 |
| 5.18.104.55 | 147.237.77.225 | Russian Federation | 2 |
| 5.22.130.252 | 147.237.76.26 | Israel | 9 |
| 5.22.131.89 | 147.237.0.64 | Israel | 6 |
| 5.28.153.147 | 147.237.76.26 | Israel | 2 |
| 5.28.156.89 | 147.237.0.64 | Israel | 1 |
| 5.28.184.245 | 147.237.0.64 | Israel | 2 |
| 5.29.251.84 | 147.237.76.192 | Israel | 3 |
| 5.102.195.158 | 147.237.77.238 | Israel | 10 |
| 5.102.195.232 | 147.237.0.64 | Israel | 2 |
| 5.102.209.159 | 147.237.0.64 | Israel | 1 |
| 5.102.213.243 | 147.237.77.18 | Israel | 3 |
| 5.102.234.190 | 147.237.76.26 | Israel | 6 |
| 5.102.254.65 | 147.237.0.64 | Israel | 1 |
| 5.102.254.195 | 147.237.77.250 | Israel | 2 |
| 14.207.47.34 | 147.237.77.225 | Thailand | 1 |
| 31.154.41.17 | 147.237.0.61 | Israel | 14 |
| 31.154.50.68 | 147.237.76.192 | Israel | 10 |
| 31.154.151.80 | 147.237.0.64 | Israel | 1 |
| 31.168.50.146 | 147.237.76.26 | Israel | 2 |
| 31.168.79.187 | 147.237.72.65 | Israel | 1 |
| 31.168.101.163 | 147.237.76.20 | Israel | 17 |
| 31.168.158.31 | 147.237.0.64 | Israel | 4 |
| 31.168.192.81 | 147.237.77.250 | Israel | 7 |
| 31.168.213.151 | 147.237.0.64 | Israel | 2 |
| 31.168.219.250 | 147.237.0.64 | Israel | 2 |
| 37.26.146.220 | 147.237.76.26 | Israel | 6 |
| 37.26.147.238 | 147.237.0.64 | Israel | 1 |

04-18-2016-19:02:08 to 04-18-2016-20:02:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Message | Device Action | Count |
|---|---|---|---|---|---|
| 189.23.85.130 | 147.237.76.32 | Brazil | EmbassiesRedirect | monitor | 380 |
| 169.0.178.151 | 147.237.0.194 | South Africa | | drop | 356 |
| 66.249.78.37 | 147.237.0.194 | United States | | drop | 288 |
| 207.46.13.186 | 147.237.0.194 | United States | | drop | 258 |
| 186.3.32.114 | 147.237.3.133 | Ecuador | | drop | 232 |
| 186.3.32.114 | 147.237.13.23 | Ecuador | | drop | 232 |
| 217.132.121.217 | 147.237.76.239 | Israel | egius.gov.il | drop | 222 |
| 195.200.205.2 | 147.237.76.139 | Israel | call.health.gov.il | drop | 216 |
| 82.81.20.159 | 147.237.72.103 | Israel | land.gov.il | drop | 180 |
| 72.37.140.45 | 147.237.0.121 | Italy | | drop | 176 |
| 46.19.85.179 | 147.237.76.239 | Israel | egius.gov.il | drop | 174 |
| 40.77.167.1 | 147.237.0.194 | United States | | drop | 153 |
| 89.139.235.88 | 147.237.76.239 | Israel | egius.gov.il | drop | 117 |
| 85.64.39.0 | 147.237.76.239 | Israel | egius.gov.il | drop | 114 |
| 109.67.189.229 | 147.237.76.239 | Israel | egius.gov.il | drop | 114 |
| 193.37.128.117 | 147.237.76.174 | Israel | map.govmap.gov.il | drop | 108 |
| 2.53.42.26 | 147.237.76.174 | Israel | map.govmap.gov.il | drop | 108 |
| 173.196.250.218 | 147.237.76.239 | United States | egius.gov.il | drop | 108 |
| 79.176.98.160 | 147.237.72.103 | Israel | land.gov.il | drop | 106 |
| 149.88.199.199 | 147.237.76.106 | Israel | mfa.gov.il | monitor | 102 |
| 165.225.72.64 | 147.237.0.121 | Germany | | drop | 99 |
| 31.154.254.132 | 147.237.76.174 | Israel | map.govmap.gov.il | drop | 96 |
| 85.250.177.35 | 147.237.72.103 | Israel | land.gov.il | drop | 96 |
| 201.28.116.118 | 147.237.76.32 | Brazil | EmbassiesRedirect | monitor | 94 |
| 5.28.155.17 | 147.237.72.103 | Israel | land.gov.il | drop | 93 |
| 5.28.155.232 | 147.237.76.174 | Israel | map.govmap.gov.il | drop | 84 |
| 176.13.19.65 | 147.237.76.174 | Israel | map.govmap.gov.il | drop | 84 |
| 77.127.84.130 | 147.237.0.194 | Israel | | drop | 81 |
| 66.249.78.44 | 147.237.0.194 | United States | | drop | 81 |
| 87.71.74.31 | 147.237.72.103 | Israel | land.gov.il | drop | 81 |
| 208.87.233.201 | 147.237.72.58 | United States | | drop | 81 |
| 93.173.201.241 | 147.237.72.103 | Israel | land.gov.il | drop | 80 |
| 92.105.26.228 | 147.237.0.194 | Switzerland | | drop | 78 |
| 212.179.221.203 | 147.237.72.103 | Israel | land.gov.il | drop | 78 |
| 212.199.175.251 | 147.237.72.103 | Israel | land.gov.il | drop | 78 |
| 46.120.166.164 | 147.237.77.233 | Israel | atal.idf.il | monitor | 76 |
| 80.178.202.72 | 147.237.0.194 | Israel | | drop | 75 |
| 99.197.12.206 | 147.237.76.106 | United States | mfa.gov.il | reject | 74 |
| 99.197.12.206 | 147.237.76.106 | United States | mfa.gov.il | monitor | 74 |
| 46.121.202.15 | 147.237.76.239 | Israel | egius.gov.il | drop | 72 |
| 65.19.138.33 | 147.237.0.194 | United States | | drop | 72 |
| 109.65.24.144 | 147.237.76.239 | Israel | egius.gov.il | drop | 72 |
| 79.182.136.130 | 147.237.72.103 | Israel | land.gov.il | drop | 72 |
| 192.116.245.249 | 147.237.72.103 | Israel | land.gov.il | drop | 72 |
| 79.182.180.114 | 147.237.76.239 | Israel | egius.gov.il | drop | 72 |
| 157.55.39.75 | 147.237.0.194 | United States | | drop | 72 |
| 149.78.28.118 | 147.237.76.239 | United States | egius.gov.il | drop | 66 |
| 81.218.80.226 | 147.237.0.194 | Israel | | drop | 66 |
| 197.245.173.9 | 147.237.76.32 | South Africa | EmbassiesRedirect | monitor | 63 |
| 66.249.93.24 | 147.237.76.239 | Europe | egius.gov.il | drop | 63 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action |
|---|---|---|---|---|---|
| 2.53.2.238 | 147.237.77.246 | Israel | 4 | Distributed _vti_ | Block |
| 2.53.22.78 | 147.237.77.238 | Israel | 2 | Distributed _vti_ | Block |
| 2.53.25.37 | 147.237.77.250 | Israel | 1 | Distributed _vti_ | Block |
| 2.53.26.82 | 147.237.76.43 | Israel | 2 | Distributed _vti_ | Block |
| 2.53.29.162 | 147.237.77.250 | Israel | 4 | Distributed _vti_ | Block |
| 2.53.36.114 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 2.53.36.216 | 147.237.76.31 | Israel | 1 | Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile | Block |
| 2.53.39.88 | 147.237.76.43 | Israel | 3 | Distributed _vti_ | Block |
| 2.53.48.4 | 147.237.77.18 | Israel | 9 | Distributed _vti_ | Block |
| 2.53.48.165 | 147.237.76.132 | Israel | 18 | Distributed _vti_ | Block |
| 2.53.53.13 | 147.237.76.26 | Israel | 4 | Distributed Unauthorized URL Access on www.justice.gov.il/_vti_bin/sites.asmx | Block |
| 2.53.55.75 | 147.237.76.26 | Israel | 2 | Distributed Unauthorized URL Access on www.justice.gov.il/_vti_bin/sites.asmx | Block |
| 2.53.62.40 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 2.53.131.90 | 147.237.76.43 | Israel | 2 | Distributed _vti_ | Block |
| 2.53.134.176 | 147.237.77.238 | Israel | 2 | Distributed _vti_ | Block |
| 2.53.151.253 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 2.53.154.65 | 147.237.72.166 | Israel | 1 | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block |
| 2.53.159.166 | 147.237.77.250 | Israel | 2 | Distributed _vti_ | Block |
| 2.53.176.18 | 147.237.76.20 | Israel | 7 | Distributed _vti_ | Block |
| 2.55.34.214 | 147.237.0.163 | Israel | 1 | Multiple Unauthorized Method for Known URL from 2.55.34.214 | None |
| 2.55.130.57 | 147.237.77.68 | Israel | 1 | Double URL Encoding - parameter: ReturnUrl in www.people.iaf.org.il/templates/login/login.aspx | Block |
| 2.55.149.159 | 147.237.77.115 | Israel | 4 | Distributed Too Many Headers per Response | Block |
| 2.55.149.159 | 147.237.77.115 | Israel | 1 | Unauthorized URL Access to agmon.tehila.gov.il/pages/.agmoncarousel | Block |
| 2.71.250.93 | 147.237.76.106 | Sweden | 8 | Distributed _vti_ | Block |
| 2.216.192.89 | 147.237.76.20 | United Kingdom | 8 | Distributed _vti_ | Block |
| 2.216.192.89 | 147.237.77.18 | United Kingdom | 3 | Distributed _vti_ | Block |
| 5.9.59.79 | 147.237.72.42 | Germany | 1 | Admin Blocking | Block |
| 5.9.59.79 | 147.237.72.42 | Germany | 2 | Distributed PHP Attempt | Block |
| 5.9.59.79 | 147.237.72.42 | Germany | 1 | Multiple Admin Blocking from 5.9.59.79 | Block |
| 5.22.129.77 | 147.237.77.90 | Israel | 2 | Distributed Illegal Parameter Encoding | None |
| 5.22.129.237 | 147.237.0.71 | Israel | 3 | Unauthorized URL Access to www.mossad.gov.il/(x(1)s(tikixh1gjp0ryhlzczol3kgo))/heb/careers/pages/all.aspx | Block |
| 5.22.130.252 | 147.237.77.90 | Israel | 2 | Distributed Illegal Parameter Encoding | None |
| 5.22.131.5 | 147.237.1.105 | Israel | 1 | Distributed Abnormally Long Request | None |
| 5.22.131.41 | 147.237.76.43 | Israel | 58 | Distributed _vti_ | Block |
| 5.22.131.62 | 147.237.76.26 | Israel | 23 | Distributed Unauthorized Http Methods | Block |
| 5.22.131.70 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 5.22.135.163 | 147.237.76.43 | Israel | 2 | Distributed _vti_ | Block |
| 5.28.153.147 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 5.28.163.176 | 147.237.0.228 | Israel | 10 | Distributed Abnormally Long Request | None |
| 5.28.191.139 | 147.237.76.43 | Israel | 2 | Distributed _vti_ | Block |
| 5.29.5.232 | 147.237.72.201 | Israel | 2 | Parameter Value Length Violation language in forms.gov.il/globaldata/getsequence/gethtmlform.aspx | None |
| 5.29.22.118 | 147.237.76.43 | Israel | 59 | Distributed _vti_ | Block |
| 5.29.27.242 | 147.237.76.43 | Israel | 2 | Distributed _vti_ | Block |
| 5.29.150.153 | 147.237.77.90 | Israel | 1 | Distributed Illegal Parameter Encoding | None |
| 5.29.201.6 | 147.237.76.43 | Israel | 1 | Distributed _vti_ | Block |
| 5.29.251.84 | 147.237.72.26 | Israel | 1 | Unauthorized URL Access to 147.237.72.26/library.asp | Block |
| 5.29.251.84 | 147.237.76.192 | Israel | 4 | Distributed _vti_ | Block |
| 5.102.195.155 | 147.237.0.64 | Israel | 1 | Unauthorized URL Access to www.mof.gov.il/customs/ | Block |
| 5.102.195.158 | 147.237.77.238 | Israel | 8 | Distributed _vti_ | Block |
| 5.102.195.197 | 147.237.72.201 | Israel | 2 | Unauthorized Method HEAD for forms.gov.il/download/signandverify.exe | None |