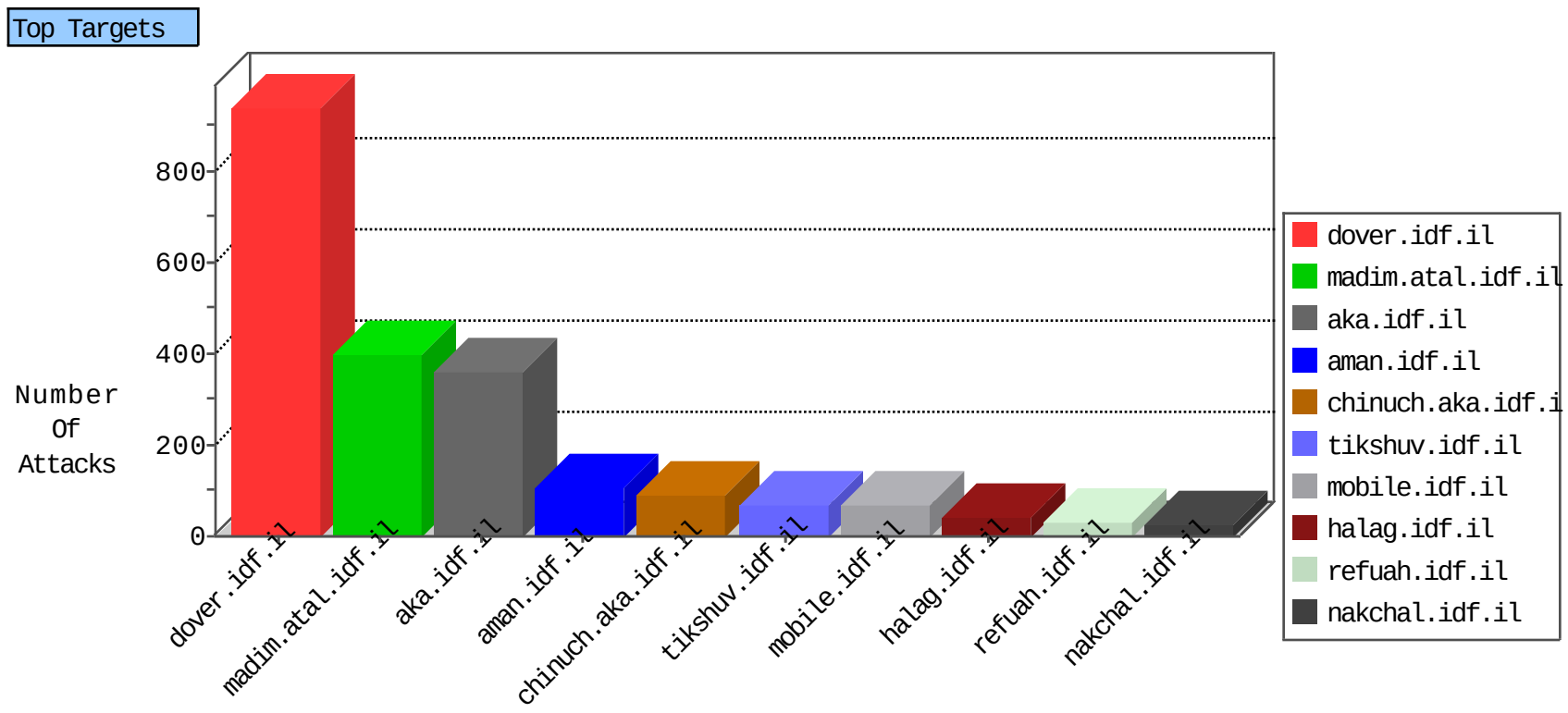
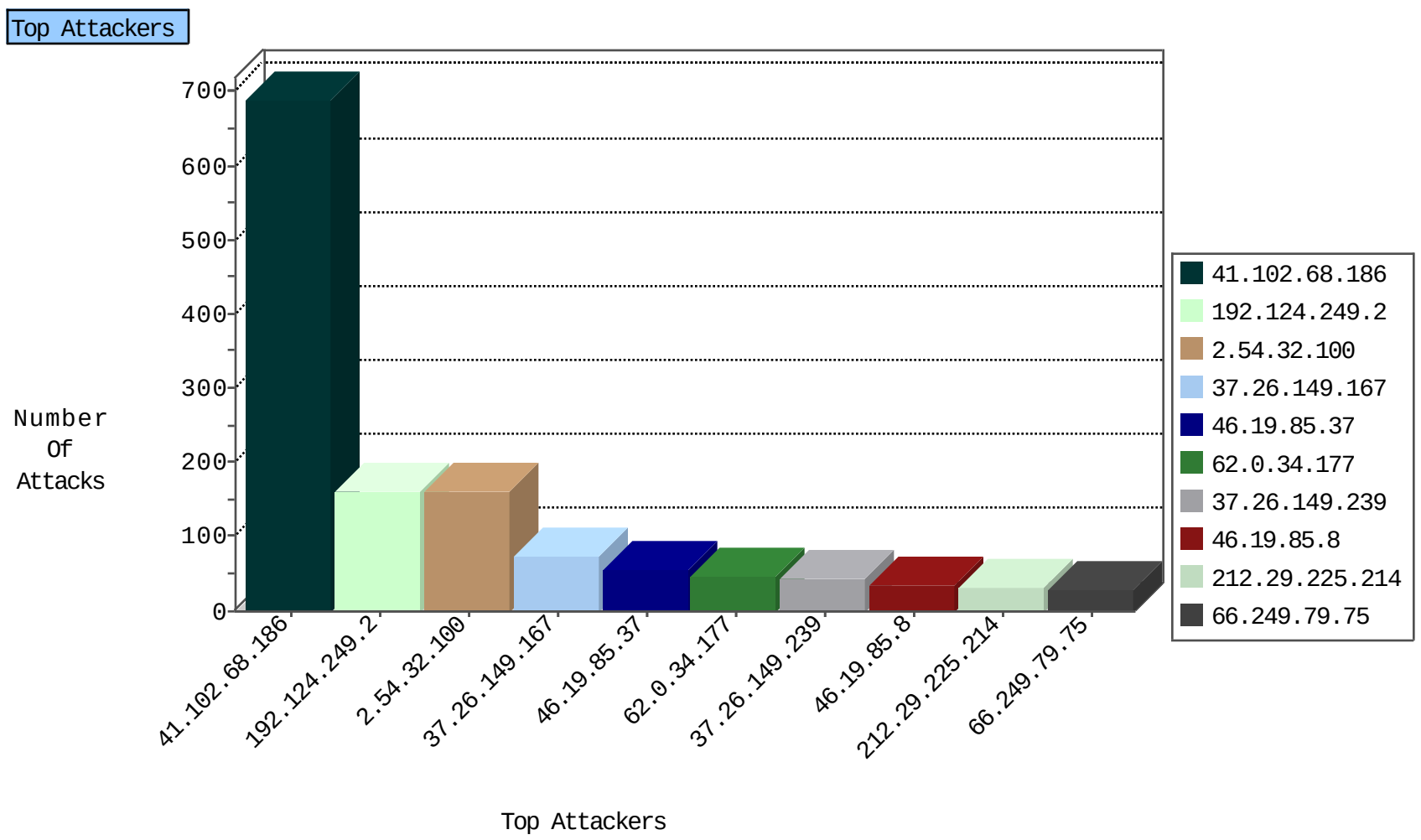
02-28-2016-15:04:09 to 02-28-2016-16:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-28-2016-15:04:09 to 02-28-2016-16:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 41 |
| 62.0.34.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 12 |
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 46.19.85.252 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 134.147.203.115 | Germany | 147.237.0.200 | m4u.idf.il | Block_Ntp_All_Net | drop | 2 |
| 134.147.203.115 | Germany | 147.237.8.45 | e.eitan.idf.il | Block_Ntp_All_Net | drop | 2 |
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 104.243.223.8 | | 147.237.72.217 | e.idf.il | Block_Udp_All_Nets | drop | 1 |
| 179.43.144.33 | Switzerland | 147.237.0.16 | my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 179.43.144.33 | Switzerland | 147.237.0.34 | tikshuv.idf.il | Block_Ntp_All_Net | drop | 1 |
| 104.243.223.8 | | 147.237.8.14 | e.orchot.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.29.242.67 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 176.102.202.32 | Ukraine | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

02-28-2016-15:04:09 to 02-28-2016-16:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.126.164.57 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 12 |
| 109.65.39.39 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 212.25.84.200 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 94.159.157.78 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 37.26.147.164 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 213.151.52.153 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 85.65.167.127 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 84.109.12.29 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 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 |
| 149.78.56.158 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |

02-28-2016-15:04:09 to 02-28-2016-16:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 5 |
| 82.80.196.44 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 36.235.205.174 | 147.237.76.44 | Taiwan | e.refuah.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 212.179.42.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.170.21 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.67.194.60 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.27.37 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.130.3 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.8.27 | China | e.madim.atal.idf.i | ET SCAN Potential SSH Scan | 1 |
| 46.19.86.89 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.46.38.139 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 31.168.77.218 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.88.54.204 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.235.55.21 | 147.237.77.74 | China | law.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 109.65.128.32 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.178.143.82 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.116.28.62 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

02-28-2016-15:04:09 to 02-28-2016-16:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 533 |
| 192.124.249.2 | | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 82 |
| 192.124.249.2 | | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 80 |
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | drop | | drop | 76 |
| 212.29.225.214 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 32 |
| 62.0.34.177 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 85.65.120.49 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 23 |
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 22 |
| 37.26.148.184 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 5.29.212.105 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 77.127.209.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 194.56.215.218 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 15 |
| 80.178.97.72 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 109.253.205.246 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.64.25.140 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 41.102.68.186 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 2.54.39.58 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 149.78.58.99 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 10 |
| 46.19.85.255 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 2.54.38.216 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.177.164.1 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 185.3.144.97 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.11 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 62.0.34.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 37.26.148.164 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 6 |
| 2.54.177.255 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.23 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.23 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 2.52.45.125 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.255 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 85.65.48.119 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 46.19.85.163 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.117.63.153 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 46.19.85.190 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 4 |
| 31.154.34.174 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 46.117.63.153 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 89.138.187.13 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 31.154.34.174 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 2.54.136.47 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 31.154.34.174 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 5.22.130.225 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 37.46.39.16 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.85.252 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 77.127.218.123 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.164 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.85.47 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

02-28-2016-15:04:09 to 02-28-2016-16:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.54.32.100 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 161 |
| 37.26.149.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 74 |
| 46.19.85.37 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 56 |
| 37.26.149.239 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 43 |
| 46.19.85.8 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 36 |
| 66.249.79.75 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.75 | Block | 29 |
| 2.54.166.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 109.64.73.193 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 109.64.73.193 | Block | 14 |
| 216.72.34.89 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 216.72.34.89 | Block | 6 |
| 216.72.34.89 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381 | Block | 6 |
| 46.121.254.223 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/ | Block | 4 |
| 80.178.97.72 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 66.249.66.69 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 66.249.66.69 | Block | 4 |
| 81.218.33.77 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 81.218.33.77 | Block | 3 |
| 46.117.217.99 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.117.217.99 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index | Block | 3 |
| 46.19.85.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.205.246 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.4 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 194.56.215.218 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 2 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 2 |
| 66.249.64.3 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.64.3 | Block | 2 |
| 109.253.195.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 41.137.69.2 | Morocco | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 62.219.163.105 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 85.65.122.255 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 46.19.85.86 | Israel | 147.237.77.74 | law.idf.il | Abnormally Long Request request version | Block | 1 |
| 79.181.63.13 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/9/112899.pdf | Block | 1 |
| 66.249.69.38 | United States | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 66.249.69.38 | Block | 1 |
| 37.26.146.188 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 169.229.3.91 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 66.249.64.69 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/mobile/ | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 149.88.93.150 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 66.249.64.243 | United States | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to kosher-kravi.idf.il/templates/sitemap/sitemap.aspx | Block | 1 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 95.86.93.118 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/bamahane | Block | 1 |
| 79.182.107.134 | 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 |
| 46.19.85.86 | Israel | 147.237.77.74 | law.idf.il | Illegal HTTP Version __atuvs=56d2f530a3e3867e000 | Block | 1 |
| 66.249.69.46 | United States | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1749 | Block | 1 |
| 176.12.135.217 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 109.253.209.42 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 1 |
| 66.249.64.101 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/page.asp | Block | 1 |
| 81.218.33.77 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/3/size338x0/1763.jpg | Block | 1 |
| 194.56.215.218 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 5.29.72.191 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 157.55.39.101 | United States | 147.237.77.233 | atal.idf.il | Distributed Abnormally Long Request | Block | 1 |
| 66.249.66.33 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx | Block | 1 |
| 65.208.151.119 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/ | Block | 1 |
| 79.250.173.201 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 1 |

02-28-2016-15:04:09 to 02-28-2016-16:04:09