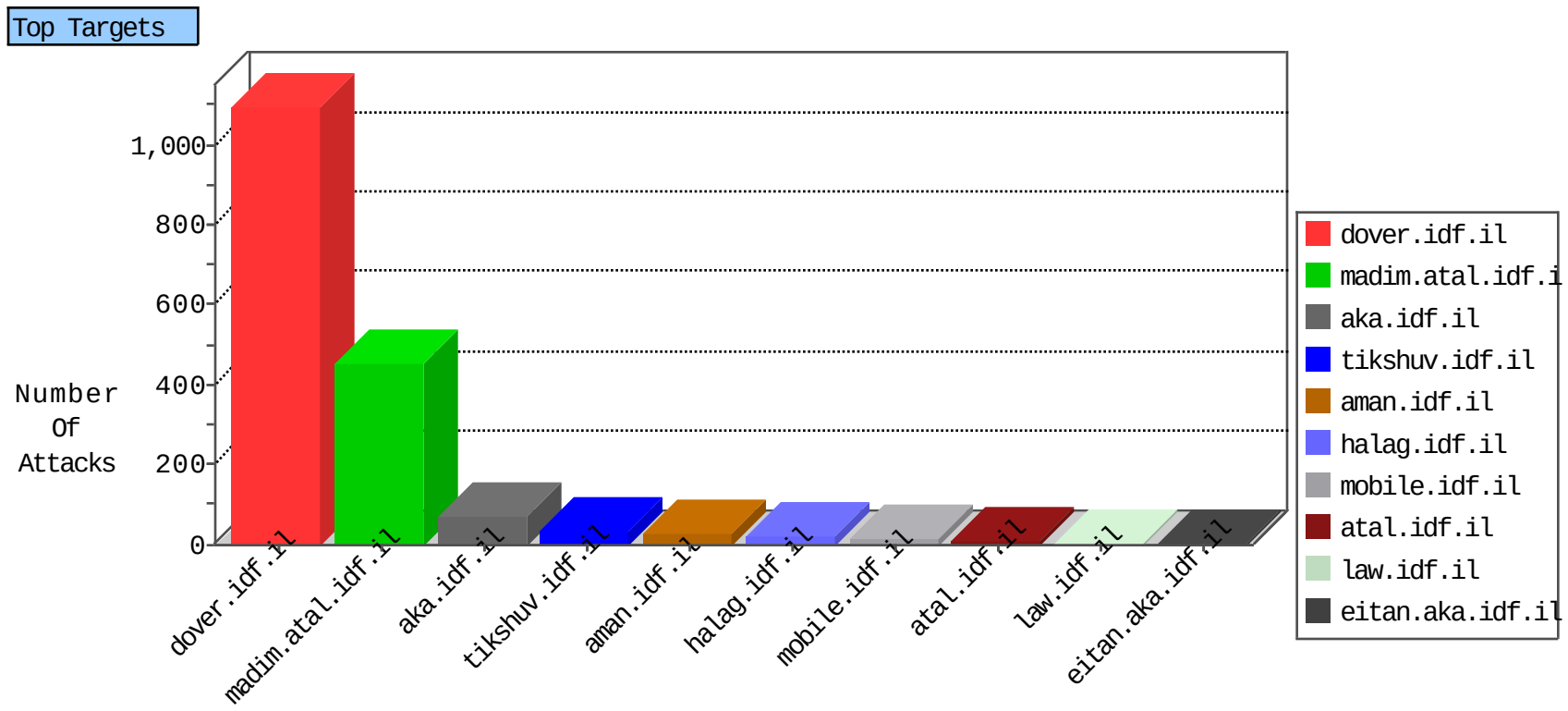
02-26-2016-22:04:01 to 02-26-2016-23:04:01

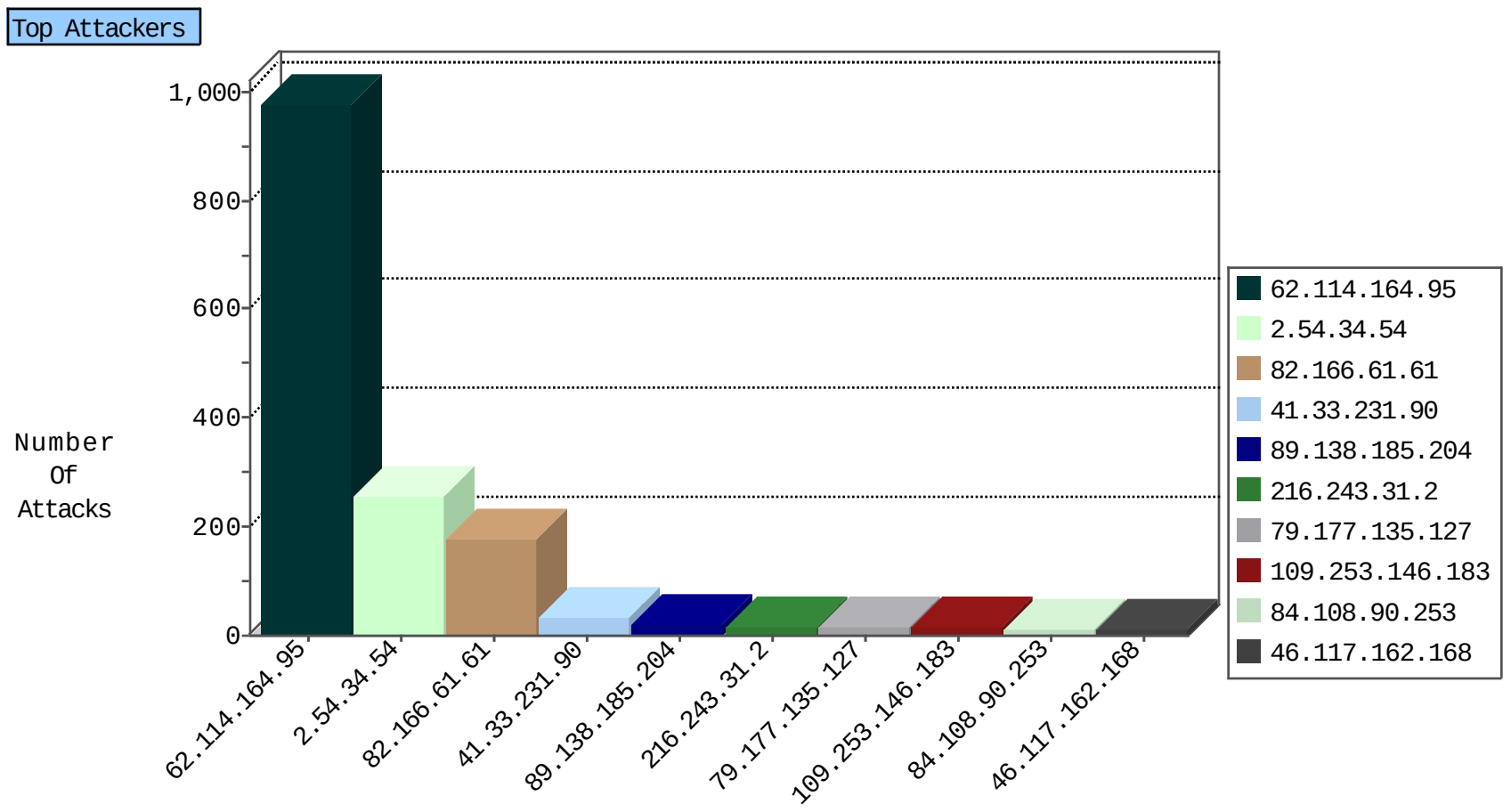
# IDF Under Attack
# Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

02-26-2016-22:04:01 to 02-26-2016-23:04:01

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 4 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 2 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 188.138.102.50 | Germany | 147.237.77.235 | sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 136.243.102.221 | Germany | 147.237.8.27 | e.madim.atal.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 59.42.95.193 | China | 147.237.72.217 | e.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | | 147.237.8.45 | e.eitan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 104.245.97.224 | | 147.237.77.227 | e.hamaz.idf.il | Block_Udp_All_Nets | drop | 1 |
| 193.182.144.142 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 158.255.208.29 | Hong Kong | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 1 |
| 109.236.93.206 | Netherlands | 147.237.77.212 | e.dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 23.228.101.206 | United States | 147.237.8.24 | e.lifestyle.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.94.111.1 | | 147.237.77.216 | dover.idf.il | Block_Ntp_All_Net | drop | 1 |
| 134.147.203.115 | Germany | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 23.228.101.206 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | | 147.237.8.27 | e.madim.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 82.79.205.124 | Romania | 147.237.72.156 | aman.idf.il | JLM_Under_Attack_Con_Tcp | drop | 1 |

02-26-2016-22:04:01 to 02-26-2016-23:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.253.146.183 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 14 |
| 79.177.135.127 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 11 |
| 123.126.113.102 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 51.255.65.60 | United Kingdom | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.69 | United Kingdom | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.86 | United Kingdom | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 51.255.65.94 | United Kingdom | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

02-26-2016-22:04:01 to 02-26-2016-23:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 146.185.250.2 | 147.237.76.42 | Russian Federation | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.193 | 147.237.76.202 | Netherlands | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.91.29 | 147.237.77.216 | Netherlands | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 45.43.226.154 | 147.237.76.31 | | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.216.176.244 | 147.237.0.35 | Latvia | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.3.202.115 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 146.185.250.2 | 147.237.76.197 | Russian Federation | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 146.185.250.2 | 147.237.76.42 | Russian Federation | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.193 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 45.43.226.154 | 147.237.76.196 | | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 45.43.226.154 | 147.237.76.30 | | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.246.0.97 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 146.185.250.2 | 147.237.76.202 | Russian Federation | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |

02-26-2016-22:04:01 to 02-26-2016-23:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 338 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 332 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 204 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 51 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 34 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 33 |
| 89.138.185.204 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 14 |
| 87.68.74.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 68.180.228.109 | United States | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 6 |
| 79.181.161.9 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 84.108.90.253 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 31.210.187.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 80.246.136.230 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 2.54.165.54 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 84.108.90.253 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 199.30.24.119 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 84.108.90.253 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 4 |
| 2.54.18.164 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 93.158.152.49 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.117.162.168 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 37.26.148.203 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 5.28.157.193 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.182.135.12 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.226.16.56 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.135.127 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.134.174 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.154.152.129 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.125.126 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.204.128 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 185.3.144.96 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.174.163 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.181.179.71 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.94.109.214 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 185.89.217.227 | | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 185.3.144.40 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 185.89.217.230 | | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 46.117.162.168 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 46.121.121.14 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 46.19.85.232 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 94.228.34.248 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 46.117.162.168 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 5.22.135.134 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 77.125.130.72 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 46.19.85.232 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 208.115.113.89 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 185.89.217.233 | | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |

02-26-2016-22:04:01 to 02-26-2016-23:04:01

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.54.34.54 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 252 |
| 82.166.61.61 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 179 |
| 109.253.220.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 9 |
| 79.176.221.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 9 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 2 |
| 109.253.204.128 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 87.71.0.20 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 2 |
| 84.109.233.54 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 2.54.174.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 185.130.5.149 | | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/xmlrpc.php | Block | 1 |
| 84.228.246.191 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 2.54.34.54 | Israel | 147.237.0.19 | madim.atal.idf.i | Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** ********** ******* | None | 1 |
| 79.178.39.37 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 1 |
| 62.114.164.95 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 190.226.229.130 | Argentina | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.66.25 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.66.25 | Block | 1 |
| 207.46.13.28 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 89.138.185.204 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx | Block | 1 |
| 2.54.174.53 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 174.44.38.195 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.66.25 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 207.46.13.70 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 91.204.15.187 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 1 |
| 77.237.146.28 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to / | Block | 1 |
| 185.82.200.91 | | 147.237.72.156 | aman.idf.il | Unauthorized Method HEAD for 147.237.72.156/ | Block | 1 |
| 84.109.233.54 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 213.6.8.86 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.54.28.120 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 104.131.147.112 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp | None | 1 |
| 46.117.229.253 | 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 |

02-26-2016-22:04:01 to 02-26-2016-23:04:01