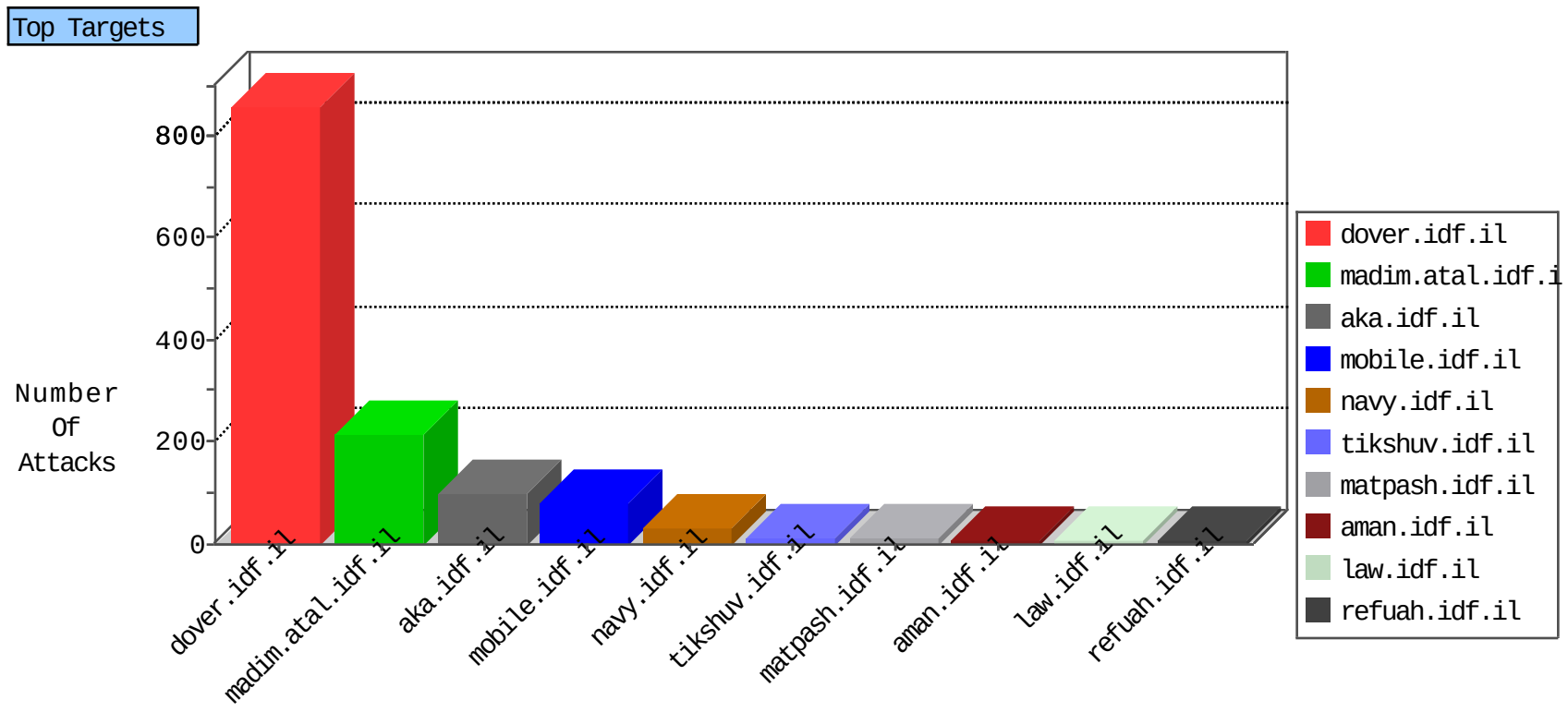
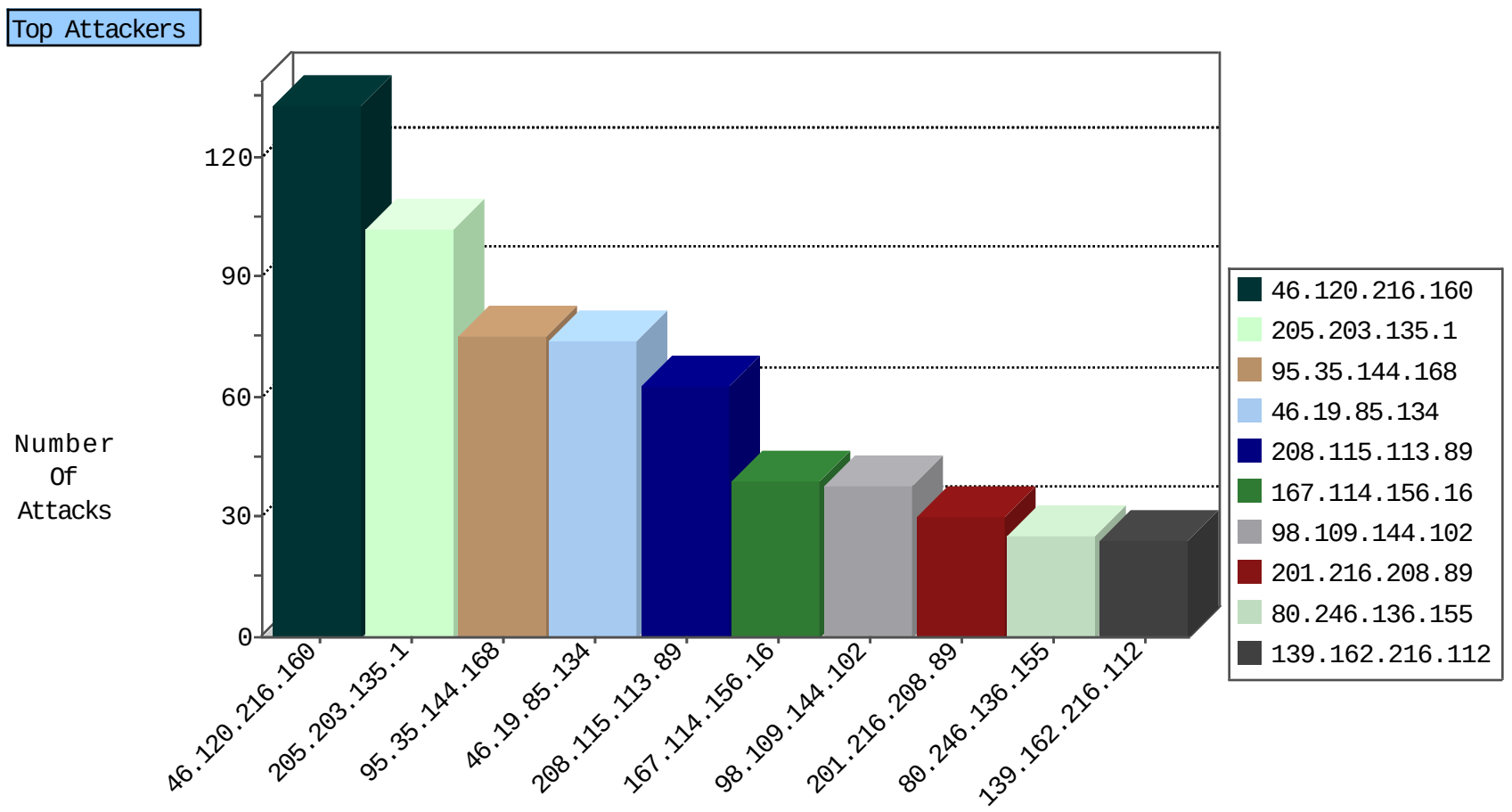
04-28-2016-21:04:00 to 04-28-2016-22:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



04-28-2016-21:04:00 to 04-28-2016-22:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1506 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 690 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 4 |
| 38.229.1.13 | United States | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Block_Ntp_All_Net | drop | 1 |
| 123.100.181.144 | Korea, Republic of | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

04-28-2016-21:04:00 to 04-28-2016-22:04:00

## Top Attackers In IPS

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

04-28-2016-21:04:00 to 04-28-2016-22:04:00

## 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 | 4 |
| 182.181.148.140 | 147.237.77.216 | Pakistan | dover.idf.il | Xenu Link Sleuth User Agent | 1 |
| 180.97.106.36 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 82.117.208.243 | 147.237.76.148 | | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.153.238.58 | 147.237.77.212 | Chile | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 180.97.106.37 | 147.237.72.166 | China | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.249.106.23 | 147.237.8.45 | Turkey | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.204.211 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |

04-28-2016-21:04:00 to 04-28-2016-22:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 205.203.135.1 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 102 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 98.109.144.102 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 201.216.208.89 | Argentina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 139.162.216.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 207.46.13.137 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 80.246.136.155 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 5.22.129.64 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 95.35.144.168 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 18 |
| 176.13.10.169 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 162.210.196.130 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 216.182.250.2 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 86.199.125.117 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 70.192.192.9 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 141.0.14.106 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 107.167.99.158 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 157.55.39.209 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.19.85.161 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 128.157.160.13 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 198.58.96.215 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 198.58.103.115 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 157.55.39.106 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 37.8.23.8 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 12 |
| 12.161.168.178 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 207.46.13.2 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 46.19.85.134 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 95.35.144.168 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 66.249.66.184 | United States | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 95.35.144.168 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 95.35.144.168 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 9 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 95.35.144.168 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 95.35.144.168 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 152.33.72.15 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 95.35.144.168 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 95.35.144.168 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 173.252.95.17 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 95.35.144.168 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 108.61.19.4 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 186.101.152.241 | Ecuador | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 188.120.154.191 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |

04-28-2016-21:04:00 to 04-28-2016-22:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.120.216.160 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 133 |
| 46.19.85.134 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 64 |
| 80.246.136.155 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 199.30.25.16 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 195.154.59.69 | France | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.10.169 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.167 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.161 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.182.90.253 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.168 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 66.249.79.89 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 72.215.157.123 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 72.215.157.123 | Block | 2 |
| 46.120.128.228 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 72.215.157.123 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/mobile | Block | 2 |
| 185.32.179.16 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 157.55.39.134 | United States | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/opmissingperson.in.aspx | Block | 1 |
| 46.19.86.188 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 1 |
| 185.120.125.17 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 80.246.133.125 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 62.210.254.52 | France | 147.237.72.166 | aka.idf.il | Unknown Parameter &bc in www.aka.idf.il/main/giyus/captcha.ashx | None | 1 |
| 220.255.148.10 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 40.77.167.75 | United States | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 157.55.39.136 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/... | Block | 1 |
| 68.180.229.241 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx | Block | 1 |
| 46.60.110.164 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/home/pniot.aspx | Block | 1 |
| 220.255.148.247 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 164.132.161.9 | Italy | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-19149-he/dover | Block | 1 |
| 87.139.236.153 | Germany | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/broadweb/bwroot.asp | Block | 1 |
| 66.249.64.154 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx | Block | 1 |
| 46.19.85.134 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 207.46.13.137 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 157.55.39.134 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx | None | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 46.120.248.116 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 220.255.148.8 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |

04-28-2016-21:04:00 to 04-28-2016-22:04:00