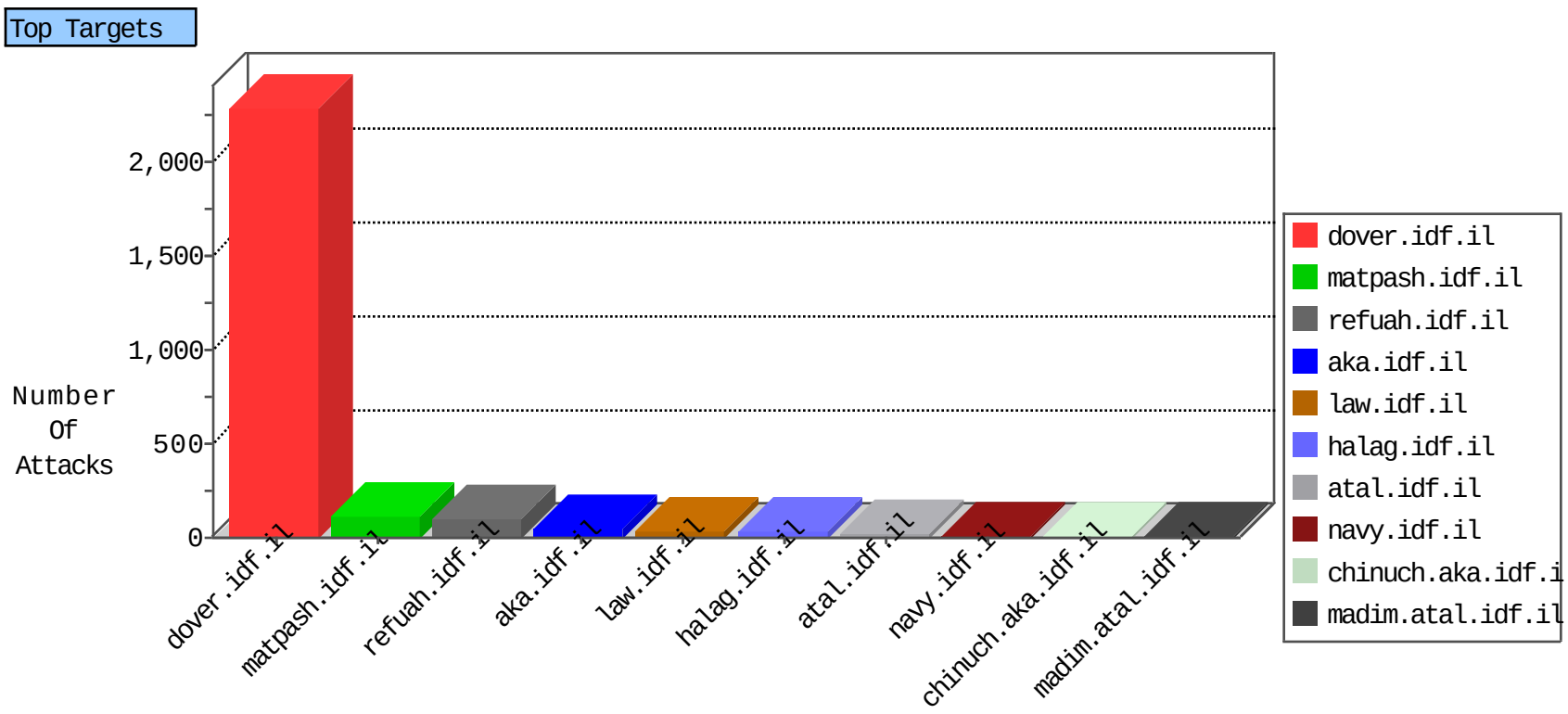
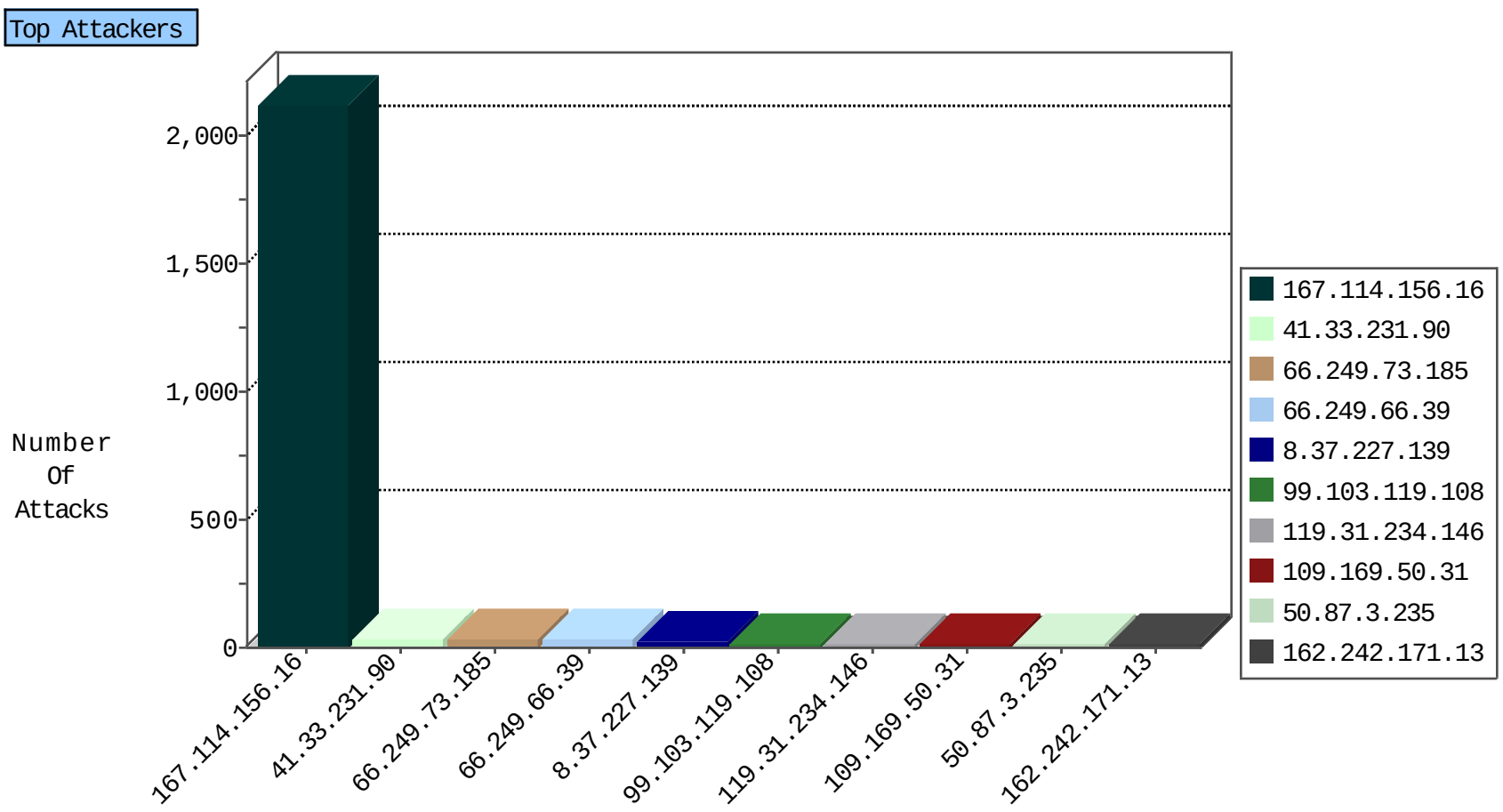
11-28-2015-06:04:04 to 11-28-2015-07:04:04

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



11-28-2015-06:04:04 to 11-28-2015-07:04:04

## 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 | DOS-Tool-SwitchbladG | dest-reset | 3246 |
| 8.37.227.139 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | JLM_Dover_Con_Limit_Https | drop | 28 |
| 8.37.227.139 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Http | drop | 2 |
| 153.31.119.142 | United States | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 93.174.93.181 | Netherlands | 147.237.76.30 | himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 153.31.119.142 | United States | 147.237.76.177 | ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 8.37.227.139 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Htps | drop | 1 |
| 93.174.93.181 | Netherlands | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.174.93.181 | Netherlands | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |

11-28-2015-06:04:04 to 11-28-2015-07:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 24.230.181.31 | United States | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 1 |
| 51.254.121.184 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 1 |
| 158.69.192.207 | United States | 147.237.77.216 | dover.idf.il | C1000106: HTTP: majestic bot | Block | 1 |

11-28-2015-06:04:04 to 11-28-2015-07:04:04

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 |
| 66.249.78.147 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 82.117.208.243 | 147.237.76.199 | | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.67.224 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 149.202.186.50 | 147.237.72.167 | Germany | ishurim.aka.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 119.96.120.14 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 185.93.187.49 | 147.237.72.166 | | aka.idf.il | SERVER-WEBAPP admin.php access | 1 |
| 149.202.186.50 | 147.237.72.156 | Germany | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-28-2015-06:04:04 to 11-28-2015-07:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 34 |
| 66.249.66.39 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 28 |
| 99.103.119.108 | United States | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 15 |
| 8.37.227.139 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 66.249.83.155 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 66.249.66.61 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.249.83.161 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 8.37.227.139 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 199.30.25.90 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 113.110.235.238 | China | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 74.85.66.62 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 3 |
| 2.54.183.158 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.136.113.86 | Sweden | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 84.22.107.124 | Netherlands | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 3 |
| 93.125.99.42 | Belarus | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 3 |
| 46.19.85.170 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.8.24 | e.lifestyle.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 46.19.85.170 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 128.232.110.28 | United Kingdom | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 5.29.148.112 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 40.77.167.35 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 5.29.148.112 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 128.232.110.28 | United Kingdom | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 195.154.227.118 | France | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 139.162.203.26 | Netherlands | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 216.218.206.95 | United States | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 74.82.47.7 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.139.67 | United States | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 46.120.106.180 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.113 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 74.208.105.30 | United States | 147.237.77.216 | dover.idf.il | Header Rejection | header rejection pattern found in request | monitor | 1 |
| 151.0.58.20 | Bulgaria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 1 |
| 139.162.203.26 | Netherlands | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 112.74.67.109 | China | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 216.218.206.106 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 74.82.47.7 | United States | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 184.105.139.79 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 64.125.239.72 | United States | 147.237.72.217 | e.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.114 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 24.230.181.31 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 209.251.133.98 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.19.86.247 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 140.207.198.157 | China | 147.237.77.226 | www.chamatz.aka.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 74.82.47.12 | United States | 147.237.72.217 | e.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |

11-28-2015-06:04:04 to 11-28-2015-07:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 40.77.167.14 | United States | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 4 |
| 81.95.96.233 | Czech Republic | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 95.85.19.27 | Netherlands | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 67.222.12.77 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 198.46.81.6 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 62.212.152.123 | Netherlands | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 109.169.50.31 | United Kingdom | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 192.163.238.217 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 216.180.241.106 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 95.85.19.27 | Netherlands | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 173.44.38.200 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 195.178.106.120 | Romania | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 217.78.1.159 | Ireland | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 62.24.32.14 | Norway | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 192.145.239.3 | United States | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 92.53.125.204 | Russian Federation | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 175.107.131.153 | Australia | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 162.249.4.102 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 50.87.3.235 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 188.124.17.15 | Turkey | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 177.85.96.86 | Brazil | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 92.53.98.31 | Russian Federation | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 162.242.171.13 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 50.87.3.235 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 186.202.127.81 | Brazil | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.185.213.137 | Slovenia | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 162.242.171.13 | United States | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 109.67.201.174 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 119.31.234.146 | Singapore | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 46.118.155.216 | Ukraine | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 46.118.155.216 | Block | 3 |
| 109.204.243.17 | Finland | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.146.107.207 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 104.155.4.193 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 119.31.234.146 | Singapore | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 3 |
| 198.46.81.8 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 109.169.50.31 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 162.242.171.13 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/index.php | Block | 2 |
| 119.31.234.146 | Singapore | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 119.31.234.146 | Block | 2 |
| 37.142.68.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.204.243.17 | Finland | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 109.204.243.17 | Block | 2 |
| 157.55.39.112 | United States | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 104.155.4.193 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 104.155.4.193 | Block | 2 |
| 119.31.234.146 | Singapore | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 119.31.234.146 | Block | 2 |
| 198.46.81.8 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 198.46.81.8 | Block | 2 |
| 41.230.218.175 | Tunisia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 2 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 109.169.50.31 | United Kingdom | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 109.169.50.31 | Block | 2 |
| 67.222.12.77 | United States | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 67.222.12.77 | Block | 2 |
| 109.169.50.31 | United Kingdom | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 109.169.50.31 | Block | 2 |
| 192.163.238.217 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 192.163.238.217 | Block | 2 |

11-28-2015-06:04:04 to 11-28-2015-07:04:04