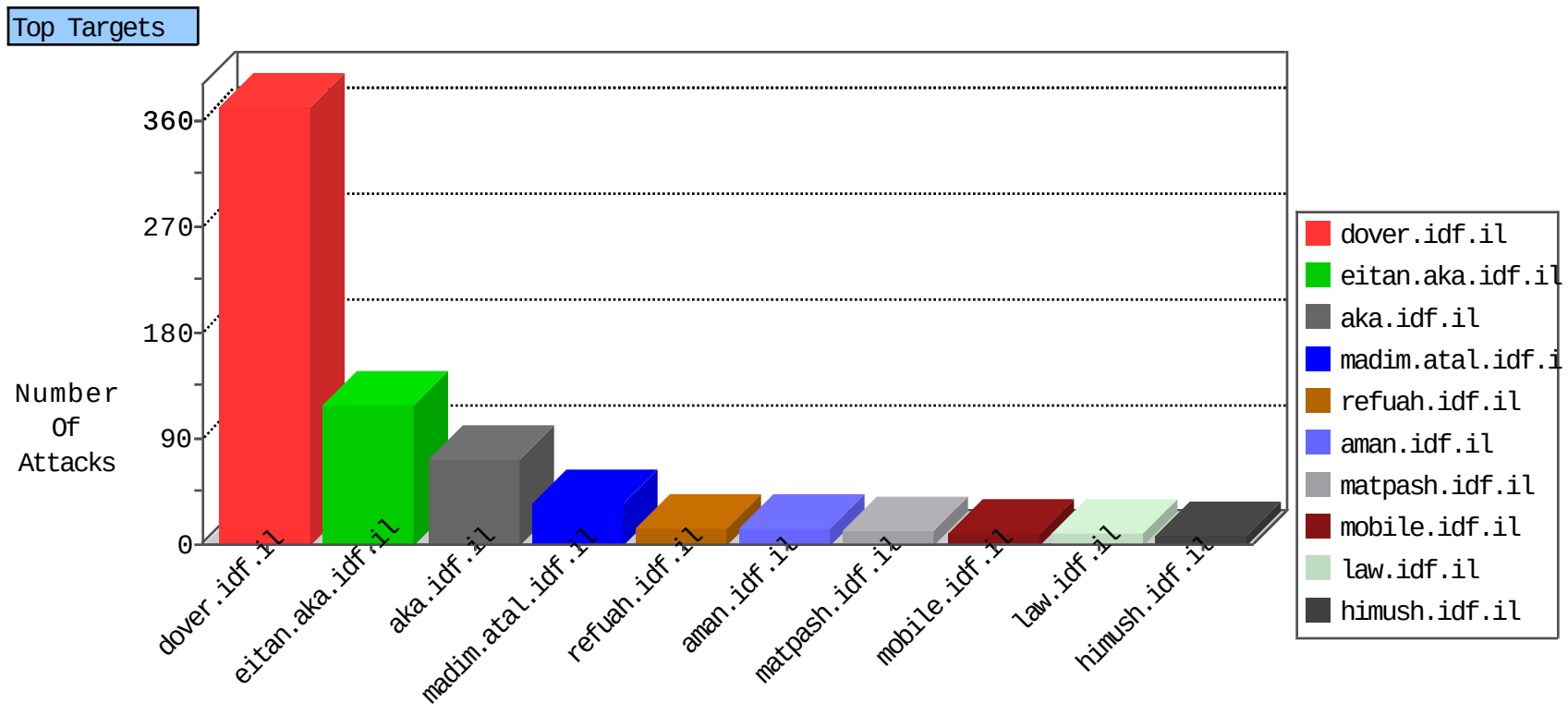
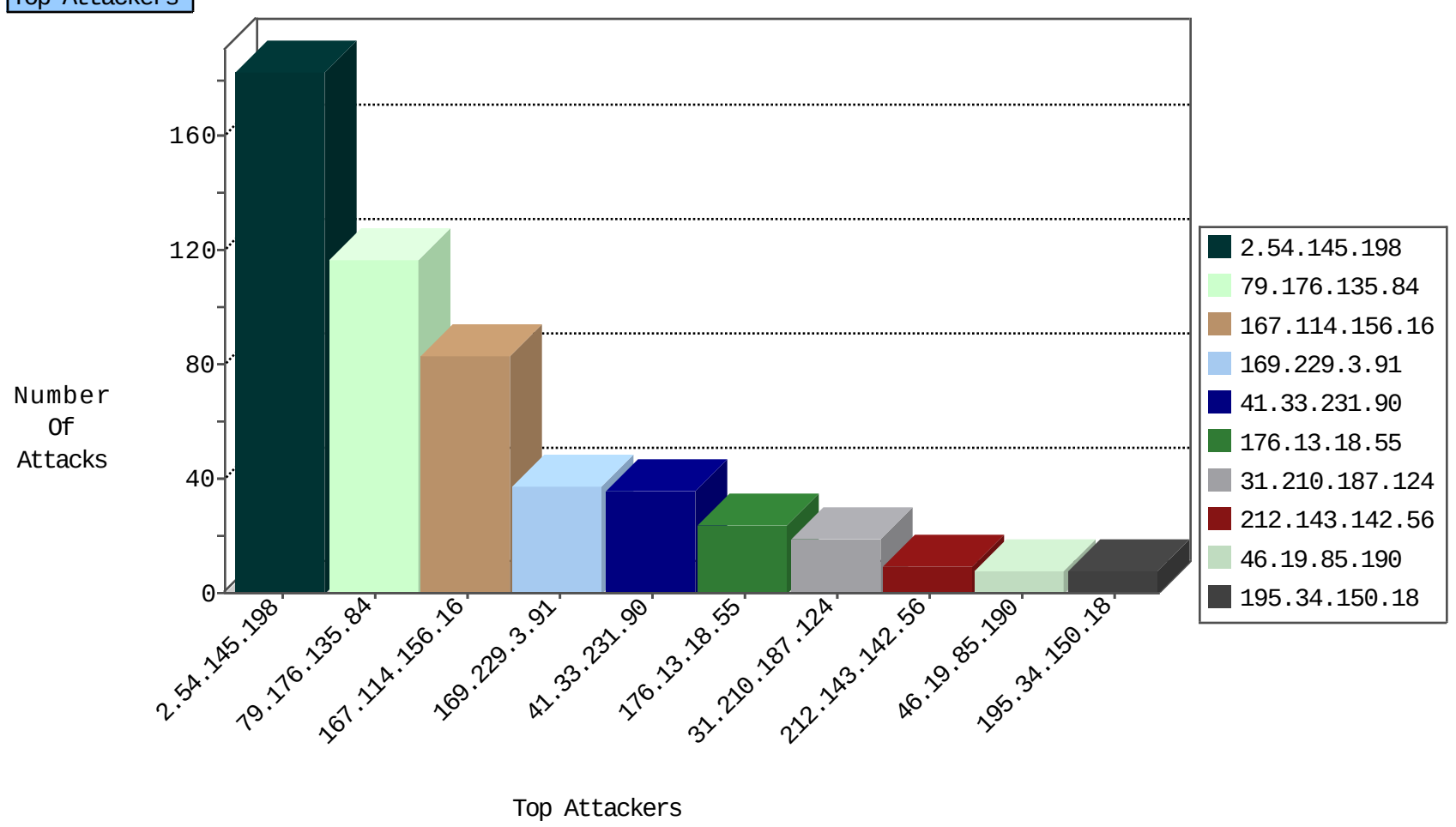
12-29-2015-06:04:01 to 12-29-2015-07:04:01

# IDF Under Attack Daily Report

Top Targets




Top Attackers



12-29-2015-06:04:01 to 12-29-2015-07:04:01

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 | 1489 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 184 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Http | drop | 3 |
| 119.120.55.90 | China | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.161.14.116 | Vietnam | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.35.62.178 | Switzerland | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 77.247.178.132 | Netherlands | 147.237.76.39 | mobile.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 119.120.55.90 | China | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.161.14.116 | Vietnam | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 119.120.55.90 | China | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.161.14.116 | Vietnam | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.161.14.116 | Vietnam | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 119.120.55.90 | China | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 14.161.14.116 | Vietnam | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |

12-29-2015-06:04:01 to 12-29-2015-07:04:01

## Top Attackers In IPS

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

12-29-2015-06:04:01 to 12-29-2015-07:04:01

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 | 4 |
| 64.233.173.151 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 151.217.178.88 | 147.237.8.27 | | e.madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 104.219.238.10 | 147.237.72.166 | | aka.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 190.249.184.162 | 147.237.76.177 | Colombia | ncore.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 50.204.188.142 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -f -sS | 1 |
| 190.249.184.162 | 147.237.76.177 | Colombia | ncore.idf.il | ET SCAN NMAP -f -sS | 1 |
| 5.39.222.253 | 147.237.77.226 | Netherlands | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.162 | 147.237.76.30 | China | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.39.222.253 | 147.237.77.170 | Netherlands | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 151.217.178.88 | 147.237.77.227 | | e.hamaz.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 151.217.178.88 | 147.237.76.38 | | e.e.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 151.217.178.88 | 147.237.72.14 | | dover.idf.il(old) | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 123.4.93.137 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 104.143.14.247 | 147.237.0.33 | United States | idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.204.188.142 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 190.249.184.162 | 147.237.76.177 | Colombia | ncore.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 12.139.41.189 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 182.207.206.75 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 5.39.222.253 | 147.237.77.178 | Netherlands | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 168.62.238.153 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 151.217.178.88 | 147.237.76.44 | | e.refuah.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 151.217.178.88 | 147.237.72.167 | | ishurim.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

12-29-2015-06:04:01 to 12-29-2015-07:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.54.145.198 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 183 |
| 79.176.135.84 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 114 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 31.210.187.124 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 31.210.187.124 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 96.224.252.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.85.190 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 128.127.107.80 | Netherlands | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 46.19.85.123 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 176.12.148.144 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 79.183.102.213 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.176.135.84 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.228.251.53 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 207.81.209.149 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 79.180.64.133 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 192.116.55.126 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.190 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 128.127.107.80 | Netherlands | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.181.195.161 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.64.75 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 46.19.85.41 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 66.249.66.46 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 46.19.85.65 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 128.232.110.28 | United Kingdom | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 208.54.86.161 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 5.175.193.232 | Germany | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 94.230.86.159 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 46.19.85.41 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 2.54.16.108 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 77.125.5.169 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.125 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 212.130.122.155 | Denmark | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.112 | United States | 147.237.76.201 | e.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 185.3.144.143 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 169.229.3.91 | United States | 147.237.76.201 | e.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 169.229.3.91 | United States | 147.237.8.27 | e.madim.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 74.82.47.16 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 141.212.122.114 | United States | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 46.19.86.64 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 137.116.71.170 | United States | 147.237.8.27 | e.madim.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 184.105.139.75 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 169.229.3.91 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.126 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.112 | United States | 147.237.77.234 | halag.idf.il | drop | SAM rule | drop | 1 |
| 185.3.146.193 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 169.229.3.91 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |

12-29-2015-06:04:01 to 12-29-2015-07:04:01

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.18.55 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 24 |
| 80.246.140.144 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 3 |
| 46.19.85.226 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.198.226 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.29.217.116 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 3 |
| 46.118.155.216 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 46.118.155.216 | Block | 2 |
| 84.108.217.31 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 185.3.146.226 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 84.108.237.116 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 2 |
| 207.46.13.46 | United States | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 46.120.186.132 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 87.69.137.150 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 2 |
| 185.32.179.224 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 169.229.3.91 | United States | 147.237.76.30 | himush.idf.il | Multiple NULL Character in Method from 169.229.3.91 | Block | 1 |
| 66.249.66.23 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx | Block | 1 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 169.229.3.91 | Block | 1 |
| 109.253.199.158 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 1 |
| 85.250.113.144 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 1 |
| 5.102.236.77 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 169.229.3.91 | United States | 147.237.76.42 | refuah.idf.il | NULL Character in Method | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.30 | himush.idf.il | Abnormally Long Request method | Block | 1 |
| 66.249.66.52 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 212.130.122.155 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/en | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Header Value | Block | 1 |
| 66.249.64.166 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/1073-he/nakhal.aspx | Block | 1 |
| 181.196.135.11 | Ecuador | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 40.77.167.77 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/news/main.stm. | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.176 | matpash.idf.il | NULL Character in Header Name at | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.30 | himush.idf.il | Unknown HTTP Request Method 8fÃ·[[#16]]F+[[#0]]{cQÃ?%Ã‡Â™[[#8]]Ã¯Â†[[#27]]Â¹Â″sÂ·E in URL Â¼×œÂ§Ö¿:ÂŸ[[#25]]×– | Block | 1 |
| 66.249.66.28 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Abnormally Long Request method | Block | 1 |
| 109.253.201.201 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.118.155.216 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/blog/ | Block | 1 |
| 176.13.23.74 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 1 |
| 87.68.47.171 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 31.210.187.124 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 169.229.3.91 | United States | 147.237.77.176 | matpash.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.30 | himush.idf.il | Illegal Byte Code Character in URL Â¼×œÂ§Ö¿:ÂŸ[[#25]]×– | Block | 1 |
| 68.180.229.173 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 213.57.238.109 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx | None | 1 |
| 169.229.3.91 | United States | 147.237.72.166 | aka.idf.il | Malformed URL | Block | 1 |
| 66.249.65.112 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2306.jpg | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.176 | matpash.idf.il | Unknown HTTP Request Method !Â„Â›^AÂ…JÂ¤Ã·[[#30]]ÂžnÃž{dÂ¡Â¢= in URL | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 2.52.8.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 169.229.3.91 | United States | 147.237.76.31 | nakchal.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 66.249.66.29 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |

12-29-2015-06:04:01 to 12-29-2015-07:04:01