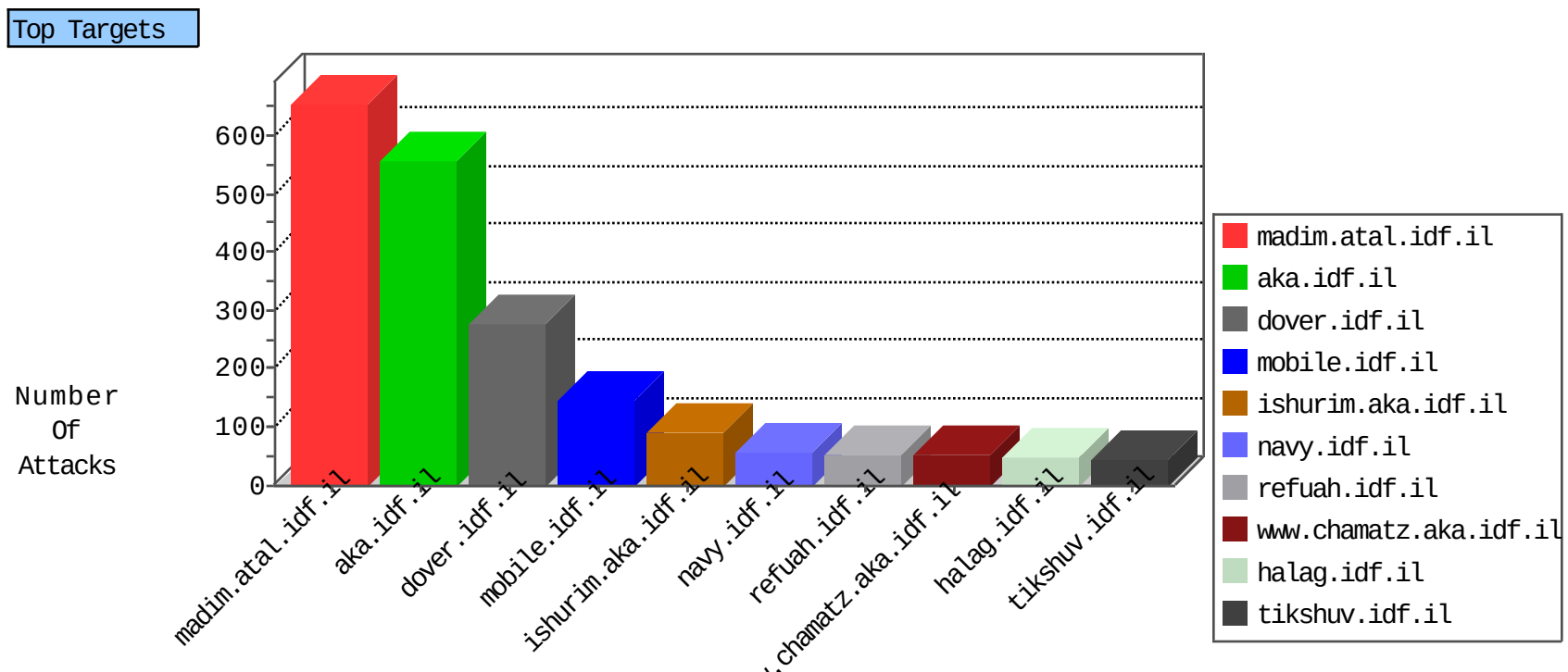
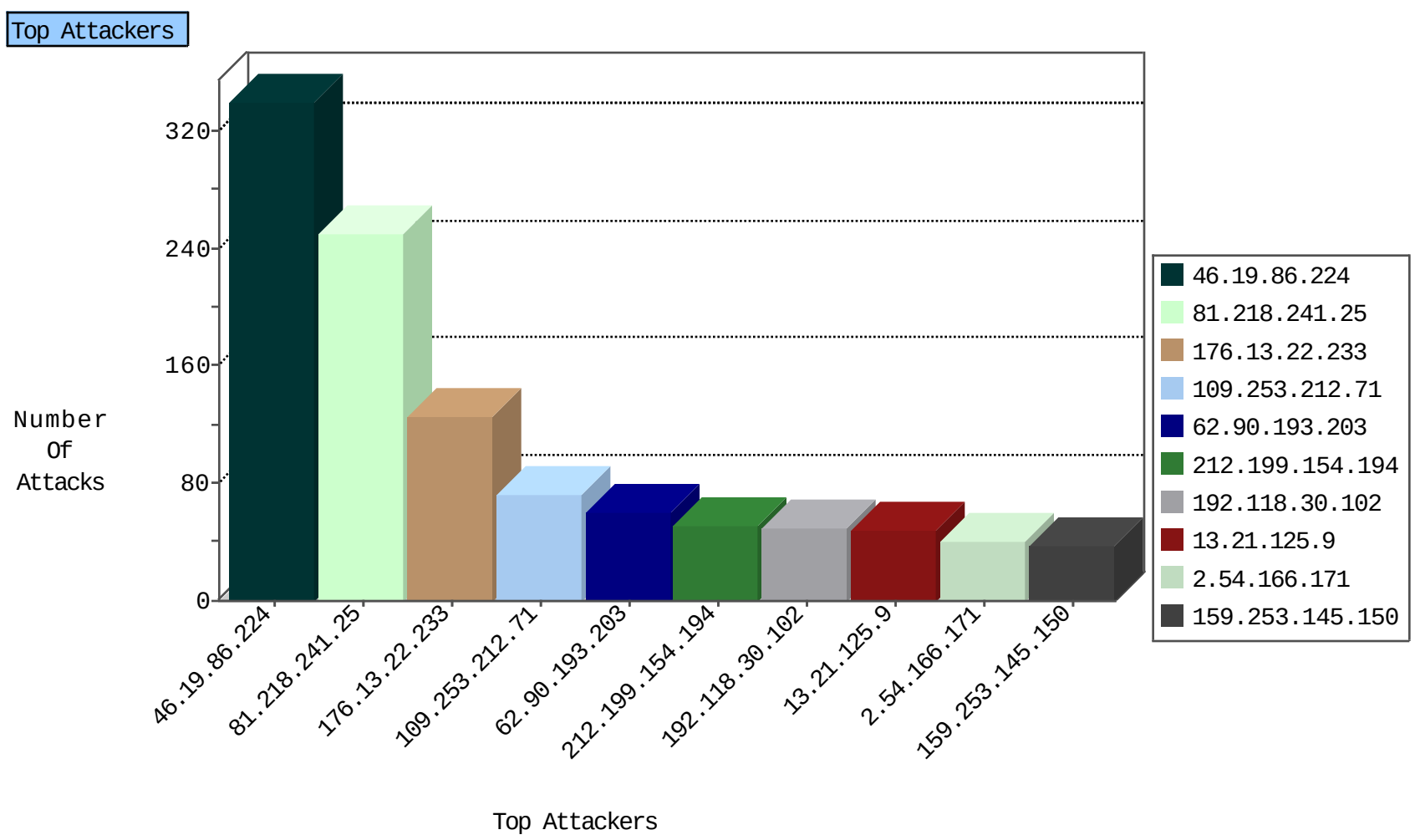
01-28-2016-10:04:07 to 01-28-2016-11:04:07

# IDF Under Attack Daily Report

Top Targets




Top Attackers



01-28-2016-10:04:07 to 01-28-2016-11:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1214 |
| 192.118.30.102 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 511 |
| 212.199.154.194 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 292 |
| 77.125.96.130 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 20 |
| 81.218.206.82 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.151.130 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 162.248.143.101 | Canada | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 162.248.143.101 | Canada | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.130.5.201 | | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 80.246.130.34 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 188.120.148.244 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |

01-28-2016-10:04:07 to 01-28-2016-11:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 159.253.145.150 | United States | 147.237.76.86 | navy.idf.il | C095: Suspicious Addresses MFA | Permit | 23 |
| 159.253.145.150 | United States | 147.237.77.216 | dover.idf.il | C095: Suspicious Addresses MFA | Permit | 14 |

01-28-2016-10:04:07 to 01-28-2016-11:04:07

## 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 | 3 |
| 46.19.85.239 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.51.180 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 198.20.69.74 | 147.237.77.19 | United States | law-forum.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 149.88.101.120 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.114 | 147.237.8.28 | Ukraine | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.65.107.230 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.80.198.164 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 77.126.8.158 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.45.137.67 | 147.237.76.39 | Turkey | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 149.78.80.100 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.138.202.114 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.229.0.41 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.21.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.219.191.138 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

01-28-2016-10:04:07 to 01-28-2016-11:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 79 |
| 62.90.193.203 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 60 |
| 13.21.125.9 | United Kingdom | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 48 |
| 82.166.97.26 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 31 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 22 |
| 212.199.154.194 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 19 |
| 176.13.15.231 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 19 |
| 80.246.139.136 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 2.52.1.47 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 176.13.17.158 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 14 |
| 46.19.85.62 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 12 |
| 2.52.1.47 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 212.76.127.44 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 109.253.204.116 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.148.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 46.19.86.187 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.149.136 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 109.253.143.138 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 62.0.197.69 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 7 |
| 80.179.122.253 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 109.253.144.90 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.17.214 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.13.0 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 81.149.108.111 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 46.19.85.10 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 176.13.19.26 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.130.232.75 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.85 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.10 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.54.168.82 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.85 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.54.172.117 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 2.54.8.188 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 2.52.129.71 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.22.199 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.177 | 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 |
| 192.118.30.102 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 2.54.140.39 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 37.26.146.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 2.54.167.49 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 207.46.13.49 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.85.42 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 2.52.129.105 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 4 |
| 188.120.148.201 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |

01-28-2016-10:04:07 to 01-28-2016-11:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.224 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 171 |
| 46.19.86.224 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 114 |
| 176.13.22.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 103 |
| 109.253.212.71 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 72 |
| 46.19.86.224 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 46.19.86.224 | Block | 54 |
| 2.54.166.171 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 40 |
| 2.52.161.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 35 |
| 109.67.105.58 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 33 |
| 176.13.22.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 22 |
| 79.176.166.1 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 79.176.166.1 | Block | 15 |
| 81.218.192.91 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 81.218.192.91 | Block | 11 |
| 95.86.82.14 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/&sa=u&ved=0ahukewjowjd1kszkahxd1rqkharoc5iqffggtmae&usg=afqjcngdvrvylyncir6whv95j8jic2kcmw | Block | 11 |
| 109.253.204.116 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390 | Block | 7 |
| 94.142.141.119 | Russian Federation | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 6 |
| 46.19.86.152 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 94.142.141.119 | Russian Federation | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 94.142.141.119 | Block | 5 |
| 2.54.134.208 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 80.246.139.136 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 176.13.13.6 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.29.67.96 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.197.5 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$ | Block | 3 |
| 109.253.223.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 149.78.18.226 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 3 |
| 176.13.2.213 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.215 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.102.206.47 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.65.149.218 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.143.138 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.210.65 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 2 |
| 80.246.136.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 37.26.149.136 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 81.218.192.91 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/5/size338x0/1565.jpg | Block | 2 |
| 46.19.86.187 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.65.48.123 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 109.65.48.123 | Block | 2 |
| 176.13.1.116 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.204.116 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.14.253 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.160 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 176.13.3.213 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 5.102.206.47 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 212.76.102.69 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/&sa=u&ved=0ahukewjb-o3ekszkahwdvxqkhwnqdtqqfgghmaa&usg=afqjcnf_fje3yg7to4w4oieabks8rp37hw | Block | 1 |
| 77.127.165.76 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 169.229.3.91 | United States | 147.237.77.176 | matpash.idf.il | Illegal Byte Code Character in URL | Block | 1 |
| 46.19.86.224 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many 403: Response Code per Session | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 2.54.134.99 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 85.250.165.128 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |

01-28-2016-10:04:07 to 01-28-2016-11:04:07