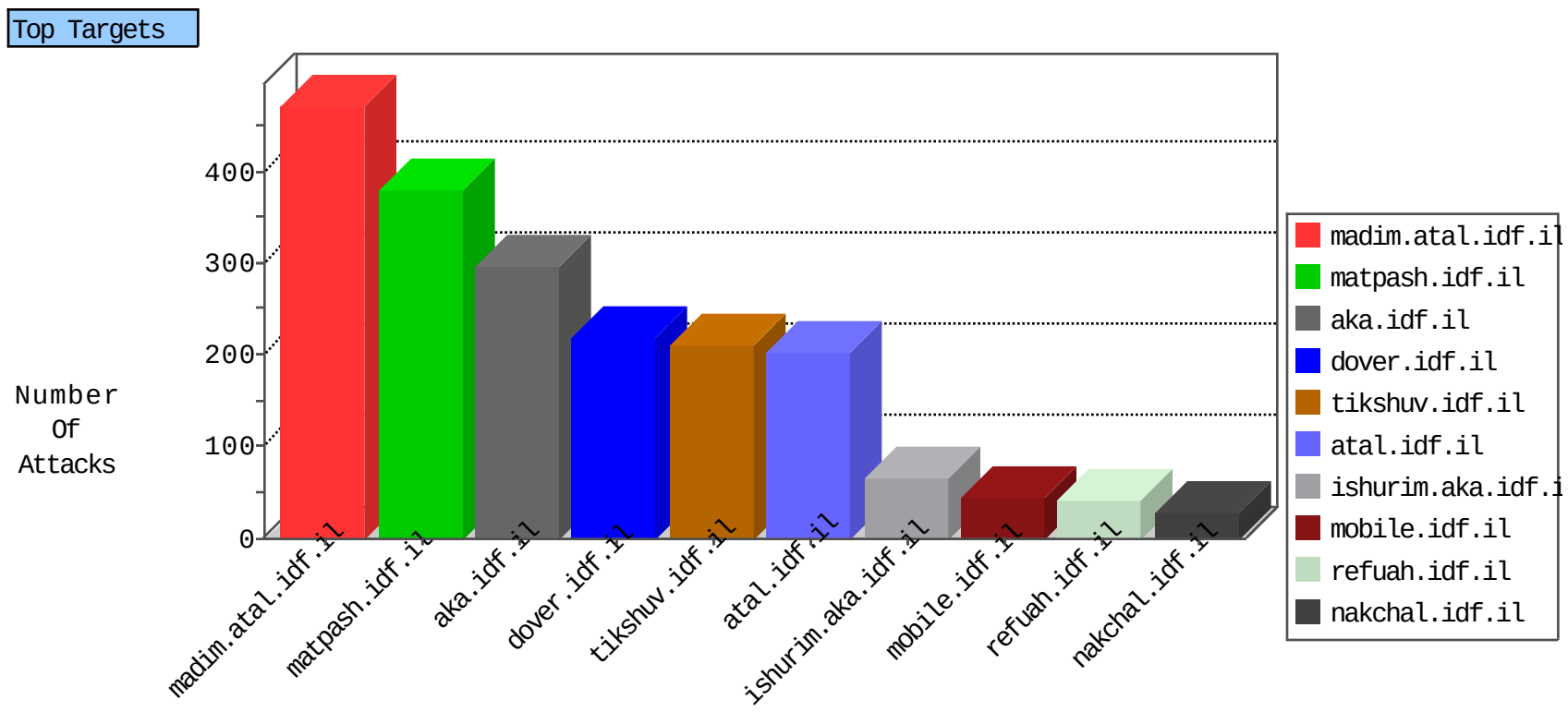
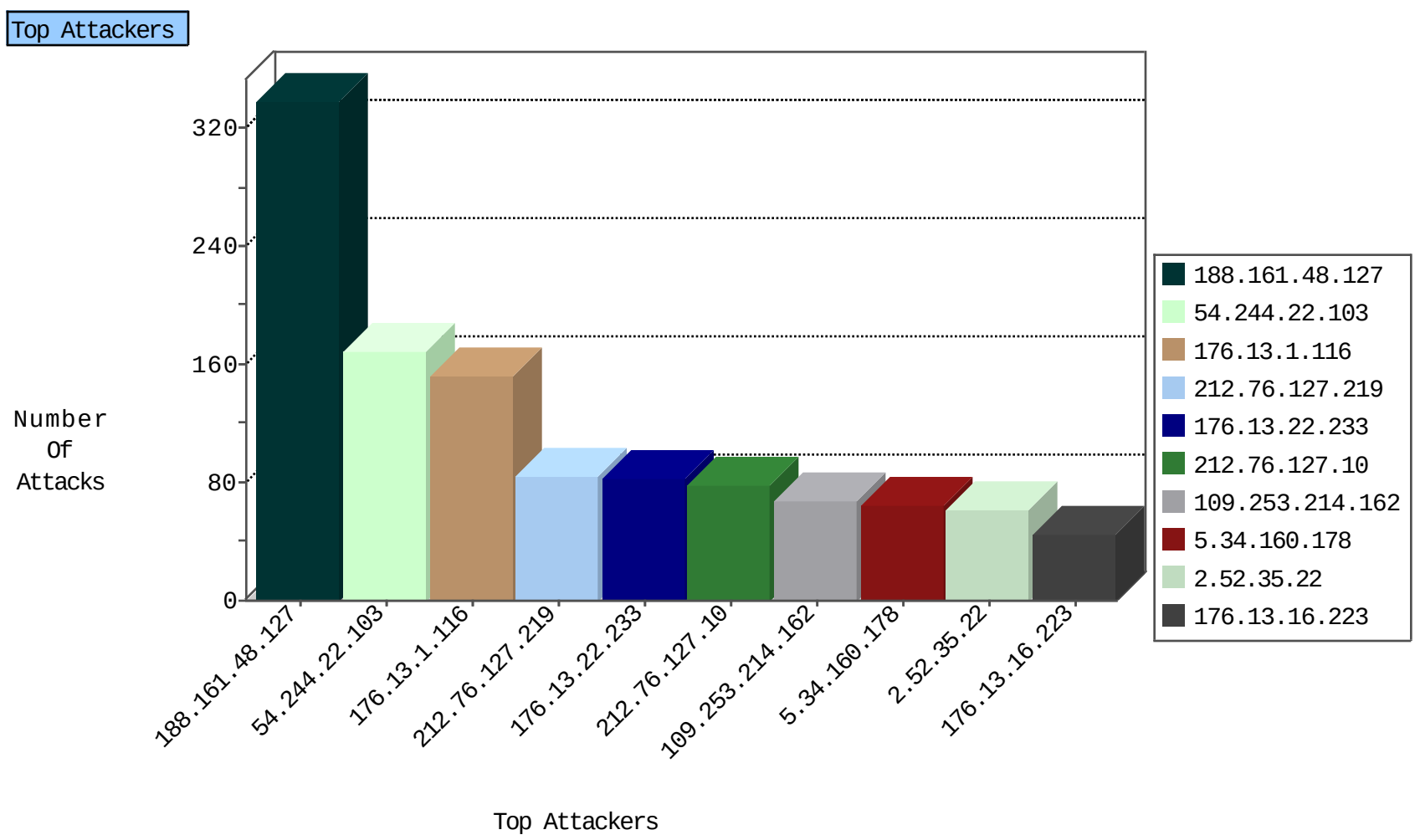
01-28-2016-09:04:03 to 01-28-2016-10:04:03

# IDF Under Attack Daily Report

Top Targets




Top Attackers



01-28-2016-09:04:03 to 01-28-2016-10:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 207.232.36.181 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 239 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 87 |
| 82.132.223.85 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 9 |
| 81.218.206.82 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |

01-28-2016-09:04:03 to 01-28-2016-10:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 51.255.194.33 | United Kingdom | 147.237.77.216 | dover.idf.il | C106: HTTP: majestic bot | Block | 1 |
| 5.9.111.70 | Germany | 147.237.72.166 | aka.idf.il | C106: HTTP: majestic bot | Block | 1 |
| 51.255.48.154 | United Kingdom | 147.237.77.216 | dover.idf.il | C106: HTTP: majestic bot | Block | 1 |

01-28-2016-09:04:03 to 01-28-2016-10:04:03

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 | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 188.0.236.123 | 147.237.76.30 | Moldova, Republic of | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 149.50.112.44 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.240.144.64 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.148.18.162 | 147.237.76.199 | Lithuania | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.86.217 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.224.128.55 | 147.237.8.28 | Tunisia | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 212.179.46.16 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 31.154.94.48 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.0.236.123 | 147.237.76.39 | Moldova, Republic of | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 176.106.44.147 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.81.27.229 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 47.18.200.87 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.148.18.162 | 147.237.72.167 | Lithuania | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.158 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.224.128.55 | 147.237.8.27 | Tunisia | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.26.148.230 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

01-28-2016-09:04:03 to 01-28-2016-10:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 255 |
| 54.244.22.103 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 145 |
| 212.76.127.219 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 84 |
| 212.76.127.10 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 78 |
| 5.34.160.178 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 64 |
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 31 |
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 109.253.156.129 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 176.13.1.116 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 54.244.22.103 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 16 |
| 109.160.166.123 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 13 |
| 109.160.166.123 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 109.253.146.5 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 37.26.148.196 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.13.0.218 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.253.214.187 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 176.12.160.1 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 212.76.127.44 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 79.179.149.53 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 2.54.44.204 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.187 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 212.76.127.111 | Israel | 147.237.77.233 | atal.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 8 |
| 54.244.22.103 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 8 |
| 176.13.22.135 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 62.0.251.1 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 109.226.20.106 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 7 |
| 192.116.239.196 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 2.52.177.92 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 2.54.5.70 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.7.105 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.183.254.74 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.54.6.146 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.64.38.227 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.183.254.74 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 2.54.184.247 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.86.150 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 46.19.85.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 176.13.1.7 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.52.33.88 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.183.254.74 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 188.161.48.127 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 212.199.154.194 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 217.132.84.207 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |

01-28-2016-09:04:03 to 01-28-2016-10:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.1.116 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 86 |
| 176.13.22.233 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 82 |
| 2.52.35.22 | Israel | 147.237.0.34 | tikshuv.idf.il | Too Many of the Same Response Code (404) in Session from 2.52.35.22 | Block | 61 |
| 176.13.1.116 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 45 |
| 176.13.16.223 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 42 |
| 2.54.130.128 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 41 |
| 109.253.214.162 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 39 |
| 46.19.85.189 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 30 |
| 109.253.214.162 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 27 |
| 2.54.184.247 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 15 |
| 213.111.233.25 | Ukraine | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 6 |
| 109.253.210.65 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 6 |
| 213.111.233.25 | Ukraine | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 213.111.233.25 | Block | 5 |
| 176.13.14.253 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 46.19.85.23 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 84.94.171.201 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 84.94.171.201 | Block | 3 |
| 109.253.143.138 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.144 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.147.43 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.216 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.1.161 | Israel | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.nakhal.idf.il/1120-he/nakhal.aspx | Block | 2 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 2 |
| 46.19.86.103 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.81 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 79.179.149.53 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar | Block | 2 |
| 2.54.167.15 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 109.253.215.83 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 192.114.23.18 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg | Block | 1 |
| 31.13.112.121 | Ireland | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on www.refua.atal.idf.il/sip_storage/files/2/2152.doc&ved=0ahukewibxqrx_cvkahvelhokhvdbcpkqfggfmai&usg=afqjcng6aaxhlu5ewf9fz1vw2r2i6ow2ng&sig2=j1_tqhkrlu1dzffknx61hw | Block | 1 |
| 80.246.136.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 149.78.145.47 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$0 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 66.249.78.102 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 213.111.233.25 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php | Block | 1 |
| 46.19.85.189 | Israel | 147.237.0.19 | madim.atal.idf.i | SSL Untraceable Connection - Open Mode | None | 1 |
| 204.13.201.138 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 109.160.166.123 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 37.142.68.5 | Israel | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 1 |
| 185.24.206.45 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Unknown SSL Session | None | 1 |
| 79.179.197.150 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.184.247 | Israel | 147.237.0.19 | madim.atal.idf.i | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.65.17 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 66.249.65.17 | Block | 1 |
| 212.199.244.112 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 46.19.85.45 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 194.54.168.65 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd | None | 1 |
| 31.154.94.81 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.13.22.135 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 81.218.127.74 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 217.132.38.127 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |

01-28-2016-09:04:03 to 01-28-2016-10:04:03