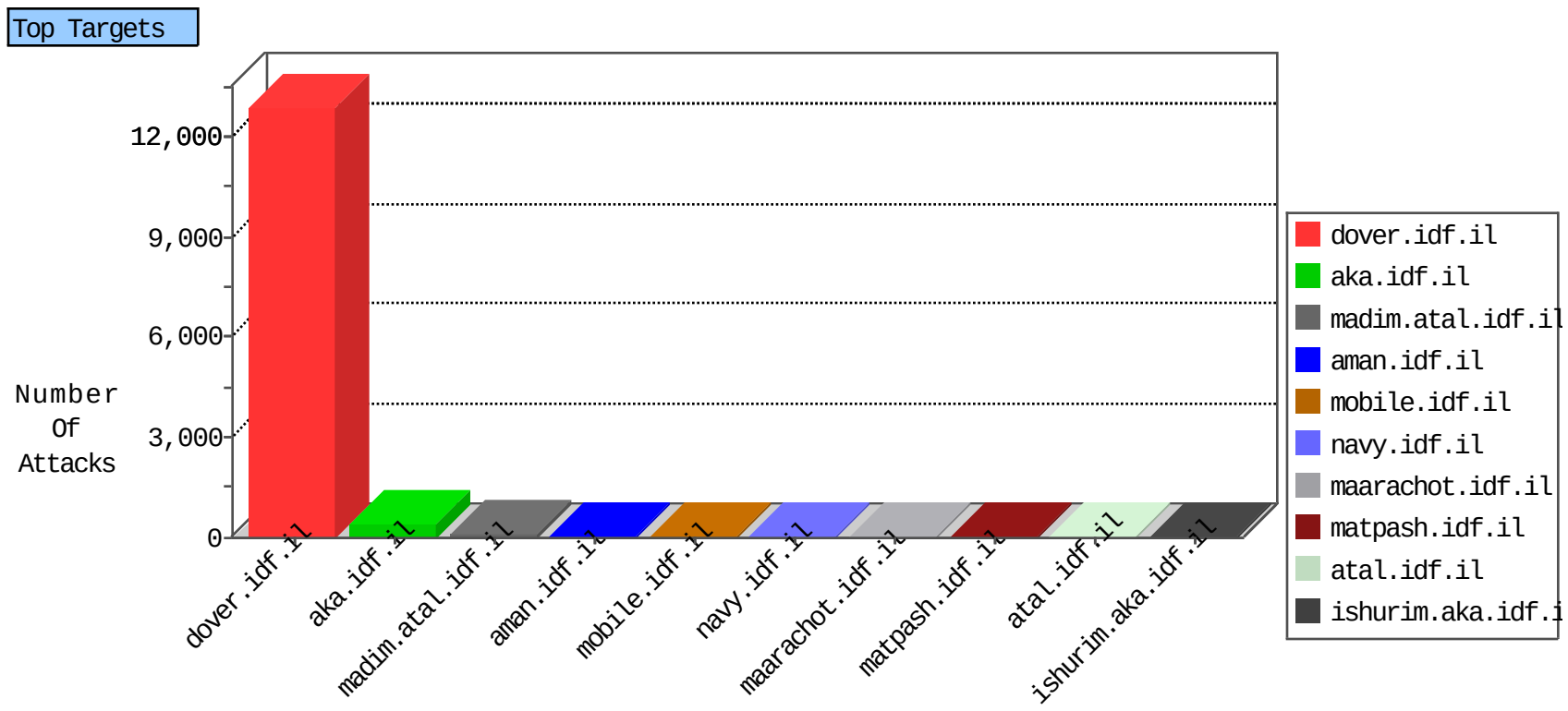
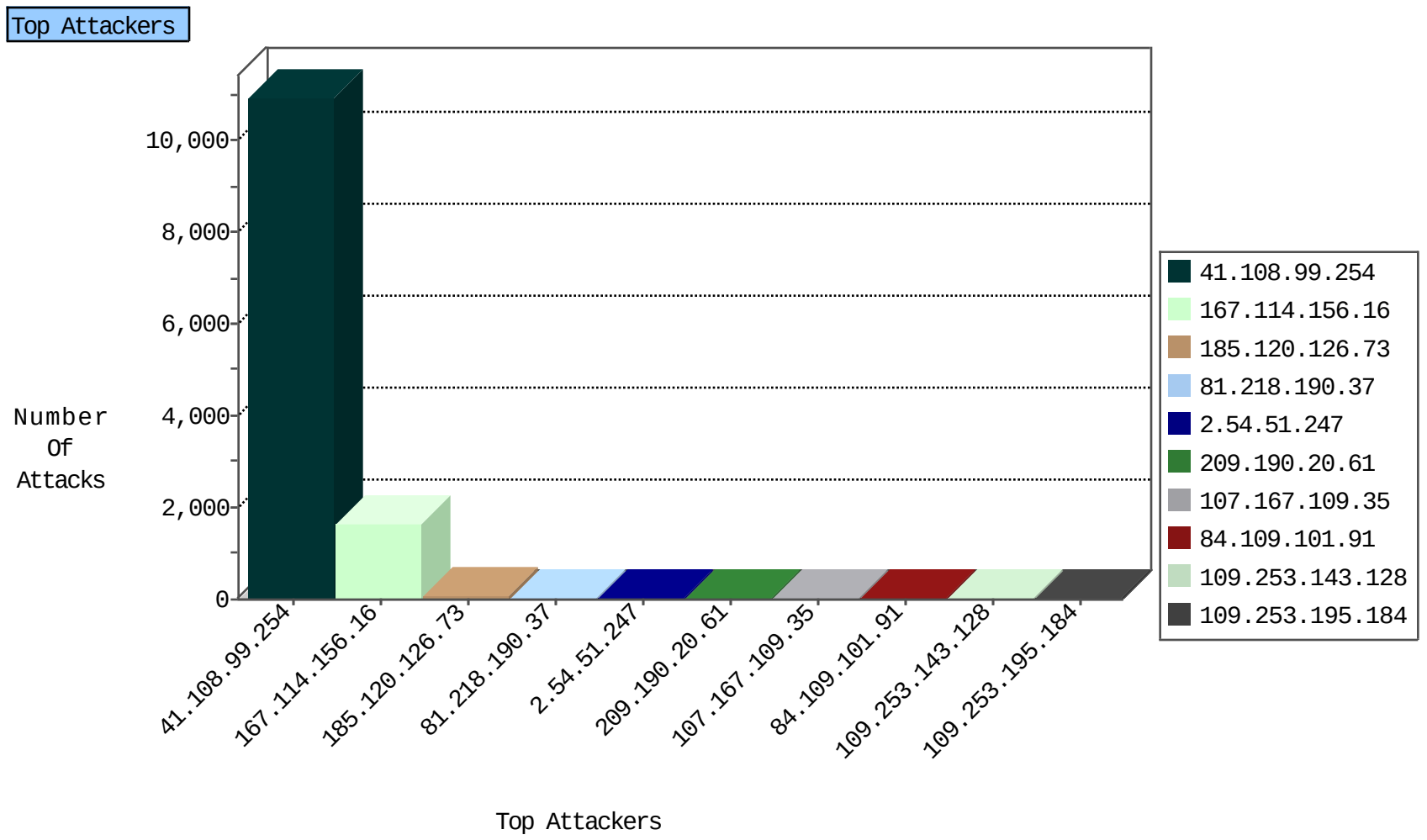
01-06-2016-18:04:06 to 01-06-2016-19:04:06

# IDF Under Attack Daily Report

Top Targets




Top Attackers



01-06-2016-18:04:06 to 01-06-2016-19:04:06

## 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 | 3041 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | DOS-LOIC-TCP-80-cat | dest-reset | 366 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 6 |
| 71.6.167.142 | United States | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

01-06-2016-18:04:06 to 01-06-2016-19:04:06

## Top Attackers In IPS

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

01-06-2016-18:04:06 to 01-06-2016-19:04:06

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 | 10 |
| 66.249.73.206 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 109.65.204.158 | 147.237.76.42 | Israel | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 91.201.236.113 | 147.237.8.28 | Ukraine | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.248.162.131 | 147.237.77.227 | Netherlands | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 198.20.69.74 | 147.237.77.233 | United States | atal.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 89.248.162.131 | 147.237.77.176 | Netherlands | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.130.5.231 | 147.237.77.227 | | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.162.131 | 147.237.77.121 | Netherlands | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.231 | 147.237.77.61 | | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.130.5.231 | 147.237.76.39 | | mobile.meitav.idf.i | ET SCAN Potential SSH Scan | 1 |
| 37.26.147.236 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.149.89 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.230.134.108 | 147.237.8.45 | Germany | e.eitan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 93.174.93.203 | 147.237.8.27 | Netherlands | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.248.162.131 | 147.237.77.243 | Netherlands | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.162.131 | 147.237.77.178 | Netherlands | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.162.131 | 147.237.77.176 | Netherlands | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.231 | 147.237.77.170 | | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.162.131 | 147.237.76.198 | Netherlands | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.231 | 147.237.76.44 | | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.130.5.231 | 147.237.72.167 | | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.230.134.108 | 147.237.8.45 | Germany | e.eitan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 109.67.56.67 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.35.254 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 106.75.199.201 | 147.237.76.86 | China | navy.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |

01-06-2016-18:04:06 to 01-06-2016-19:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Response out of state | monitor | 5064 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 293 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 56 |
| 81.218.190.37 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 39 |
| 107.167.109.35 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 31 |
| 84.109.101.91 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 29 |
| 2.54.51.247 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 28 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 28 |
| 2.52.2.67 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 18 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 17 |
| 84.228.78.60 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 15 |
| 109.67.56.67 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 5.102.238.54 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 12 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 176.13.10.188 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 109.64.153.59 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 5.102.238.54 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 37.26.148.183 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 84.108.149.11 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 217.132.135.246 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.160.199.217 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 61.216.2.13 | Taiwan | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 6 |
| 109.64.189.79 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.195.184 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.52.60.193 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.86.162 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 84.94.56.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.65.102.141 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 217.132.135.246 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.160.199.217 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.11 | Israel | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 2.54.158.151 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 5 |
| 46.19.85.71 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 185.110.110.231 | | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 85.130.129.46 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 128.127.107.108 | Netherlands | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 2.54.158.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 5.22.129.67 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.158.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.108.139.129 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 109.253.218.33 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.54.158.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 4 |
| 2.54.51.247 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 77.127.32.193 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.52.179.29 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 46.19.86.173 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.54.1.71 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

01-06-2016-18:04:06 to 01-06-2016-19:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Unknown HTTP Request Method from 41.108.99.254 | Block | 5123 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Abnormally Long Request from 41.108.99.254 | Block | 35 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Multiple Malformed URL from 41.108.99.254 | Block | 35 |
| 109.253.143.128 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 209.190.20.61 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 209.190.20.61 | Block | 26 |
| 46.19.85.197 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 20 |
| 80.246.136.112 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 15 |
| 109.253.195.184 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 109.253.195.184 | Block | 12 |
| 109.253.194.194 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 7 |
| 2.54.9.123 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 7 |
| 37.26.146.194 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 46.19.85.220 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 6 |
| 109.253.195.184 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 4 |
| 209.190.20.61 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 209.190.20.61 | Block | 3 |
| 2.54.148.176 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.10.188 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.142.71 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.197.164 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.54.28.114 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.64.144.142 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 46.19.85.165 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 109.64.153.59 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 91.200.12.5 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 2 |
| 109.253.156.127 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 2 |
| 185.32.179.117 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 109.253.193.203 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.220 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 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 |
| 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 |
| 5.29.245.45 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 52.90.166.120 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx | Block | 1 |
| 183.79.221.37 | Japan | 147.237.72.166 | aka.idf.il | Illegal HTTP Version http://www.facebook.com/pages/%D7%97%D7%99%D7%9C-%D7%94%D7%9E%D7%A9%D7%98%D7%A8%D7%94-%D7%94%D7%A6%D7%91%D7%90%D7%99%D7%AA/180205332010999 HTTP/1.0 | Block | 1 |
| 2.54.34.55 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 95.86.118.39 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 95.86.118.39 | Block | 1 |
| 84.109.156.94 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 1 |
| 217.132.153.168 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method No in URL seturpirbno | Block | 1 |
| 176.13.3.68 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/robots.txt | Block | 1 |
| 195.154.226.90 | France | 147.237.77.216 | dover.idf.il | Illegal HTTP Version HTTP/ | Block | 1 |
| 176.13.23.13 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.7.207 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 89.138.178.30 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 41.108.99.254 | Algeria | 147.237.77.216 | dover.idf.il | Malformed URL seturpirbno | Block | 1 |
| 114.97.49.4 | China | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/1570-he/shared/usercontrols/headerupper/ | Block | 1 |
| 79.181.188.75 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 212.179.9.140 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |

01-06-2016-18:04:06 to 01-06-2016-19:04:06