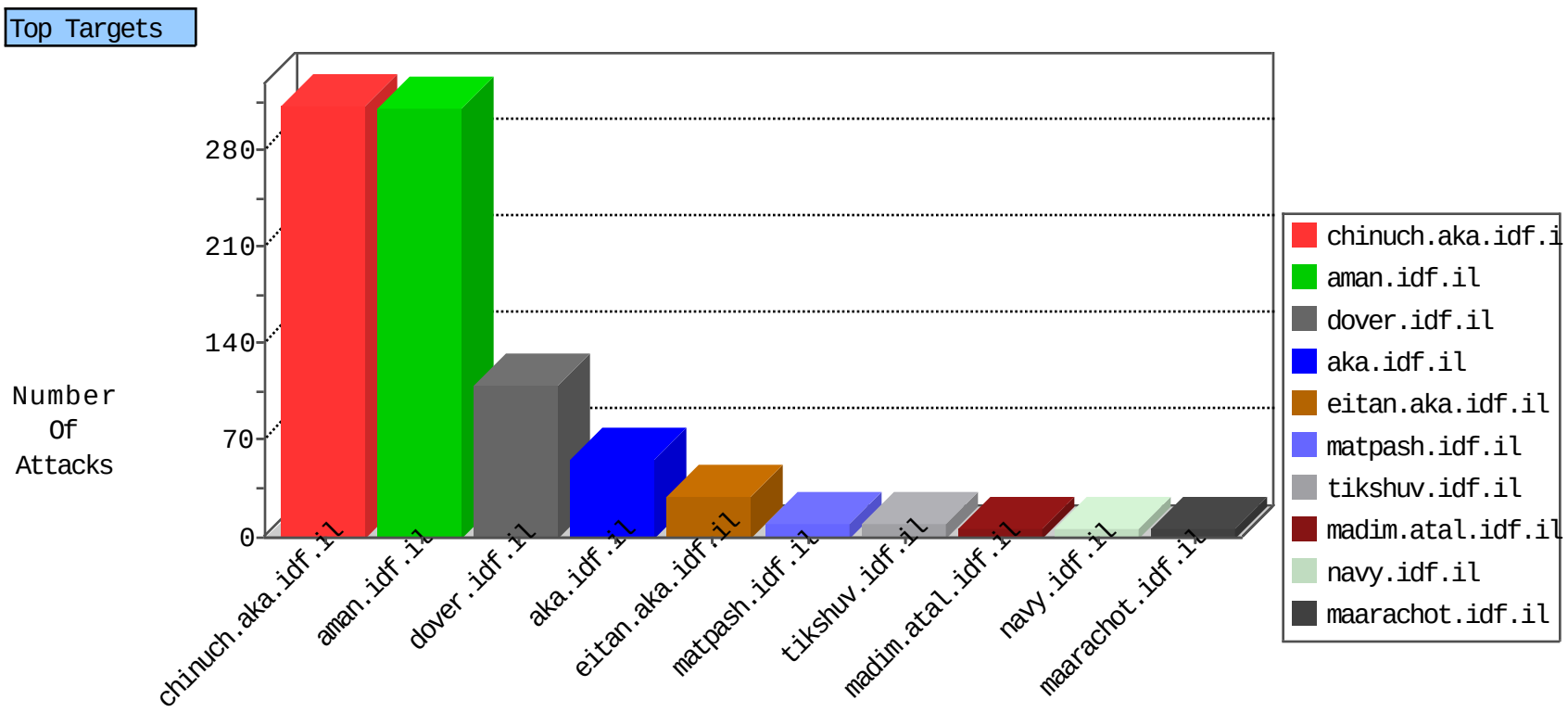
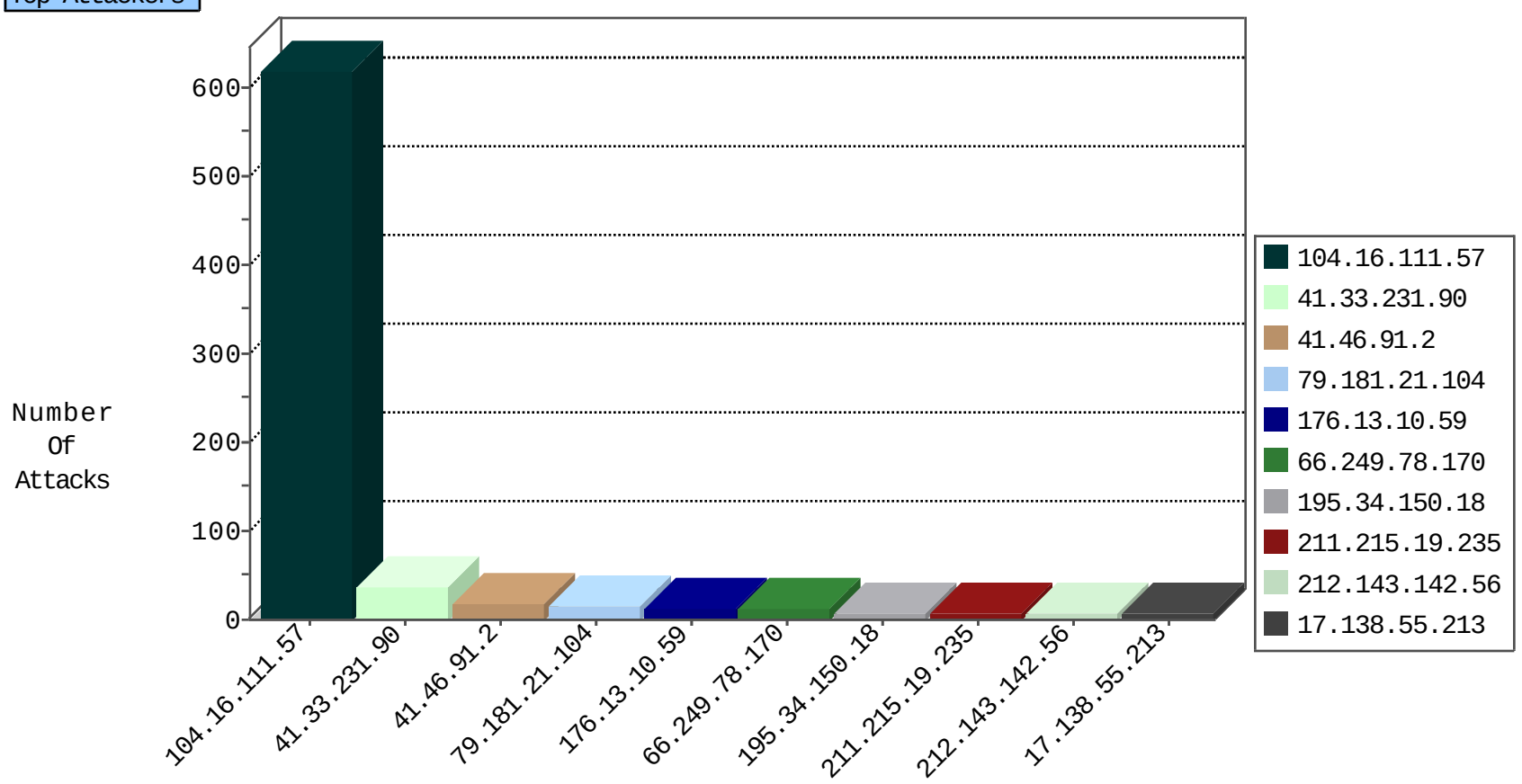
02-06-2016-01:04:04 to 02-06-2016-02:04:04

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-06-2016-01:04:04 to 02-06-2016-02:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 8 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 2 |
| 212.179.54.237 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 2 |
| 185.130.5.201 | | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

02-06-2016-01:04:04 to 02-06-2016-02:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 165.215.209.15 | United States | 147.237.77.216 | dover.idf.il | 14511: HTTP: Win32/Oliga Fake User Agent | Block | 1 |

02-06-2016-01:04:04 to 02-06-2016-02:04:04

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 |
| 112.196.49.101 | 147.237.0.34 | India | tikshuv.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 211.215.19.235 | 147.237.76.176 | Korea, Republic of | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.64 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 211.215.19.235 | 147.237.76.86 | Korea, Republic of | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.64 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 211.215.19.235 | 147.237.76.39 | Korea, Republic of | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.148.22.26 | 147.237.76.199 | Lithuania | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 211.215.19.235 | 147.237.76.34 | Korea, Republic of | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.148.22.26 | 147.237.76.86 | Lithuania | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 209.126.116.147 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 189.219.93.219 | 147.237.0.34 | Mexico | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 151.11.201.3 | 147.237.76.39 | Italy | mobile.meitav.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 112.196.49.101 | 147.237.0.34 | India | tikshuv.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 218.246.0.97 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 112.196.49.101 | 147.237.0.34 | India | tikshuv.idf.il | ET SCAN NMAP -f -sS | 1 |
| 211.215.19.235 | 147.237.76.148 | Korea, Republic of | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.64 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 211.215.19.235 | 147.237.76.44 | Korea, Republic of | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.64 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 211.215.19.235 | 147.237.76.38 | Korea, Republic of | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.148.22.26 | 147.237.76.148 | Lithuania | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 211.215.19.235 | 147.237.76.31 | Korea, Republic of | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.148.22.26 | 147.237.76.42 | Lithuania | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 151.11.201.3 | 147.237.76.39 | Italy | mobile.meitav.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 151.11.201.3 | 147.237.76.39 | Italy | mobile.meitav.idf.il | ET SCAN NMAP -f -sS | 1 |

02-06-2016-01:04:04 to 02-06-2016-02:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 104.16.111.57 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 308 |
| 104.16.111.57 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 307 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 79.181.21.104 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 66.249.78.170 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 89.238.166.141 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 6 |
| 176.13.10.59 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 176.13.10.59 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.179.216.105 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 66.249.78.252 | United States | 147.237.0.19 | madim.atal.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 | 5 |
| 213.8.204.51 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 66.249.78.239 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | 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 |
| 66.249.78.177 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 37.26.149.201 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.178.201.175 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.64.49.111 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.254.217 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 104.16.111.57 | United States | 147.237.72.156 | aman.idf.il | SYN Attack |  | reject | 2 |
| 66.249.65.88 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 66.249.78.245 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 37.46.39.78 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 198.46.159.29 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 37.46.39.78 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 61.135.190.69 | China | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 40.77.167.31 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 66.249.78.233 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 41.46.91.2 | Egypt | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 1 |
| 173.161.52.213 | United States | 147.237.77.216 | dover.idf.il | Header Rejection | header rejection pattern found in request | monitor | 1 |
| 79.176.10.178 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 2.54.158.0 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 61.135.190.200 | China | 147.237.0.33 | idf.il | drop |  | drop | 1 |
| 197.247.84.159 | Morocco | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 104.16.111.57 | United States | 147.237.76.147 | chinuch.aka.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 1 |
| 31.210.186.236 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 84.110.184.105 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 220.181.108.160 | China | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 41.46.91.2 | Egypt | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 1 |
| 37.46.39.56 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 2.54.158.0 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 198.20.69.74 | United States | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 37.8.114.196 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 85.65.228.253 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 41.46.91.2 | Egypt | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 2.54.191.3 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 109.73.127.69 | United Kingdom | 147.237.77.74 | law.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |
| 41.46.91.2 | Egypt | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 1 |

02-06-2016-01:04:04 to 02-06-2016-02:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 17.138.55.213 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.138.55.213 | Block | 8 |
| 213.251.182.103 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 3 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 2 |
| 188.143.232.35 | Russian Federation | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx | Block | 2 |
| 41.46.91.2 | Egypt | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 41.46.91.2 | Block | 1 |
| 192.243.55.131 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/kadatz | Block | 1 |
| 93.172.227.135 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 66.249.69.126 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/robots.txt | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/xmlrpc.php | Block | 1 |
| 176.228.141.76 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.78.239 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to eitan.aka.idf.il/404.aspx | Block | 1 |
| 50.62.176.236 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/ | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.76.42 | refuah.idf.il | PHP Attempt | Block | 1 |
| 192.243.55.132 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.132 | Block | 1 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/dover | Block | 1 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx | None | 1 |
| 41.46.91.2 | Egypt | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 40.77.167.31 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com | Block | 1 |
| 185.20.6.2 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 66.249.78.239 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in eitan.aka.idf.il/1002-en/eitan.aspx | None | 1 |
| 61.135.190.197 | China | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 1 |
| 192.243.55.132 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/kadatz | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 41.46.91.2 | Block | 1 |
| 173.161.52.213 | United States | 147.237.77.216 | dover.idf.il | E-mail collector robots 14 | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 41.46.91.2 | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 41.46.91.2 | Block | 1 |
| 84.229.155.196 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 66.249.65.152 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 1 |
| 41.46.91.2 | Egypt | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 173.161.52.213 | United States | 147.237.77.216 | dover.idf.il | eMail Hoarding | Block | 1 |
| 66.249.78.170 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in www.eitan.aka.idf.il/1012-en/eitan.aspx | None | 1 |
| 41.46.91.2 | Egypt | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.0.34 | tikshuv.idf.il | PHP Attempt | Block | 1 |
| 188.143.232.35 | Russian Federation | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1393-en/dover.aspx | Block | 1 |
| 86.153.13.169 | United Kingdom | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/test/wp-admin/ | Block | 1 |
| 66.249.69.115 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/1073-he/nakhal.aspx | Block | 1 |
| 41.46.91.2 | Egypt | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 1 |
| 173.192.138.226 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/blog/wp-admin/ | Block | 1 |
| 5.29.164.247 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.78.233 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in eitan.aka.idf.il/1086-en/eitan.aspx | None | 1 |

02-06-2016-01:04:04 to 02-06-2016-02:04:04