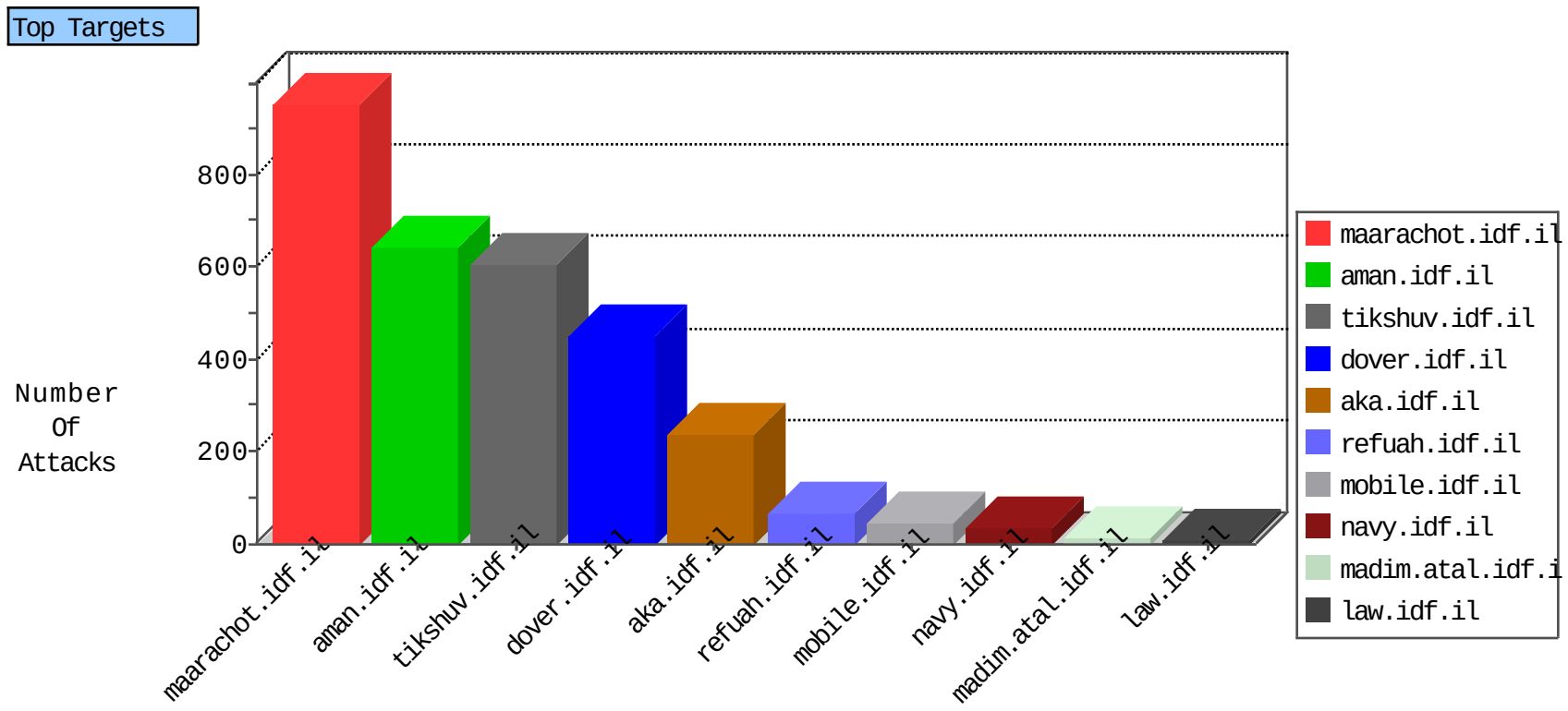
12-29-2015-00:04:04 to 12-29-2015-01:04:04

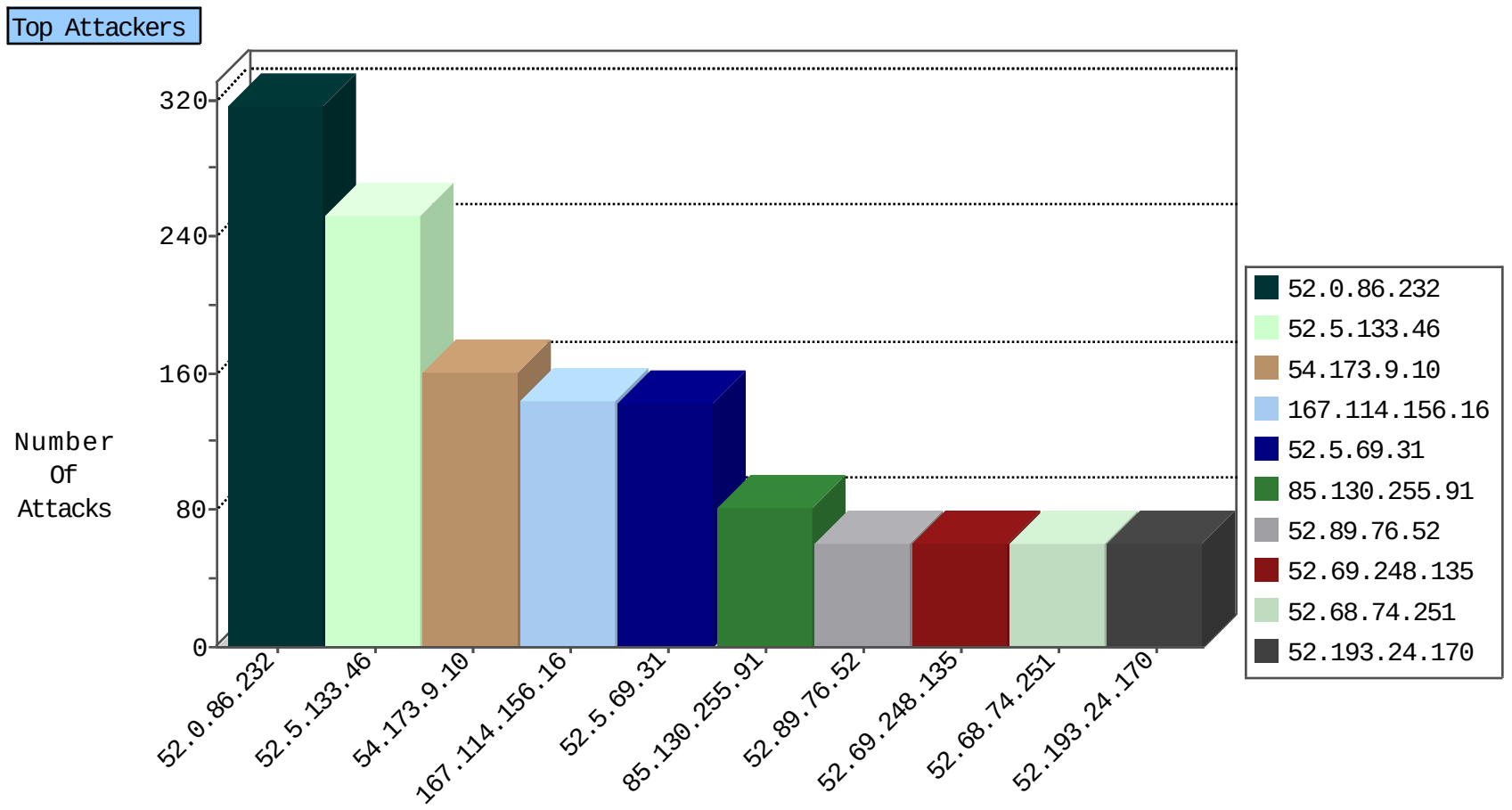
# IDF Under Attack
# Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

12-29-2015-00:04:04 to 12-29-2015-01:04:04

## 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 | 3327 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Http | drop | 5 |
| 80.82.64.177 | Netherlands | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |

12-29-2015-00:04:04 to 12-29-2015-01:04:04

## Top Attackers In IPS

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

12-29-2015-00:04:04 to 12-29-2015-01:04:04

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 |
| 66.249.66.61 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 162.222.185.165 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 149.202.248.121 | 147.237.72.14 | Germany | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 179.183.250.12 | 147.237.0.19 | Brazil | madim.atal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 115.182.17.13 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.55.154.39 | 147.237.8.45 | Brazil | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.114 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.55.154.39 | 147.237.0.200 | Brazil | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 81.101.206.244 | 147.237.76.38 | United Kingdom | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.55.154.39 | 147.237.0.15 | Brazil | kosher-kravi.idf.i | ET SCAN Potential SSH Scan | 1 |
| 78.193.2.8 | 147.237.76.31 | France | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 168.62.238.153 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.39.222.253 | 147.237.77.216 | Netherlands | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.77.216 | United States | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 162.222.185.165 | 147.237.76.30 | United States | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.182.17.13 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 177.55.154.39 | 147.237.8.46 | Brazil | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.192.0.18 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.55.154.39 | 147.237.8.28 | Brazil | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.114 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 177.55.154.39 | 147.237.0.35 | Brazil | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 78.193.2.8 | 147.237.76.42 | France | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 168.62.238.153 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 167.114.156.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 162.222.185.165 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |

12-29-2015-00:04:04 to 12-29-2015-01:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 52.0.86.232 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 317 |
| 52.5.133.46 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 249 |
| 54.173.9.10 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 155 |
| 52.5.69.31 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 142 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 154.72.166.57 | Cameroon | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 34 |
| 52.7.46.16 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 34 |
| 85.130.255.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 31 |
| 52.76.46.56 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.203.189 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.193.24.170 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.169.210.74 | Singapore | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.74.139.99 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.105.14 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.65.161.147 | Japan | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.88.168.51 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.203.189 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.68.74.251 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.193.24.170 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.76.32.115 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.76.32.115 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.169.210.74 | Singapore | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.65.161.147 | Japan | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.105.14 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.88.168.51 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.248.135 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.68.74.251 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.76.32.115 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.69.147.194 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.89.76.52 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.69.248.135 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.76.46.56 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 54.69.147.194 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.89.76.52 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 30 |
| 52.74.139.99 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 30 |
| 85.130.255.91 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 28 |
| 213.57.247.100 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 85.130.255.91 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 52.7.32.143 | United States | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 22 |
| 31.154.17.190 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 213.57.130.12 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 20 |
| 213.57.130.12 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 18 |
| 85.130.213.81 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 85.130.213.81 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 17 |
| 52.69.169.147 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 17 |
| 54.165.118.117 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 17 |
| 52.20.200.222 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.19.85.6 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 52.69.169.147 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 16 |
| 54.165.118.117 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 16 |
| 87.69.161.254 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |

12-29-2015-00:04:04 to 12-29-2015-01:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.228 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 46.19.85.228 | Block | 13 |
| 2.54.157.54 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 9 |
| 69.163.144.121 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 69.163.144.121 | Block | 5 |
| 109.67.198.189 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.167.38 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.120.129.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.9.126 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.182.166 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 66.249.66.61 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.66.61 | Block | 2 |
| 2.54.155.44 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 207.46.13.46 | United States | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 46.19.85.80 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 128.232.110.29 | United Kingdom | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to 147.237.76.147/ | Block | 1 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | Malformed URL ×œ [[#0]]Â²â€ž[[#17]] | Block | 1 |
| 5.29.43.182 | Israel | 147.237.76.200 | eitan.aka.idf.il | PHP Attempt | Block | 1 |
| 109.64.217.236 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal HTTP Version | Block | 1 |
| 77.127.57.57 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.66.183 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/miluim/templates/inner.asp | Block | 1 |
| 182.73.97.174 | India | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 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 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | NULL Character in URL ×œ [[#0]]Â²â€ž[[#17]] | Block | 1 |
| 46.121.105.38 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Illegal Byte Code Character in URL | Block | 1 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Method Âµ | Block | 1 |
| 31.210.188.91 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.64.217.236 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in Header Name | Block | 1 |
| 66.249.93.29 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 207.46.13.113 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 147.237.76.86/robots.txt | Block | 1 |
| 178.62.128.67 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/en | Block | 1 |
| 79.249.216.240 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.66.55 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 149.78.163.150 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Request from 79.179.161.90 | Block | 1 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | Abnormally Long Header Line request header name | Block | 1 |
| 5.29.43.182 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php | Block | 1 |
| 109.64.217.236 | Israel | 147.237.72.166 | aka.idf.il | Distributed Malformed HTTP Header Line | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx | Block | 1 |
| 195.154.191.97 | France | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 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 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 54.173.9.10 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/checksite/custom-error-page-test | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Unknown HTTP Request Method Â¯vlÂ¦Ã˜ | Block | 1 |
| 79.179.161.90 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL ×œ [[#0]]Â²â€ž[[#17]] | Block | 1 |
| 37.142.149.150 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 109.67.198.189 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 109.64.217.236 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in Header Value | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 66.249.66.61 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 180.76.15.7 | China | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

12-29-2015-00:04:04 to 12-29-2015-01:04:04