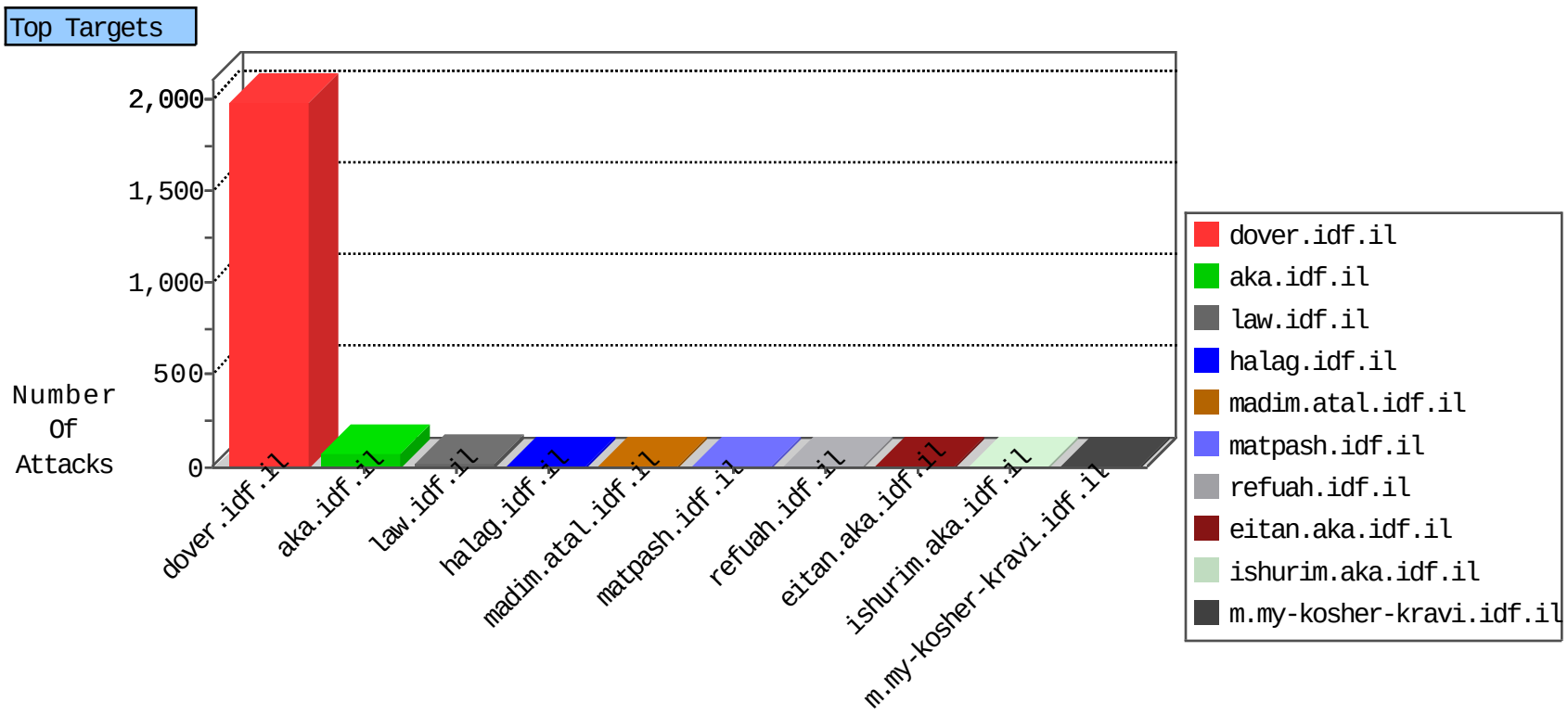
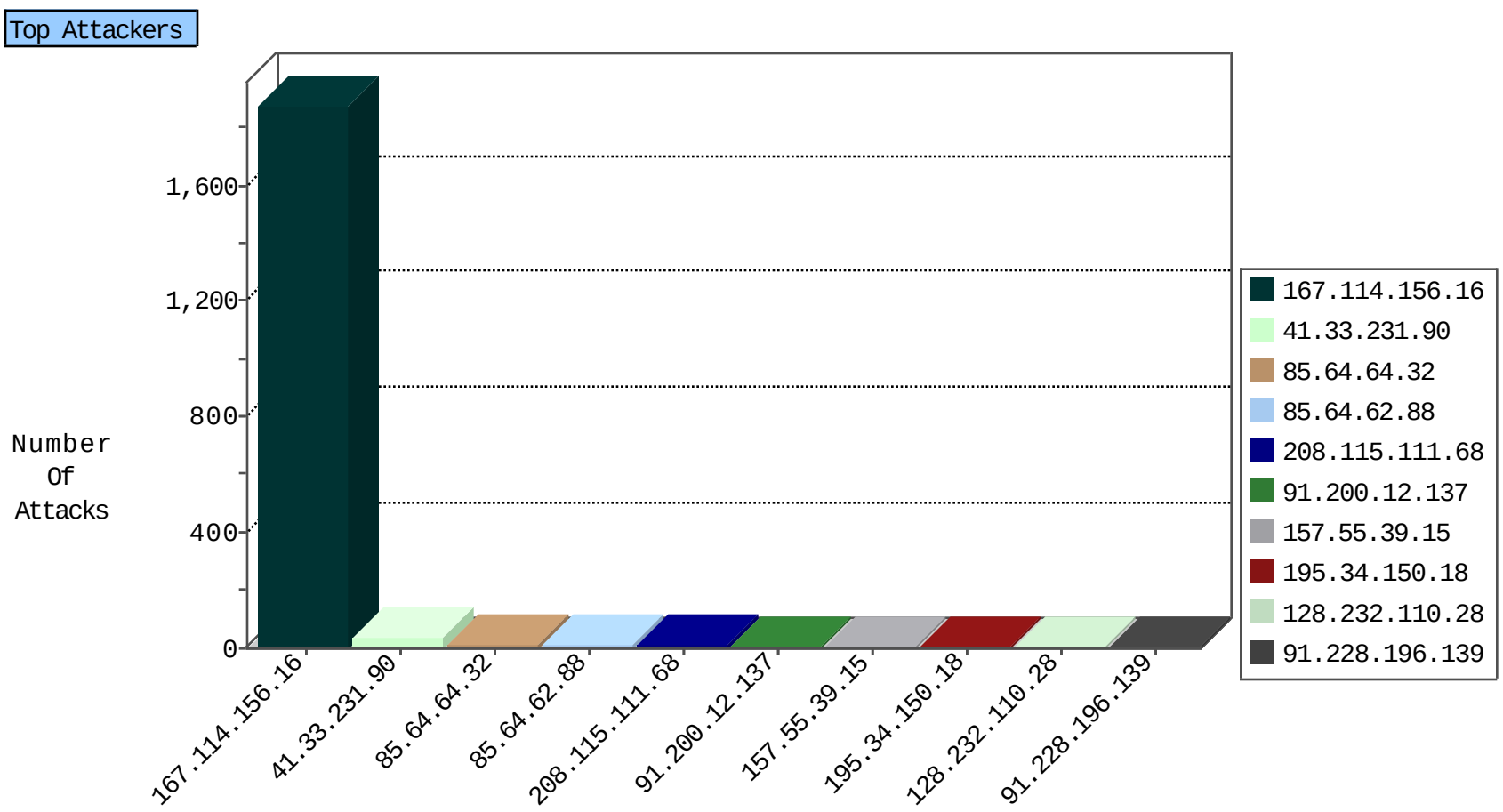
12-26-2015-02:04:08 to 12-26-2015-03:04:08

# IDF Under Attack Daily Report




Top Attackers

12-26-2015-02:04:08 to 12-26-2015-03:04:08

## 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 | 3134 |

12-26-2015-02:04:08 to 12-26-2015-03:04:08

## Top Attackers In IPS

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

12-26-2015-02:04:08 to 12-26-2015-03:04:08

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 |
| 104.255.67.115 | 147.237.72.166 | | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 3 |
| 66.249.69.254 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.66.75 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 24.37.76.186 | 147.237.72.167 | Canada | ishurim.aka.idf.i | ET SCAN NMAP -sS window 2048 | 1 |
| 187.161.89.238 | 147.237.77.74 | Mexico | law.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.228.196.139 | 147.237.77.176 | Poland | matpash.idf.il | SERVER-WEBAPP modules.php access | 1 |
| 24.37.76.186 | 147.237.72.167 | Canada | ishurim.aka.idf.i | ET SCAN NMAP -f -sS | 1 |
| 187.161.89.238 | 147.237.77.235 | Mexico | sviva.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

12-26-2015-02:04:08 to 12-26-2015-03:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 85.64.64.32 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 14 |
| 85.64.62.88 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 208.115.111.68 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 11 |
| 157.55.39.15 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 141.8.132.112 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 91.200.12.137 | Ukraine | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 4 |
| 91.200.12.137 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | 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 |
| 79.182.204.51 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 95.108.158.145 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 128.232.110.28 | United Kingdom | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 188.120.148.150 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 8.37.227.81 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Response out of state | monitor | 2 |
| 128.232.110.28 | United Kingdom | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 46.19.85.111 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 157.55.39.178 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 84.109.3.6 | Israel | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 78.46.7.81 | Germany | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 208.115.111.73 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 157.55.39.179 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 208.115.111.73 | United States | 147.237.76.31 | nakchal.idf.il | drop | SAM rule | drop | 1 |
| 2.54.132.141 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 198.20.69.74 | United States | 147.237.76.197 | e.himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 2.54.132.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 80.246.133.91 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 208.115.111.73 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 1 |
| 2.54.189.181 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 207.46.13.183 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 2.54.132.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 157.55.39.54 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 80.246.133.91 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 88.75.61.15 | Germany | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 2.54.132.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 1 |
| 123.125.71.21 | China | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 1 |
| 37.26.146.210 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 195.154.227.118 | France | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 91.200.12.136 | Ukraine | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 2.54.132.141 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 123.125.71.21 | China | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 84.228.166.97 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 37.187.114.171 | France | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 198.20.69.74 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 149.88.210.55 | Israel | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |

12-26-2015-02:04:08 to 12-26-2015-03:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.160 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 5 |
| 109.65.33.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Suspicious Response Code | Block | 3 |
| 157.55.39.164 | United States | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 157.55.39.164 | Block | 2 |
| 91.228.196.139 | Poland | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 91.228.196.139 | Block | 2 |
| 46.121.140.73 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 40.77.167.5 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 2 |
| 176.13.9.187 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 91.228.196.139 | Poland | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 2 |
| 195.154.191.97 | France | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 79.177.201.43 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/xmlrpc.php | Block | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 45.55.58.61 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 109.169.50.31 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17506.jpg | Block | 1 |
| 72.47.234.114 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 157.55.39.179 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 150.70.97.85 | Japan | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.64.118 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 5.29.94.107 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 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 |
| 195.154.191.97 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/wp-login.php | Block | 1 |
| 80.246.136.68 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.79.235 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif | Block | 1 |
| 157.55.39.164 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/api/clientconfig | Block | 1 |
| 110.232.112.157 | Australia | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 91.228.196.139 | Poland | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/index.php | 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 |
| 173.254.55.58 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 72.47.234.114 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 150.70.97.85 | Japan | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/watch | Block | 1 |
| 5.255.253.62 | Russian Federation | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 107.178.194.83 | Block | 1 |
| 198.1.68.234 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 85.64.16.240 | 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/1397-en/dover.aspx | Block | 1 |
| 157.55.39.166 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/bundles/css | Block | 1 |
| 110.232.112.157 | Australia | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 94.230.86.170 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 173.254.55.58 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 77.247.181.165 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 150.70.173.5 | Japan | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.64.235 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-17163-he/dover.aspx | Block | 1 |
| 198.1.68.234 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 85.64.64.32 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 69.195.124.229 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 157.55.39.178 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 117.222.16.146 | India | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx | Block | 1 |
| 50.62.177.227 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |

12-26-2015-02:04:08 to 12-26-2015-03:04:08