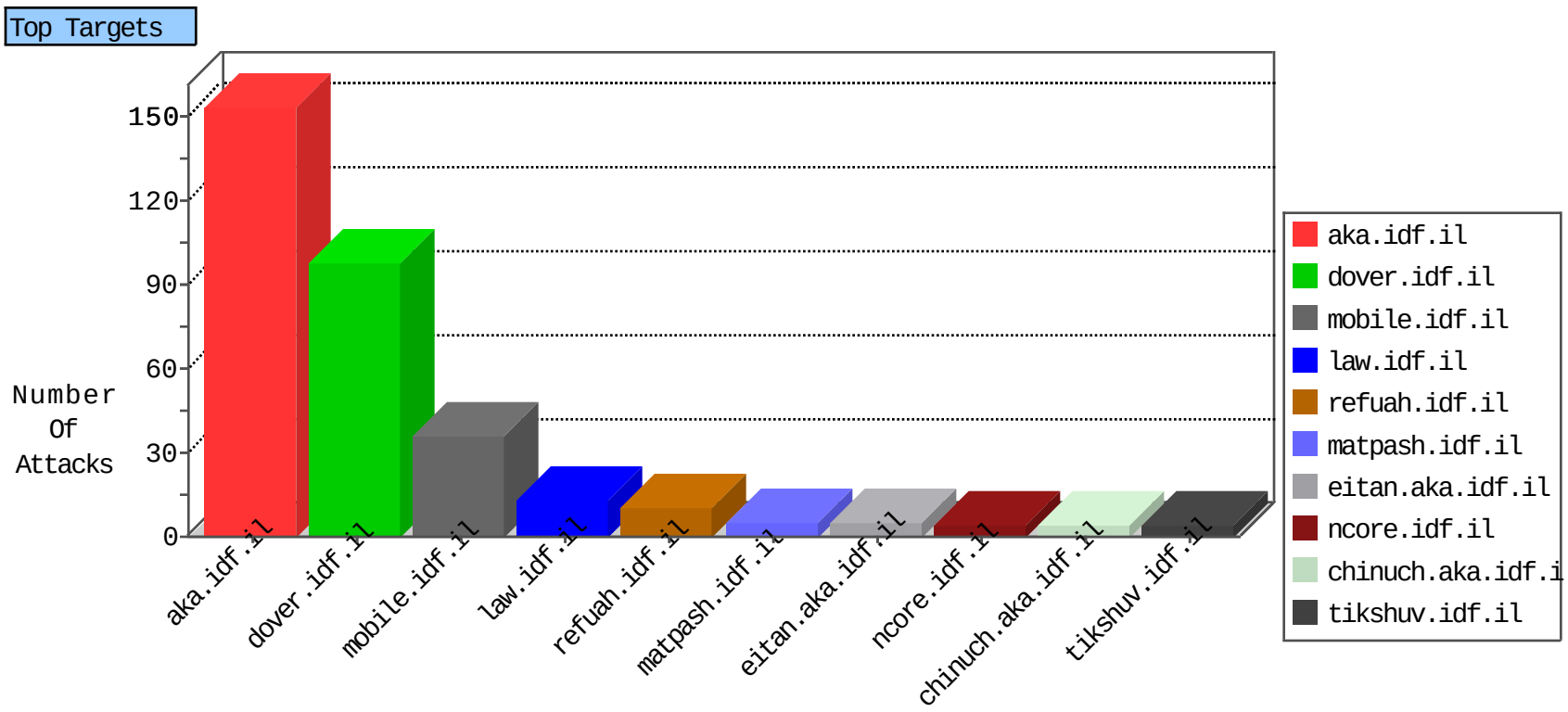
01-30-2016-03:04:03 to 01-30-2016-04:04:03

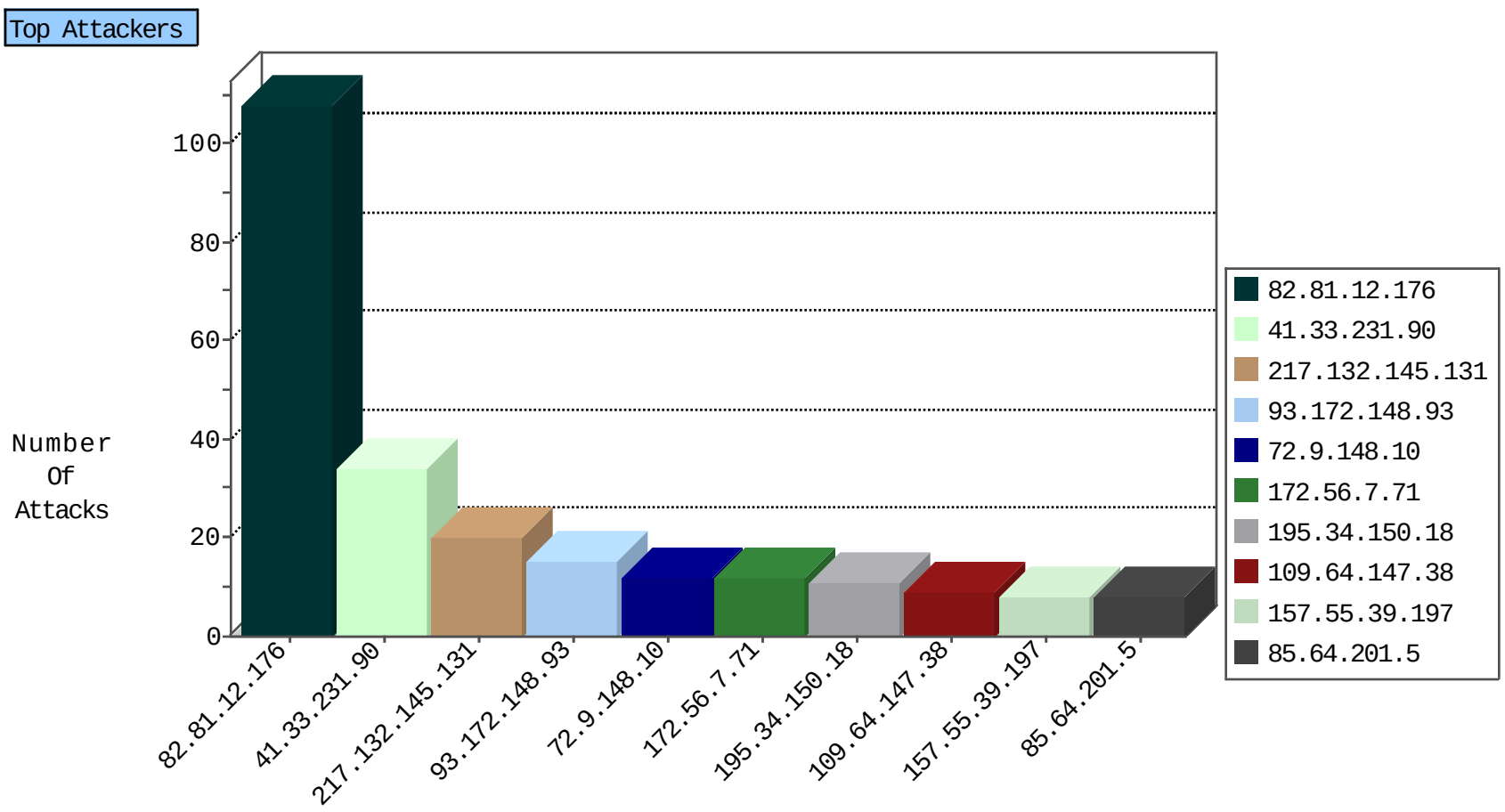
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

01-30-2016-03:04:03 to 01-30-2016-04:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 82.81.12.176 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 108 |
| 212.179.54.237 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 2 |
| 198.20.70.114 | United States | 147.237.76.30 | himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 74.91.28.60 | United States | 147.237.0.34 | tikshuv.idf.il | block-sp-traf1 | forward | 1 |
| 93.172.148.93 | Israel | 147.237.76.148 | gqcenter.aka.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 204.42.253.132 | United States | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.172.148.93 | Israel | 147.237.77.205 | prisha.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 92.103.159.171 | France | 147.237.0.33 | idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 184.26.161.65 | United States | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.172.148.93 | Israel | 147.237.76.147 | chinuch.aka.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |

01-30-2016-03:04:03 to 01-30-2016-04:04:03

## Top Attackers In IPS

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

01-30-2016-03:04:03 to 01-30-2016-04:04:03

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 | 5 |
| 154.73.170.162 | 147.237.77.243 | | mobile.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 114.112.90.54 | 147.237.77.216 | China | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 98.119.105.221 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.113 | 147.237.76.42 | Ukraine | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.39.222.253 | 147.237.77.234 | Netherlands | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 197.115.4.86 | 147.237.76.177 | Algeria | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.73.170.162 | 147.237.77.243 | | mobile.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 114.112.90.54 | 147.237.77.233 | China | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 114.112.90.54 | 147.237.77.205 | China | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 98.119.105.221 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 42.236.237.93 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 5.39.222.253 | 147.237.77.179 | Netherlands | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.246.0.97 | 147.237.77.121 | China | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 197.115.4.86 | 147.237.76.177 | Algeria | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.106.92.142 | 147.237.8.46 | | e.chinuch.idf.i | ET SCAN Potential SSH Scan | 1 |

01-30-2016-03:04:03 to 01-30-2016-04:04:03

## 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 | 34 |
| 217.132.145.131 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 72.9.148.10 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.64.147.38 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 157.55.39.197 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 41.230.14.223 | Tunisia | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 172.56.7.71 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 85.64.201.5 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.188 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.102.254.238 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 93.172.148.93 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 31.210.188.122 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.188 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 178.255.215.87 | France | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 54.244.22.103 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.209 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.176.195.79 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 157.55.39.197 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 37.142.68.50 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 172.56.7.71 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 197.115.4.86 | Algeria | 147.237.76.177 | ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 172.56.7.71 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 62.210.206.219 | France | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 91.200.12.106 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 172.56.7.71 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 2 |
| 46.19.85.209 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 2.52.19.212 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 93.172.148.93 | Israel | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 216.218.206.120 | United States | 147.237.76.199 | e.nakchal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 79.178.104.235 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.86.202 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.222 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 93.172.148.93 | Israel | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 85.93.18.64 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 2.52.19.212 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 93.172.148.93 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 216.218.206.120 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 81.7.17.171 | Germany | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 46.19.86.202 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 151.80.31.152 | Italy | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 93.172.148.93 | Israel | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 87.69.170.99 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 197.115.4.86 | Algeria | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 74.82.47.20 | United States | 147.237.8.27 | e.madim.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.221 | United States | 147.237.8.24 | e.lifestyle.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 2.54.11.57 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |

01-30-2016-03:04:03 to 01-30-2016-04:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 217.132.145.131 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 46.116.90.98 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 79.179.71.76 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 79.182.208.31 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 80.246.136.8 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 79.176.195.79 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/sahar | Block | 2 |
| 85.64.201.5 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 5.254.97.74 | Romania | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 5.254.97.74 | Block | 2 |
| 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 |
| 188.143.232.21 | Russian Federation | 147.237.77.176 | matpash.idf.il | Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx | Block | 1 |
| 5.254.97.74 | Romania | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/site/general. aspx | Block | 1 |
| 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 | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 46.166.136.162 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 191.232.136.164 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 31.210.188.122 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 216.218.206.68 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 109.160.233.83 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 68.180.230.244 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx | Block | 1 |
| 195.154.191.97 | France | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 1 |
| 40.77.167.53 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 141.212.122.209 | United States | 147.237.76.200 | eitan.aka.idf.i | Unauthorized URL Access to 147.237.76.200/ | Block | 1 |
| 195.154.191.97 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/wp-content/plugins/revslider/temp/update_extract/02386824.php | Block | 1 |
| 41.230.14.223 | Tunisia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 184.105.139.68 | United States | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to 147.237.77.243/ | Block | 1 |
| 79.179.20.232 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 204.13.201.138 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |

01-30-2016-03:04:03 to 01-30-2016-04:04:03