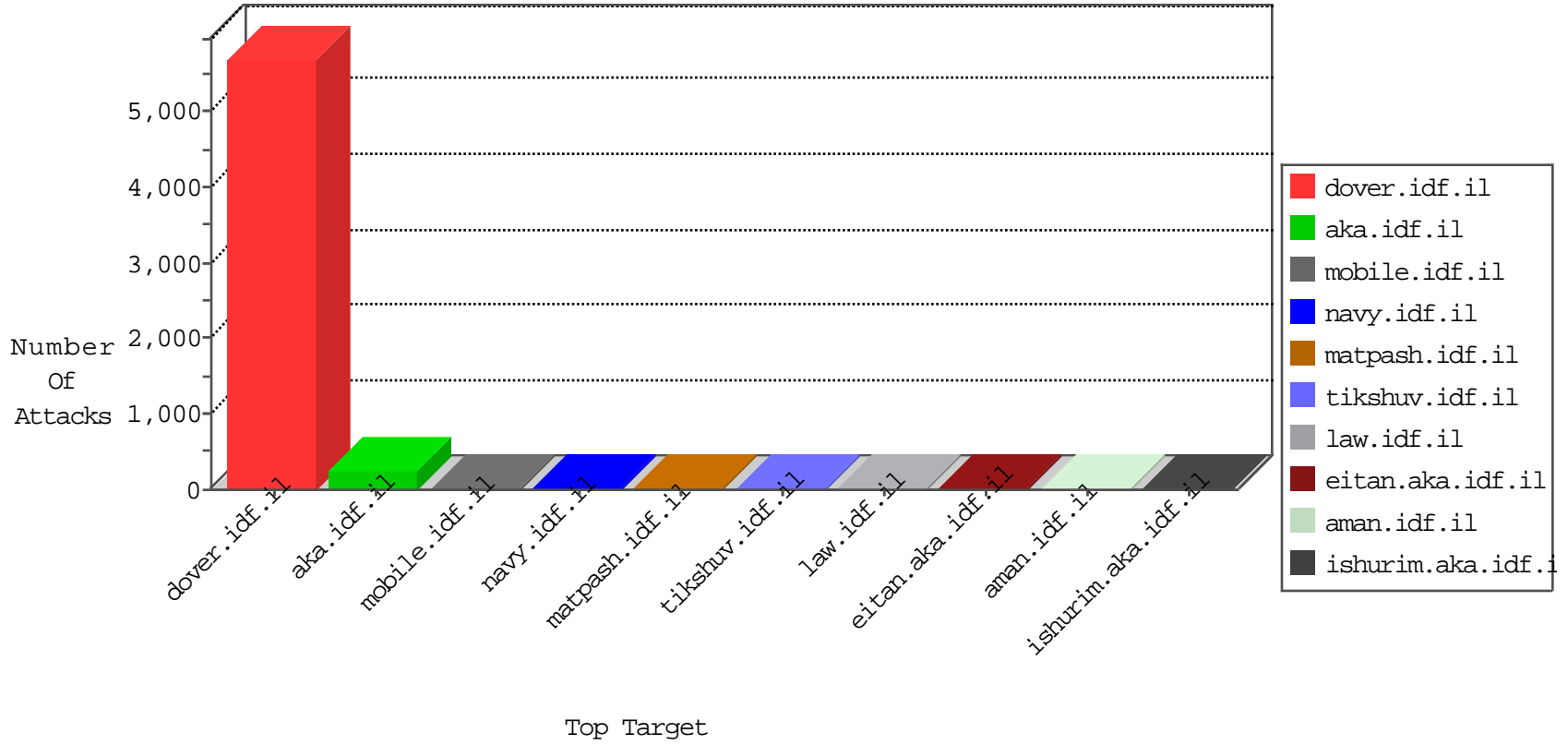


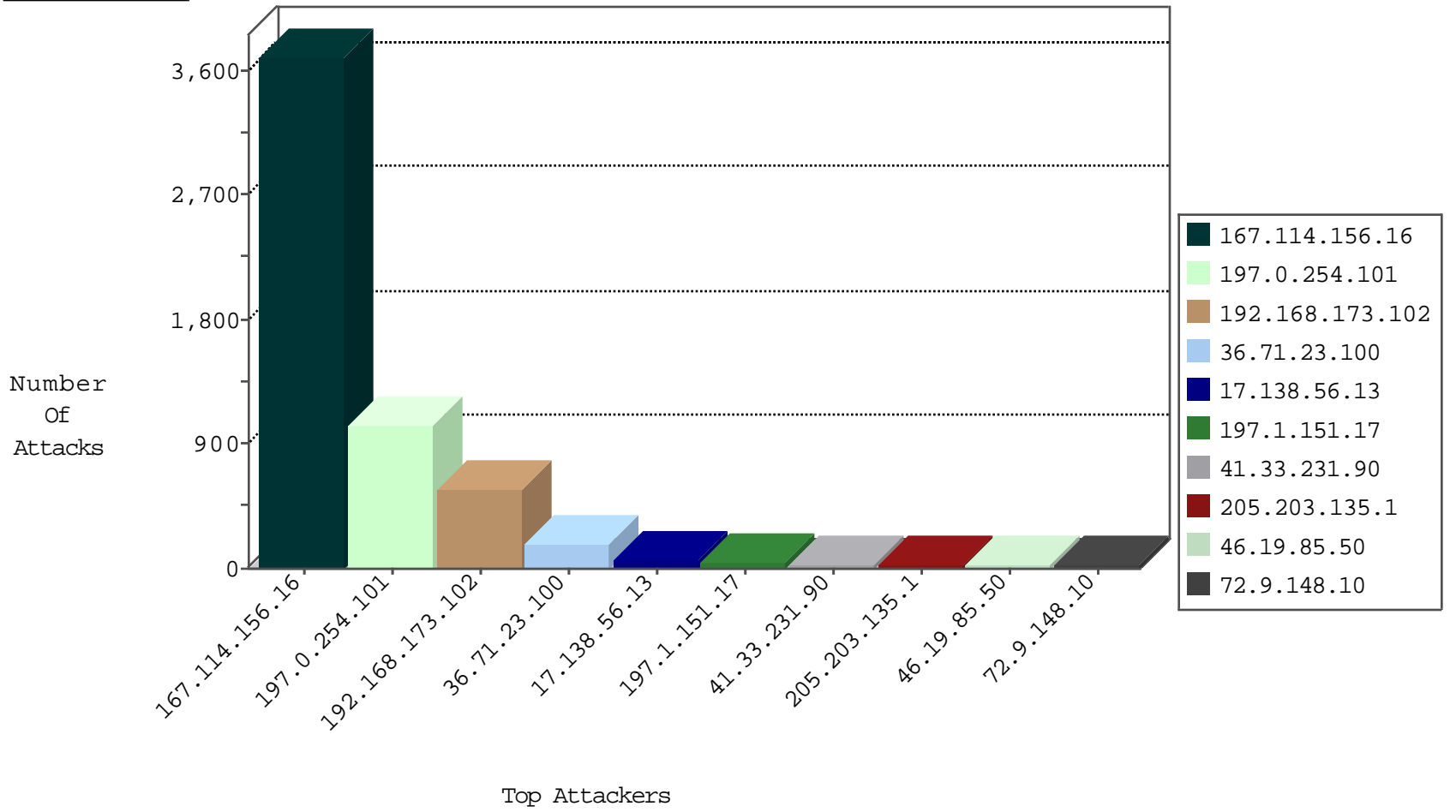
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site                     | Signature                                     | Device Action | Count |
|------------------|------------------|----------------|--------------------------|---|---------------|-------|
| 197.0.254.101    | Tunisia          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 17829 |
| 36.71.23.100     | Indonesia        | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 10850 |
| 196.206.9.35     | Morocco          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 9050  |
| 41.230.102.88    | Tunisia          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 4605  |
| 167.114.156.16   | Canada           | 147.237.77.216 | dover.idf.il             | Block_Ip_Web_In                               | drop          | 3673  |
| 197.27.76.241    | Tunisia          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 2258  |
| 54.72.0.55       | Ireland          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1754  |
| 212.143.142.56   | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1751  |
| 139.162.216.112  | United States    | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 718   |
| 8.37.70.104      | United States    | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 538   |
| 197.0.254.101    | Tunisia          | 147.237.77.216 | dover.idf.il             | DOS-Tool-SwitchbladG                          | dest-reset    | 354   |
| 149.50.103.142   | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 152   |
| 205.203.135.1    | United States    | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 45    |
| 81.218.65.210    | Israel           | 147.237.77.176 | matpash.idf.il           | Block_Udp_All_Nets                            | drop          | 12    |
| 149.78.154.69    | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 4     |
| 81.218.65.210    | Israel           | 147.237.72.166 | aka.idf.il               | Block_Udp_All_Nets                            | drop          | 3     |
| 197.1.151.17     | Tunisia          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 3     |
| 197.0.254.101    | Tunisia          | 147.237.77.216 | dover.idf.il             | JLM_Purple_Con_Limit_Http                     | drop          | 3     |
| 149.50.15.122    | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 2     |
| 0.0.0.0          |                  | 147.237.77.216 | dover.idf.il             | HTTP Page Flood Attack                        | drop          | 2     |
| 197.0.254.101    | Tunisia          | 147.237.77.216 | dover.idf.il             | JLM_Under_Attack_Con_Http                     | drop          | 2     |
| 91.15.198.165    | Germany          | 147.237.0.35   | akaws.idf.il             | Block_Ntp_All_Net                             | drop          | 1     |
| 91.15.198.165    | Germany          | 147.237.0.17   | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net                             | drop          | 1     |
| 54.72.73.168     | Ireland          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 180.211.121.198  | India            | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 109.67.49.226    | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 209.126.127.17   | United States    | 147.237.8.27   | e.madim.atal.idf.il      | Block_Udp_All_Nets                            | drop          | 1     |
| 91.15.198.165    | Germany          | 147.237.0.19   | madim.atal.idf.il        | Block_Ntp_All_Net                             | drop          | 1     |
| 54.72.182.187    | Ireland          | 147.237.77.216 | dover.idf.il             | Block_Udp_All_Nets                            | drop          | 1     |
| 192.3.220.210    | United States    | 147.237.77.176 | matpash.idf.il           | Block_Udp_All_Nets                            | drop          | 1     |
| 121.55.231.241   | Guam             | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 91.15.198.165    | Germany          | 147.237.0.15   | kosher-kravi.idf.il      | Block_Ntp_All_Net                             | drop          | 1     |
| 46.19.85.50      | Israel           | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 209.126.127.17   | United States    | 147.237.8.46   | e.chinuch.idf.il         | Block_Udp_All_Nets                            | drop          | 1     |
| 91.15.198.165    | Germany          | 147.237.0.33   | idf.il                   | Block_Ntp_All_Net                             | drop          | 1     |
| 66.240.192.138   | United States    | 147.237.0.17   | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net                             | drop          | 1     |
| 197.116.186.233  | Algeria          | 147.237.77.216 | dover.idf.il             | TCP handshake violation, first packet not syn | drop          | 1     |
| 91.15.198.165    | Germany          | 147.237.0.16   | my-kosher-kravi.idf.il   | Block_Ntp_All_Net                             | drop          | 1     |

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site           | Signature                                   | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 109.64.223.223   | Israel           | 147.237.0.34   | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL      | Block         | 8     |
| 123.126.113.80   | China            | 147.237.72.166 | aka.idf.il     | C1000071: HTTP: User Agent Sogou+web+spider | Block         | 1     |
| 197.0.254.101    | Tunisia          | 147.237.77.216 | dover.idf.il   | 8262: HTTP: Slowloris DoS Tool              | Block         | 1     |
| 66.249.66.59     | Israel           | 147.237.0.34   | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL      | Block         | 1     |
| 66.249.66.62     | Israel           | 147.237.0.34   | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL      | Block         | 1     |

## 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     |
| 79.177.68.191    | 147.237.0.34   | Israel                          | tikshuv.idf.il         | ET SCAN NMAP -sA (2)  | 2     |
| 198.54.90.200    | 147.237.0.34   | United States                   | tikshuv.idf.il         | Tehila - Perl LWP with fake user agent  | 2     |
| 82.205.41.196    | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il           | ET SCAN NMAP -sA (2)  | 2     |
| 104.171.122.176  | 147.237.76.148 | United States                   | ggcenter.aka.idf.il    | ET SCAN NMAP -sS window 4096  | 1     |
| 104.171.122.176  | 147.237.76.148 | United States                   | ggcenter.aka.idf.il    | ET SCAN NMAP -f -sS   | 1     |
| 93.183.201.2     | 147.237.0.16   | Ukraine                         | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan  | 1     |
| 52.38.94.200     | 147.237.8.46   | United States                   | e.chimuch.idf.il       | ET SCAN NMAP -sS window 1024  | 1     |
| 190.124.35.113   | 147.237.72.166 | Nicaragua                       | aka.idf.il             | ET SCAN NMAP -sS window 1024  | 1     |
| 189.198.45.96    | 147.237.77.235 | Mexico                          | sviva.idf.il           | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1     |
| 120.209.17.110   | 147.237.0.19   | China                           | madim.atal.idf.il      | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1     |
| 104.171.122.176  | 147.237.76.148 | United States                   | ggcenter.aka.idf.il    | ET SCAN NMAP -sS window 2048  | 1     |
| 93.183.201.2     | 147.237.76.31  | Ukraine                         | nakchal.idf.il         | ET SCAN Potential SSH Scan  | 1     |
| 216.55.143.94    | 147.237.77.216 | United States                   | dover.idf.il           | ET WEB_SERVER PHP Crawler   | 1     |
| 52.38.94.200     | 147.237.8.46   | United States                   | e.chimuch.idf.il       | ET SCAN NMAP -sS window 4096  | 1     |
| 195.216.176.244  | 147.237.77.74  | Latvia                          | law.idf.il             | ET SCAN NMAP -sS window 1024  | 1     |
| 190.124.35.113   | 147.237.72.166 | Nicaragua                       | aka.idf.il             | ET SCAN NMAP -sS window 2048  | 1     |
| 190.124.35.113   | 147.237.72.166 | Nicaragua                       | aka.idf.il             | ET SCAN NMAP -f -sS   | 1     |
| 180.76.170.207   | 147.237.77.121 | China                           | e.navy.idf.il          | ET SCAN NMAP -sS window 1024  | 1     |

## Top Attackers In FW

| Attacker Address | Attacker Country                | Target Address | Site               | Signature                                    | Message   | Device Action | Count |
|------------------|---------------------------------|----------------|--------------------|--|---|---------------|-------|
| 197.0.254.101    | Tunisia                         | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 642   |
| 192.168.173.102  |                                 | 147.237.77.216 | dover.idf.il       | Geo-location enforcement                     | Geo-location inbound enforcement                | monitor       | 375   |
| 197.0.254.101    | Tunisia                         | 147.237.77.216 | dover.idf.il       | SYN Attack                                   | SYN -> SYN-ACK -> Timeout                       | reject        | 230   |
| 192.168.173.102  |                                 | 147.237.72.166 | aka.idf.il         | Geo-location enforcement                     | Geo-location inbound enforcement                | monitor       | 187   |
| 36.71.23.100     | Indonesia                       | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 160   |
| 197.1.151.17     | Tunisia                         | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 45    |
| 17.138.56.13     | United States                   | 147.237.77.216 | dover.idf.il       | drop   | SAM rule  | drop          | 40    |
| 41.33.231.90     | Egypt                           | 147.237.77.216 | dover.idf.il       | drop   | SAM rule  | drop          | 30    |
| 205.203.135.1    | United States                   | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 25    |
| 17.138.56.13     | United States                   | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 19    |
| 72.9.148.10      | United States                   | 147.237.77.216 | dover.idf.il       | drop   | SAM rule  | drop          | 16    |
| 46.19.85.252     | Israel                          | 147.237.77.216 | dover.idf.il       | SYN Attack                                   | SYN -> SYN-ACK -> RST                           | reject        | 12    |
| 139.162.216.112  | United States                   | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 12    |
| 46.19.85.36      | Israel                          | 147.237.76.200 | eitan.aka.idf.il   | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 12    |
| 155.254.239.120  | Iraq                            | 147.237.77.216 | dover.idf.il       | SYN Attack                                   | SYN -> SYN-ACK -> RST                           | reject        | 10    |
| 212.143.142.56   | Israel                          | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 9     |
| 149.78.154.69    | Israel                          | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 9     |
| 185.27.105.159   | Israel                          | 147.237.72.166 | aka.idf.il         | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 9     |
| 46.19.86.206     | Israel                          | 147.237.77.243 | mobile.idf.il      | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 9     |
| 46.19.85.50      | Israel                          | 147.237.76.86  | navy.idf.il        | Bad TCP sequence                             | Invalid ACK number                              | alert         | 6     |
| 2.55.17.31       | Israel                          | 147.237.76.86  | navy.idf.il        | SYN Attack                                   | SYN -> SYN-ACK -> RST                           | reject        | 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     |
| 46.19.85.50      | Israel                          | 147.237.76.86  | navy.idf.il        | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 6     |
| 109.64.223.223   | Israel                          | 147.237.0.34   | tikshuv.idf.il     | SYN Attack                                   | SYN -> SYN-ACK -> Timeout                       | reject        | 6     |
| 46.19.85.50      | Israel                          | 147.237.77.216 | dover.idf.il       | Bad TCP sequence                             | Invalid ACK number                              | alert         | 6     |
| 109.65.214.41    | Israel                          | 147.237.72.166 | aka.idf.il         | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 6     |
| 212.199.53.161   | Israel                          | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 6     |
| 46.19.85.50      | Israel                          | 147.237.77.216 | dover.idf.il       | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 6     |
| 185.3.144.34     | Israel                          | 147.237.72.156 | aman.idf.il        | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 6     |
| 31.13.162.246    | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 6     |
| 208.115.111.68   | United States                   | 147.237.77.74  | law.idf.il         | drop   | SAM rule  | drop          | 5     |
| 123.126.113.109  | China                           | 147.237.77.216 | dover.idf.il       | drop   | SAM rule  | drop          | 5     |
| 84.111.216.183   | Israel                          | 147.237.77.243 | mobile.idf.il      | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 4     |
| 72.9.148.10      | United States                   | 147.237.77.176 | matpash.idf.il     | drop   | SAM rule  | drop          | 4     |
| 197.45.132.217   | Egypt                           | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 4     |
| 82.81.64.200     | Israel                          | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 4     |
| 5.22.131.68      | Israel                          | 147.237.77.216 | dover.idf.il       | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 4     |
| 185.3.144.34     | Israel                          | 147.237.72.166 | aka.idf.il         | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 3     |
| 109.253.158.113  | Israel                          | 147.237.77.243 | mobile.idf.il      | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 3     |
| 66.249.78.223    | United States                   | 147.237.77.243 | mobile.idf.il      | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 3     |
| 130.203.136.75   | United States                   | 147.237.77.74  | law.idf.il         | drop   | SAM rule  | drop          | 3     |
| 185.6.56.247     | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 3     |
| 5.22.129.248     | Israel                          | 147.237.72.166 | aka.idf.il         | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 3     |
| 94.159.169.234   | Israel                          | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 3     |
| 64.246.165.10    | United States                   | 147.237.77.74  | law.idf.il         | Header Rejection                             | header rejection pattern found in request       | monitor       | 3     |
| 49.145.173.34    | Philippines                     | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 3     |
| 79.183.100.129   | Israel                          | 147.237.72.166 | aka.idf.il         | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 3     |
| 207.46.13.71     | United States                   | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 3     |
| 72.9.148.10      | United States                   | 147.237.77.74  | law.idf.il         | drop   | SAM rule  | drop          | 2     |
| 141.8.132.78     | Russian Federation              | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 2     |

## Top Attackers In WAF

| Attacker Address | Attacker Country   | Target Address | Site                 | Signature   | Device Action | Count |
|------------------|--------------------|----------------|----------------------|---|---------------|-------|
| 5.44.169.128     | Russian Federation | 147.237.77.216 | dover.idf.il         | Unauthorized URL Access to www.idf.il/mazi'a=0  | Block         | 6     |
| 185.130.5.163    | Lithuania          | 147.237.72.166 | aka.idf.il           | Multiple Unauthorized URL Access from 185.130.5.163   | Block         | 5     |
| 185.130.5.163    | Lithuania          | 147.237.72.166 | aka.idf.il           | PHP Attempt   | Block         | 5     |
| 84.111.216.183   | Israel             | 147.237.77.243 | mobile.idf.il        | Multiple Unauthorized URL Access from 84.111.216.183  | Block         | 3     |
| 41.193.160.42    | South Africa       | 147.237.77.216 | dover.idf.il         | Multiple Unauthorized URL Access from 41.193.160.42   | Block         | 2     |
| 157.55.39.161    | United States      | 147.237.77.216 | dover.idf.il         | Multiple Unauthorized URL Access from 157.55.39.161   | Block         | 2     |
| 46.19.86.206     | Israel             | 147.237.0.19   | madim.atal.idf.il    | Distributed Suspicious Response Code  | Block         | 2     |
| 84.111.216.183   | Israel             | 147.237.77.243 | mobile.idf.il        | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362                            | Block         | 2     |
| 84.111.1.84      | Israel             | 147.237.0.19   | madim.atal.idf.il    | Distributed Suspicious Response Code  | Block         | 2     |
| 84.111.216.183   | Israel             | 147.237.77.243 | mobile.idf.il        | Distributed Suspicious Response Code  | Block         | 1     |
| 157.55.39.205    | United States      | 147.237.77.216 | dover.idf.il         | Multiple Unauthorized URL Access from 157.55.39.205   | Block         | 1     |
| 109.253.158.113  | Israel             | 147.237.77.243 | mobile.idf.il        | Distributed Suspicious Response Code  | Block         | 1     |
| 66.249.66.26     | Israel             | 147.237.72.156 | aman.idf.il          | Unauthorized URL Access to www.aman.idf.il/mobile/  | Block         | 1     |
| 157.55.39.205    | United States      | 147.237.77.216 | dover.idf.il         | Unauthorized URL Access to www.idf.il/error.htm   | Block         | 1     |
| 156.212.206.6    | Egypt              | 147.237.77.176 | matpash.idf.il       | PHP Attempt   | Block         | 1     |
| 68.180.229.241   | United States      | 147.237.77.176 | matpash.idf.il       | Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx  | Block         | 1     |
| 2.52.179.179     | Israel             | 147.237.77.216 | dover.idf.il         | SSL Untraceable Connection - Open Mode  | None          | 1     |
| 157.55.39.161    | United States      | 147.237.77.216 | dover.idf.il         | Unauthorized URL Access to www.idf.il/1523-en/dover.aspx+idf blog   | Block         | 1     |
| 46.101.163.114   | Germany            | 147.237.77.233 | atal.idf.il          | Unauthorized URL Access to 147.237.77.233/  | Block         | 1     |
| 157.55.39.241    | United States      | 147.237.72.166 | aka.idf.il           | Unauthorized URL Access to aka.idf.il/main/sitemap.aspx   | Block         | 1     |
| 156.212.206.6    | Egypt              | 147.237.77.176 | matpash.idf.il       | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php  | Block         | 1     |
| 79.183.179.70    | Israel             | 147.237.72.166 | aka.idf.il           | SSL Untraceable Connection - Open Mode  | None          | 1     |
| 207.46.13.67     | United States      | 147.237.77.216 | dover.idf.il         | Abnormally Long Request URL   | Block         | 1     |
| 157.55.39.194    | United States      | 147.237.72.166 | aka.idf.il           | Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx                                    | Block         | 1     |
| 93.179.68.209    | United Kingdom     | 147.237.76.86  | navy.idf.il          | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/   | Block         | 1     |
| 66.249.65.12     | Israel             | 147.237.0.19   | madim.atal.idf.il    | Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association                                       | Block         | 1     |
| 176.13.21.11     | Israel             | 147.237.76.39  | mobile.meitav.idf.il | Parameter Type Violation ctl00\$ContentPlaceholder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx | Block         | 1     |
| 157.55.39.108    | United States      | 147.237.72.166 | aka.idf.il           | Unauthorized URL Access to aka.idf.il/main/misrot.aspx  | Block         | 1     |
| 37.187.114.171   | France             | 147.237.72.167 | ishurim.aka.idf.il   | Unauthorized URL Access to /irj/portal  | Block         | 1     |
| 157.55.39.194    | United States      | 147.237.76.200 | eitan.aka.idf.il     | Multiple Unauthorized URL Access from 157.55.39.194   | Block         | 1     |
| 109.65.50.56     | Israel             | 147.237.76.31  | nakchal.idf.il       | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc   | Block         | 1     |
| 66.249.65.223    | Israel             | 147.237.77.216 | dover.idf.il         | Unauthorized URL Access to 147.237.77.216/1380-he/dover.aspx  | Block         | 1     |
| 180.76.15.14     | China              | 147.237.76.42  | refuah.idf.il        | Unauthorized URL Access to 147.237.76.42/994-9697-he/refuah.aspx  | Block         | 1     |
| 157.55.39.108    | United States      | 147.237.72.166 | aka.idf.il           | Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx  | None          | 1     |