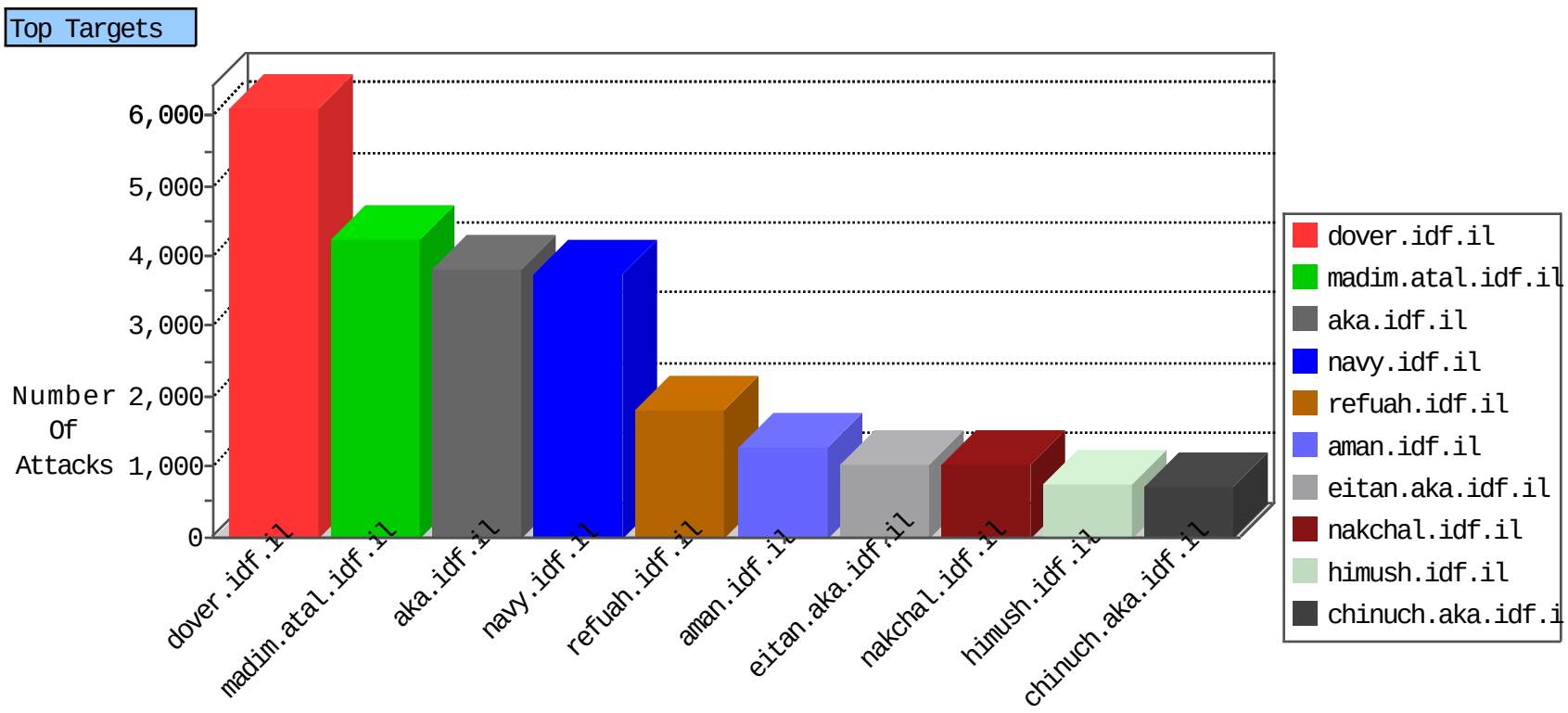
09-08-2016 to 09-09-2016

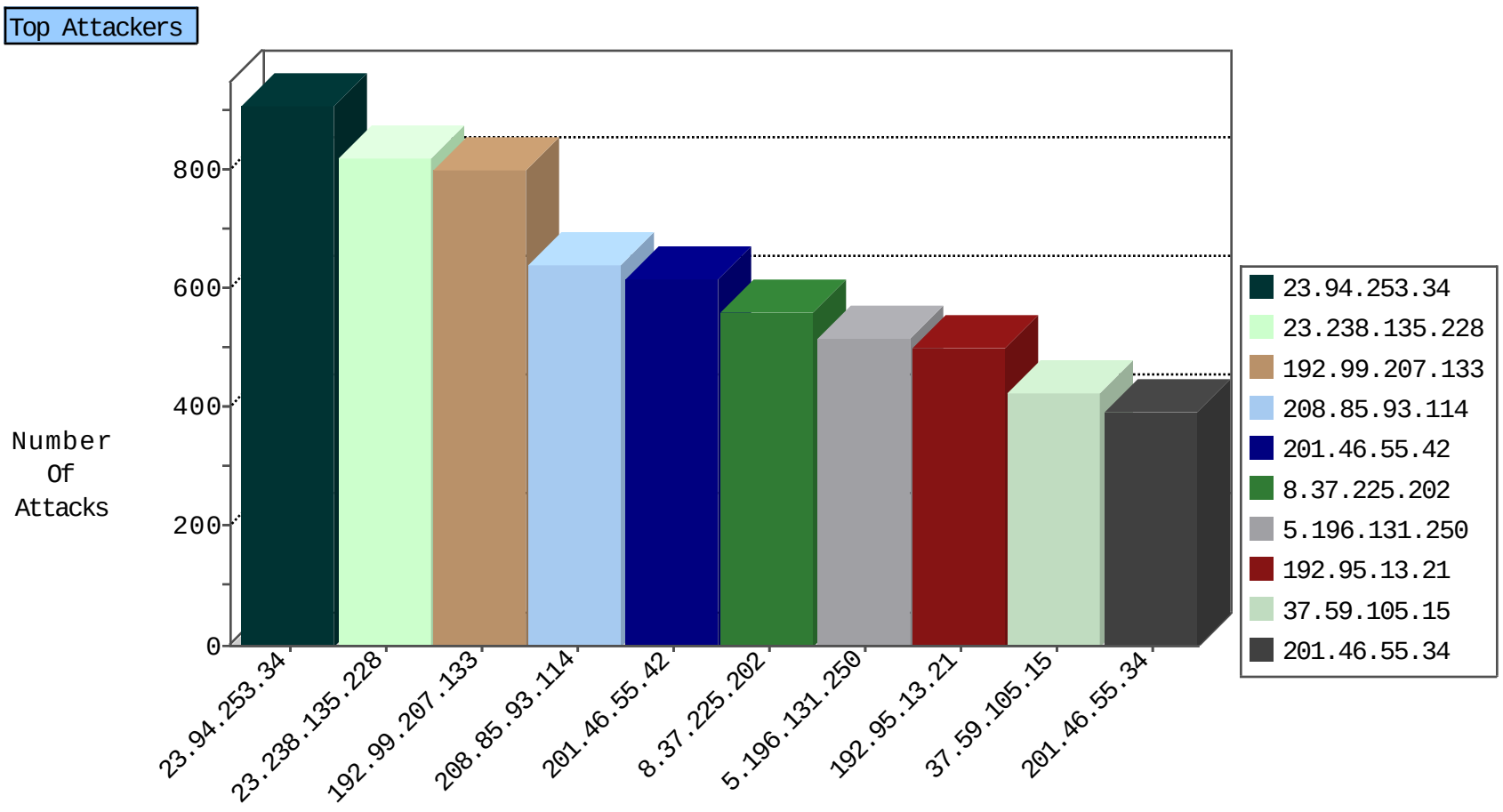
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

09-08-2016 to 09-09-2016

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 94.102.60.21 | Netherlands | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2776 |
| 109.67.160.125 | Israel | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 2236 |
| 212.199.154.194 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 392 |
| 109.67.160.125 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 144 |
| 46.19.86.143 | Israel | 147.237.77.216 | dover.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 89 |
| 46.19.86.246 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 16 |
| 212.143.165.165 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 16 |
| 212.143.187.240 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 12 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 10 |
| 132.76.61.52 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 8 |
| 212.25.74.130 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 6 |
| 176.13.18.245 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 6 |
| 109.67.228.32 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 5 |
| 156.205.14.33 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 37.142.3.0 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 77.139.89.242 | France | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 85.64.146.126 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 120.132.50.135 | China | 147.237.0.34 | tikshuv.idf.il | block-sp-traf1 | forward | 4 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 46.117.65.139 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 4 |
| 94.102.60.21 | Netherlands | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Url | dest-reset | 4 |
| 2.53.58.120 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 79.182.137.182 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 2.53.138.160 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 185.94.111.1 | Russian Federation | 147.237.76.201 | e.atal.idf.il | Black List | drop | 3 |
| 8.37.225.202 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 66.249.83.219 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 213.244.82.139 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 168.235.207.249 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 3 |
| 37.142.8.209 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 109.253.134.145 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 3 |
| 46.19.86.229 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 37.59.93.4 | France | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 58.218.200.137 | China | 147.237.76.176 | test.ncore.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 123.59.59.52 | China | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | forward | 2 |
| 185.94.111.1 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 2 |
| 58.218.200.137 | China | 147.237.76.177 | ncore.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 207.46.13.93 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 71.6.216.57 | United States | 147.237.76.201 | e.atal.idf.il | Black List | drop | 1 |
| 104.232.66.18 | United States | 147.237.76.176 | test.ncore.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 66.240.219.146 | United States | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 94.177.164.99 | Romania | 147.237.76.38 | e.e.meitav.idf.il | Black List | drop | 1 |
| 89.163.242.39 | Germany | 147.237.72.166 | aka.idf.il | Frk_Purple_Con_Limit_Tcp | drop | 1 |
| 149.202.57.201 | France | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 137.74.155.25 | Hong Kong | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |

09-08-2016 to 09-09-2016

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 206.248.70.7 | Puerto Rico | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 213 |
| 62.210.148.246 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 30 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 26 |
| 192.166.219.136 | Poland | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 26 |
| 188.40.95.70 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 23 |
| 62.210.148.246 | France | 147.237.76.200 | eitan.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 23 |
| 198.27.100.198 | Canada | 147.237.77.216 | dover.idf.il | C1000026: HTTP: Access to - index.php?option=com_jce | Permit | 18 |
| 206.248.70.7 | Puerto Rico | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 16 |
| 62.210.148.246 | France | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 10 |
| 69.30.221.242 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 9 |
| 192.166.219.136 | Poland | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 7 |
| 192.166.219.136 | Poland | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 7 |
| 184.168.46.19 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 69.30.198.242 | United States | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 6 |
| 77.67.47.7 | France | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 199.58.86.206 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 83.149.126.98 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 198.27.100.198 | Canada | 147.237.77.216 | dover.idf.il | 22280: HTTP: Joomla Object Injection Vulnerability | Block | 4 |
| 162.210.196.130 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 51.254.97.218 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 206.248.70.7 | Puerto Rico | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 119.90.51.21 | China | 147.237.76.86 | navy.idf.il | 34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10) | Block | 2 |
| 91.209.51.22 | Ukraine | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 69.30.198.242 | United States | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 144.76.29.66 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 106.38.241.105 | China | 147.237.0.34 | tikshuv.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 2 |
| 92.222.94.120 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 199.58.86.209 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 149.202.48.246 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 51.255.51.249 | France | 147.237.77.226 | www.chamatz.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 5.9.89.170 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 69.30.198.242 | United States | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 149.202.48.246 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 61.135.189.125 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 2 |
| 106.38.241.105 | China | 147.237.76.86 | navy.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 2 |
| 162.210.196.100 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 5.29.217.24 | Israel | 147.237.72.156 | aman.idf.il | 32390: HTTP: Suspicious User-Agent (Mozilla) | Block | 2 |
| 69.30.221.242 | United States | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 91.209.51.22 | Ukraine | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 69.30.198.242 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 144.76.12.78 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 176.31.7.241 | France | 147.237.77.216 | dover.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.39 | mobile.meitav.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 151.80.31.163 | France | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 123.126.68.101 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |
| 198.20.69.74 | United States | 147.237.77.179 | e.mazi.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 64.137.242.231 | Canada | 147.237.77.216 | dover.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |
| 151.80.31.169 | France | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

09-08-2016 to 09-09-2016

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.102.6.117 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 36 |
| 66.249.64.107 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 30 |
| 79.178.136.47 | 147.237.0.19 | Israel | madim.atal.idf.il | ET SCAN NMAP -sA (2) | 16 |
| 77.67.47.7 | 147.237.77.74 | France | law.idf.il | SQL Injection - Select From | 10 |
| 46.120.122.219 | 147.237.77.176 | Israel | matpash.idf.il | Xenu Link Sleuth User Agent | 10 |
| 46.120.122.219 | 147.237.77.74 | Israel | law.idf.il | Xenu Link Sleuth User Agent | 10 |
| 82.80.157.30 | 147.237.76.147 | Israel | chinuch.aka.idf.il | ET SCAN NMAP -sA (2) | 9 |
| 184.168.46.19 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 7 |
| 91.121.143.113 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 6 |
| 62.210.113.183 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 6 |
| 45.79.103.178 | 147.237.72.166 | United States | aka.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 5 |
| 185.27.106.90 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 62.210.97.57 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 4 |
| 45.79.71.122 | 147.237.0.34 | United States | tikshuv.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 4 |
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 4 |
| 79.181.136.76 | 147.237.72.156 | Israel | aman.idf.il | ET SCAN NMAP -sA (2) | 3 |
| 109.66.29.242 | 147.237.0.34 | Israel | tikshuv.idf.il | ET SCAN NMAP -sA (2) | 3 |
| 79.177.238.90 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 3 |
| 94.102.48.195 | 147.237.76.177 | Netherlands | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.79.103 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 80.246.137.30 | 147.237.0.19 | Israel | madim.atal.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 2 |
| 91.121.136.34 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 132.252.173.4 | 147.237.77.216 | Germany | dover.idf.il | GPL SCAN nmap TCP | 2 |
| 45.79.103.178 | 147.237.0.34 | United States | tikshuv.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 2 |
| 91.224.160.106 | 147.237.76.38 | Netherlands | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 195.88.208.193 | 147.237.77.205 | Russian Federation | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 218.24.171.223 | 147.237.8.24 | China | e.lifestyle.idf.il | GPL SCAN nmap TCP | 2 |
| 62.210.38.242 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 59.67.64.13 | 147.237.77.121 | China | e.navy.idf.il | GPL SCAN nmap TCP | 2 |
| 45.56.96.80 | 147.237.77.216 | United States | dover.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 2 |
| 195.88.208.193 | 147.237.77.19 | Russian Federation | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 69.164.205.7 | 147.237.76.31 | United States | nakchal.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 2 |
| 195.88.208.193 | 147.237.76.38 | Russian Federation | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 195.88.208.193 | 147.237.0.15 | Russian Federation | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 46.19.85.207 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 58.218.200.137 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.121.147.218 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 91.121.142.227 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 77.138.22.23 | 147.237.77.216 | France | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 58.218.200.137 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 192.114.1.155 | 147.237.77.74 | Israel | law.idf.il | WEB-FRONTPAGE /_vti_bin/ access | 2 |
| 62.210.113.216 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 59.46.193.114 | 147.237.8.24 | China | e.lifestyle.idf.il | GPL SCAN nmap TCP | 2 |
| 195.88.208.193 | 147.237.76.177 | Russian Federation | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 46.120.122.219 | 147.237.77.170 | Israel | maarachot.idf.il | Xenu Link Sleuth User Agent | 2 |
| 178.62.224.34 | 147.237.76.31 | Netherlands | nakchal.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 2 |
| 54.72.0.55 | 147.237.77.216 | Ireland | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 37.48.93.217 | 147.237.77.178 | Netherlands | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 108.12.246.131 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 84.111.66.18 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

09-08-2016 to 09-09-2016

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 8.37.225.202 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 495 |
| 68.193.171.170 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 228 |
| 108.61.129.93 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 198 |
| 207.248.203.19 | Chile | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 191 |
| 98.30.244.225 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 141 |
| 108.61.129.97 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 140 |
| 168.235.207.249 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 139 |
| 23.94.253.34 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 110 |
| 23.94.253.34 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 110 |
| 23.94.253.34 | United States | 147.237.76.39 | mobile.meitav.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 109 |
| 23.94.253.34 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 109 |
| 23.94.253.34 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 109 |
| 23.94.253.34 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 107 |
| 23.94.253.34 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 106 |
| 23.94.253.34 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 105 |
| 192.99.207.133 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 99 |
| 192.99.207.133 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 99 |
| 192.99.207.133 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 98 |
| 192.99.207.133 | Canada | 147.237.76.39 | mobile.meitav.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 98 |
| 192.99.207.133 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 98 |
| 192.99.207.133 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 98 |
| 85.98.232.203 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 97 |
| 192.99.207.133 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 97 |
| 192.99.207.133 | Canada | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 96 |
| 23.238.135.228 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 94 |
| 23.238.135.228 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 93 |
| 23.238.135.228 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 93 |
| 23.238.135.228 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 91 |
| 23.238.135.228 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 91 |
| 23.238.135.228 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 89 |
| 23.238.135.228 | United States | 147.237.76.39 | mobile.meitav.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 89 |
| 23.238.135.228 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 88 |
| 77.124.242.69 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 87 |
| 108.61.129.99 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 83 |
| 209.6.205.183 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 80 |
| 201.46.55.42 | Brazil | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 73 |
| 201.46.55.42 | Brazil | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 73 |
| 201.46.55.42 | Brazil | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 72 |
| 89.139.132.84 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 72 |
| 84.94.41.253 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 69 |
| 152.156.247.233 | Uruguay | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 69 |
| 201.46.55.42 | Brazil | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 66 |
| 194.28.132.100 | Ukraine | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 66 |
| 201.46.55.42 | Brazil | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 66 |
| 108.61.135.13 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 66 |
| 208.85.93.114 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 63 |
| 208.85.93.114 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 63 |
| 108.61.232.109 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 62 |
| 208.85.93.114 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 62 |
| 208.85.93.114 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 62 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 80.246.136.231 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 301 |
| 2.55.25.168 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 263 |
| 37.26.149.129 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 242 |
| 89.138.170.137 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 184 |
| 80.246.137.30 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 176 |
| 176.13.9.104 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 163 |
| 109.253.241.146 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 159 |
| 176.13.248.0 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 154 |
| 109.253.211.166 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 146 |
| 5.102.242.178 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 135 |
| 109.253.198.179 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 122 |
| 77.124.29.241 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 112 |
| 77.127.76.238 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 110 |
| 46.19.85.99 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 105 |
| 2.53.145.196 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 94 |
| 5.102.192.140 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 91 |
| 176.13.231.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 80 |
| 2.53.55.179 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 77 |
| 37.26.149.184 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 73 |
| 46.19.85.177 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 69 |
| 46.19.85.71 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 64 |
| 46.117.108.240 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 63 |
| 79.181.217.56 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 60 |
| 176.13.16.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 59 |
| 2.53.150.43 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 52 |
| 109.253.202.121 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 51 |
| 176.13.12.76 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 50 |
| 37.26.149.176 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 44 |
| 2.53.0.165 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 44 |
| 176.13.20.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 37 |
| 46.19.85.151 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 33 |
| 109.186.76.154 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 33 |
| 113.71.255.4 | China | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 113.71.255.4 | Block | 30 |
| 37.26.146.142 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 2.53.17.62 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 29 |
| 176.13.233.8 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 27 |
| 37.26.147.175 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 25 |
| 79.178.24.19 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 79.178.24.19 | Block | 25 |
| 37.26.149.136 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 24 |
| 80.246.137.39 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 24 |
| 109.253.134.145 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 23 |
| 176.13.16.43 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 23 |
| 192.114.1.155 | Israel | 147.237.77.74 | law.idf.il | Distributed Unauthorized HTTP Method | Block | 22 |
| 85.64.219.23 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 85.64.219.23 | Block | 22 |
| 212.179.21.194 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 212.179.21.194 | Block | 20 |
| 85.64.219.23 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx | Block | 20 |
| 2.55.145.73 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 20 |
| 46.19.86.19 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 19 |
| 2.53.59.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 19 |
| 218.17.231.155 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 218.17.231.155 | Block | 18 |

09-08-2016 to 09-09-2016