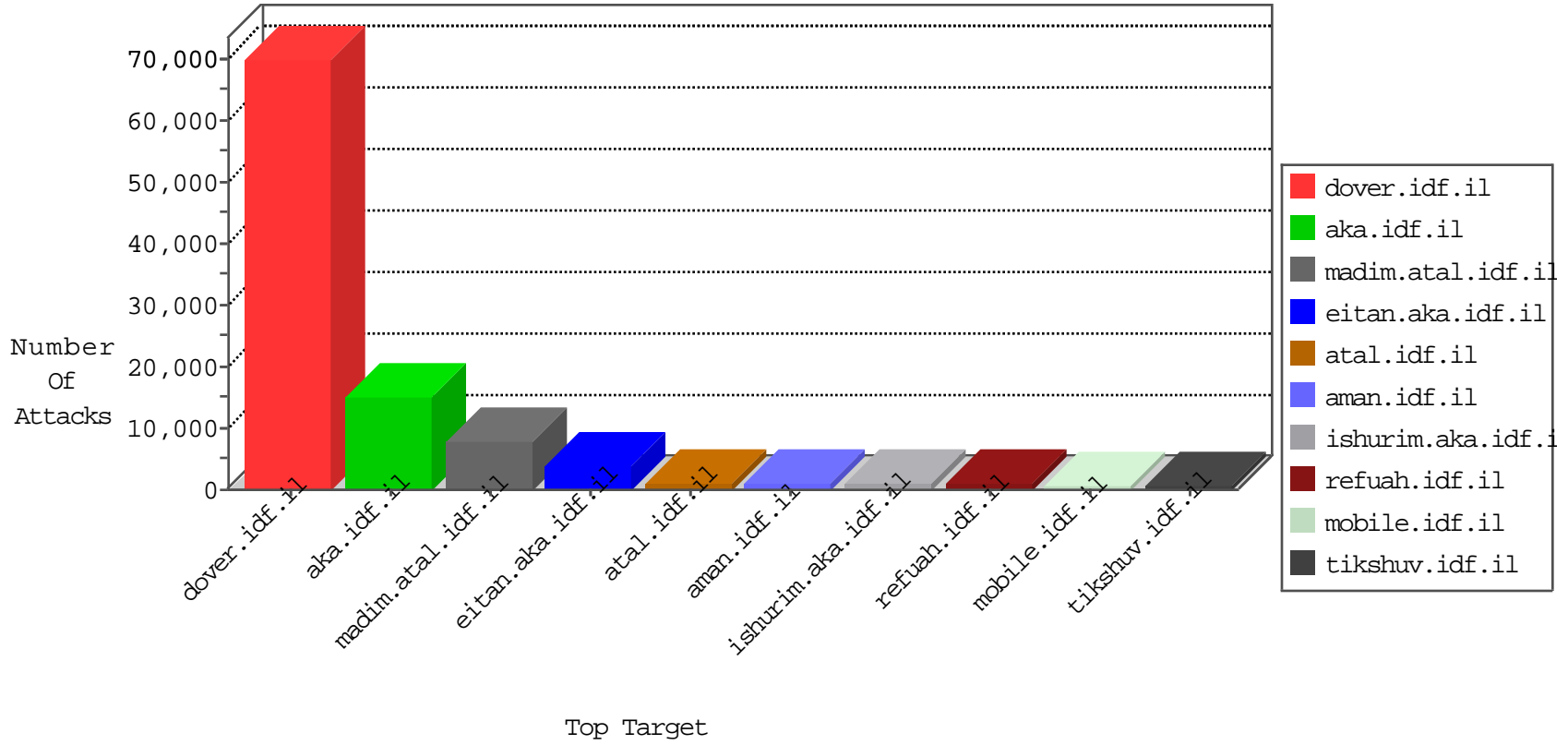


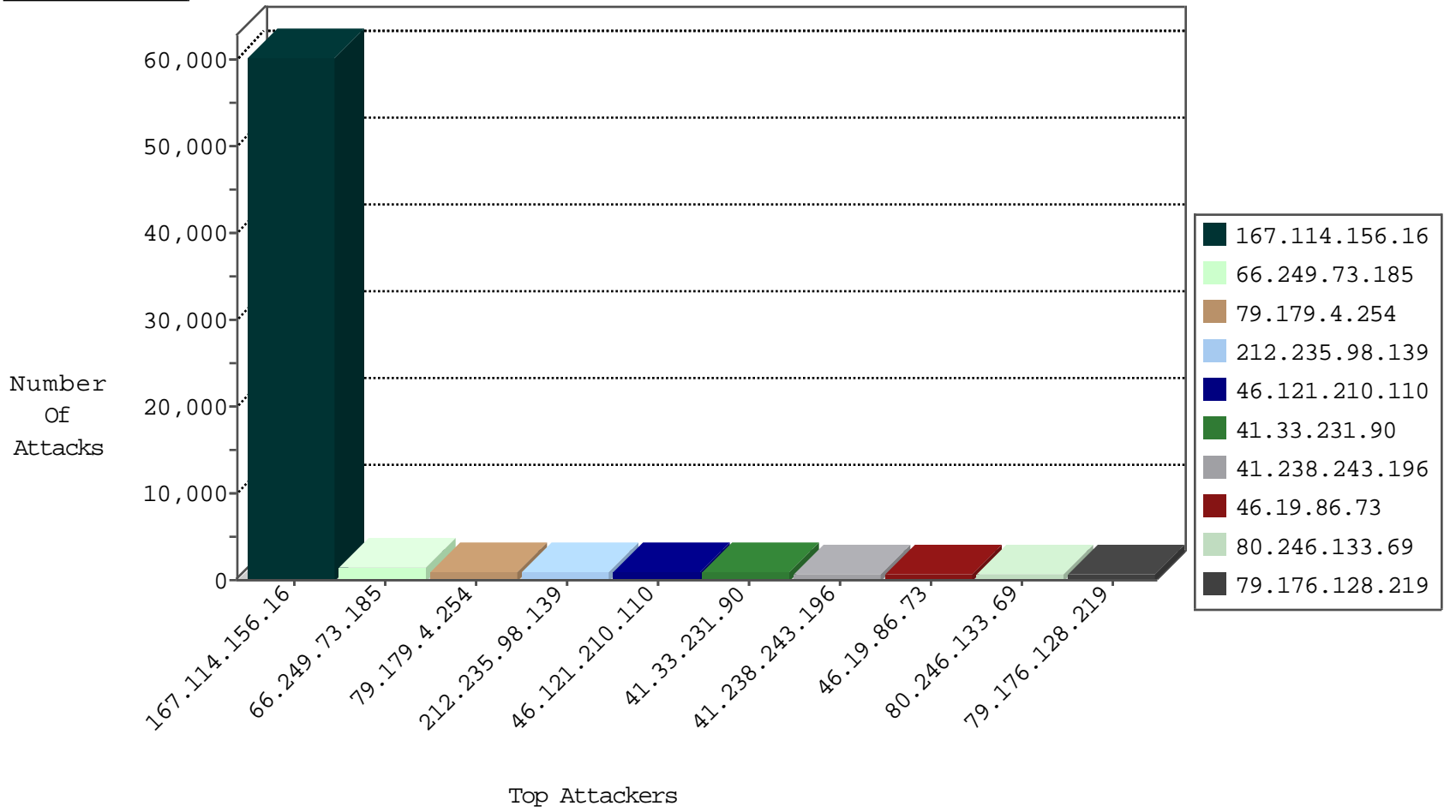
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	92521
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10565
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4621
66.249.66.78	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	968
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	920
71.232.12.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	452
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	371
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	234
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	179
198.240.128.75	United Kingdom	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	148
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	132
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block Udp_All_Nets	drop	108
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	101
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	82
37.26.147.225	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	58
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	53
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	22
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	15
82.145.209.86	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
149.88.190.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block Udp_All_Nets	drop	9
149.88.190.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
79.177.183.157	Israel	147.237.72.156	aman.idf.il	Block Udp_All_Nets	drop	6
82.145.217.93	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block Udp_All_Nets	drop	5
84.108.235.46	Israel	147.237.0.34	tikshuv.idf.il	Block Udp_All_Nets	drop	4
84.108.235.46	Israel	147.237.77.216	dover.idf.il	Block Udp_All_Nets	drop	4
114.161.225.244	Japan	147.237.76.39	mobile.meitav.idf.il	Block Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.170	maarachot.idf.il	Block Udp_All_Nets	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block Udp_All_Nets	drop	3
46.242.113.131	Russian Federation	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	3
84.111.196.22	Israel	147.237.72.166	aka.idf.il	Block Udp_All_Nets	drop	3
178.214.66.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block Udp_All_Nets	drop	3
198.58.102.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
178.214.66.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
92.232.155.105	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
115.230.124.164	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.196	e.sviva.idf.il	Block Udp_All_Nets	drop	2
105.98.250.253	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	14
41.185.31.40	South Africa	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
213.8.145.99	Israel	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
209.173.241.141	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
94.73.145.90	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.208.133.60	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	8
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
203.171.41.47	New Zealand	147.237.77.233	atal.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	8
74.208.133.60	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
41.185.31.40	South Africa	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
63.143.34.37	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	5
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	5
212.199.63.46	Israel	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	5
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	4
24.47.146.194	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
31.154.190.209	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
89.138.243.60	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
89.202.105.211	Germany	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
64.186.146.196	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
188.165.15.160	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	3
2.54.134.110	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.194.4.65	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.186.160.125	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
80.179.8.225	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
185.120.125.9		147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.150.245.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
193.105.199.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.15.193	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
79.178.181.48	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.196	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
41.185.31.40	South Africa	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
167.114.242.198	Canada	147.237.76.39	mobile.meitav.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
91.121.112.142	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.227	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.29.28.154	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
93.172.162.134	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
64.186.146.196	United States	147.237.77.216	dover.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
198.20.69.74	United States	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
24.47.146.194	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.106.241.59	Germany	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	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	71
41.185.31.40	147.237.76.31	South Africa	nakchal.idf.il	SQL Injection - Select From	34
23.91.70.95	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	26
63.143.34.37	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	24
213.8.145.99	147.237.72.166	Israel	aka.idf.il	SQL Injection - Select From	24
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
94.73.145.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	15
2.54.37.208	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
209.173.241.141	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	11
95.211.70.193	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	10
203.171.41.47	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	8
24.47.146.194	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
64.186.146.196	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	6
203.171.41.47	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	6
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	5
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	4
149.78.56.233	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	3
162.216.19.183	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
66.249.78.120	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
111.49.145.192	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
194.114.146.227	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.134	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
92.54.208.167	147.237.77.216	Georgia	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.196	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.80.31	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.252	147.237.76.177	Ukraine	noore.idf.il	ET SCAN NMAP -sS window 1024	1
121.40.144.59	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
2.54.174.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.226	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.97.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.157.244.243	147.237.72.166	Somalia	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
176.13.2.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.85.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
118.69.135.26	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN Potential SSH Scan	1



## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1383
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	927
79.179.4.254	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	813
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	800
46.121.210.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	783
80.246.133.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	632
2.54.165.180	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	492
2.54.164.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	477
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	451
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	340
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	340
109.66.214.100	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	243
77.127.182.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	212
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	198
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
31.9.9.228	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
85.130.141.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	174
85.130.141.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	173
213.57.128.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	159
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	146
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	146
213.57.143.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	137
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	133
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	130
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	128
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	122
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
41.238.243.196	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	112
2.54.56.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	104
68.67.73.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	101
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	100
212.179.214.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
100.100.116.202		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	75
100.100.80.152		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	71
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
100.100.124.9		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	68
84.109.92.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
213.57.128.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
109.66.173.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
79.183.101.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
213.57.143.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
5.29.212.11	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
213.57.143.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	60
212.179.214.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
167.114.156.198	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	60
213.57.53.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	60

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	475
79.176.128.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	393
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	322
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	272
176.13.17.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	240
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	224
109.66.214.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	224
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	186
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
79.179.4.254	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
79.178.175.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
79.178.151.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	161
46.121.210.110	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.210.110	Block	153
176.13.10.209	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	141
176.13.17.27	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.17.27	Block	139
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
79.176.128.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
109.67.175.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
176.13.17.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
95.35.64.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.24.188	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 2.54.24.188	Block	107
37.26.148.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
2.54.18.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
79.179.140.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
2.54.18.121	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.18.121	Block	100
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.56	Block	100
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
2.54.178.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
5.29.212.11	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
2.54.178.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
176.12.138.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
176.12.147.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
95.35.64.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	77
79.180.125.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
80.246.136.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
2.54.41.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	65
37.26.147.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
109.67.191.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.107	Block	59
176.12.143.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.54.165.180	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.165.180	Block	55
2.54.164.212	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
176.12.144.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
176.13.3.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50