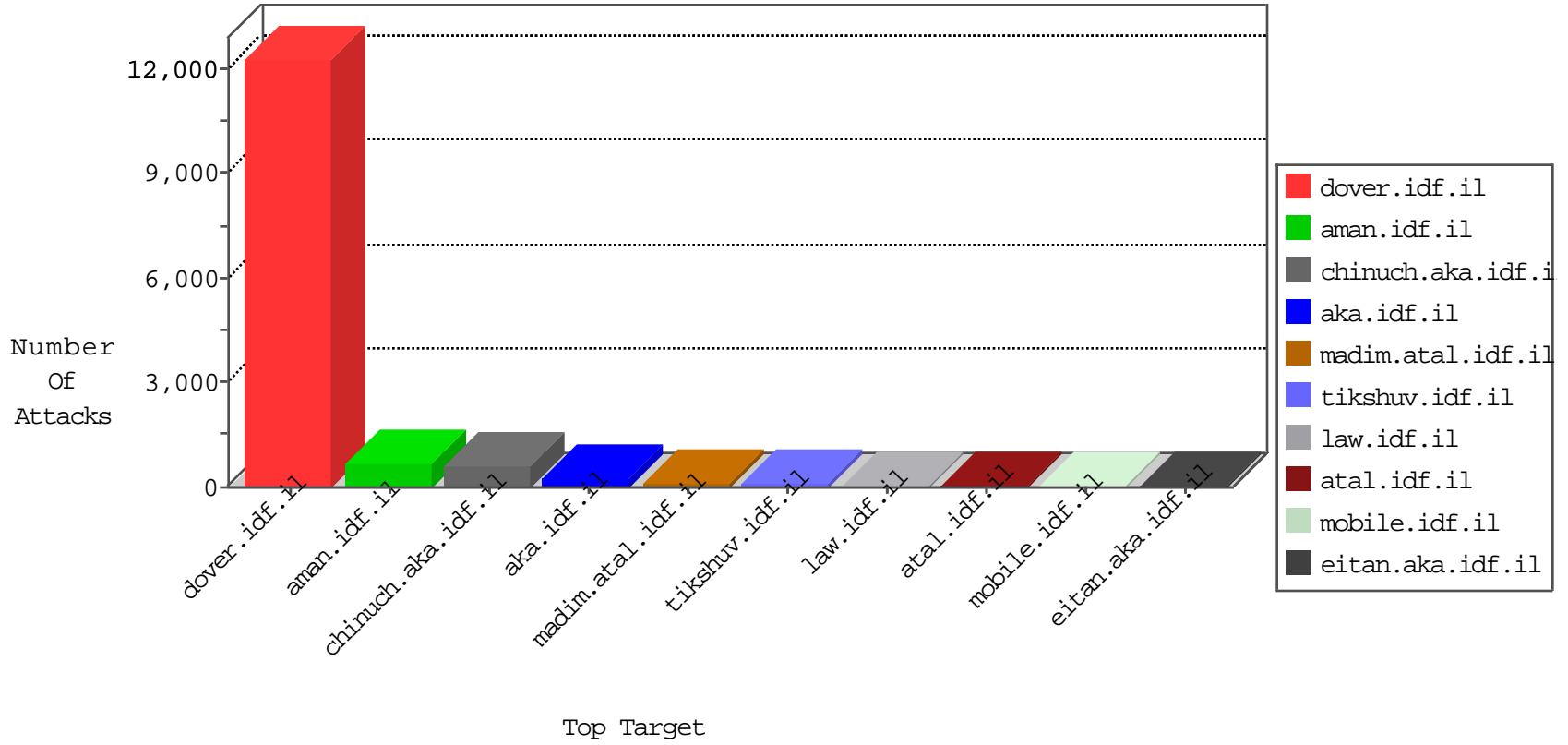


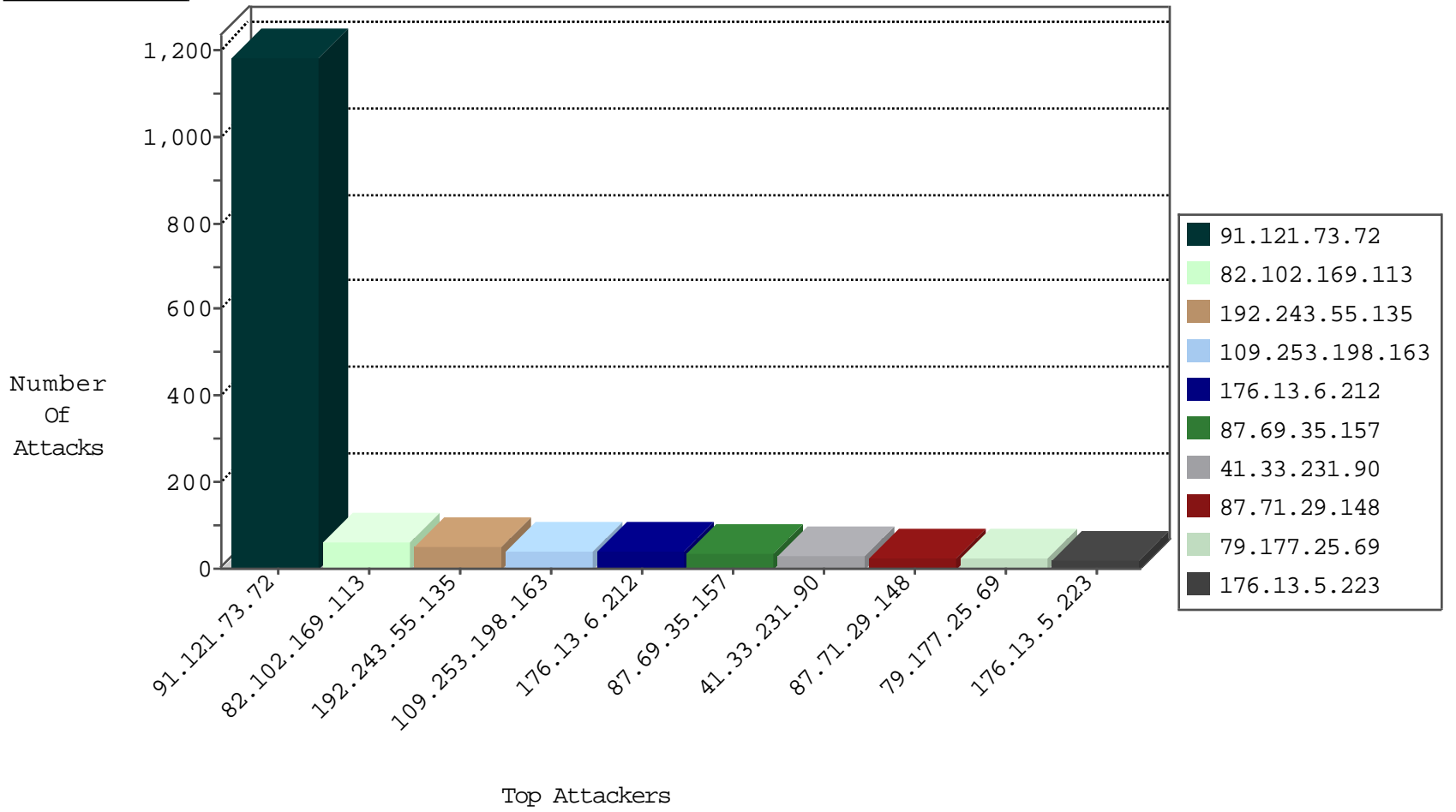
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.93.245.246	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34631
219.1.32.108	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34237
96.118.141.93	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34232
35.224.81.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34143
71.137.4.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34026
21.3.68.85	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33967
16.162.182.64	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33815
143.229.217.226	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33697
16.116.98.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33377
148.239.24.106	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32947
155.52.16.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32876
205.93.155.250	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32790
172.97.199.27		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32756
43.110.84.160	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32754
156.122.37.165	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32679
193.114.122.37	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32495
78.233.176.246	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32383
239.59.76.138		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32372
102.147.55.242		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32328
97.43.233.14	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32327
237.10.43.152		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32276
120.123.112.168	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32259
19.145.248.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32220
113.124.54.219	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32202
111.64.247.99	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32155
208.97.84.238	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32150
115.153.49.28	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32131
246.163.99.95		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32101
45.39.68.81		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32100
229.16.56.84		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32097
238.130.101.45		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32096
210.226.121.38	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32081
215.151.159.202	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32063
36.38.139.33	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32060
107.123.114.115	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32048
24.195.34.18	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32017
0.124.163.241		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31996
222.234.48.234	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31980
237.87.228.169		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31959
16.215.180.222	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31951
85.64.62.200	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31948
85.17.29.72	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31946
167.236.229.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31921
247.203.216.9		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31889
33.91.243.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31838
25.90.125.161	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31783
204.13.219.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31777
211.136.123.95	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31702
118.240.120.95	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31689
215.82.179.31	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31669

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.25.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
213.57.34.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.177.186	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.70.84.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.181.183.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
192.116.55.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
94.159.209.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
245.89.129.227		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
247.1.61.217		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
247.168.68.175		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
241.211.16.132		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
243.132.163.213		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
249.87.21.36		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
243.167.127.236		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
251.7.108.117		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
252.198.102.63		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
245.135.26.229		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.42.255.25		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
254.139.237.193		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
248.127.77.40		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
241.252.241.225		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
250.44.231.47		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
251.221.240.157		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
244.140.141.150		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
253.164.32.165		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
246.77.88.21		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.255.97.31		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
255.114.159.234		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
242.212.62.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
245.117.155.163		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
247.26.235.91		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
247.189.6.245		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
249.106.221.99		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
243.196.9.175		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
251.25.128.2		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
252.219.242.170		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
245.156.79.204		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.66.253.141		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
254.162.196.137		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
248.144.219.26		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
242.20.138.72		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
250.69.44.156		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
251.245.212.120		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
244.165.55.64		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
253.186.40.12		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
246.98.50.203		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
241.23.158.186		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
255.134.217.233		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
242.231.95.196		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
247.212.219.103		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.72.179.221	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.228.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.54.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.121.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.103.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.180.215.112	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.136.91.26	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.147.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.238.99	147.237.77.243	France	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.166.208.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.106.154.88	147.237.76.31	Mexico	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.27.85.27	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
189.202.241.84	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -sS window 2048	1
79.178.118.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.67	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.162	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.254.212	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
2.54.32.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.136.91.26	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.91.26	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1
93.173.147.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.184.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.212.40.229	147.237.77.216	Slovakia	dover.idf.il	portscan: TCP Distributed Portscan	1
212.47.238.99	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.81.19.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -sS window 4096	1
79.180.6.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -f -sS	1
46.120.164.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.73.72	France	147.237.72.156	aman.idf.il	drop	SAM rule	drop	593
91.121.73.72	France	147.237.76.147	chimuch.aka.idf.il	drop	SAM rule	drop	593
87.69.35.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
176.13.6.212	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
87.71.29.148	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
176.13.5.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
92.236.75.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
80.246.133.224	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
109.253.211.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.196.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.177.35	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.111.41.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.183.195.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
156.33.255.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.175.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.6.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.142.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.92.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.85.68.68	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.253.205.236	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
197.252.0.134	Sudan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.142.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
46.19.85.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.84	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.2.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.17.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.166.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.11.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.127.3.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.145.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.70.72.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3



## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
109.253.198.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
84.109.9.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.9.72	Block	13
79.176.177.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main /giyus	Block	4
109.253.131.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.211.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
66.249.84.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.71.140.53	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	2
80.246.130.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.27.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.66.74	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
109.160.253.216	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
89.3.154.247	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
37.26.146.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.253.137	France	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
84.109.9.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
109.253.205.236	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
92.255.208.54	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
5.157.57.82	Sweden	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
207.241.229.223	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
81.218.179.164	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
176.241.250.4	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.129.72	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
89.3.154.247	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
37.142.189.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.253.137	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
84.111.41.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
79.176.217.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpSachar\$ct163 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.121.136.195	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
95.86.112.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/recruitlane.aspx&sa=u&ved=0ahukewiu7zkegkxlahwgwiwkhyppbzgqjbaifa&usg=afqjncneucsy18h8d_v65qc-rs_u7_on_gfw	Block	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 17.142.156.171	Block	1
207.241.229.223	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.114.119.2	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
89.138.82.144	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
40.77.167.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
198.20.87.98	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
84.228.24.43	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.221.226	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/927-he/atal.aspx	Block	1
106.185.28.171	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
85.114.119.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
207.241.229.224	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 207.241.229.224	Block	1