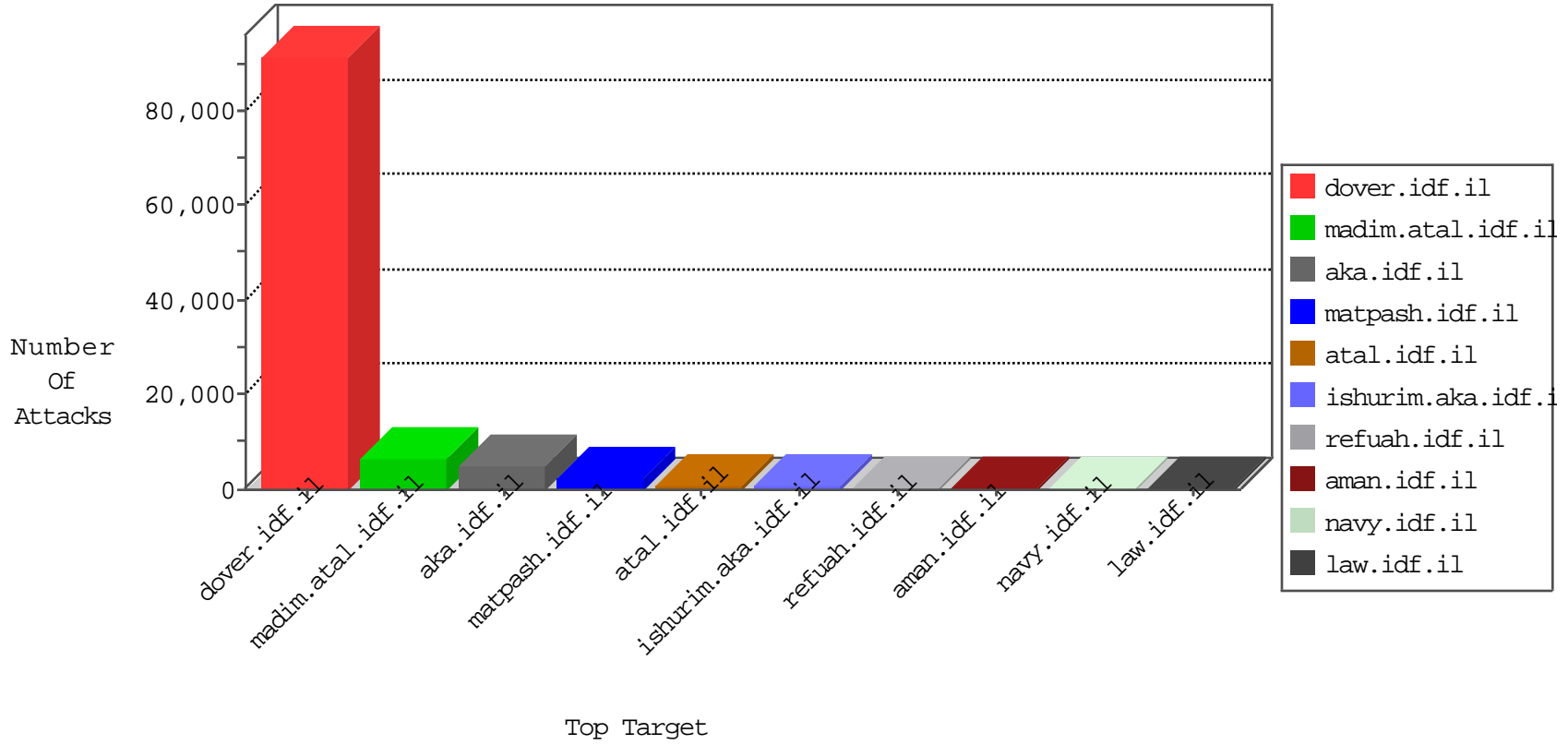


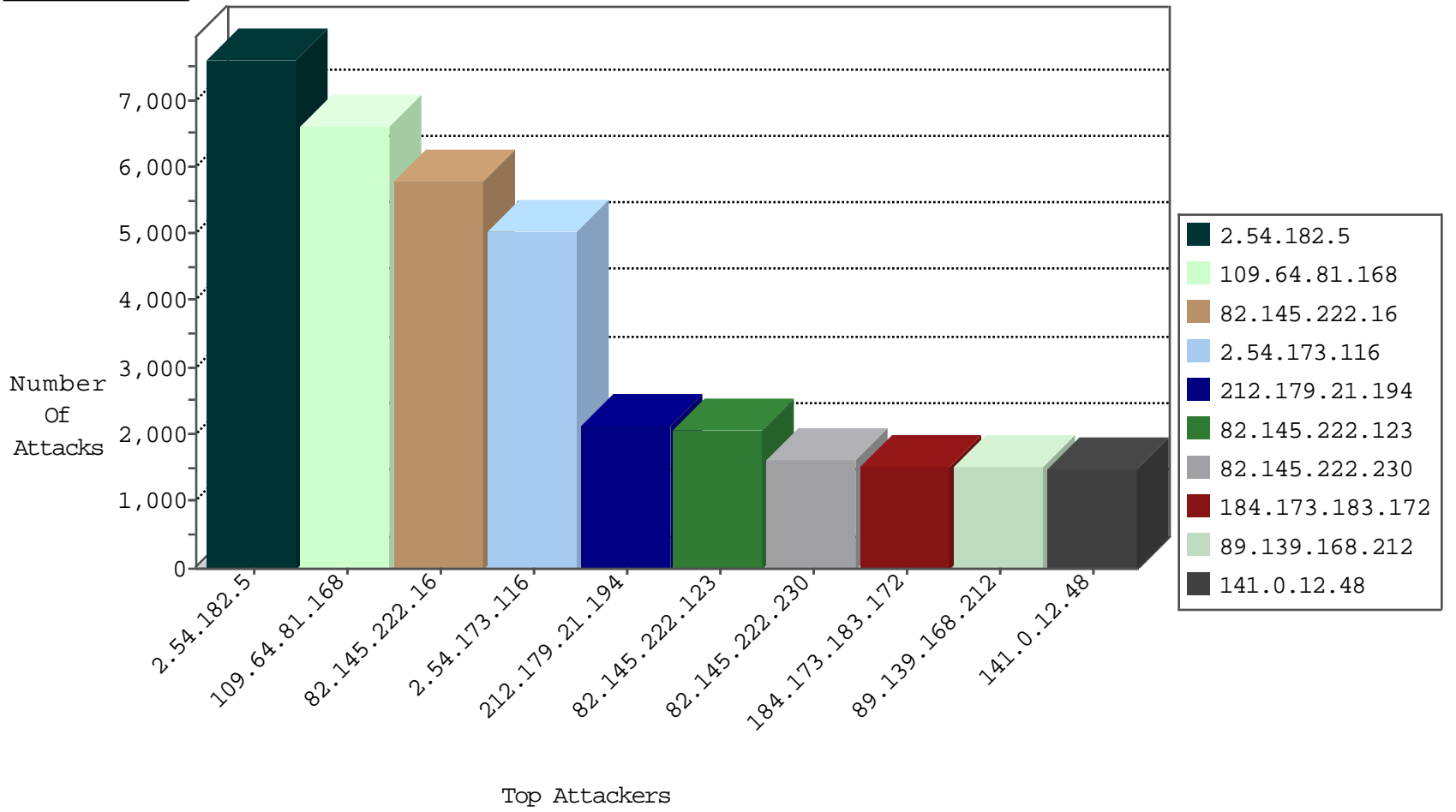
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
89.139.168.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5641
109.64.81.168	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4239
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3759
46.19.85.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3406
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3175
212.179.46.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3072
81.218.181.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2774
82.145.221.5	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2506
141.0.12.48	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1439
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1210
220.181.108.108	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	839
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	615
85.65.222.105	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	528
76.29.159.90	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
109.64.81.168	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	394
212.76.112.32	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
109.67.58.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	347
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	343
213.57.195.79	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
81.218.104.83	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
77.125.84.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	223
79.183.161.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
31.168.244.253	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
220.181.108.156	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	196
79.176.134.84	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
79.181.34.170	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
5.29.155.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
109.253.149.254	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	162
220.181.108.82	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	159
213.57.48.130	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
194.90.119.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	127
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
109.64.204.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
46.116.152.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
132.74.151.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
220.181.108.162	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	114
84.228.41.141	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
213.151.35.218	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
109.66.101.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	101
80.246.136.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
2.54.55.185	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
80.246.136.132	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
2.54.158.59	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1481
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	811
85.65.224.210	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	490
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	351
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	305
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	156
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	114
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	23
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
81.218.251.252	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
79.176.134.84	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
5.144.57.166	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
193.47.165.251	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	7
37.26.147.171	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
85.250.207.169	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
91.230.121.131	Ukraine	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	6
85.250.157.2	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	6
212.116.172.230	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
84.109.89.178	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.143.158.153	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.226.41.252	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	6
37.26.147.171	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
212.143.172.110	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
5.29.91.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5
85.250.186.146	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
212.25.102.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5

Top Attackers In IDF

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	201
80.246.136.225	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
89.139.168.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	4
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
80.246.136.103	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
183.131.76.133	China	147.237.76.31	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
61.183.128.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.132	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.188	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.132	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
81.218.229.29	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.132	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.83.153	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
169.54.233.120	Switzerland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
31.168.244.253	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.132	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.24	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
200.53.156.245	Mexico	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.132	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.244	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.81	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.188.33.146	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.131.157	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.131	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.216.121	Netherlands	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
209.222.234.58	Canada	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.188.189.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
141.212.122.122	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.133	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
103.56.71.31		147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
37.78.250.202	Russian Federation	147.237.77.176	matpash.idf.il	GPL WEB_SERVER webalizer access	1
79.182.134.113	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.130	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
82.80.196.44	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.182.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7614
82.145.222.16	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5795
2.54.173.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5052
82.145.222.123	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2080
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2046
82.145.222.230	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1615
141.0.12.48	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1502
89.139.168.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1472
109.64.81.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1298
95.86.111.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1135
2.54.169.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1037
46.19.86.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	965
77.127.158.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	948
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	918
46.19.85.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	891
82.145.222.121	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	708
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	681
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	593
2.54.165.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	576
131.137.245.209	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	490
212.179.57.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	485
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	455
160.79.39.236	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	441
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	426
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	421
109.64.81.168	Israel	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	413
200.53.156.245	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	405
2.54.2.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	355
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	347
8.37.228.95	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	345
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
78.182.38.208	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
213.151.35.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	306
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	303
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	300
213.57.118.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
37.231.21.218	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
82.145.221.208	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	281
82.145.221.5	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	275
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	269
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	250
82.145.220.219	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	244
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	242
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	242
5.102.254.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	239
46.210.114.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	213

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.51.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	967
80.246.136.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.225	Block	874
80.246.136.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	638
46.19.85.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.231	Block	401
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	392
176.12.146.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.146.77	Block	368
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	327
91.135.102.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	323
2.52.159.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	246
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.123	Block	225
176.12.149.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	224
2.52.178.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
37.26.146.178	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.178	Block	201
109.64.81.168	Israel	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 109.64.81.168	Block	183
149.78.12.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
109.64.81.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	173
46.19.86.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	171
46.120.50.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
176.12.147.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
46.116.188.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	111
176.12.144.105	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.144.105	Block	96
2.54.152.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	83
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	83
94.159.151.62	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.159.151.62	Block	49
176.12.148.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	44
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	25
5.28.137.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
66.249.64.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
217.66.243.171	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	19
85.65.11.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.11.95	Block	16
79.176.96.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
94.230.86.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	14
5.29.24.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	11
212.199.75.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.75.29	Block	11
79.182.182.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
212.179.21.194	Israel	147.237.77.74	law.idf.il	Suspicious Response Code	Block	10
213.151.37.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
87.68.231.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
66.249.64.92	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	9
79.178.31.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
77.127.231.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
109.160.134.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8