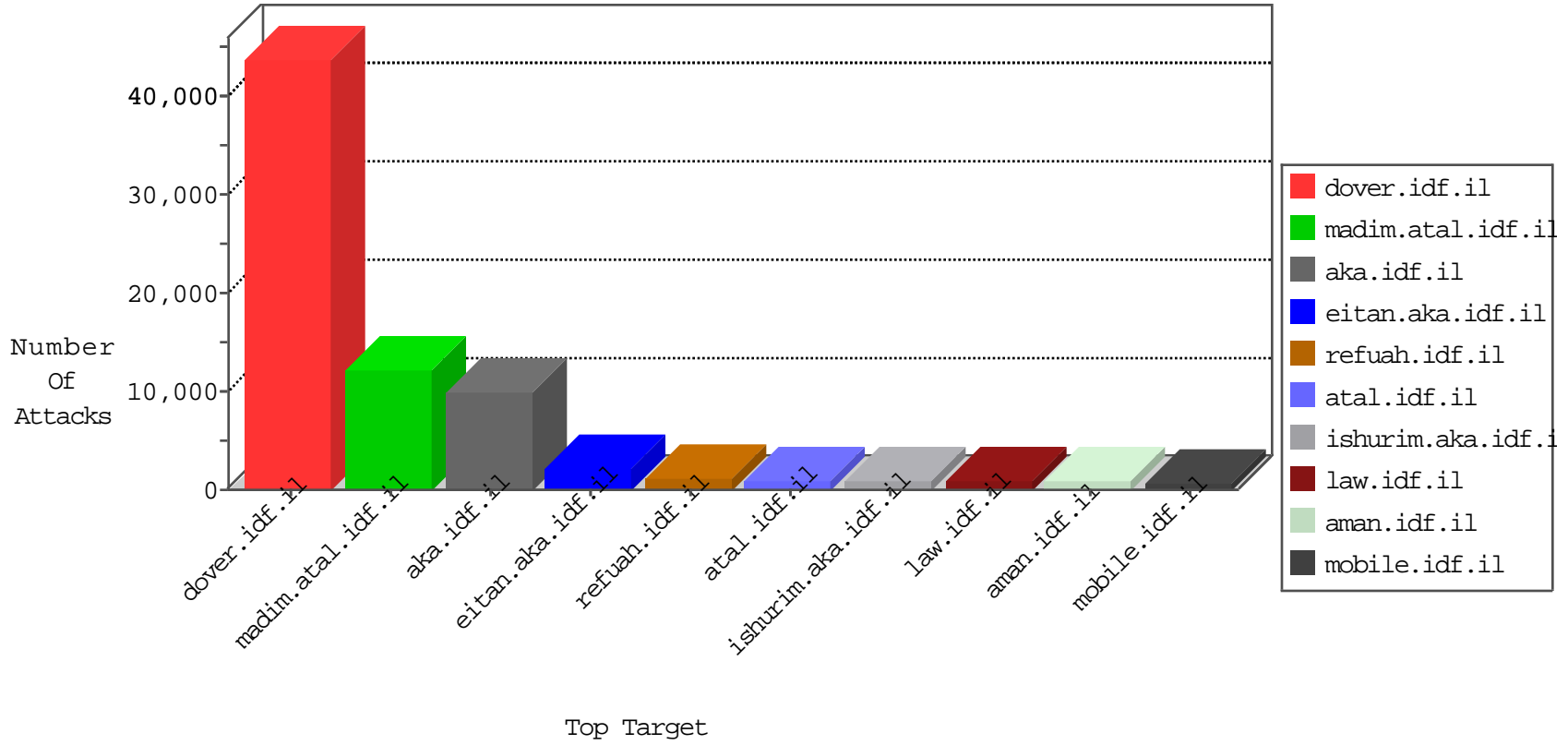


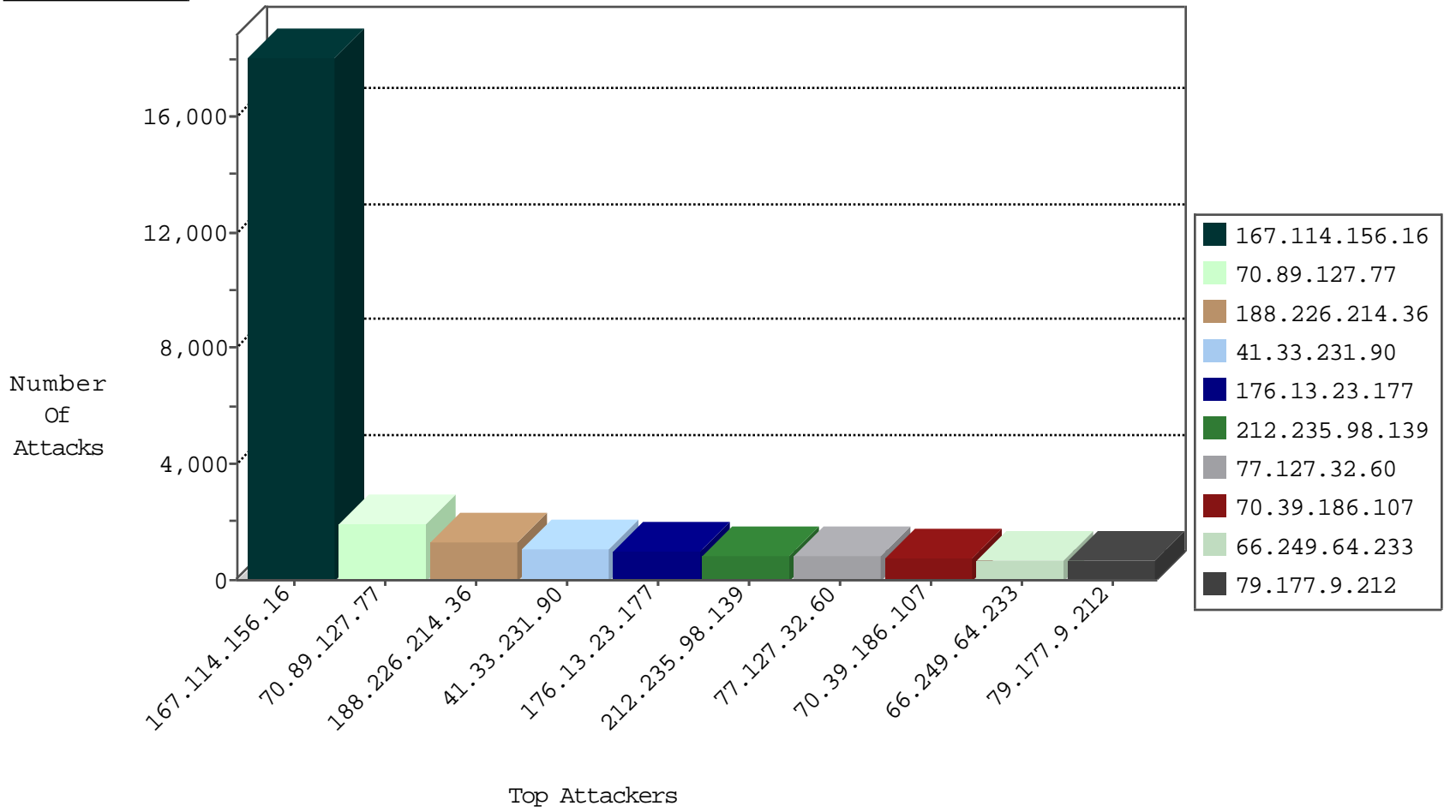
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
169.241.28.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	546405
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	58990
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9615
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8251
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7584
66.249.64.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6722
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4990
66.249.64.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3180
66.249.66.107	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3143
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	992
66.249.78.15	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	907
66.249.93.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	628
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	419
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	407
66.249.64.200	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	404
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
167.114.156.198	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	212
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	182
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	77
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	62
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	36
37.26.146.227	Israel	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	16
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
82.145.209.17	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	7
109.64.181.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
93.81.206.14	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	6
109.65.25.165	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.80.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.65.214.190	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.80.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
109.67.59.4	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
115.239.228.8	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	4
109.67.132.187	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.48.73.60	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
84.111.196.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.21.133	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.25.165	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.233	atal.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
109.65.25.165	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.88.154.138	Poland	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	100
194.88.154.138	Poland	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	78
70.89.127.78	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	69
96.48.22.37	Canada	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	63
192.117.12.65	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	40
216.201.148.210	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	19
83.169.8.217	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	16
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	15
178.63.18.196	Germany	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	15
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
194.88.154.138	Poland	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	10
216.249.104.194	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
83.169.8.217	Germany	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.63.228.226	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
178.63.18.196	Germany	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.185.43.135	United States	147.237.77.233	atal.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
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	7
108.168.219.174	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	6
81.218.251.250	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
96.48.22.37	Canada	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.252	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
67.228.38.74	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
194.90.209.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
70.89.127.77	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
216.201.148.210	United States	147.237.76.42	refuah.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	5
67.228.38.74	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
188.165.15.127	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	4
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	4
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.54.165.84	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	4
87.68.158.61	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	4
194.88.154.138	Poland	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	3
151.80.31.139	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	3
96.48.22.37	Canada	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	3
81.218.130.222	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
151.80.31.130	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.130	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
62.128.35.131	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.186.33.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
189.38.80.71	Brazil	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
82.80.46.158	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
105.154.75.29	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
79.176.193.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
70.89.127.77	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	1953
68.48.156.101	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	551
194.88.154.138	147.237.77.216	Poland	dover.idf.il	SQL Injection - Select From	399
96.48.22.37	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	391
70.89.127.78	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	189
83.169.8.217	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	82
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	73
178.63.18.196	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	39
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	33
216.201.148.210	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	32
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
203.171.41.47	147.237.76.31	New Zealand	nakchal.idf.il	SQL Injection - Select From	15
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	13
94.73.145.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	12
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
189.38.80.71	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	7
216.249.104.194	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
90.44.93.107	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	4
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
176.13.12.19	147.237.76.42	Israel	refuah.idf.il	INDICATOR-SCAN myscan	2
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.158	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
74.117.209.136	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
37.26.147.225	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.240.213.93	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.138	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
212.143.3.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
183.62.78.18	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.67	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
74.117.209.136	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.218	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.136.163	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
82.205.0.245	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
176.13.12.19	147.237.76.42	Israel	refuah.idf.il	GPL SCAN myscan	2
66.240.213.93	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
74.117.209.136	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.231	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
77.126.93.245	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
176.12.147.139	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
31.6.71.154	147.237.76.42	Poland	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.240.213.93	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
90.44.93.107	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
208.80.155.223	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14975
188.226.214.36	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1288
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	850
70.39.186.107	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	784
77.127.32.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	690
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	616
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	593
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	589
79.179.28.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	483
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	367
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
79.180.149.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	342
79.182.144.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	335
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	326
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	318
94.252.167.154	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	291
80.178.157.40	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	270
84.108.86.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	250
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	246
198.45.19.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	235
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	207
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	201
66.171.228.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	160
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
85.64.49.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	143
66.249.66.76	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	140
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	134
85.128.142.60	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
123.103.8.41	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
148.177.129.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
96.48.22.37	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
140.254.70.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	102
74.93.46.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
100.100.79.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	97
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
173.231.115.59	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
5.22.134.66	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	83
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	613
79.177.9.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	346
176.12.147.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	345
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	298
2.54.139.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	289
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
176.13.23.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	267
213.57.177.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	265
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	216
176.12.147.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	210
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	198
37.142.219.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	197
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.144	Block	168
213.57.177.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	162
79.177.9.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	158
2.54.55.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
2.54.156.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	153
176.13.8.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
176.13.8.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
37.142.219.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	135
79.177.9.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
176.12.150.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
2.52.159.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
2.54.139.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	116
176.13.8.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
77.127.32.60	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
176.13.23.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	111
176.13.0.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.139.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.8.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	107
212.199.244.112	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
213.57.177.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
2.52.3.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
176.12.136.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	100
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
37.26.147.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92