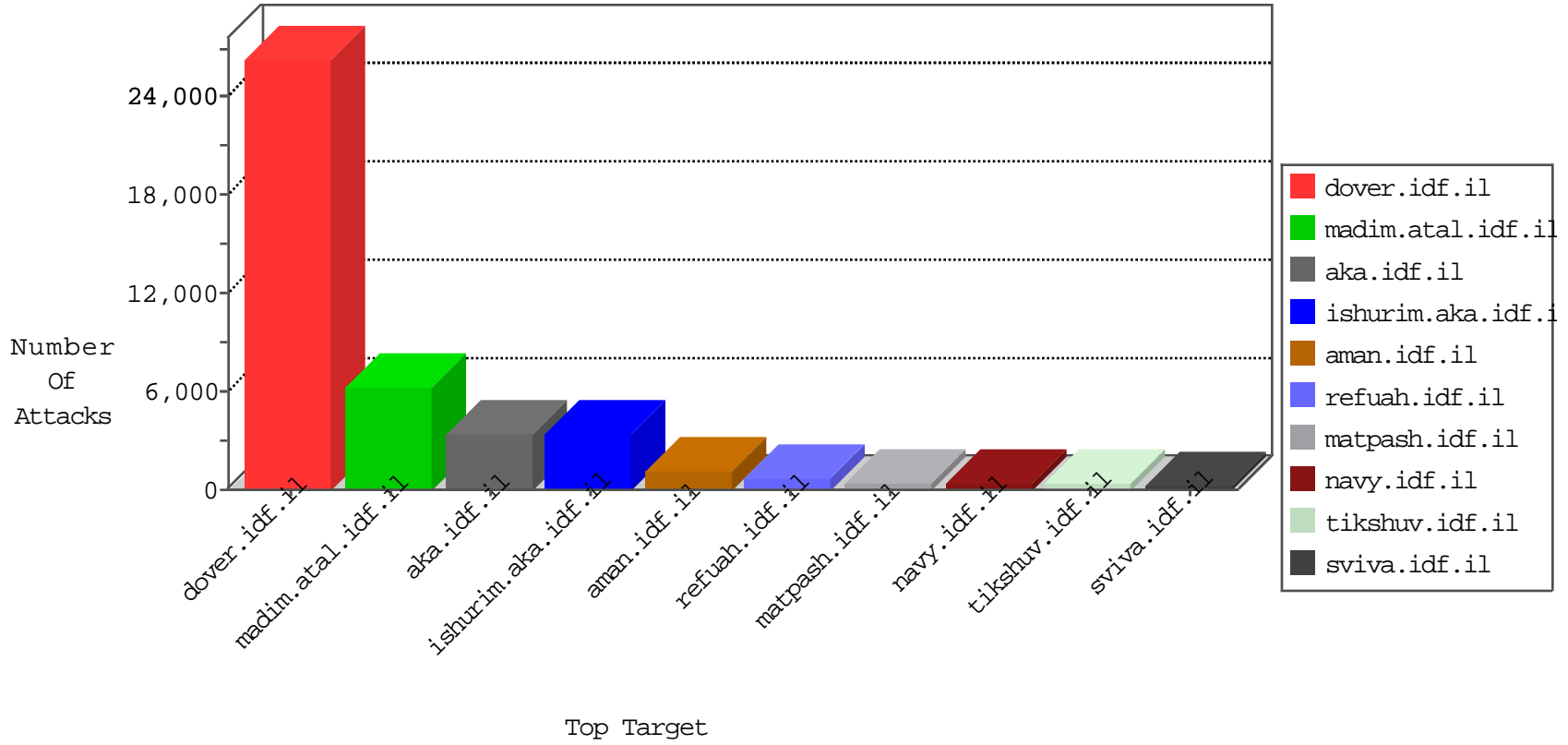


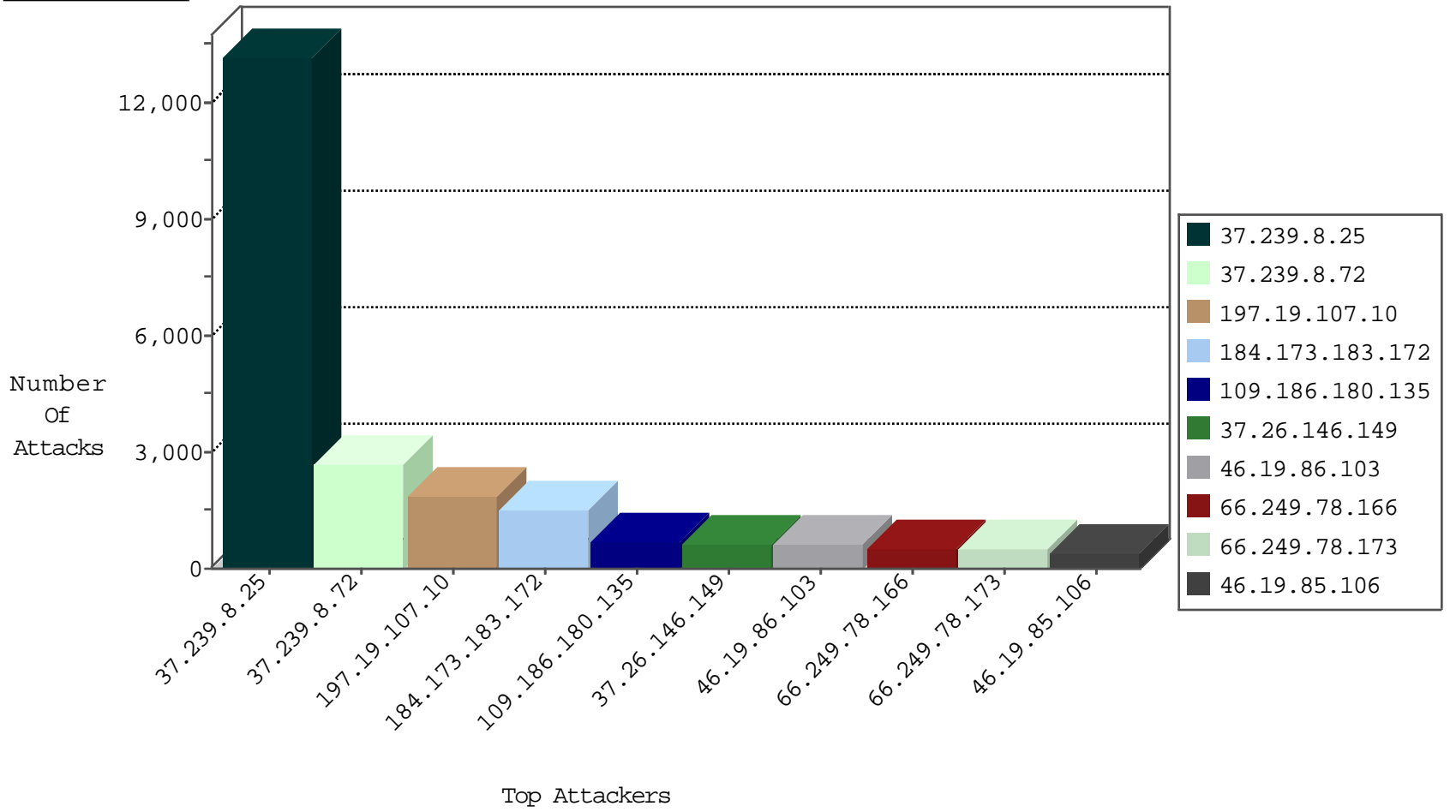
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.65.140.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1505
81.218.83.34	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1032
94.159.174.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	677
77.125.105.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	668
109.186.116.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	635
5.29.218.156	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	547
5.28.146.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	377
176.228.136.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	298
93.173.149.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	272
85.250.81.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
207.232.36.210	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
46.121.245.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
109.253.128.8	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
185.32.179.116	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	184
84.228.192.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.182.134.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
37.142.227.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.183.123.133	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	162
95.86.88.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
93.172.147.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
149.78.245.245	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
149.88.110.238	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
77.125.151.195	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
85.130.247.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
85.64.87.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
80.178.222.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
46.19.86.29	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	113
79.178.63.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
46.120.17.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
46.116.141.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
93.173.5.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
5.28.182.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
109.253.131.165	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.19.85.248	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
109.253.139.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
2.54.155.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
46.19.86.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
80.246.136.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
109.253.128.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
46.117.45.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
109.253.144.176	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
62.90.212.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.86.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
80.246.138.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
2.54.163.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
84.110.194.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
85.65.143.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1085
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	318
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	168
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	125
66.249.16.211	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	121
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	112
81.218.251.252	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	48
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	38
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	30
79.180.139.211	Israel	147.237.72.166	aka.idf.il	1106: HTTP: IIS .%5c Encoded \ in URI	Permit	26
82.137.254.22	Syrian Arab Republic	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
109.67.58.141	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	7
79.179.155.79	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
132.64.31.69	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
147.236.254.48	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
116.251.221.250	Singapore	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.19.85.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
113.92.239.60	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	3
59.33.252.247	China	147.237.0.35	akaws.idf.il	DVRep_P-N_40-59	Permit	3
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
93.120.27.62	Romania	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	3
62.219.210.236	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	148
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	90
122.228.207.193	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	26
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	26
122.228.207.190	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	24
122.228.207.190	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	17
77.125.167.20	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	15
87.69.109.98	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	14
122.228.207.190	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	12
122.228.207.193	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	10
37.26.146.149	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	10
79.181.127.152	Israel	147.237.77.226	www.chamatz.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	10
31.168.172.250	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
218.77.79.43	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	9
122.228.207.193	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	9
188.120.148.74	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
5.29.197.66	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
2.54.21.224	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
122.228.207.193	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	8
211.138.34.58	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	7
122.228.207.193	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	7
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
79.182.134.254	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
122.228.207.190	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	7
61.233.31.67	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	6
87.69.108.169	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
121.42.54.18	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
85.64.87.95	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
218.77.79.43	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	6
46.120.130.24	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
218.77.79.43	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	6
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	6
122.228.207.193	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	6
122.228.207.190	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	6
122.228.207.193	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	5
122.228.207.190	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	5
109.186.187.45	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
218.77.79.43	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	5
122.228.207.190	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	5
5.102.253.34	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
122.228.207.190	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	5
183.60.127.190	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	5
85.64.159.125	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
198.154.60.27	United States	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	5
192.169.226.192	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
122.228.207.190	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	5
176.12.149.42	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	5
122.228.207.193	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	5

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.239.8.25	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7965
37.239.8.25	Iraq	147.237.77.216	dover.idf.il		drop	drop	3154
37.239.8.25	Iraq	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1118
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	452
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	426
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	356
70.194.73.104	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	184
79.177.132.50	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	156
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	86
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	84
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
212.29.249.212	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	75
109.253.129.137	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
194.170.74.98	United Arab Emirates	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	65
37.239.8.72	Iraq	147.237.77.216	dover.idf.il	SAM rule	drop	drop	64
79.180.144.39	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	63
212.150.155.130	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	50
109.65.81.79	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
109.253.156.202	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
109.253.142.122	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
109.253.158.124	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
109.253.137.66	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
109.253.133.188	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
94.230.86.50	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	37
176.12.140.109	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.139.136	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
79.176.58.215	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
79.182.7.18	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
46.19.85.20	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	33
212.179.46.22	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	32
84.109.118.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
37.26.148.207	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.148.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.85	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.66.14.141	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.141.90	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.136.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.88	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
132.64.192.96	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.151.168	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.160.234.39	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
213.8.7.232	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
176.12.141.50	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	29
91.143.227.173	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
177.177.248.129	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
79.179.99.95	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.239.8.72	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	2217
197.19.107.10	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1853
37.239.8.25	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	709
109.186.180.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	657
37.26.146.149	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.149	Block	628
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	597
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	398
185.32.178.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	314
2.54.10.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	303
185.32.179.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	302
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	241
176.12.139.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	239
2.54.21.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	237
80.246.137.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	207
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	189
2.54.146.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	181
37.239.8.72	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	173
37.239.8.72	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.239.8.72	Block	173
109.253.128.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
109.253.146.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	145
37.239.8.25	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.239.8.25	Block	115
37.239.8.25	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	114
82.102.141.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	107
109.253.134.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
109.253.138.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	90
185.32.178.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	87
66.249.65.196	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.196	Block	67
176.12.141.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	63
66.249.65.192	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.192	Block	58
66.249.65.188	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.188	Block	57
205.167.7.247	France	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	57
2.54.134.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
93.173.38.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	55
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.86	Block	51
185.32.179.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
109.253.130.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
109.253.157.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
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	42
109.253.134.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
176.12.149.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
37.26.146.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
2.54.42.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	31
176.12.146.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	31
176.12.144.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	29
79.183.53.42	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.183.53.42	Block	25