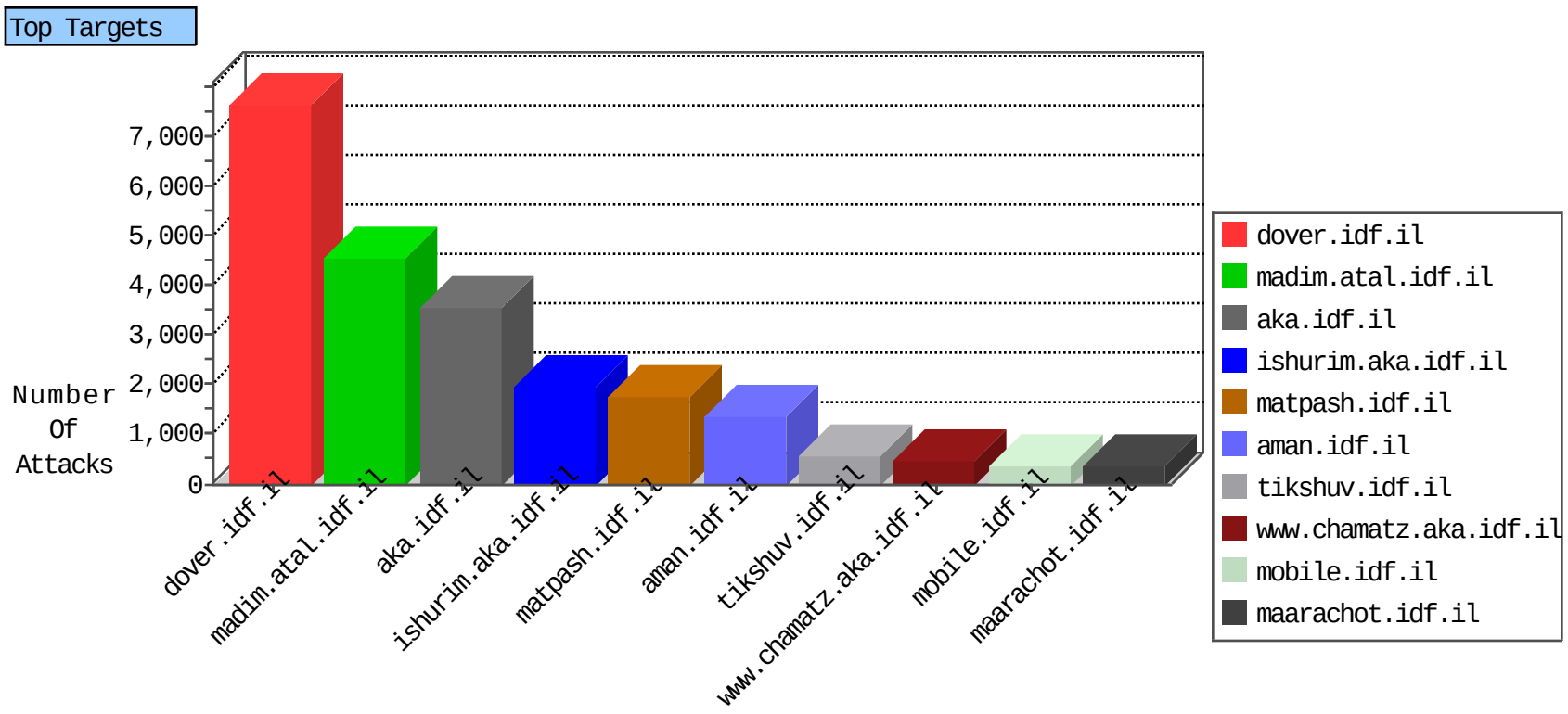
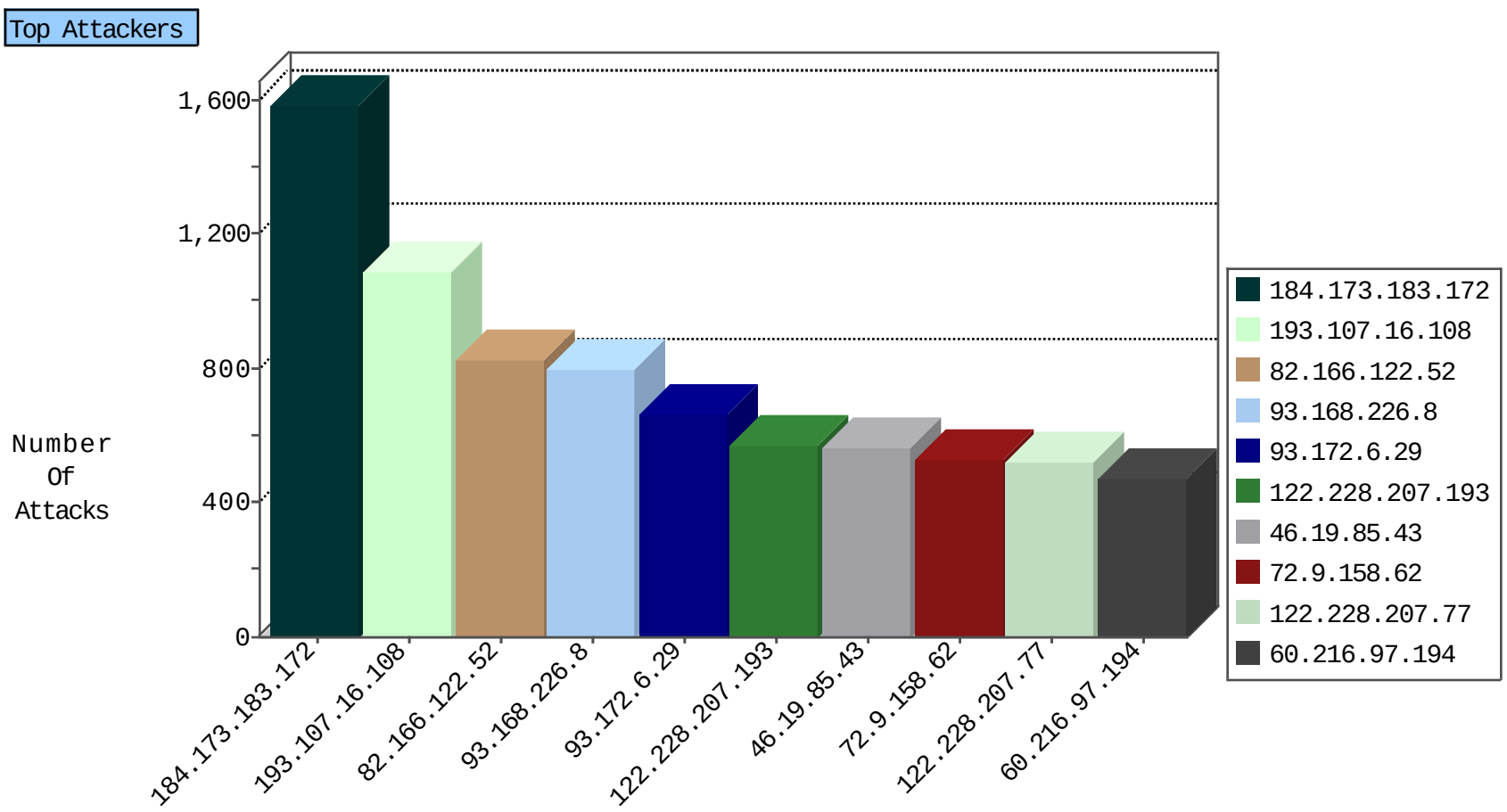
02-07-2015-00:00:02 to 02-08-2015-00:00:02

IDF Under Attack Daily Report





02-07-2015-00:00:02 to 02-08-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.131	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	7090
173.252.81.115	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1098
46.19.85.136	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	1038
82.166.122.52	Israel	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	820
176.228.217.9	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	567
77.126.225.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	437
213.57.147.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
46.121.74.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	336
84.111.85.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	326
79.179.197.235	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
82.102.141.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
79.181.222.150	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
77.127.186.24	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
46.117.190.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
46.120.131.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
79.179.141.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
93.173.131.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
85.64.75.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
84.108.219.137	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
109.64.9.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
109.65.66.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.65.178.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
5.29.35.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
84.228.229.156	Bulgaria	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
109.64.99.48	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
207.46.13.113	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	111
84.109.208.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
93.172.137.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
46.19.85.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
109.67.14.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
94.159.141.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
84.228.145.117	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
109.253.131.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
79.70.66.131	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	79
46.121.37.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
80.246.141.225	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
46.19.86.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	74
93.172.54.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
84.228.35.215	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
80.246.141.225	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	64
79.181.220.50	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
82.102.141.204	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	44
82.102.141.205	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	37
84.228.145.117	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	34
84.108.219.137	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	32
109.253.131.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	32

02-07-2015-00:00:02 to 02-08-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
193.107.16.108	Russian Federation	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	656
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	646
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	547
193.107.16.108	Russian Federation	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	432
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	200
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	192
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	169
109.186.228.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	47
77.125.87.152	Israel	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	28
77.125.87.152	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	14
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
79.180.194.120	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.8.194.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_P-N_40-59	Permit	5
49.145.85.238	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.34.12.131	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
79.179.59.200	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
206.63.82.189	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_P-N_40-59	Permit	3
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
41.74.71.75	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
100.36.132.196	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_P-N_40-59	Permit	3
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	3
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_P-N_40-59	Permit	3
46.19.85.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_P-N_40-59	Permit	3
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
84.111.105.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	3
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
158.112.86.66	Norway	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

02-07-2015-00:00:02 to 02-08-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
60.216.97.194	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	116
60.216.97.194	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	104
60.216.97.194	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	89
61.160.224.128	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	79
141.212.122.172	United States	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	73
122.228.207.193	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	68
60.216.97.194	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	65
162.222.223.86	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	64
111.205.45.254	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	59
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	58
60.216.97.194	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	53
72.9.158.62	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	53
72.9.158.62	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	47
46.121.128.142	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	45
61.160.224.128	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	44
218.6.132.45	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	43
122.228.207.190	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	42
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	42
111.205.45.254	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	41
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	41
122.228.207.193	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	41
77.125.30.197	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	41
122.228.207.193	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	40
104.220.39.44		147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	40
122.228.207.190	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	38
72.9.158.62	United States	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	38
122.228.207.193	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	37
111.205.45.254	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	37
23.234.51.21	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	37
72.9.158.62	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	36
141.212.122.85	United States	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	35
115.231.218.23	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	35
162.222.223.86	United States	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	35
111.205.45.254	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	35
104.220.39.44		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	34
111.205.45.254	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	33
104.220.39.44		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	31
122.228.207.193	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	30
61.160.224.128	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	30
162.222.223.86	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	30
193.107.16.206	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	30
72.9.158.62	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	30
68.4.179.58	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	29
111.205.45.254	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	29
175.126.103.124	Korea, Republic of	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	28
60.216.97.194	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	28
72.9.158.62	United States	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	28
103.231.43.17		147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	28
115.231.218.23	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	28
115.231.218.147	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	28

02-07-2015-00:00:02 to 02-08-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
93.168.226.8	Romania	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	692
66.249.75.121	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	386
66.249.75.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	352
66.249.75.137	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	336
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	130
93.168.226.8	Romania	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	107
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	91
94.252.11.60	Luxembourg	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	72
46.19.85.136	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	66
5.28.168.189	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
182.185.207.232	Pakistan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
176.12.144.156	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
182.178.196.195	Pakistan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
74.111.231.116	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	37
149.78.246.71	United States	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
84.109.240.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
88.15.108.205	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.143.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.158.17	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
46.19.85.111	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	30
5.102.235.180	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
82.145.223.40	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	28
66.249.75.236	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
84.228.214.26	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
79.181.48.204	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	28
109.253.151.144	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.253.137.13	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
131.253.26.192	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
187.59.246.135	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.64.119.190	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
204.12.251.37	United States	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
109.253.131.9	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
77.127.78.106	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
79.183.50.116	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
176.12.137.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	19
109.253.138.101	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.146.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.146.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.208	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.141.251	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.172.6.29	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.6.29	Block	649
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	546
84.108.36.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	464
85.65.52.53	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.52.53	Block	383
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	376
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	350
46.19.85.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.154	Block	276
80.246.138.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.138.99	Block	212
84.109.72.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
80.246.138.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	157
46.120.74.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
109.253.135.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	138
176.12.140.147	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.147	Block	117
37.77.51.208	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	116
149.88.84.247	United States	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.84.247	Block	61
37.77.51.150	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	59
86.60.201.91	Finland	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 86.60.201.91	Block	56
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	55
37.77.51.208	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	38
95.86.66.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	37
109.253.132.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
77.127.112.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
66.249.75.153	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.153	Block	32
37.77.51.116	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	31
66.249.75.137	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.137	Block	26
66.249.75.121	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.121	Block	26
77.125.4.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	25
66.249.67.135	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.135	Block	24
85.64.0.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	23
79.183.180.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	20
93.173.57.252	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 93.173.57.252	Block	18
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	15
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	14
176.12.142.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
66.249.67.119	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.119	Block	13
79.180.194.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	12
66.249.69.190	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.69.190	Block	12
46.116.230.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
84.94.163.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	11
107.170.50.206	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 107.170.50.206	Block	11
66.249.69.174	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.69.174	Block	11
212.179.42.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
198.143.187.122	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.143.187.122	Block	10
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	10
81.218.139.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.75.236	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
82.80.58.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 82.80.58.42	Block	9
207.46.13.19	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
79.183.213.44	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.183.213.44	Block	9

02-07-2015-00:00:02 to 02-08-2015-00:00:02