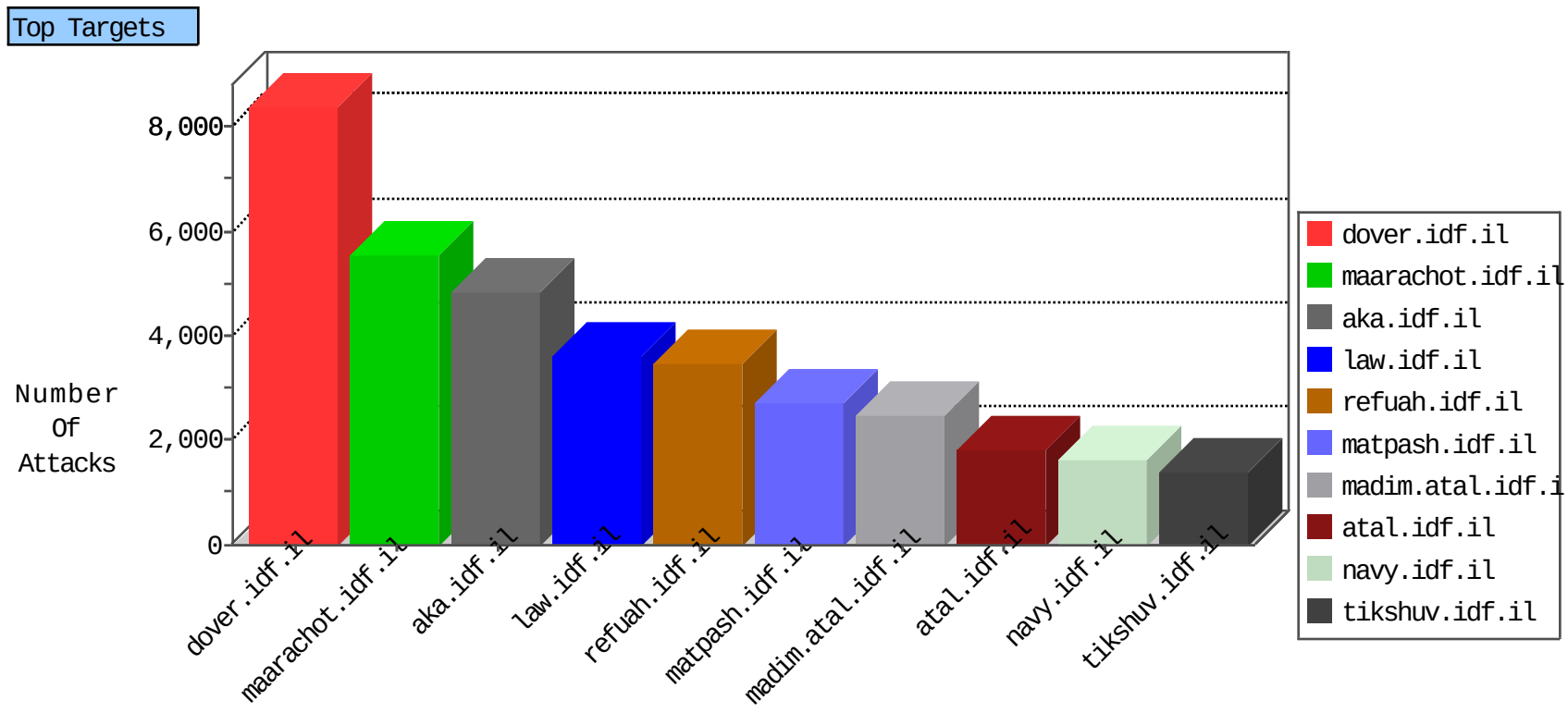
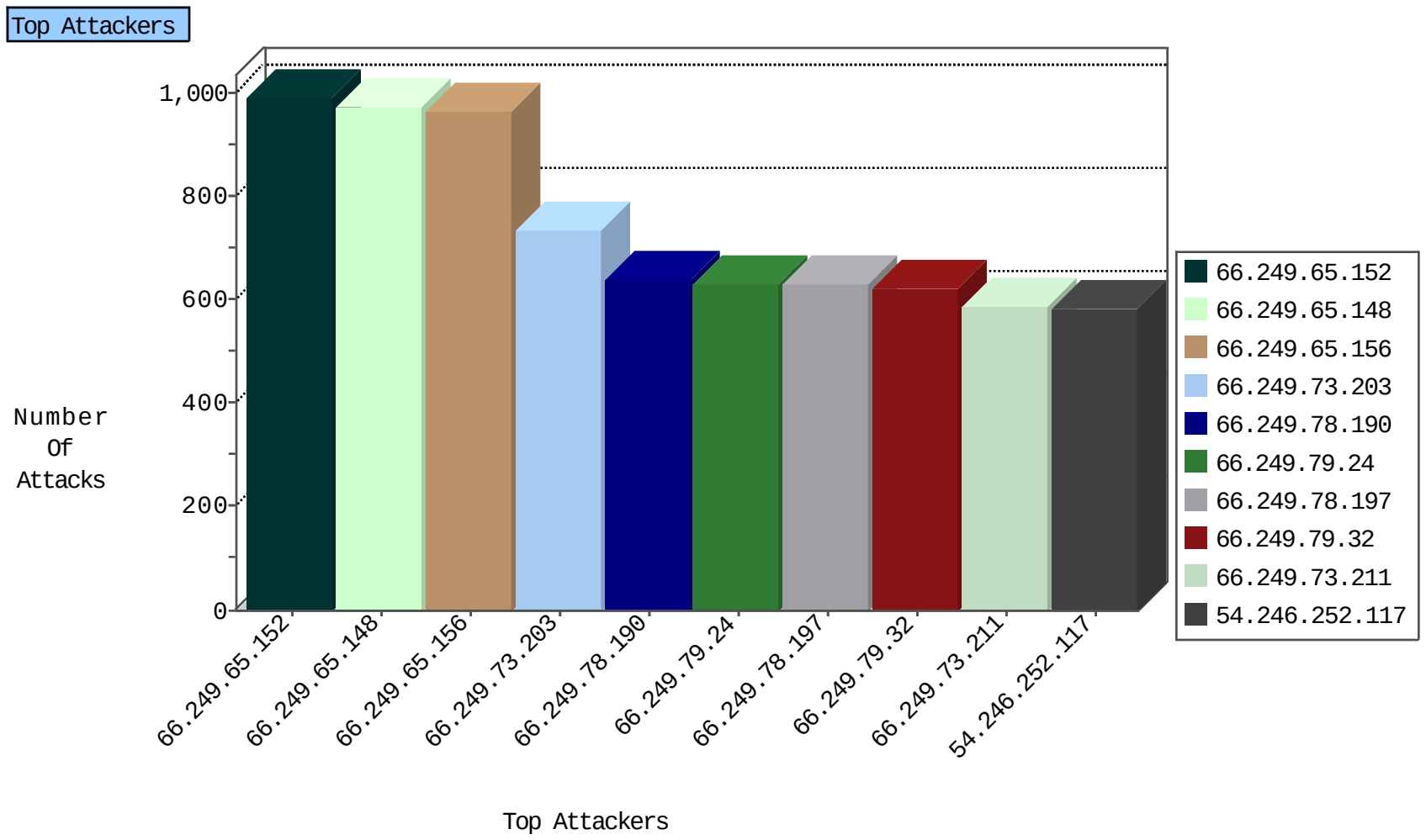
04-05-2015-00:00:03 to 04-06-2015-00:00:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-05-2015-00:00:03 to 04-06-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	991
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	972
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	965
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	735
84.109.30.45	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	709
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	639
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	631
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	629
66.249.79.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	623
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	589
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	577
79.181.139.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	554
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	547
66.249.79.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	547
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	495
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	487
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	467
46.116.65.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	450
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	446
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	442
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	439
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	418
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	409
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	393
5.28.165.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	378
66.249.67.73	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	376
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	365
79.180.35.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	351
84.110.86.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	349
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	344
149.78.219.199	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	339
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	327
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	299
66.249.67.81	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	297
77.125.248.255	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	295
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	292
66.249.67.89	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	276
66.249.73.187	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	271
66.249.65.199	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	268
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	266
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	259
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	255
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	253
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	245
66.249.73.195	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	232
79.182.195.124	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	228
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	216
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	198
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	195
2.54.136.74	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195

04-05-2015-00:00:03 to 04-06-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	177
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	152
2.52.11.2	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	79
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	57
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	19
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
109.66.125.182	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.183.7.60	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.179.8.176	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.111.38.64	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
108.61.188.90	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
46.116.148.27	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
87.160.94.96	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.160.221.81	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.54.41.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
138.25.143.166	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
192.116.177.146	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.172.147.48	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
2.54.52.161	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
87.69.248.130	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.183.115.36	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	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	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
46.117.76.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
149.78.134.244	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	3
87.68.52.128	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
80.246.139.60	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.131.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	2
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
85.250.212.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

04-05-2015-00:00:03 to 04-06-2015-00:00:03

Top Attackers In IDS

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	144
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	123
2.52.175.156	Israel	147.237.77.243	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	60
109.65.162.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
84.111.110.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
5.29.77.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	3
176.12.141.84	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
46.120.131.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.102.254.208	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
80.178.15.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.125.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.146.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.46.193.114	China	147.237.77.61	e.cogat.idf.il	GPL SCAN nmap TCP	2
121.240.226.74	India	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
62.219.161.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
128.199.157.166	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
5.28.158.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.153.18	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.102.50.40	Netherlands	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
2.54.39.213	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.102.50.40	Netherlands	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
58.20.54.249	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.188.210	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.7	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
87.69.194.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.44.128	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
87.68.151.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.146.208	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.7	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
109.186.37.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.158.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.198.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
134.191.232.69	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.64.137.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.101.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.102.50.40	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
218.56.45.132	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
46.117.125.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
37.142.31.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2

04-05-2015-00:00:03 to 04-06-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
54.246.252.117	Ireland	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	576
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	388
87.69.128.4	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	281
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	158
109.253.129.23	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
82.80.141.79	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	41
93.186.31.112	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
213.204.64.99	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.147.28	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.140.172	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
109.253.131.57	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.149.178	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
24.215.190.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
79.176.15.14	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	30
49.228.72.218	Thailand	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
109.253.145.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.146.102	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.143.49	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.139.96	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.30.25.80	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
79.177.21.216	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	27
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	27
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.143.133	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.141.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.139.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.137.156	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.143.232	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.142.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.128.111	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.145.54	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.134.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
84.228.30.36	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
212.179.85.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
109.253.132.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
173.25.32.118	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	22
75.117.1.207	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.253.139.115	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	20
105.210.180.197	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	20
109.253.128.49	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
176.12.140.170	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.143.122	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.145.138	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
91.227.164.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.145.147	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
168.63.139.43	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.147.50	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
79.179.146.21	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.179.146.21	Block	511
37.26.148.142	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.148.142	Block	365
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.242	Block	276
2.54.5.13	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.5.13	Block	276
2.54.136.74	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.136.74	Block	267
2.54.23.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	200
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	132
80.246.139.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
109.253.142.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	50
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	43
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
37.26.148.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
2.54.136.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
2.54.175.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
79.180.33.171	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	23
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	20
5.29.49.127	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.49.127	Block	20
46.116.180.43	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.180.43	Block	18
79.178.141.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
85.65.154.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	15
109.253.143.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
213.57.142.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
2.54.50.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
46.116.24.65	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	10
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	10
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
84.110.112.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
95.86.98.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
87.69.130.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	8
149.78.32.62	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.32.62	Block	7
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
79.178.193.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	7
162.244.15.23		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	6
176.228.214.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
188.165.15.198	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.150.239.100	Block	5
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.178.157.40	Block	5
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
93.173.238.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.64.195.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
109.66.39.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
84.94.68.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/main.stm	Block	5
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	5
93.173.179.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
77.126.255.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	4
79.176.181.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4