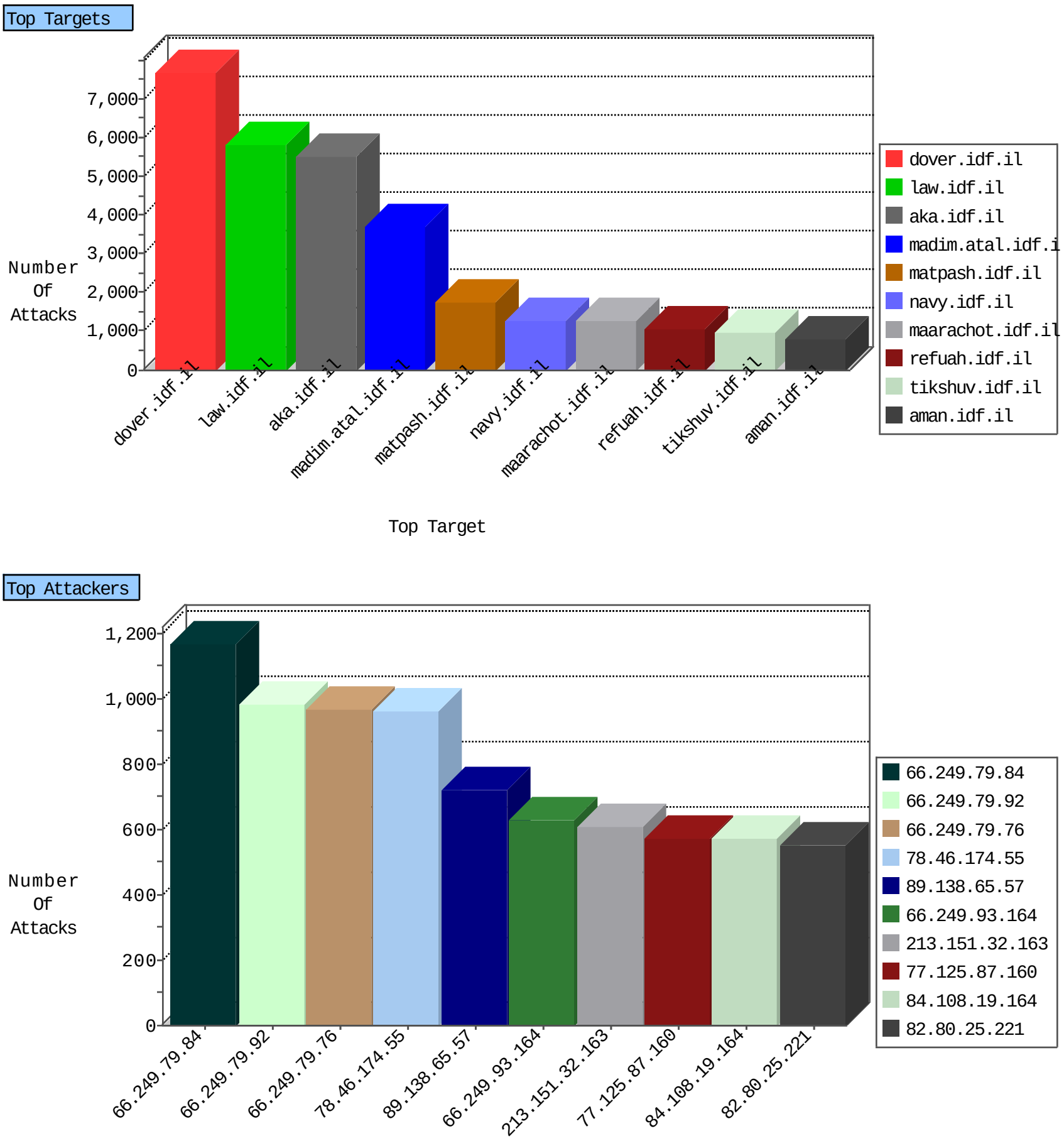
04-03-2015-00:00:05 to 04-04-2015-00:00:05

IDF Under Attack Daily Report



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
85.64.98.235	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	1993
66.249.79.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	1170
66.249.79.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	986
66.249.79.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	969
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	625
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	528
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	524
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	481
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	476
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	474
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	464
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	452
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	431
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	418
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	414
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	406
79.178.141.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	395
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
84.110.86.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	286
5.28.184.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	274
66.249.79.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	267
66.249.79.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	258
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	248
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	239
109.64.101.44	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	237
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	236
66.249.79.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	228
66.249.79.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	226
66.249.73.221	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	219
66.249.79.143	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	213
66.249.75.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	210
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	207
66.249.75.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	200
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	197
66.249.79.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	195
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	192
66.249.75.117	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	187
66.249.73.229	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	187
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	182
66.249.73.237	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	177
109.66.41.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.177.165.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	167
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	161
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	154
85.64.98.235	Israel	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	149
5.29.254.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	145
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	142

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	575
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	275
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	175
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	69
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	39
142.54.161.50	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	28
159.240.11.53	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
42.229.200.239	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
42.229.200.239	China	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
109.67.193.121	Israel	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	12
89.139.27.176	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
79.178.132.153	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.34.12.191	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
87.69.134.102	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.22.130.15	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.176.150.101	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
85.65.54.62	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
72.245.29.209	United States	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
85.65.226.211	Israel	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
75.73.255.156	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
142.54.161.50	United States	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	4
204.75.207.117	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	3
5.22.130.15	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.186.168.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
192.139.153.25	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3

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

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	141
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	56
202.113.77.254	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	6
60.30.204.2	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	6
123.150.255.194	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	6
221.238.82.194	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	6
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
85.64.98.235	Israel	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
208.80.155.146	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	3
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.210	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
79.180.11.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
79.176.167.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.168	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
218.24.171.223	China	147.237.77.243	mobile.idf.il	GPL SCAN nmap TCP	2
77.126.234.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.168	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
89.248.162.228	Netherlands	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
188.138.9.51	Germany	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.77	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.168	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
85.64.69.251	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.166	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
180.169.108.158	China	147.237.76.38	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
221.235.188.210	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
93.172.37.6	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.141.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
37.26.146.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.60.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.168	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
85.250.5.163	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.35.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.168	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.170	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
77.127.187.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.168	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.161	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.168	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	496
197.179.202.40	Kenya	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	234
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
222.77.227.34	China	147.237.76.86	navy.idf.il	SAM rule	drop	drop	53
176.12.137.185	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
85.64.217.108	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	45
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
136.243.36.97	Germany	147.237.77.216	dover.idf.il	SAM rule	drop	drop	42
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	40
176.12.149.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.141.193	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.147.36	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.142.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.144.199	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.133.244	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.143.203	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.141.231	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
149.78.125.184	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.141.191	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
114.143.204.171	India	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
188.139.234.159	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	24
176.12.142.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.136.57	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
197.134.89.67	Egypt	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
176.12.141.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
188.75.173.21	Czech Republic	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
176.12.147.244	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.149.42	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.147.27	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.102.6.194	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
109.253.145.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
62.212.119.109	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.157.97	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.145.246	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.145.241	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.142	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.149.125	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
199.30.26.143	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
197.34.83.48	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.121.150.51	Israel	147.237.76.86	navy.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	17
46.121.150.51	Israel	147.237.76.86	navy.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
41.43.81.135	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
94.249.8.201	Jordan	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	16
105.228.43.13	South Africa	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	16
199.30.24.174	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.65.57	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 89.138.65.57	Block	719
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	609
84.108.19.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.108.19.164	Block	573
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	441
109.64.117.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	259
89.138.193.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	241
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	233
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	233
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	227
46.19.85.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	190
2.54.158.161	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.158.161	Block	127
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
2.54.166.122	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.166.122	Block	103
37.26.147.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	63
109.253.156.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
176.12.137.204	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.137.204	Block	48
176.12.145.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
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
109.253.145.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
2.54.174.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
2.54.156.8	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.156.8	Block	28
109.253.129.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	26
185.16.27.21	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.16.27.21	Block	20
109.160.238.175	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.160.238.175	Block	17
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	15
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	14
188.75.173.21	Czech Republic	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	10
109.65.17.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	9
37.26.146.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
77.126.96.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
2.54.171.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
77.126.144.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	6
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
91.207.7.74	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	6
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.142.207.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
109.253.135.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
62.219.21.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	5
46.121.212.38	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
80.179.225.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
213.57.31.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
17.142.152.34	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.34	Block	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	4
213.57.57.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4