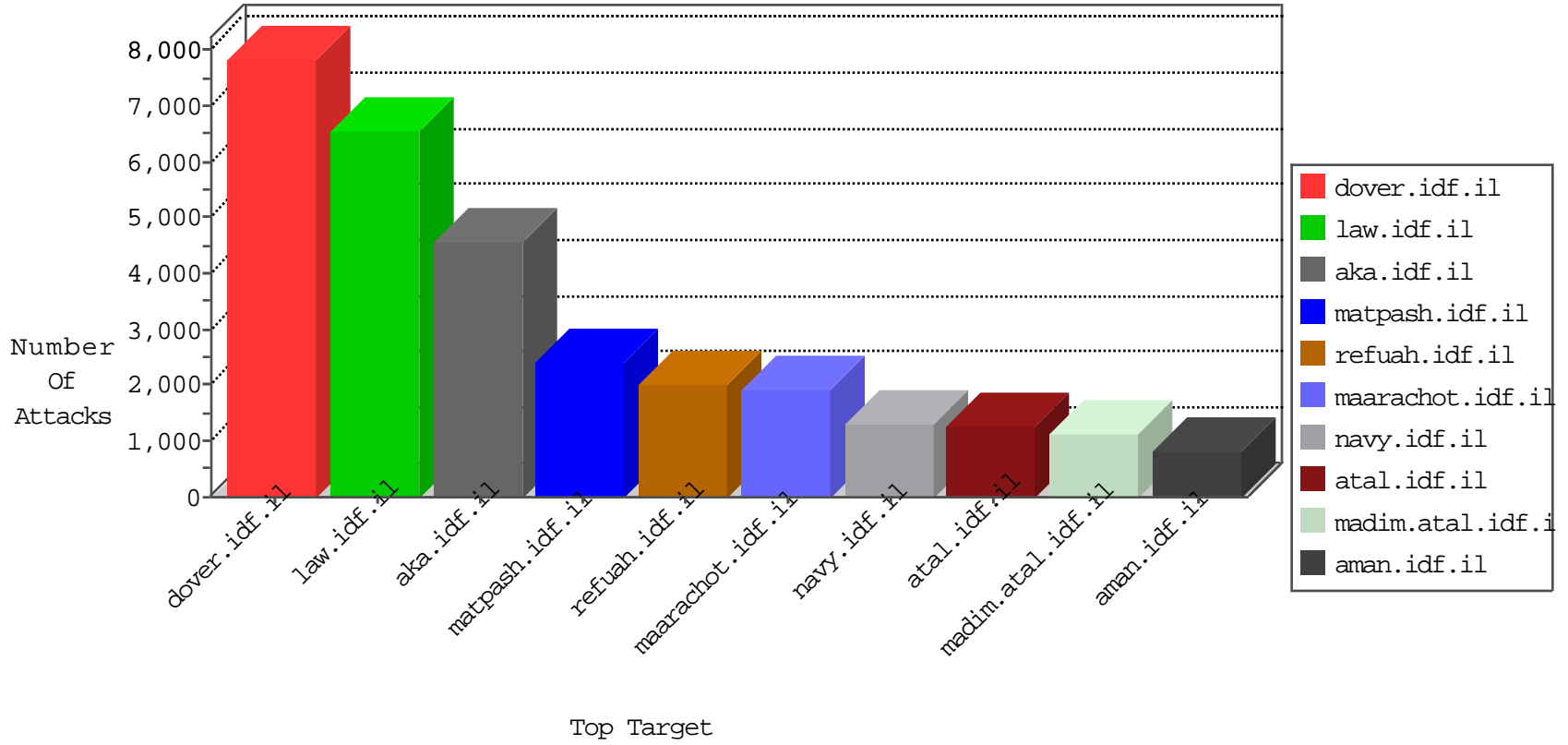


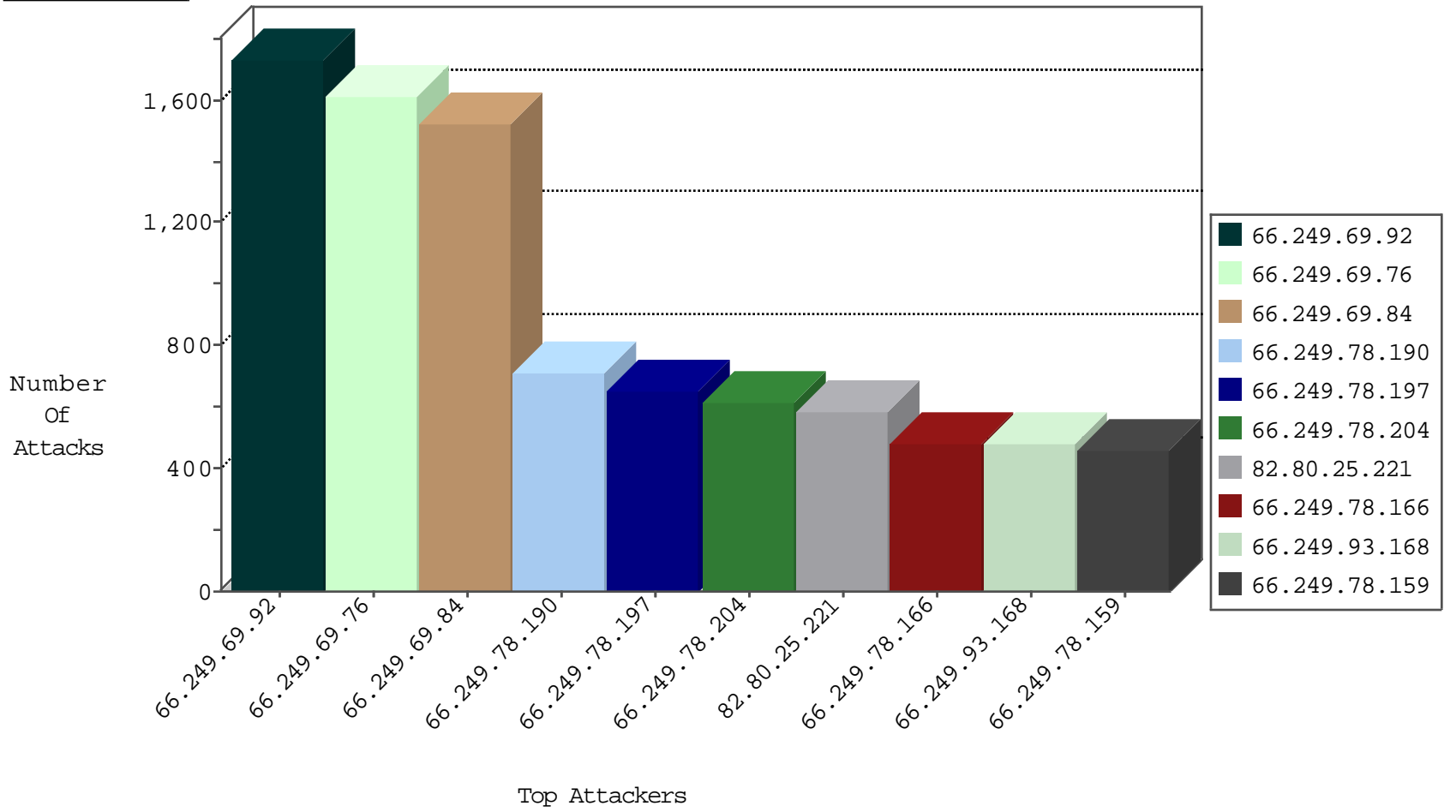
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	1733
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	1610
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	1523
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	711
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	649
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	618
213.57.61.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	566
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	483
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	466
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	461
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	454
66.249.75.68	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	446
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	417
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	414
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	412
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	371
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	356
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	314
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	313
66.249.64.114	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	306
93.172.210.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	302
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	298
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	298
85.250.70.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	295
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	292
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	286
66.249.67.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	286
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	284
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	283
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	278
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	275
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	274
66.249.67.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	266
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	260
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	252
46.116.202.82	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	239
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	235
84.110.109.159	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	233
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	225
79.178.177.132	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	216
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	211
84.109.96.63	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	202
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	198
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	191
85.65.48.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
199.203.120.178	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	179
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	178
84.110.86.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
46.120.4.202	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	171

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	DVRRep_P-N_40-59	Permit	299
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRRep_P-N_40-59	Permit	89
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRRep_P-N_40-59	Permit	22
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRRep_P-N_40-59	Permit	20
86.115.24.193	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
84.111.48.148	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.108.103.193	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.29.53.20	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.65.23.79	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.178.141.120	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.34.12.144	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
95.211.81.104	Netherlands	147.237.77.216	dover.idf.il	DVRRep_B-N_60_100	Block	5
84.228.124.245	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.50.195	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.96	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRRep_P-N_40-59	Permit	4
50.40.232.158	United States	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	147.237.8.28	e.mobile-ks.idf.il	DVRRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRRep_P-N_40-59	Permit	3
2.54.37.110	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	147.237.77.178	e.matpash.idf.il	DVRRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRRep_B-N_60_100	Block	3
190.85.110.1	Colombia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.223	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.30	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.62.67	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.147.166	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.165.45	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRRep_B-N_60_100	Block	3
46.19.85.33	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	147.237.77.226	www.chamatz.aka.idf.il	DVRRep_B-N_60_100	Block	3
77.125.147.157	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRRep_B-N_60_100	Block	3
85.65.210.40	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.64	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
128.84.126.83	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRRep_P-N_40-59	Permit	2
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRRep_B-N_60_100	Block	2
83.226.154.245	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.32.178.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.78.102.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRRep_P-N_40-59	Permit	2
79.176.111.102	Israel	147.237.72.166	aka.idf.il	DVRRep_B-N_60_100	Block	2
218.6.132.45	China	147.237.76.38	e.e.meitav.idf.il	DVRRep_B-N_60_100	Block	2
197.37.202.27	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.148	ggcenter.aka.idf.il	DVRRep_B-N_60_100	Block	2
79.183.38.115	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	418
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	141
46.105.114.103	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	12
105.104.18.8	Algeria	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	12
46.105.114.103	France	147.237.77.216	dover.idf.il	ETPRO WEB_SERVER PHP Open Flash Charts File Upload Attempt	12
105.104.2.204	Algeria	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	12
46.105.114.103	France	147.237.77.216	dover.idf.il	ETPRO WEB_SERVER PHP Possible Open Flash Direct Access to File Upload Directory	12
88.241.7.12	Turkey	147.237.77.170	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
197.202.240.207	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	4
89.234.68.85	Ireland	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
83.71.247.38	Ireland	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
147.236.32.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
43.255.191.141	Japan	147.237.8.27	e.medim.atal.idf.il	ET SCAN Potential SSH Scan	3
31.31.76.206	Czech Republic	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
190.85.110.1	Colombia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
85.250.148.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.163.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.37.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
85.65.177.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.25.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.178.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.76.30	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
81.218.215.141	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.76.177	noore.idf.il	ET SCAN Potential SSH Scan	2
5.29.207.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
176.228.156.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.76.176	test.noore.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
85.250.150.177	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
79.182.195.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
173.242.113.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
85.250.98.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.168.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.54.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
119.188.6.231	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
37.26.147.214	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
46.116.81.64	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.213	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.140.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.213	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2

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	166
204.93.58.10	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	138
77.125.107.105	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	81
178.32.128.216	France	147.237.77.74	law.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	70
78.149.115.60	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	69
213.57.215.129	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	64
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
110.87.23.210	China	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	50
109.253.141.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
41.254.8.243	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	37
31.186.228.26	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	37
31.186.228.31	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	36
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
31.186.228.91	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	34
109.253.140.217	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
31.186.228.29	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	32
49.228.72.218	Thailand	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
109.253.140.178	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.146.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
49.228.72.218	Thailand	147.237.72.166	aka.idf.il	SAM rule	drop	drop	30
31.186.228.90	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	30
31.186.228.60	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	27
110.87.23.210	China	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	27
212.34.12.146	Jordan	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	27
89.138.199.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
105.104.18.8	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
70.196.131.52	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
176.12.140.31	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.24	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
109.253.134.182	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.95	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
31.186.228.86	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
176.12.139.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.145.145	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.93	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
109.253.139.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.59	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	23
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
176.12.139.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
80.246.138.12	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
80.246.138.12	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	21
31.186.228.58	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
80.246.138.12	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	20
31.186.228.23	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.186.228.62	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
176.12.146.232	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
31.186.228.32	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	18
109.253.135.226	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.15	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
80.246.141.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
185.32.179.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	190
2.54.147.181	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.147.181	Block	165
2.54.172.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
213.14.82.153	Turkey	147.237.77.216	dover.idf.il	Multiple Malformed URL from 213.14.82.153	Block	131
213.14.82.153	Turkey	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 213.14.82.153	Block	131
213.14.82.153	Turkey	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 213.14.82.153	Block	130
2.54.32.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	44
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	41
109.253.130.31	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.130.31	Block	38
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	33
46.105.114.103	France	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	24
46.105.114.103	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	23
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.160.183.8	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	17
31.168.210.16	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.210.16	Block	16
46.19.86.98	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	16
85.65.170.58	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 85.65.170.58	Block	12
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
174.89.107.111	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 174.89.107.111	Block	10
213.57.165.45	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	9
2.54.136.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
109.253.142.179	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.142.179	Block	8
84.228.14.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
110.87.23.210	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 110.87.23.210	Block	7
31.168.210.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
171.107.126.153	China	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	6
76.102.116.177	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	6
84.228.64.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
69.89.8.39	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.89.8.39	Block	5
216.104.160.133	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 216.104.160.133	Block	5
95.86.75.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
79.179.155.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
136.243.36.97	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 136.243.36.97	Block	5
85.64.66.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
105.108.9.164	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.108.9.164	Block	4
46.19.86.253	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	4
84.108.94.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.186.144.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.186.144.30	Block	4
79.180.4.52	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.186.144.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
105.109.134.24	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.109.134.24	Block	4
176.228.178.232	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationervice.aspx/getuserdetails	Block	4
85.250.47.155	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	4
85.64.153.187	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	4