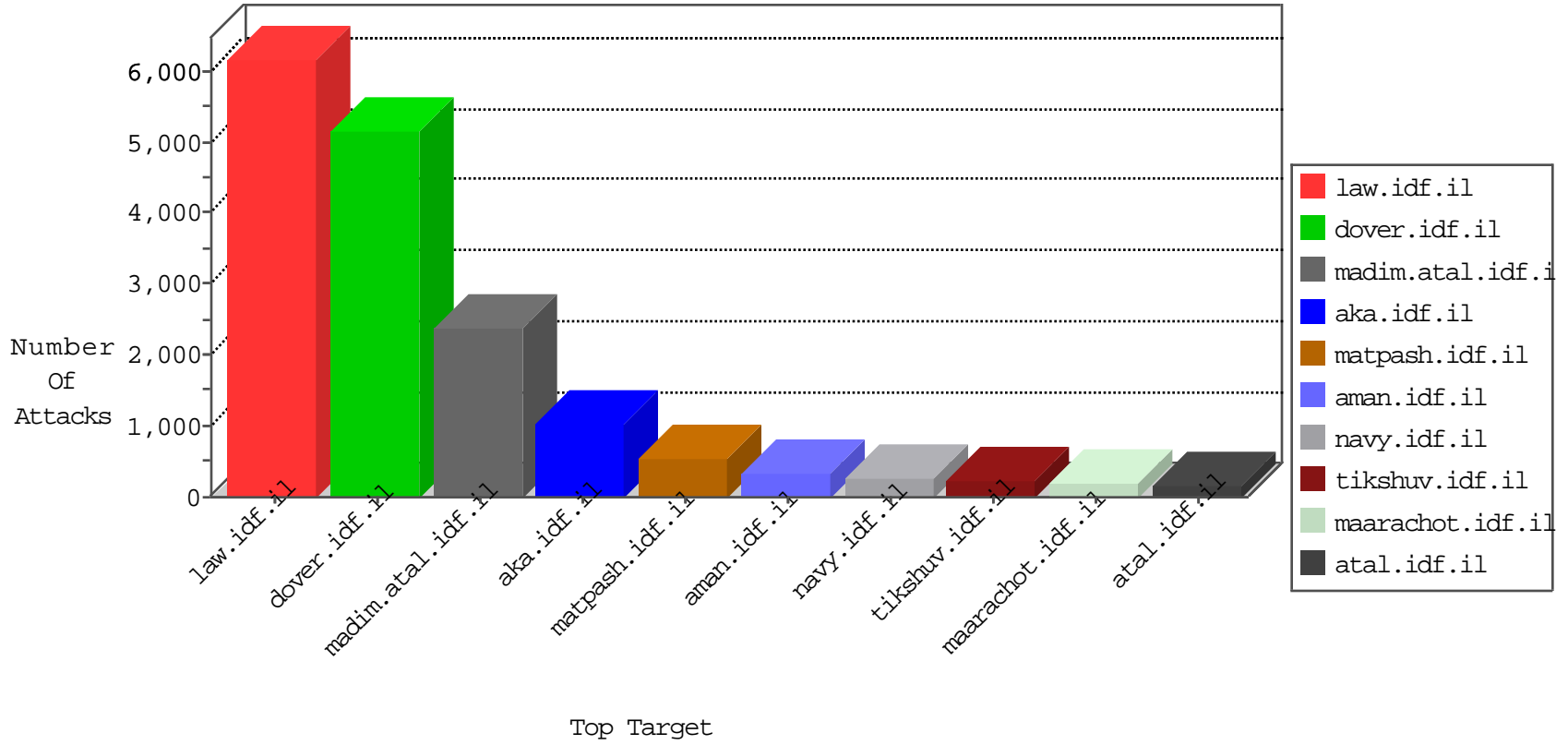


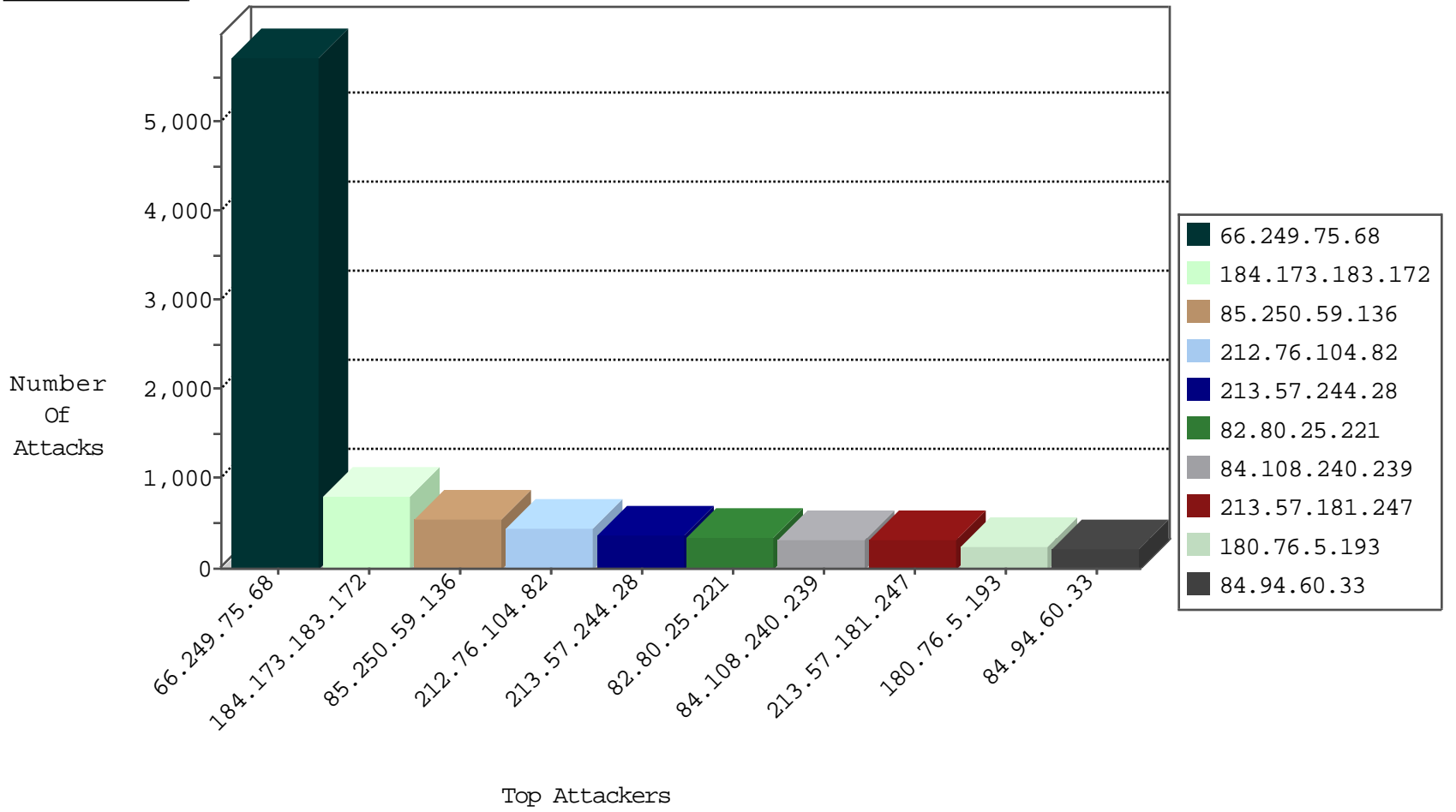
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.69.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	35098
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	25298
66.249.75.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	23621
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22068
66.249.69.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	21342
66.249.75.5	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	19426
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	15537
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	13979
77.127.215.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13545
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	13485
66.249.78.86	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	13337
93.215.75.193	Germany	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	12695
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	12482
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	12412
66.249.81.209	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11683
149.88.74.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10446
66.249.69.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9741
220.181.108.181	China	147.237.0.19	madim.atal.idf.il	TCP handshake violation, first packet not syn	drop	9518
82.145.209.47	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8652
66.249.78.93	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	7572
66.249.75.117	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7542
66.249.91.142	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7298
129.100.205.213	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6763
66.249.93.242	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6471
109.110.126.23	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6372
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6105
82.205.52.103	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6063
66.249.78.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	5911
107.167.102.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5393
93.222.214.158	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5350
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	5275
66.249.69.74	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5051
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4957
66.249.64.4	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4318
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4253
66.249.81.134	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4098
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4013
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3461
66.249.75.105	Israel	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	3425
220.181.108.108	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3310
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3238
66.249.75.109	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3010
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2962
184.148.8.249	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2958
10.0.0.8		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2832
46.19.86.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2599
157.55.39.58	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2547

04-25-2015-00:00:03 to 04-26-2015-00:00:03

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
149.88.81.174	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2441
79.180.143.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2263
79.181.12.39	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2225

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	356
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	316
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	182
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	127
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	66
61.41.4.6	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
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	20
199.168.141.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	17
46.19.85.184	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
176.228.56.240	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
77.127.231.70	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.65.73.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.187.90	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
223.73.47.211	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
46.116.175.178	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
79.181.6.241	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
89.139.31.120	Israel	147.237.77.233	atal.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
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	4
89.164.198.59	Croatia	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
80.178.28.251	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	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
77.127.196.121	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
79.176.111.55	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	3
85.10.202.245	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
163.47.14.86	Japan	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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
37.142.44.24	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5729
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	349
132.72.224.217	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	176
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	139
79.177.197.22	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	63
80.246.138.108	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	30
222.84.7.148	China	147.237.72.166	aka.idf.il	SQL Injection - Select From	17
79.177.197.22	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
2.54.187.105	Israel	147.237.77.243	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
66.249.75.64	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
66.249.75.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
79.178.145.177	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
66.249.78.51	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt	6
63.115.50.73	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	5
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spanhaus DROP Listed Traffic Inbound	5
202.207.240.35	China	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	5
66.249.75.80	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
5.101.157.38	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.72	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
46.120.106.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.67.17.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
176.12.146.143	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
222.48.110.22	China	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
69.165.167.117	Canada	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	GPL WEB_SERVER webalizer access	3
61.183.128.6	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	3
209.54.58.90	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
169.199.27.68	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	3
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP webalizer access	3
109.66.127.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability	2
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	2
88.249.106.23	Turkey	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss web console access attempt	2
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
209.54.58.90	United States	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
169.199.27.68	United States	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.76.104.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	450
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	143
84.228.17.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
82.145.220.10	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
77.125.3.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
109.253.142.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
84.229.208.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
65.255.37.223	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
85.250.146.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
166.137.252.122	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
149.88.74.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
188.103.97.166	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
84.108.236.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
130.154.0.250	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	27
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
213.57.208.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
188.102.129.122	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
68.100.96.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
76.20.225.18	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
85.65.244.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.86.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.129.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
79.177.160.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
91.232.101.24	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.19.86.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.120.40.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
149.78.245.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
82.145.216.128	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.66.152.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
149.88.21.87	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
213.57.109.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.19.85.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
64.233.173.151	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.150.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.229.177.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
188.225.140.29	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.116.253.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.59.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.250.59.136	Block	555
213.57.244.28	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.244.28	Block	358
84.108.240.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	323
213.57.181.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	312
84.94.60.33	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.94.60.33	Block	209
109.253.149.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	103
46.19.85.32	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.32	Block	100
109.253.147.152	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.147.152	Block	97
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	85
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	85
46.117.135.158	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.117.135.158	Block	71
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	64
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	46
79.176.2.151	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.176.2.151	Block	35
77.126.66.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.126.66.164	Block	32
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	25
79.183.181.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	20
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	18
85.65.2.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.2.57	Block	16
109.67.24.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.24.60	Block	16
46.117.135.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
62.90.117.133	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	15
109.253.130.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	13
164.138.116.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
149.88.158.169	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
37.26.146.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
95.86.104.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
197.36.135.219	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	8
79.176.215.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
164.138.121.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	7
85.64.246.105	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
95.86.113.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
79.182.151.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
84.108.187.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
217.12.204.155	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
37.142.126.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
12.151.36.19	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	5
187.45.240.69	Brazil	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 187.45.240.69	Block	5
79.182.31.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
134.249.53.8	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	5