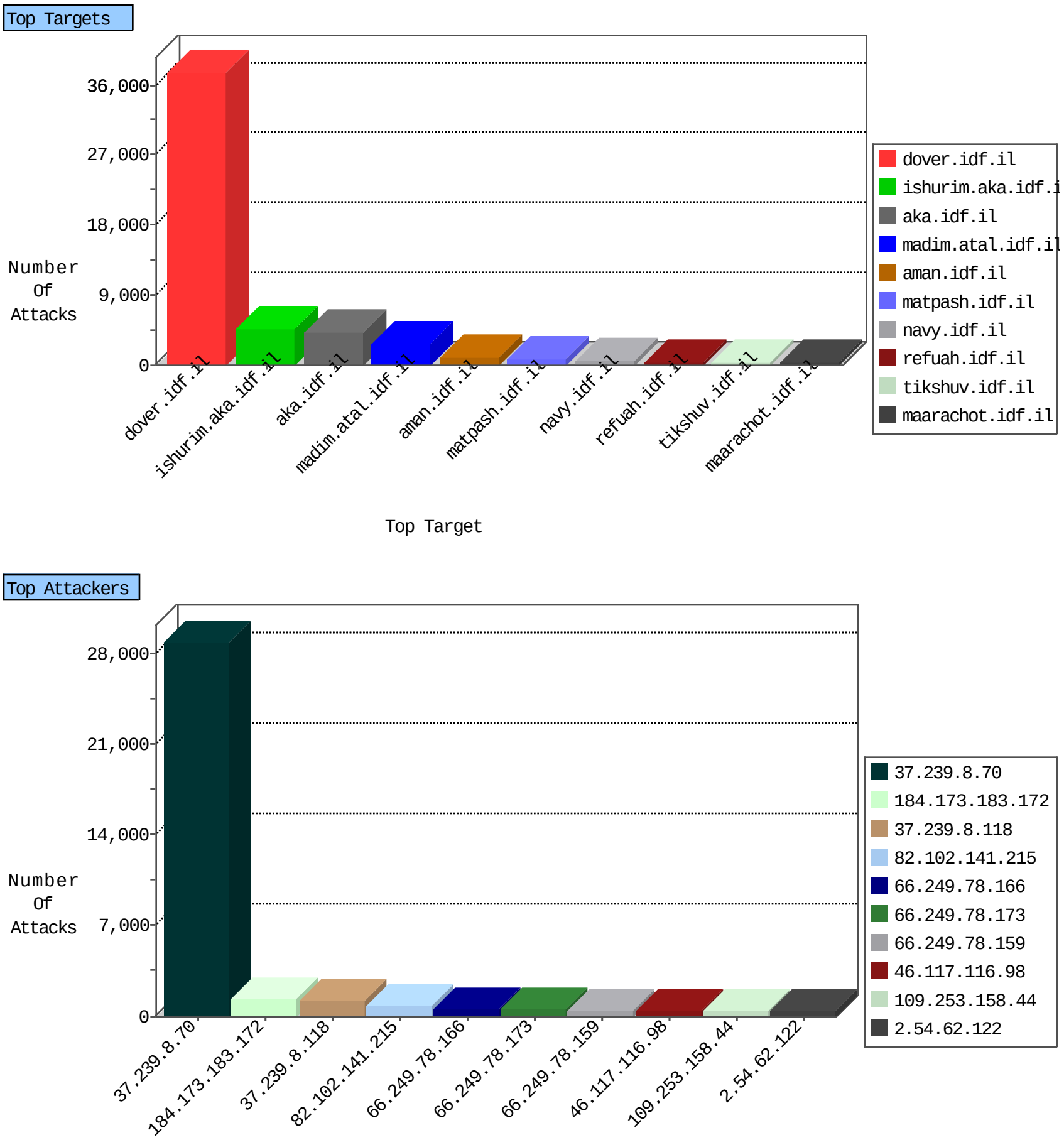
02-05-2015-00:00:06 to 02-06-2015-00:00:06

IDF Under Attack Daily Report



02-05-2015-00:00:06 to 02-06-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.66.154.153	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	1971
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	682
109.65.104.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	599
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	446
109.65.164.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	355
192.114.23.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	329
93.173.165.213	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	329
46.19.86.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	323
185.32.179.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	286
46.19.86.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	258
31.44.132.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	248
213.57.112.79	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	244
79.180.118.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	194
95.86.79.228	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	193
83.130.103.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
80.246.141.39	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	160
192.116.128.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	156
87.69.80.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
80.246.136.108	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	124
94.230.86.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
213.57.231.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
37.142.6.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
84.108.217.87	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	112
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
89.139.4.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
213.57.112.79	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
87.69.222.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
37.142.114.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.120.178.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
2.54.185.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
193.109.199.173	United Kingdom	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	85
5.29.33.122	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
109.65.144.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
82.102.141.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.253.149.201	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
85.65.143.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
87.69.14.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
37.26.148.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
212.179.41.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
77.125.213.106	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.182.121.217	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
82.102.141.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.85.166	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	72
82.102.141.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
31.168.155.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.86.79	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
176.12.142.72	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	63
109.65.104.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
2.54.155.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61

02-05-2015-00:00:06 to 02-06-2015-00:00:06

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	533
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	483
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	302
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	210
162.247.96.94		147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	37
103.224.248.24	Hong Kong	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	37
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	20
192.115.248.2	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
84.108.233.58	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
85.64.84.211	Israel	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	10
212.25.126.82	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
106.138.53.113	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
116.251.221.226	Singapore	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
85.64.84.211	Israel	147.237.76.42	refuah.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	7
87.98.159.231	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	6
212.179.132.203	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
62.210.74.137	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
147.236.38.204	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.43.94	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
2.247.196.240	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
72.52.75.27	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
193.105.199.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_P-N_40-59	Permit	4
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4

02-05-2015-00:00:06 to 02-06-2015-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
2.54.62.122	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	320
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	102
61.160.224.128	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	72
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	70
122.228.207.190	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	69
218.77.79.43	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	53
122.228.207.190	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	47
61.160.224.128	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	47
218.77.79.43	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	43
41.89.165.7	Kenya	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	42
197.203.205.0	Algeria	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	42
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	35
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	33
164.138.118.198	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	27
61.160.224.128	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	26
205.189.94.13	Canada	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	25
61.160.224.128	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	24
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	23
122.228.207.190	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	23
122.228.207.190	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	21
218.77.79.43	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	21
61.160.224.128	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	20
78.24.220.21	Russian Federation	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	18
122.228.207.190	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	17
61.160.224.128	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	16
61.160.224.128	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	16
222.186.52.95	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	16
218.77.79.43	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	16
222.186.52.95	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	16
79.180.135.177	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	16
84.228.72.193	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	16
195.238.181.159	Ukraine	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	15
78.24.220.21	Russian Federation	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	15
77.126.191.63	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	14
122.228.207.199	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	14
71.6.165.200	United States	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	14
71.6.135.131	United States	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	14
5.29.33.122	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	13
195.238.181.159	Ukraine	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	13
189.112.5.152	Brazil	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	13
46.19.85.47	Israel	147.237.76.86	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	13
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	13
79.179.29.114	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	12
122.228.207.190	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	12
5.102.253.9	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
61.160.224.128	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	12
176.103.48.38	Ukraine	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	12
212.76.102.131	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
122.228.207.190	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	12

02-05-2015-00:00:06 to 02-06-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.239.8.70	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15480
37.239.8.70	Iraq	147.237.77.216	dover.idf.il		drop	drop	10482
37.239.8.70	Iraq	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1213
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	340
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	298
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	260
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
37.239.8.118	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
197.203.205.0	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	116
80.179.122.185	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	89
194.90.134.254	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	78
195.212.29.164	Europe	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
109.186.93.149	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
79.177.96.52	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	53
93.157.87.62	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	52
2.54.62.122	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	51
212.117.152.34	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
66.102.6.208	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
109.253.158.92	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
175.42.40.137	China	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	44
37.239.8.118	Iraq	147.237.77.216	dover.idf.il		drop	drop	43
176.12.144.12	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.149.248	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	42
5.22.129.192	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	40
178.62.192.185	Netherlands	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	40
82.102.141.195	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
212.143.233.33	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
147.236.238.159	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
91.228.248.251	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	38
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
132.74.58.101	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	38
213.57.113.137	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
2.54.166.201	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.64.97.117	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	35
79.177.122.2	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
168.63.139.43	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
176.12.156.150	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.64.50.95	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
46.19.86.81	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	31
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.80	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.146.99	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
5.22.129.192	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	30
176.12.146.86	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
89.69.190.175	Poland	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.239.8.70	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1589
37.239.8.118	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	610
82.102.141.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.141.215	Block	594
109.253.158.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	417
213.57.112.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	252
46.117.116.98	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	243
46.117.116.98	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in IP from 46.117.116.98	Block	242
109.253.140.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.189	Block	233
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	204
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	195
37.239.8.118	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	180
37.239.8.118	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.239.8.118	Block	179
82.102.141.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
5.29.33.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.33.122	Block	167
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	116
109.253.138.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
109.253.133.94	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.133.94	Block	102
109.253.147.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
109.253.146.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
37.239.8.70	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	76
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	72
109.253.143.68	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.143.68	Block	71
37.239.8.70	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.239.8.70	Block	60
109.253.133.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
201.251.19.23	Argentina	147.237.72.166	aka.idf.il	PHP Attempt	Block	48
91.207.7.178	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.207.7.178	Block	39
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	38
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
66.249.64.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	34
80.178.235.36	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	29
46.121.132.215	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.121.132.215	Block	29
66.249.64.141	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	25
201.251.19.23	Argentina	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 201.251.19.23	Block	23
79.182.137.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	23
95.211.190.198	Netherlands	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.211.190.198	Block	21
109.253.158.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
66.249.78.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	21
195.212.29.164	Europe	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	21
2.54.131.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
85.64.26.3	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	16
79.178.48.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
66.249.64.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	16
132.70.43.8	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	14
66.249.64.149	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.149	Block	13
79.180.203.120	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	13
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	12
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	12
104.173.225.247		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	11
84.108.152.40	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 84.108.152.40	None	11
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	11