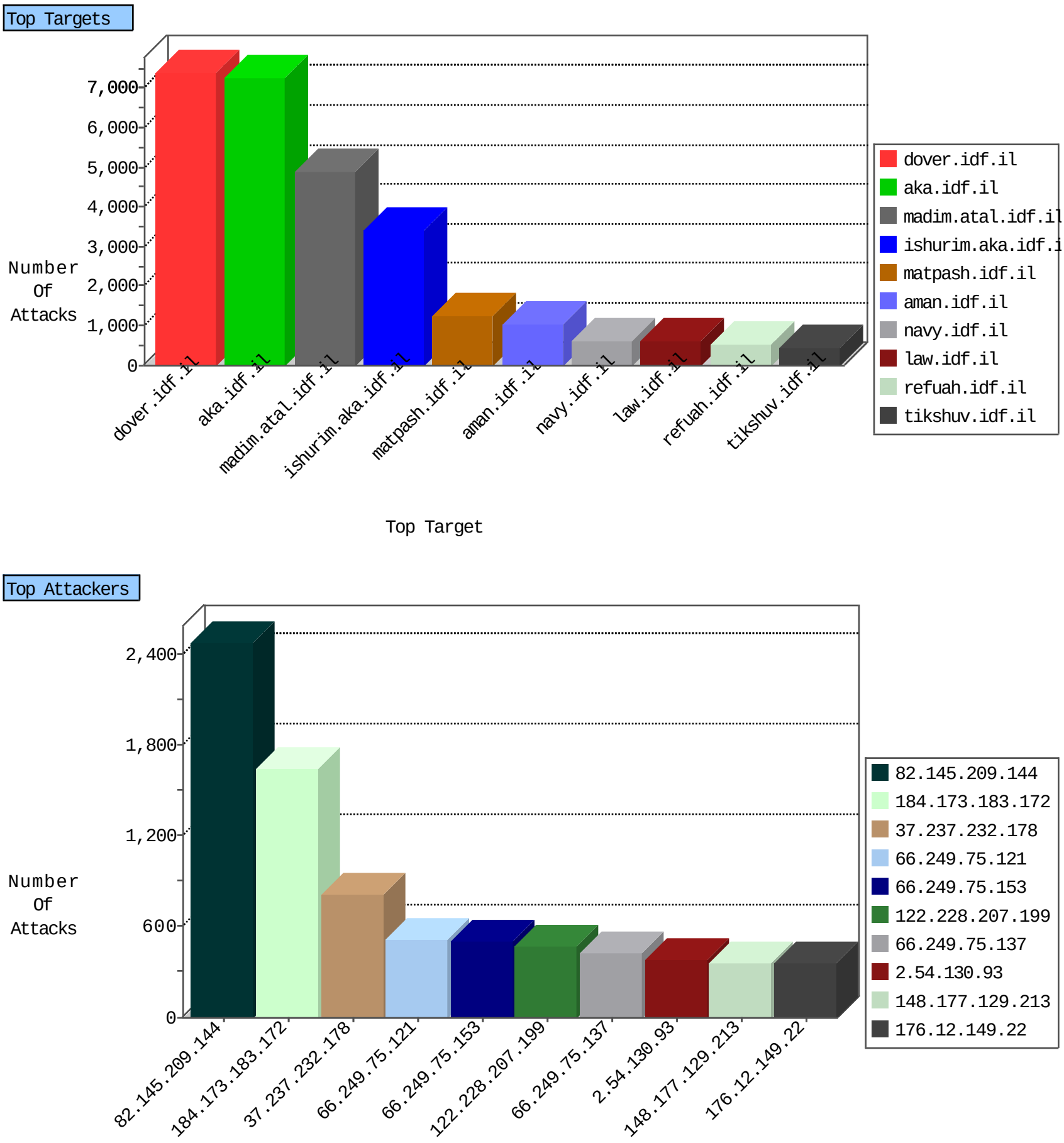
02-08-2015-00:00:06 to 02-09-2015-00:00:06

IDF Under Attack Daily Report



02-08-2015-00:00:06 to 02-09-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11349
84.108.220.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	2799
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1667
5.28.174.81	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1480
66.249.67.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1214
46.116.228.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	961
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	959
82.80.17.247	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	540
79.176.53.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	520
68.196.241.248	United States	147.237.72.167	ishurim.aka.idf.i	TCP handshake violation, first packet not syn	drop	449
31.168.103.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	399
79.178.126.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	361
66.249.67.142	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	301
37.142.37.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	298
66.249.78.96	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	271
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
212.25.67.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	233
77.126.96.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	TCP handshake violation, first packet not syn	drop	200
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
85.64.185.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
79.177.13.134	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
94.159.214.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
84.109.240.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
192.117.138.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
213.57.49.216	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
132.73.203.178	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	150
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	148
85.64.56.101	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	137
87.69.222.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
46.120.165.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
94.159.151.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
82.102.141.252	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	130
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
82.102.141.197	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	125
79.176.173.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.179.105.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.176.113.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
46.19.86.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
46.117.16.111	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	111
192.116.142.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	109
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
212.235.28.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
84.228.220.228	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
5.29.83.3	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	96
66.249.64.123	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	92
87.69.119.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
37.142.46.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
2.54.4.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87

02-08-2015-00:00:06 to 02-09-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.145.209.144	Europe	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	2476
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	749
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	516
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	282
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	232
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	72
109.186.228.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	49
46.165.222.65	Germany	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	35
46.117.17.211	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
212.179.132.201	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
5.28.181.220	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
85.250.143.154	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	8
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	7
109.65.60.251	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
5.144.49.212	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
210.245.122.47	Vietnam	147.237.77.216	dover.idf.il	EgovRep_B-N_70-99	Block	5
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
182.50.130.87	Singapore	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
212.34.12.121	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.154.99.24	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
173.244.35.100	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.175.86	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
91.149.157.169	Belarus	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
85.65.171.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.1.229	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.135	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
95.130.15.96	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.81	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	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_P-N_40-59	Permit	3
109.160.251.16	Israel	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	147.237.0.33	idf.il	DVRep_P-N_40-59	Permit	3
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
184.168.193.35	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
5.29.158.46	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3

02-08-2015-00:00:06 to 02-09-2015-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.81.184	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	180
184.168.193.35	United States	147.237.77.74	law.idf.il	SQL Injection - Select From	122
182.50.130.87	Singapore	147.237.77.74	law.idf.il	SQL Injection - Select From	101
198.154.99.24	United States	147.237.77.74	law.idf.il	SQL Injection - Select From	91
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	82
122.228.207.199	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	61
220.248.17.110	China	147.237.76.198	e.yohalan.idf.il	GPL SCAN nmap TCP	55
85.113.113.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL Injection - Select From	52
197.203.94.31	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Select From	44
91.149.157.169	Belarus	147.237.77.74	law.idf.il	SQL Injection - Select From	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	31
118.26.143.50	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	29
104.152.105.117		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	29
122.228.207.199	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	27
122.228.207.199	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	27
5.196.147.122	Germany	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	25
180.169.108.158	China	147.237.76.198	e.yohalan.idf.il	GPL SCAN nmap TCP	25
122.228.207.199	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	24
66.249.75.121	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	22
122.228.207.199	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	22
122.228.207.199	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	22
176.12.147.120	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	21
104.152.105.117		147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	20
122.228.207.199	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	19
122.228.207.199	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	18
118.26.143.50	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	17
74.82.51.190	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	17
119.48.248.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	16
118.26.143.50	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	16
122.228.207.199	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	15
119.48.248.77	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	15
119.48.248.77	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	14
122.228.207.199	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	14
188.120.148.55	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	14
122.228.207.199	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	13
122.228.207.199	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	13
122.228.207.199	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	13
5.102.253.20	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
96.45.180.58	Canada	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
122.228.207.199	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	12
111.73.45.242	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
122.228.207.199	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	11
216.172.94.8	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	11
178.63.126.73	Germany	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	10
96.45.180.58	Canada	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	10
122.228.207.199	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	10
122.228.207.199	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	10
164.138.124.155	Israel	147.237.72.166	aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
122.228.207.199	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	9
104.152.105.117		147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	9

02-08-2015-00:00:06 to 02-09-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.75.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	474
66.249.75.121	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	472
66.249.75.137	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	410
148.177.129.213	Europe	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	360
194.170.16.85	United Arab Emirates	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	324
8.37.226.5	Anonymous Proxy	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	271
79.183.137.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	156
179.236.65.234	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	110
195.64.208.129	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
198.143.187.122	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
46.19.85.13	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
66.249.64.120	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
212.143.158.173	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
98.183.186.210	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
188.15.62.197	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
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
84.95.133.56	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
62.201.200.11	Iraq	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	33
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.180.218.111	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
213.8.123.112	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
77.127.84.130	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	31
84.228.73.177	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.145.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.60	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.144.121	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.100	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
212.29.249.212	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.184	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.64.96.199	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
109.253.134.14	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.253.143.177	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.253.132.102	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
93.173.251.245	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	27
82.80.64.158	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	26
192.99.12.99	Canada	147.237.0.15	kosher-kravi.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	25
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	25
176.12.137.48	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
80.246.141.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	24
176.12.141.42	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.228.82.18	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
176.12.143.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.178.71.200	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
46.43.103.115	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
62.90.161.153	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
86.171.247.121	United Kingdom	147.237.77.176	matpash.idf.il	Invalid sequence number	Bad TCP sequence	monitor	23
66.102.6.208	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22

02-08-2015-00:00:06 to 02-09-2015-00:00:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.237.232.178	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	815
2.54.130.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	374
176.12.149.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	361
109.253.157.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	270
109.253.132.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
37.26.146.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
176.12.146.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.146.213	Block	216
79.176.149.214	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.176.149.214	Block	212
176.12.147.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
176.12.141.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	166
109.253.146.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	164
2.54.0.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	152
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.47	Block	142
176.12.144.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	142
176.12.140.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
176.12.149.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
176.12.148.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	102
176.12.136.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.157	Block	91
109.253.128.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	87
176.12.136.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
109.253.149.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	80
176.12.139.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.139.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	72
109.253.139.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	70
109.253.141.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.136.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
176.12.148.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
82.102.141.207	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 82.102.141.207	Block	55
109.253.151.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
109.253.146.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.138.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
176.12.156.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
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	31
109.253.157.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
109.253.135.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
84.108.127.14	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	26
66.249.75.153	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.153	Block	23
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.54	Block	23
109.253.143.115	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.143.115	Block	23
109.253.138.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
79.180.111.162	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	20
109.253.157.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
31.168.70.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
176.12.140.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
176.12.148.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
66.249.75.137	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.137	Block	17
2.54.4.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
79.181.102.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
5.29.93.26	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

02-08-2015-00:00:06 to 02-09-2015-00:00:06