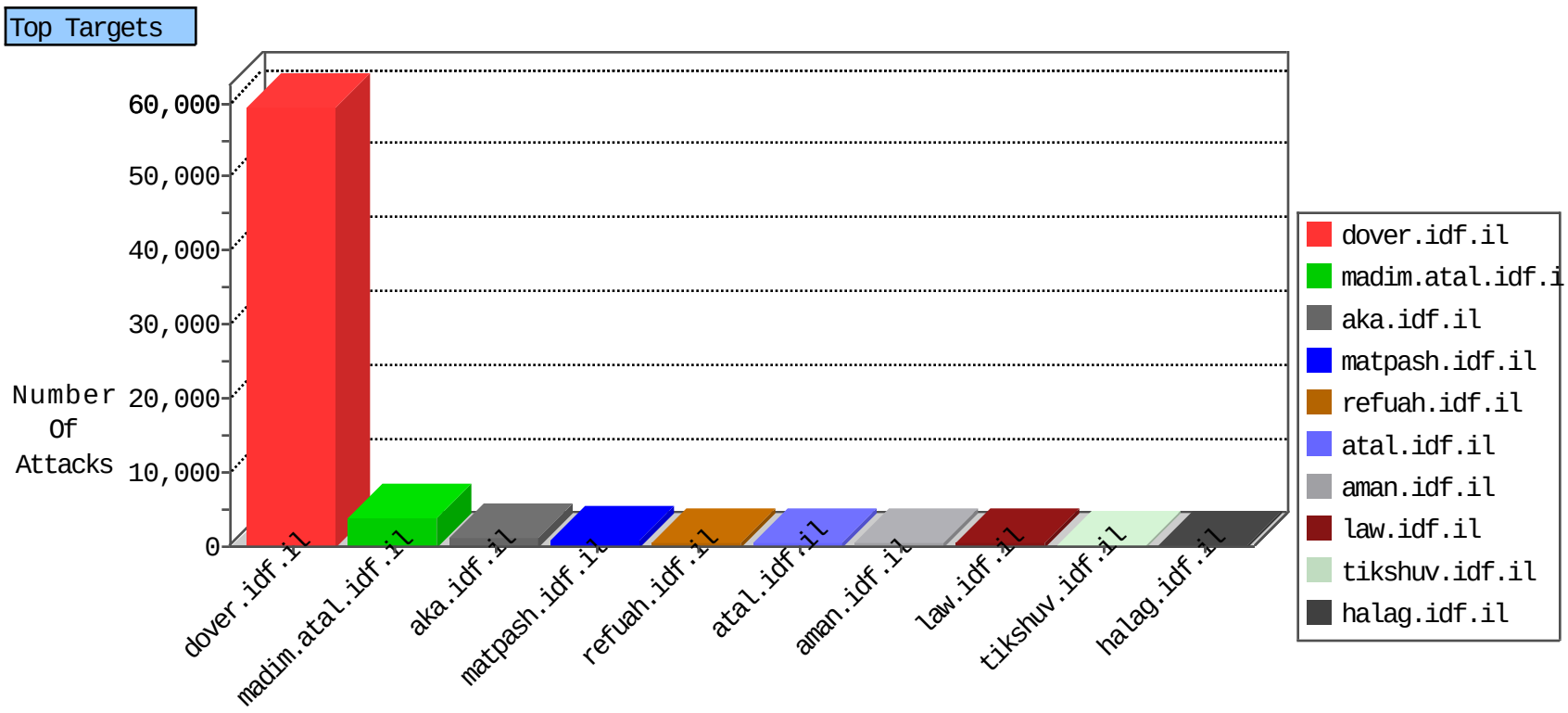
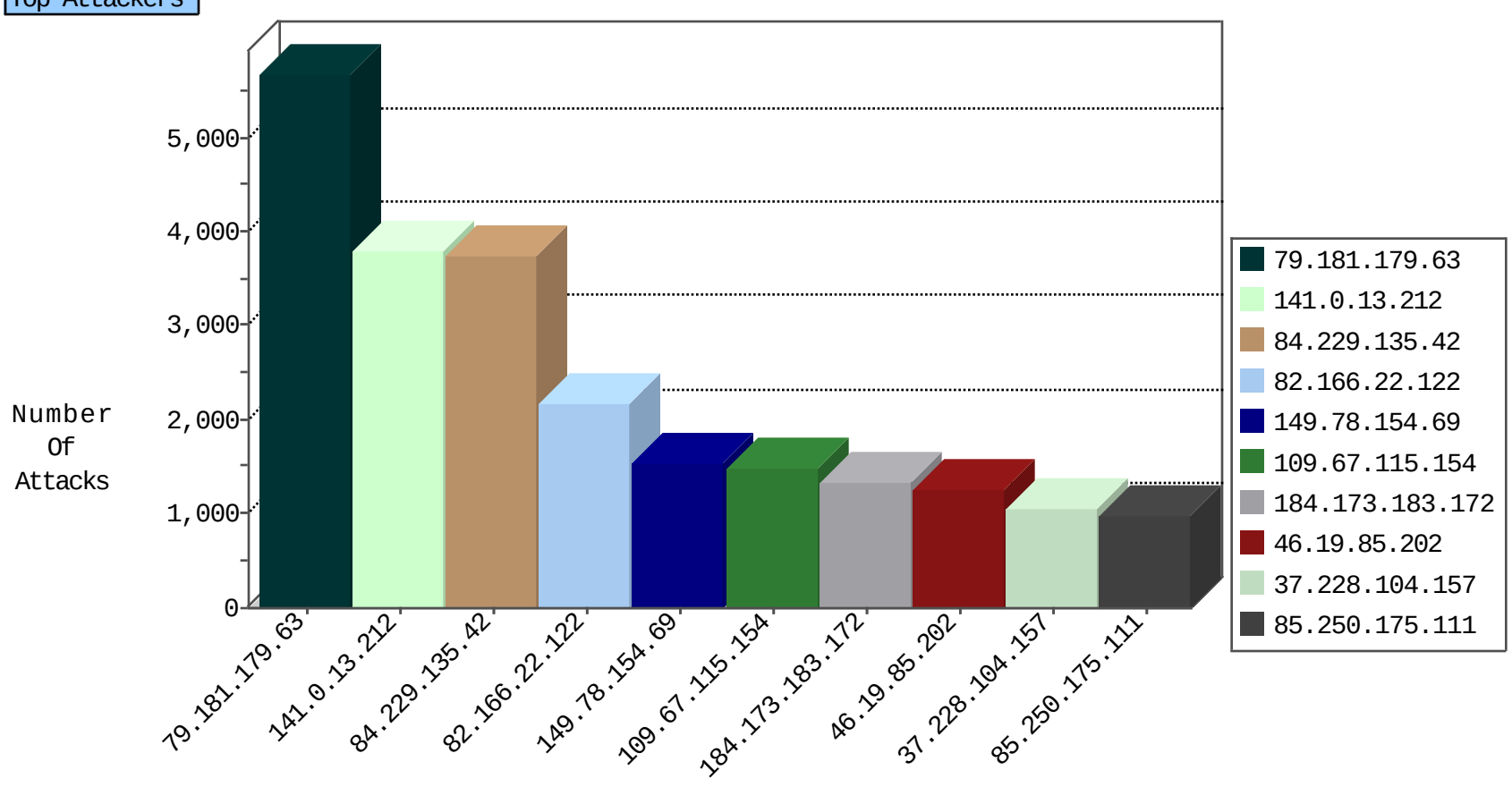
06-26-2015-00:00:01 to 06-27-2015-00:00:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



06-26-2015-00:00:01 to 06-27-2015-00:00:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3343
141.0.13.212	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1060
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	830
198.52.155.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	754
82.166.22.128	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	546
109.186.180.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	319
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	317
79.183.97.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	282
46.117.9.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	247
77.125.116.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
109.67.30.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
31.154.170.146	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
2.54.156.183	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
220.181.108.91	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	173
46.121.144.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
79.183.199.183	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
87.69.108.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
93.172.54.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
213.57.112.190	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
84.111.64.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
80.246.136.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
176.13.0.130	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.117.136.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
77.126.175.208	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
46.19.85.242	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	92
213.57.48.130	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	86
87.69.0.232	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
77.127.203.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	82
5.28.174.251	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
85.65.22.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
77.127.191.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
185.32.178.134	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
2.54.38.108	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
2.54.173.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	65
82.166.1.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
77.126.215.167	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
176.12.147.60	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
79.183.97.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	61
109.186.180.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57
164.138.112.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
46.210.209.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
212.143.121.82	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
79.180.204.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
5.102.103.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	13
81.218.85.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
82.145.210.29	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
194.90.39.41	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.168.14.42		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12

06-26-2015-00:00:01 to 06-27-2015-00:00:01

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	398
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	374
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	243
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	168
184.173.183.172	United States	147.237.76.200	eitan.aka.idf.il	DVRep_P-N_40-59	Permit	121
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	23
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	8
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	8
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	6
46.120.5.59	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.182.145.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
211.25.14.180	Malaysia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
73.36.167.240	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5

06-26-2015-00:00:01 to 06-27-2015-00:00:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	139
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	13
82.205.47.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	10
97.74.24.193	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
109.65.5.220	Israel	147.237.77.170	maarachot.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	5
43.255.188.133	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	4
178.137.164.105	Ukraine	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
66.249.73.225	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
43.255.188.132	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	3
198.52.155.201	United States	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.65.5.220	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
198.52.155.201	United States	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
198.52.155.201	United States	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
43.255.188.133	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.198	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
31.210.187.221	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
43.255.188.133	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
198.52.155.201	United States	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
43.255.188.131	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.76.177	ncore.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
43.255.188.133	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
198.52.155.201	United States	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.133	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
5.189.133.241	Russian Federation	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.188	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2

06-26-2015-00:00:01 to 06-27-2015-00:00:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.181.179.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5680
141.0.13.212	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3799
84.229.135.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3738
82.166.22.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2113
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1521
109.67.115.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1485
46.19.85.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1254
37.228.104.157	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1054
85.250.175.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	926
170.148.69.141	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	810
168.235.197.31		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	675
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	636
82.145.221.4	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	595
46.19.86.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	594
2.54.55.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	413
141.0.12.45	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	398
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	357
207.46.13.120	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	322
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	317
82.145.219.193	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	313
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
46.19.85.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	299
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	295
79.178.155.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	281
164.11.203.58	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	277
95.86.76.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	276
108.22.245.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	232
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
65.49.68.178	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220
86.155.209.112	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
85.250.250.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
138.106.57.132	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	207
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	202
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
157.55.39.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
79.182.145.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	176
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	160
46.116.77.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
207.46.13.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
182.250.253.39	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
70.210.228.70	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	148
210.4.97.2	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	147
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	147
212.199.57.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	137
38.111.147.86	United States	147.237.76.42	refuah.idf.i		drop	drop	132

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.167.5	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.167.5	Block	695
109.64.128.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	494
213.57.181.247	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.181.247	Block	422
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	350
84.228.17.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.17.182	Block	333
213.57.167.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
2.52.53.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
79.178.53.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	249
2.54.17.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	245
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	89
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	80
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	70
176.12.146.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
109.253.133.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	PHP Attempt	Block	48
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	46
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	42
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	38
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	34
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
2.52.14.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
198.204.230.130	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 198.204.230.130	Block	28
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 182.50.130.47	Block	23
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
89.139.32.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.32.79	Block	18
213.8.11.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
109.65.96.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.96.243	Block	12
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	8
46.117.116.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
85.64.129.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	6
37.26.147.220	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	6
157.55.39.219	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
84.109.3.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
31.168.96.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
195.60.232.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.186.32.82	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
87.69.175.96	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
46.117.219.84	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
195.128.174.111	Denmark	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.128.174.111	Block	5
46.117.193.171	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
46.117.30.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
212.76.125.99	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	5
79.178.184.123	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.178.184.123	None	4
5.102.103.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.102.103.138	Block	4
37.142.239.135	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	4
37.26.147.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4