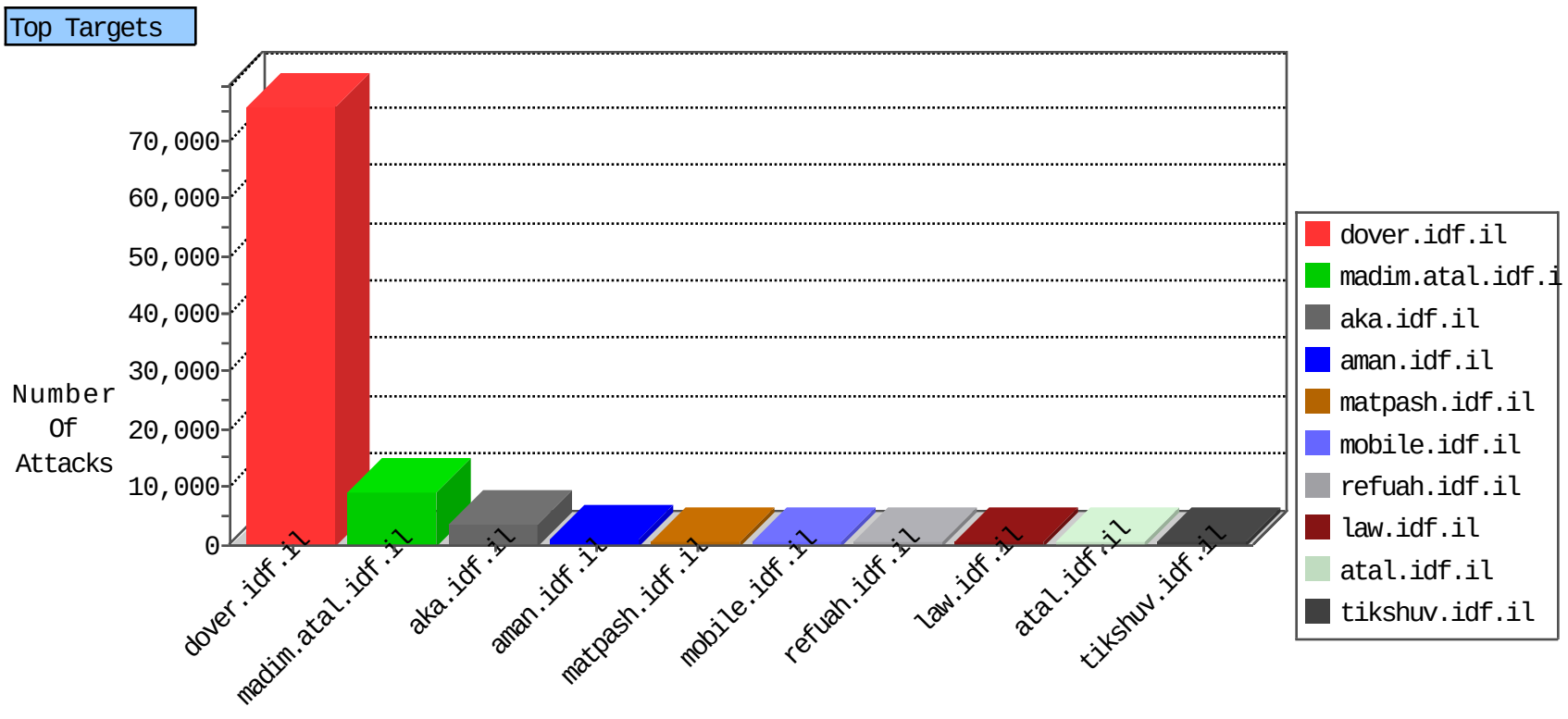
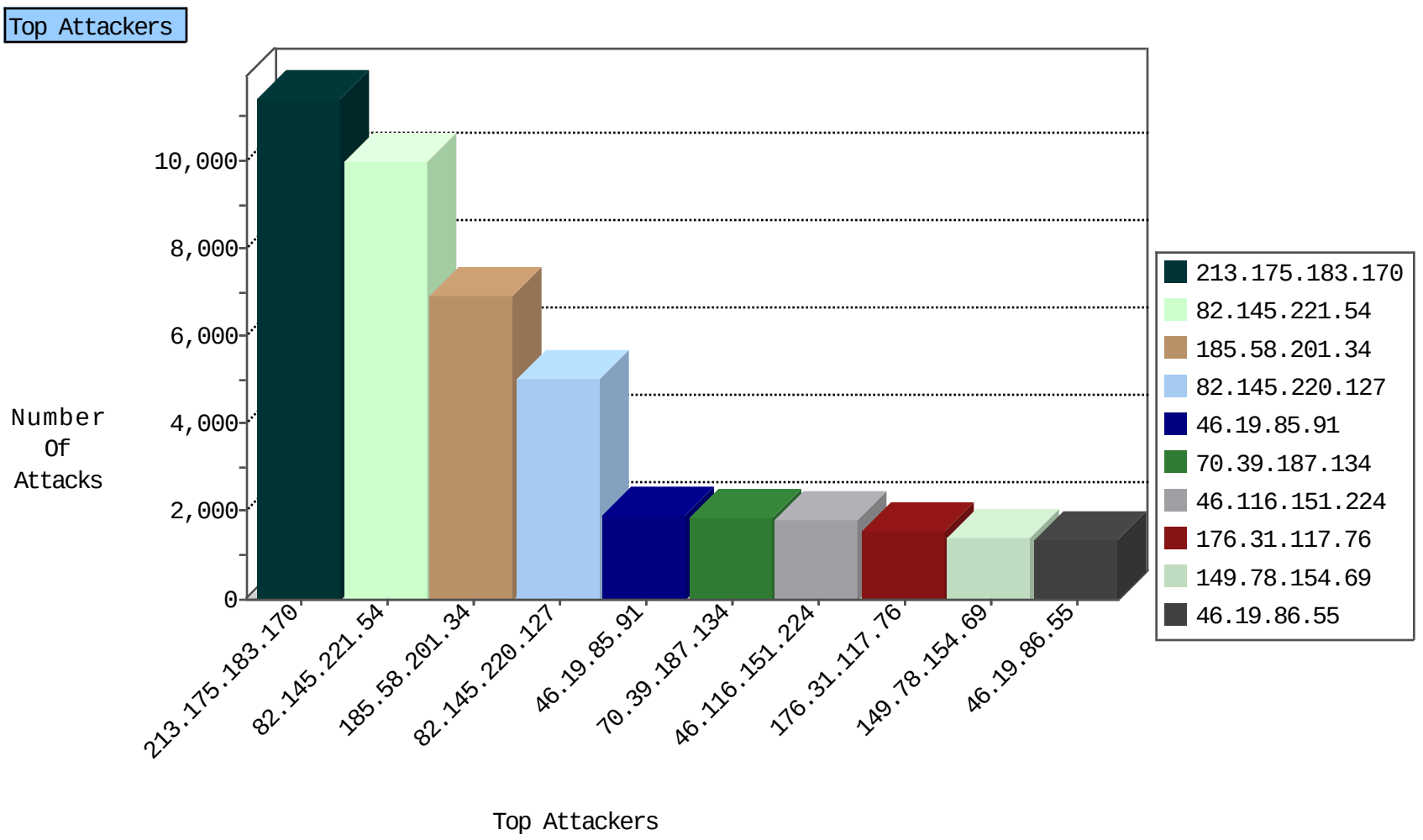
08-08-2015-00:00:00 to 08-09-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-08-2015-00:00:00 to 08-09-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	16979
66.249.67.81	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14077
107.178.194.83	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	6346
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3164
79.183.128.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3016
66.249.93.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2755
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2740
46.116.72.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2563
5.43.192.79	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1702
77.127.95.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1553
79.182.149.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	851
85.64.214.89	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	706
84.110.83.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	563
46.121.110.241	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	546
5.28.130.169	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	526
176.13.5.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	490
31.168.90.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	416
79.179.109.109	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
46.116.155.80	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	256
109.64.200.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
77.127.101.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
82.166.22.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
109.186.34.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
79.183.160.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
84.108.37.229	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
84.108.168.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
149.78.184.219	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.120.198.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
2.54.32.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
176.13.1.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81
46.117.29.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
2.54.63.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	78
84.94.80.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
176.13.10.31	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
93.172.135.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
62.219.126.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
2.52.160.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
85.64.45.45	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	58
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
10.0.0.3		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	30
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	22
79.177.61.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.19.85.19	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
46.116.94.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.179.10.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
62.0.114.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
192.168.14.119		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18

08-08-2015-00:00:00 to 08-09-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.95.156	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	105
79.182.149.149	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	62
176.228.149.147	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	21
95.179.106.151	Russian Federation	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
82.166.22.13	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
109.66.128.80	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.108.44.125	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.121.116.143	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
93.172.185.227	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.68.106	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.148.227	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
46.120.229.31	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
24.161.55.206	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
24.250.129.65	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.176.54.116	Czech Republic	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.116.179.248	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.217.31	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
95.179.34.8	Russian Federation	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
24.57.243.7	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.78.86.173	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
41.202.168.161	Sudan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
176.228.40.169	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.121.85.48	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
41.234.168.243	Egypt	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.5	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.32.179.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.159.242.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.7	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
145.116.179.251	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
41.45.121.23	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.66.128.145	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.116.233.65	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.120.134.79	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.108.4.163	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.182.53.62	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.122.84	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.109.73	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.175	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.81.11.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
79.178.137.147	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
94.159.147.154	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.117.0.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.161.186.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	10714: HTTP: Netsparker Security Scanner	Block	1
37.142.64.139	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.88.91.170	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

08-08-2015-00:00:00 to 08-09-2015-00:00:00

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
10.0.0.3		147.237.76.42	refuah.idf.il	ET SCAN TCP Traffic (ET SCAN Malformed Packet SYN FIN)	41
186.15.2.129	Costa Rica	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	30
109.67.169.151	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	16
66.249.69.63	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
45.114.11.46		147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	4
66.249.93.253	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	4
45.114.11.46		147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.46		147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.46		147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
220.194.63.2	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	3
208.80.155.222	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
45.114.11.46		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	3
220.194.63.2	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
91.236.3.196	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
5.2.156.182	Romania	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
45.114.11.46		147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.46		147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.0.15	kosher-kravi.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
45.114.11.49		147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
119.167.153.189	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
91.236.3.196	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
212.231.63.69	Spain	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
84.1.159.210	Hungary	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.146	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.46		147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
212.231.63.69	Spain	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.18	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
5.2.156.182	Romania	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.114.11.46		147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
91.236.3.196	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2

08-08-2015-00:00:00 to 08-09-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.221.54	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10018
82.145.220.127	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5059
70.39.187.134	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1864
176.31.117.76	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1547
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1398
46.19.85.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	975
77.126.233.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	930
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	522
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	508
79.177.217.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	493
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	476
85.65.185.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	474
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	457
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	454
190.229.126.235	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	447
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	401
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	384
80.179.225.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	377
79.178.206.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	374
188.165.15.209	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	354
164.138.127.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	287
212.235.93.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	287
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	274
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
185.58.201.34		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
2.54.155.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
80.178.169.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	242
89.120.146.110	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
130.154.3.250	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
31.168.164.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	216
2.54.16.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
207.46.13.29	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	206
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	204
2.52.18.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	202
212.199.205.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	195
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	194
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	193
213.57.240.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
87.69.245.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
5.43.192.79	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	178
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	178
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	176
207.46.13.108	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	174
157.55.39.122	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	166
157.55.39.113	United States	147.237.0.34	tikshuv.idf.il	SAM rule	drop	drop	162
46.19.86.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	161
37.26.146.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
5.255.253.61	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	146

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined	Block	11351
185.58.201.34		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined	Block	6426
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.91	Block	1892
46.116.151.224	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.116.151.224	Block	1809
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.55	Block	1297
89.138.216.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1073
31.154.92.249	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.154.92.249	Block	909
176.13.23.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	609
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	438
2.54.24.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	420
149.78.49.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	408
185.58.201.34		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	243
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	204
46.121.65.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	174
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	144
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	114
176.12.145.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	108
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	96
85.65.247.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	93
46.121.40.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	87
37.26.149.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	69
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	66
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	60
37.26.148.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	57
176.13.2.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
193.201.224.126	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	45
77.127.133.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
188.165.15.209	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.209	Block	45
46.19.86.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
188.143.232.35	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	42
188.143.232.35	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 188.143.232.35	Block	42
77.162.249.39	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.162.249.39	Block	39
176.13.6.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
89.138.216.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
176.13.4.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
79.179.169.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	27
79.178.14.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	27
178.137.87.228	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	24
46.19.85.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	21
176.12.140.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	21
77.127.24.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	21
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	18
77.125.80.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.80.119	Block	18
82.166.22.13	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 82.166.22.13 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	15
157.55.39.59	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.59	Block	15
157.55.39.122	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.122	Block	15
109.65.24.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
46.119.124.209	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	15