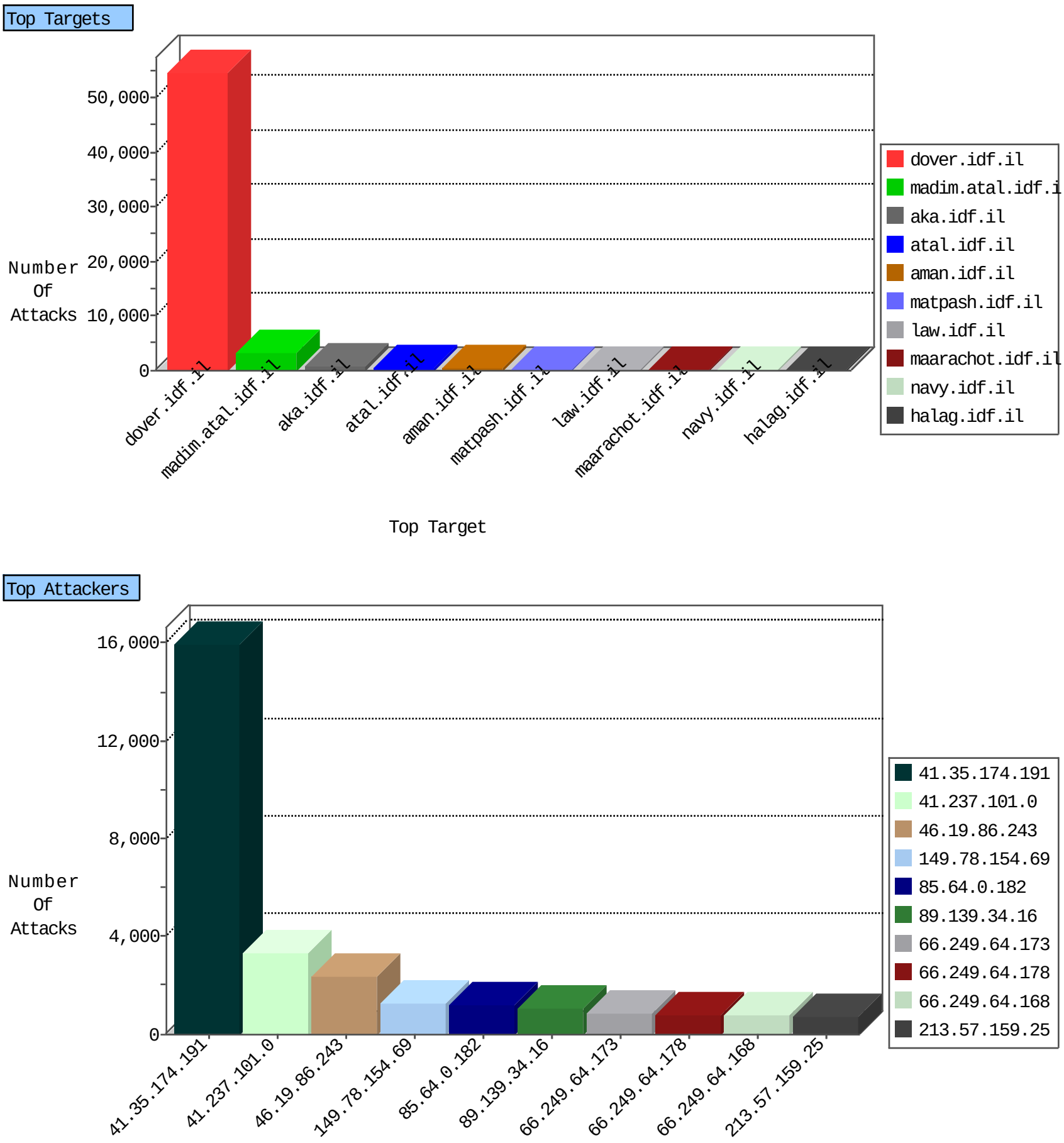
07-11-2015-00:00:08 to 07-12-2015-00:00:08

IDF Under Attack Daily Report



07-11-2015-00:00:08 to 07-12-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2981
41.237.101.0	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2720
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	439
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	328
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	323
85.250.23.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	302
217.132.79.98	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	282
85.65.122.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
213.57.60.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
5.102.219.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
66.249.64.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	180
81.218.46.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.178.198.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
77.125.151.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
46.116.76.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
84.94.175.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
109.67.157.151	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	138
188.120.148.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
188.120.148.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
93.173.59.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
85.65.112.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
79.176.72.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	100
77.127.95.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
84.95.199.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
109.186.154.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
220.181.108.92	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	79
46.120.43.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
149.78.1.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
79.180.36.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	67
109.64.57.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	64
94.159.188.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
79.177.112.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
85.64.76.118	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
85.64.76.118	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
10.0.0.5		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
5.29.140.210	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
176.12.144.54	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
66.249.64.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
192.115.177.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
2.54.40.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
192.115.177.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.120.216.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
93.173.159.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	16
213.55.184.194	Switzerland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13

07-11-2015-00:00:08 to 07-12-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.228.98.174	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	34
46.119.125.239	Ukraine	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
87.69.166.88	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
5.102.219.197	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	6
109.67.98.110	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.181.216.137	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.8.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.120.210.85	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.186.11.204	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.183	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.190	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.104.26	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.94	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.34.218	Israel	147.237.72.166	aka.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
46.19.85.127	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	2
108.231.22.57	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
202.62.17.196	Indonesia	147.237.77.170	maarachot.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
149.202.124.109	Germany	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
46.19.85.82	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
91.121.121.43	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
77.127.187.112	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
202.62.17.196	Indonesia	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
37.8.72.107	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.108.66.145	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
184.69.181.190	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.173.225.174	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.19.85.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.147.189	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
185.23.154.58	Iraq	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
106.38.241.118	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
79.179.164.241	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
37.26.148.213	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
202.62.17.196	Indonesia	147.237.72.166	aka.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
2.54.147.247	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.86.99	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
132.66.231.255	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
41.224.152.35	Tunisia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.247.252	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

07-11-2015-00:00:08 to 07-12-2015-00:00:08

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	121
184.168.193.118	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
184.168.193.118	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	8
66.249.64.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	6
202.62.17.196	Indonesia	147.237.77.170	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
66.249.64.178	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	6
202.62.17.196	Indonesia	147.237.77.176	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
202.62.17.196	Indonesia	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
88.210.166.15	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.168	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
61.183.128.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	4
218.87.111.107	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	3
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
218.87.111.107	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
61.183.128.6	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	3
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	SERVER-WEBAPP Moveable Type unauthenticated remote command execution attempt	2
218.87.111.107	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
114.111.166.251	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
93.174.91.29	Netherlands	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.156	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
221.203.3.117	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
162.216.19.183	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
5.39.216.121	Netherlands	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
99.244.136.90	Canada	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.183	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
188.138.9.51	Germany	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.140	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
5.39.216.121	Netherlands	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 2	2
221.203.3.117	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
46.185.132.148	Jordan	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss web console access attempt	2
218.87.111.107	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
58.118.73.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	2
218.87.111.107	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
93.189.25.174	Austria	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
188.138.9.51	Germany	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2

07-11-2015-00:00:08 to 07-12-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.35.174.191	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14908
41.237.101.0	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3339
46.19.86.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2359
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1273
89.139.34.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1074
213.57.159.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	748
41.35.174.191	Egypt	147.237.77.216	dover.idf.i		drop	drop	653
71.201.156.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	613
149.78.42.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	542
23.27.45.79	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	502
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	410
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	408
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	397
2.54.158.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	382
41.35.174.191	Egypt	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	359
82.166.22.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	348
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	343
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	339
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	337
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
171.25.193.235	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	294
107.167.109.103	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	282
208.184.77.186	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
46.19.85.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	253
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	253
199.190.46.192	Satellite Provide	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	245
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	213
85.64.118.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208
206.190.158.75	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	202
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	201
195.34.150.18	Austria	147.237.77.216	dover.idf.i	SAM rule	drop	drop	201
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	183
178.135.80.1	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	181
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	168
95.134.26.74	Ukraine	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	165
77.127.214.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	155
108.70.236.18	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	148
72.252.168.131	Jamaica	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	142
109.65.142.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	118
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	117
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	114
79.179.52.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	110
66.249.64.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
157.55.39.158	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
46.19.86.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
80.83.25.94	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
70.105.249.224	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
207.46.13.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	103
59.190.130.200	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	102
46.185.132.148	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	101

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.64.0.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1193
85.250.218.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	446
2.54.16.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	420
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	295
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	280
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	264
2.52.5.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	223
79.180.37.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
176.13.6.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.6.38	Block	105
176.12.140.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
176.13.6.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
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	48
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.45	Block	44
176.13.2.13	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.2.13	Block	41
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.156	Block	37
2.54.173.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
213.57.49.73	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.57.49.73	Block	34
162.244.15.155		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	29
85.64.0.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.0.182	Block	24
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	22
23.239.208.54	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 23.239.208.54	Block	16
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	15
46.116.178.242	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.116.178.242	Block	15
176.13.1.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
176.13.15.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	14
37.26.148.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	13
176.12.151.121	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.151.121	Block	13
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	11
176.13.14.19	Israel	147.237.77.74	law.idf.il	Parameter Type Violation prefixText in www.law.idf.il/webservices/wscity.asmx/getcities	Block	9
176.13.18.7	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 176.13.18.7	Block	8
176.13.18.7	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.18.7	None	8
93.172.19.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
81.17.16.247	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
157.55.39.32	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/captcha.ashx	Block	6
178.137.161.75	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	6
213.57.106.115	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
37.237.200.35	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.237.200.35	Block	6
74.6.254.122	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
46.117.213.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
37.237.208.140	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	5
157.55.39.41	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.41	Block	5
118.99.29.242	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
37.142.8.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	5
199.16.156.125	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
176.12.151.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
176.13.15.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 176.13.15.162	Block	5
54.241.198.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4

07-11-2015-00:00:08 to 07-12-2015-00:00:08