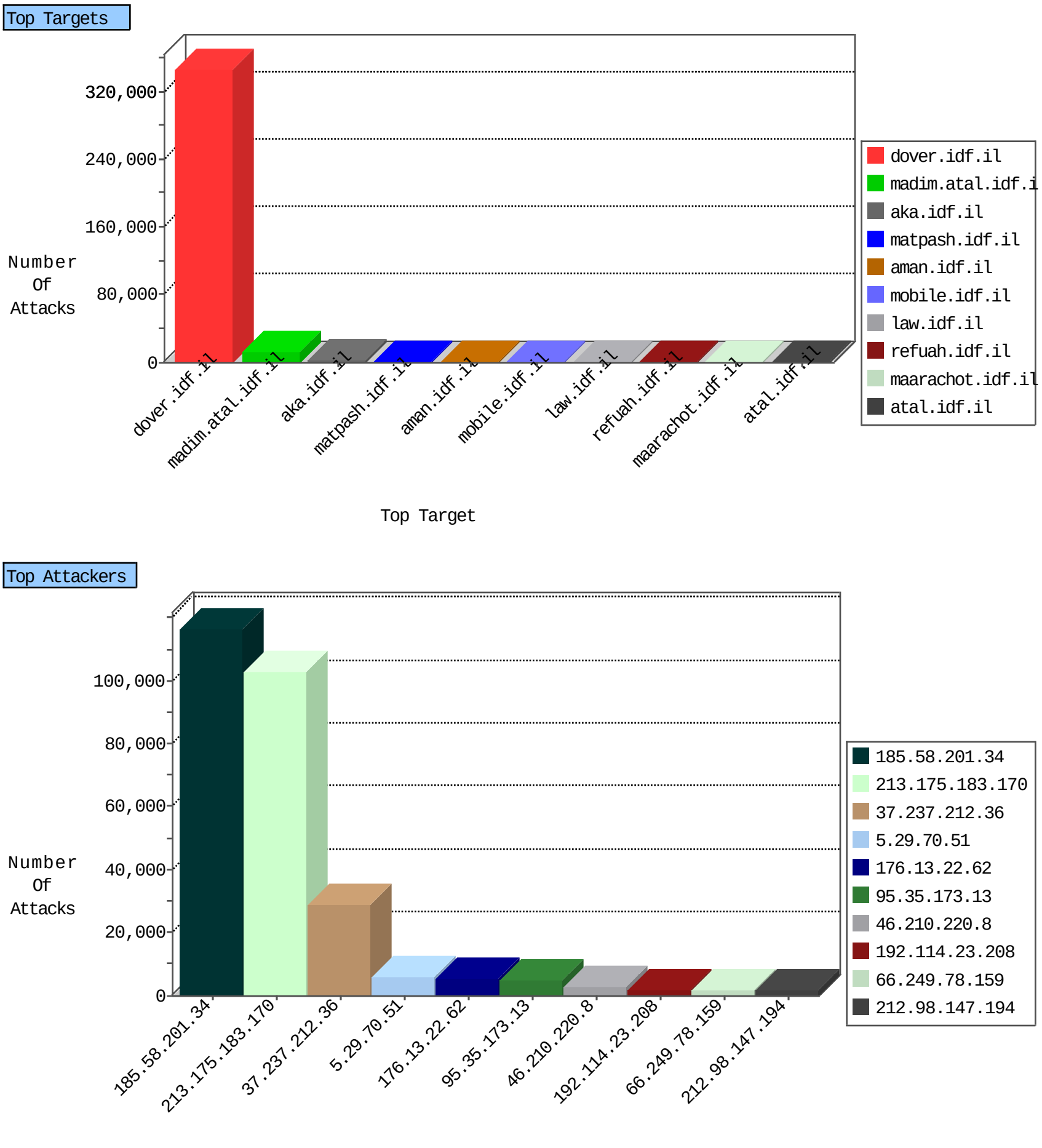
08-07-2015-00:00:02 to 08-08-2015-00:00:02

IDF Under Attack Daily Report



08-07-2015-00:00:02 to 08-08-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.79	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8054
212.98.147.194	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7449
185.58.201.34		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6896
66.249.93.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5126
37.237.212.36	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3097
31.154.91.214	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	734
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	586
95.86.70.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	554
149.88.74.37	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	496
79.181.102.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	494
213.57.102.106	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	476
109.64.159.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	470
93.172.48.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	458
37.142.64.105	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	430
31.154.92.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	371
46.116.8.166	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	326
213.57.104.44	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	324
84.109.179.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	286
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
109.186.100.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
46.117.28.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	232
37.142.64.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
77.127.60.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	217
82.166.69.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
46.120.94.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
77.127.101.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
84.109.90.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
149.88.9.171	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
37.142.64.96	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
85.65.57.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
5.28.166.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	142
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	133
79.182.202.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
37.142.64.109	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
46.19.85.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	123
5.22.135.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
213.57.42.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
79.176.159.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
149.78.118.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
213.57.164.201	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
79.179.5.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
77.125.10.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.186.16.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
37.26.148.221	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	76
37.26.148.221	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
46.19.85.105	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	74
46.117.6.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73

08-07-2015-00:00:02 to 08-08-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
45.35.20.195		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
82.102.141.252	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	19
98.126.46.227	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	14
45.35.20.195		147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
98.126.46.227	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	9
77.125.216.110	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.121.158.214	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.120.137.220	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
24.91.152.191	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
41.41.98.220	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
68.9.242.162	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.250.234.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.176.159.247	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.169.93	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.133	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
173.196.183.198	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
80.179.184.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.64.246.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.182.180.39	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.245	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.21.223	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.26.148.206	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
58.220.241.133	China	147.237.77.170	maarachot.idf.il	0854: HTTP: upload* Access	Block	2
77.126.14.174	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
146.0.79.163	Netherlands	147.237.76.86	navy.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	2
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.243.27.29	United Kingdom	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.71	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.88.149.72	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.142.64.121	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.65.81.218	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.0.234	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.155.134	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.174.93.129	Netherlands	147.237.77.234	halag.idf.il	C003: HTTP: phpMyAdmin access	Block	1
191.178.111.145	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
130.75.2.26	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.148.149	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
212.25.82.123	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
2.54.34.163	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.174.93.129	Netherlands	147.237.77.74	law.idf.il	C003: HTTP: phpMyAdmin access	Block	1
46.19.85.120	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
173.22.133.4	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.19.135	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.14.170.22	France	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.142.187.20	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
109.65.81.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.174.93.129	Netherlands	147.237.77.235	sviva.idf.il	C003: HTTP: phpMyAdmin access	Block	1
87.68.80.203	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

08-07-2015-00:00:02 to 08-08-2015-00:00:02

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	135
176.13.22.62	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	20
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	16
176.13.22.62	Israel	147.237.0.19	madim.atal.idf.il	INDICATOR-SCAN myscan	16
176.13.22.62	Israel	147.237.0.19	madim.atal.idf.il	GPL SCAN myscan	16
41.142.106.39	Morocco	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	5
41.142.106.39	Morocco	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	4
192.210.198.132	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.67	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
45.114.11.44		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	3
78.22.108.120	Belgium	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	3
84.111.232.199	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
218.65.30.107	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
78.22.108.120	Belgium	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
151.252.104.251	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
112.36.135.234	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.70	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.142.117	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.65.30.107	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
186.237.219.101	Brazil	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
37.46.39.155	Israel	147.237.72.156	aman.idf.il	INDICATOR-SCAN myscan	2
85.158.184.234	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
37.8.69.84	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
74.82.194.10	Canada	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
45.114.11.44		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
78.22.108.120	Belgium	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
89.248.174.100	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
124.41.200.147	Nepal	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
213.41.72.13	France	147.237.77.176	matpash.idf.il	GPL SCAN nmap TCP	2
45.114.11.44		147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.237	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
94.23.254.103	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2

08-07-2015-00:00:02 to 08-08-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.237.212.36	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25983
185.58.201.34		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13718
5.29.70.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6021
95.35.173.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5036
46.210.220.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2774
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1992
192.114.23.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1929
212.98.147.194	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1889
77.127.179.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1618
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1570
212.76.97.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1258
95.86.80.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1199
185.4.252.171	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1146
37.237.212.36	Iraq	147.237.77.216	dover.idf.il		drop	drop	1135
46.19.85.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	858
164.138.124.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	810
109.67.137.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	806
2.54.146.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	762
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	737
2.54.37.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	734
37.237.212.36	Iraq	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	685
79.179.21.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	649
108.12.143.25	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	647
2.54.167.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	642
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	617
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	615
62.207.60.228	Netherlands	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	590
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	589
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	586
109.67.18.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	579
82.81.3.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
37.237.212.36	Iraq	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	570
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	537
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	518
46.121.88.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	505
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	491
5.255.253.61	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	464
2.54.35.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	463
46.210.216.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	461
37.26.146.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	460
37.237.212.36	Iraq	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	459
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	458
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	458
2.52.61.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	458
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	450
79.182.165.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	448
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	446
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	446
87.68.75.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	441

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.58.201.34		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/undefined	Block	102780
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/undefined	Block	100146
176.13.22.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5523
87.69.134.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1503
77.125.113.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1302
2.54.152.132	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.152.132	Block	848
87.68.76.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	807
176.13.8.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	643
2.52.35.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	579
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	492
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	447
5.22.130.21	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.22.130.21	Block	447
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined	Block	399
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	399
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/undefined	Block	366
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	348
109.67.157.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.67.157.177	Block	213
84.111.235.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	189
77.127.24.172	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	120
109.67.192.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	108
109.67.56.127	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	105
79.182.130.231	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	96
185.58.201.34		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined	Block	84
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
31.154.91.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	66
118.123.8.204	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.123.8.204	Block	63
114.230.107.185	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 114.230.107.185	Block	57
176.12.140.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
79.182.189.165	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.189.165	Block	48
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	45
176.12.138.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	42
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.83.50	Block	41
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	36
46.121.40.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	36
176.13.9.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
176.12.147.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	30
37.26.147.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
176.13.11.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	27
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	27
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	27
149.78.231.119	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	24
207.46.13.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.70	Block	24
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	24
175.44.9.30	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 175.44.9.30	Block	24
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	21
176.13.18.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	21
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	21

08-07-2015-00:00:02 to 08-08-2015-00:00:02