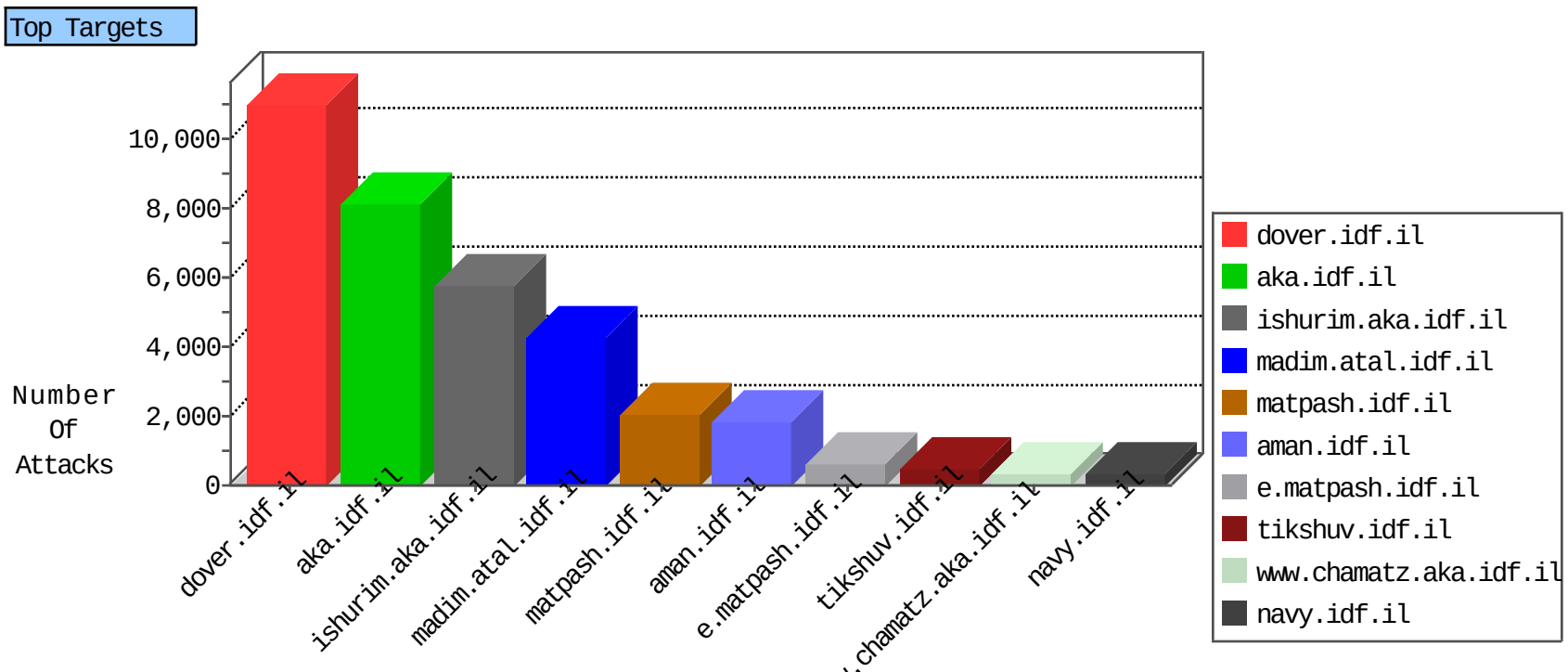
01-11-2015-00:00:00 to 01-12-2015-00:00:00

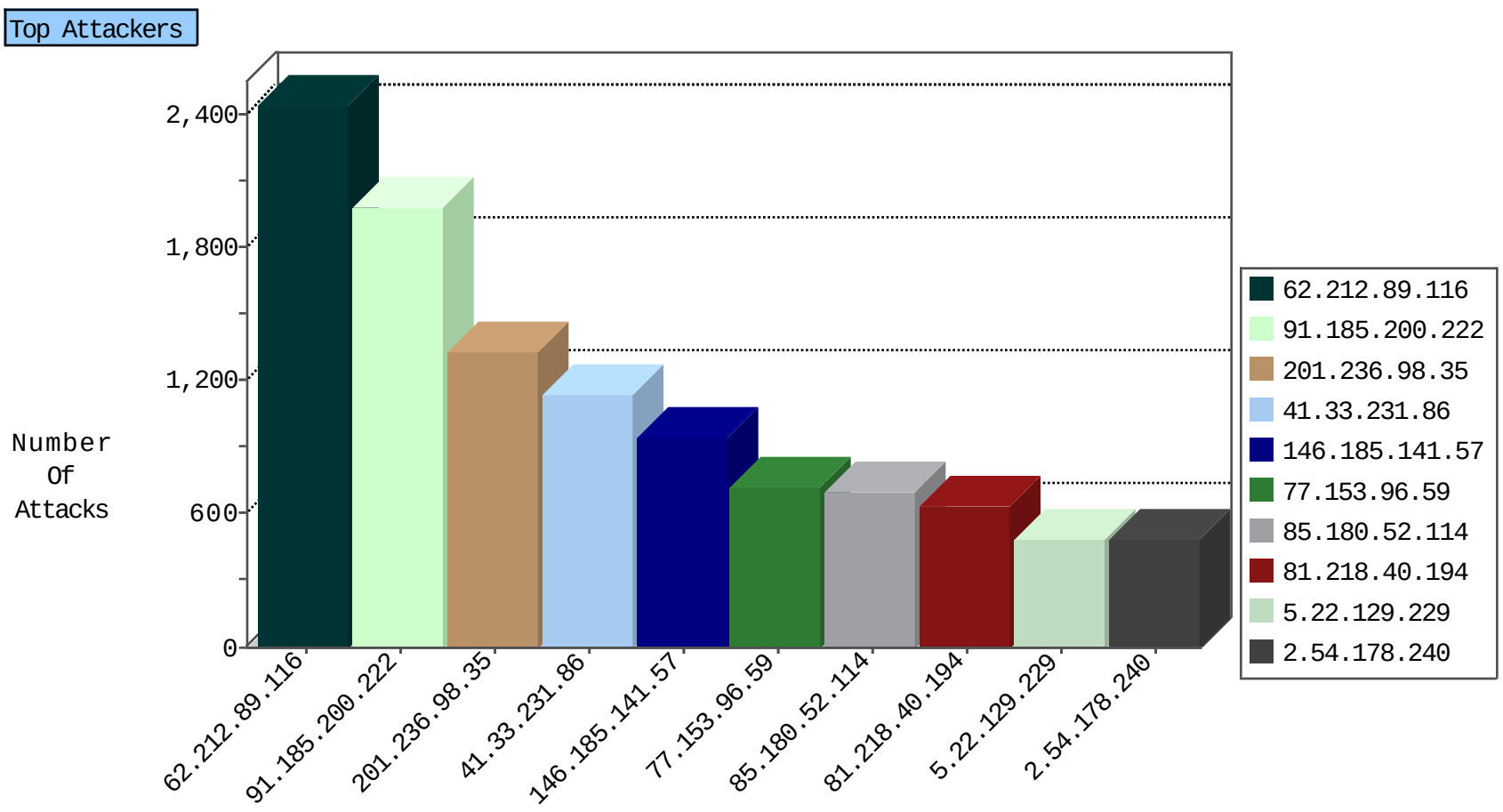
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-11-2015-00:00:00 to 01-12-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.19.85.173	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1505
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1319
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	861
85.64.82.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	739
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	611
85.250.129.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	597
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	586
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	436
149.88.97.110	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	399
77.153.96.59	France	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	374
109.65.66.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	361
82.80.25.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	358
199.59.148.210	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	347
77.153.96.59	France	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	324
109.65.185.207	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	317
46.121.193.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	290
201.236.98.35	Chile	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	267
84.108.126.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	226
201.236.98.35	Chile	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	217
84.228.122.165	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
79.182.181.208	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	203
81.196.139.252	Romania	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	202
93.173.22.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	199
84.111.5.40	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	181
91.246.218.2	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
93.173.242.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
84.108.24.80	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	149
79.177.173.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
85.65.175.133	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	137
84.229.9.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
188.66.227.169	Oman	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	130
85.250.129.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	121
85.250.29.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
5.29.40.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
46.117.237.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.183.19.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
109.160.204.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
84.110.113.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
84.108.24.80	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
2.54.34.52	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	100
37.26.147.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
2.54.132.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.120.99.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.19.86.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
2.54.143.207	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.19.86.165	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	85
84.111.104.201	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84

01-11-2015-00:00:00 to 01-12-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.212.89.116	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2441
91.185.200.222	Slovenia	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	1745
146.185.141.57	Netherlands	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	940
85.180.52.114	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	695
91.185.200.222	Slovenia	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	231
184.173.183.172	United States	147.237.76.86	navy.idf.il	Rep_Notify_Only_Tehila	Permit	143
85.17.31.120	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	119
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
212.179.239.194	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	13
85.64.73.222	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	10
197.35.22.116	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
82.102.141.216	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	8
66.240.192.138	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	7
93.172.180.224	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
200.66.73.133	Mexico	147.237.77.176	matpash.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	6
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	6
79.178.145.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.8.52.148	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.186.29.45	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
200.66.73.133	Mexico	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	6
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	Rep_Notify_Only_Tehila	Permit	6
66.240.236.119	United States	147.237.72.14	dover.idf.il(old)	Block_Level_70_100	Block	5
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	5
46.19.85.165	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	Block_Level_70_100	Block	5
93.173.172.226	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.16	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.145.148	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	Block_Level_70_100	Block	4
197.35.16.139	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	4
87.94.132.79	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	4
82.102.141.213	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.244	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	Block_Level_70_100	Block	4
213.57.132.211	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.77.234	halag.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.77.235	sviva.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	4
85.65.35.4	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.77.176	matpash.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	4

01-11-2015-00:00:00 to 01-12-2015-00:00:00

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	119
82.205.49.178	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	68
201.236.98.35	Chile	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
2.54.173.228	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
54.224.149.230	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
79.180.129.91	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
82.80.58.126	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	4
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	3
121.42.54.18	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	3
93.158.200.40	Netherlands	147.237.76.86	navy.idf.il	SERVER-WEBAPP Setup.php access	3
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
95.35.31.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.69.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.151.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.190	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.155.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.205.24.71	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
79.181.125.175	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.22.129.229	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.131.80	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.250.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.21.142	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.246.73	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
147.236.22.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.158.200.40	Netherlands	147.237.0.15	kosher-kravi.idf.i	ET WEB_SERVER Muieblackcat scanner	2
212.235.10.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.145.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.30.52.70	United States	147.237.0.34	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	2
77.126.71.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.176.93	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.116.97	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.134.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
222.186.15.202	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
46.120.99.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.136.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.38.35	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.140	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
84.111.141.32	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.172	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
192.185.2.93	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
93.172.32.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.151.48.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.5.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

01-11-2015-00:00:00 to 01-12-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
201.236.98.35	Chile	147.237.77.216	dover.idf.il		drop	drop	1237
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1141
81.218.40.194	Israel	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	413
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	407
77.153.96.59	France	147.237.77.216	dover.idf.il		drop	drop	395
207.241.229.191	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	171
80.246.133.212	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	119
65.255.37.151	Satellite Provide	147.237.72.166	aka.idf.il		drop	drop	111
213.8.96.180	Israel	147.237.72.166	aka.idf.il		drop	drop	110
77.153.96.59	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	106
77.153.96.59	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		103
81.218.40.194	Israel	147.237.77.178	e.matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	100
81.218.40.194	Israel	147.237.77.178	e.matpash.idf.il	Invalid ACK number	Bad TCP sequence		100
50.17.122.200	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	99
87.68.96.223	Israel	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	98
5.22.129.229	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence		85
5.22.129.229	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	81
77.127.89.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	80
84.94.193.22	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	74
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	64
37.26.147.145	Israel	147.237.77.216	dover.idf.il		drop	drop	64
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	62
77.126.224.113	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	55
132.64.56.90	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	49
194.146.200.68	Russian Federation	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	48
92.40.249.177	United Kingdom	147.237.72.167	ishurim.aka.idf.il		drop	drop	48
52.129.32.50	Europe	147.237.72.166	aka.idf.il		drop	drop	47
212.179.61.126	Israel	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	46
212.179.61.120	Israel	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	42
91.93.38.115	Turkey	147.237.77.216	dover.idf.il		drop	drop	41
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	40
46.121.213.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	39
77.126.105.2	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	37
84.228.68.46	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	35
77.127.166.29	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
5.22.130.236	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	34
89.174.13.1	Poland	147.237.72.166	aka.idf.il		drop	drop	34
212.179.61.120	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	33
192.115.248.2	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
37.26.147.226	Israel	147.237.0.19	madim.atal.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
212.179.61.120	Israel	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
132.64.159.211	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
77.127.166.29	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	31
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il		drop	drop	30
31.186.228.66	United Kingdom	147.237.72.166	aka.idf.il		drop	drop	29
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il		drop	drop	29
212.25.102.57	Israel	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	29
92.40.249.177	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.178.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	481
37.26.148.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	370
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
2.54.59.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
5.22.129.229	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.229	Block	316
109.186.155.208	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.155.208	Block	247
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	233
109.253.144.82	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.82	Block	183
2.54.9.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
149.78.199.225	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
84.228.122.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
207.241.226.104	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	107
109.253.151.193	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.151.193	Block	103
82.80.20.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
185.32.178.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
212.179.132.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	96
109.253.146.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
2.54.162.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
82.102.141.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
109.253.131.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
95.86.89.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	67
79.181.164.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
66.249.78.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.160	Block	61
84.94.193.22	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	60
176.12.156.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.156.118	Block	60
38.111.147.84	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/yoman/	Block	58
176.12.147.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
46.117.121.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	54
176.12.144.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	52
66.249.78.153	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	52
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	51
176.12.143.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
212.179.21.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	43
212.179.132.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	42
99.246.148.98	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	42
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.127	Block	36
31.168.143.10	Israel	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	35
79.177.112.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	34
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.134	Block	33
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	33
176.12.145.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	31
87.68.97.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	28
85.64.73.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	28
109.253.146.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
79.176.193.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	27
31.168.143.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.143.10	Block	25
95.86.114.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	25
109.253.133.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
176.12.150.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	24

01-11-2015-00:00:00 to 01-12-2015-00:00:00