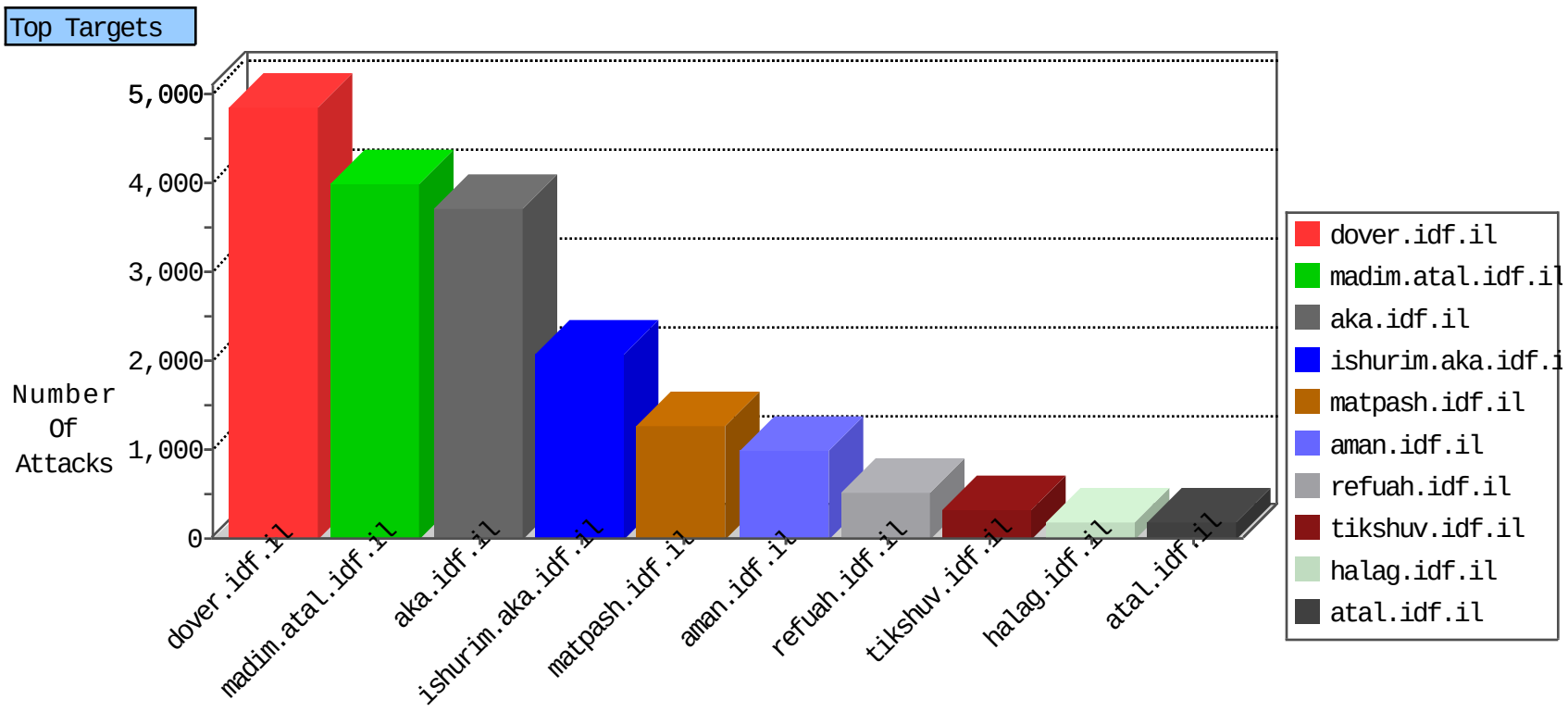
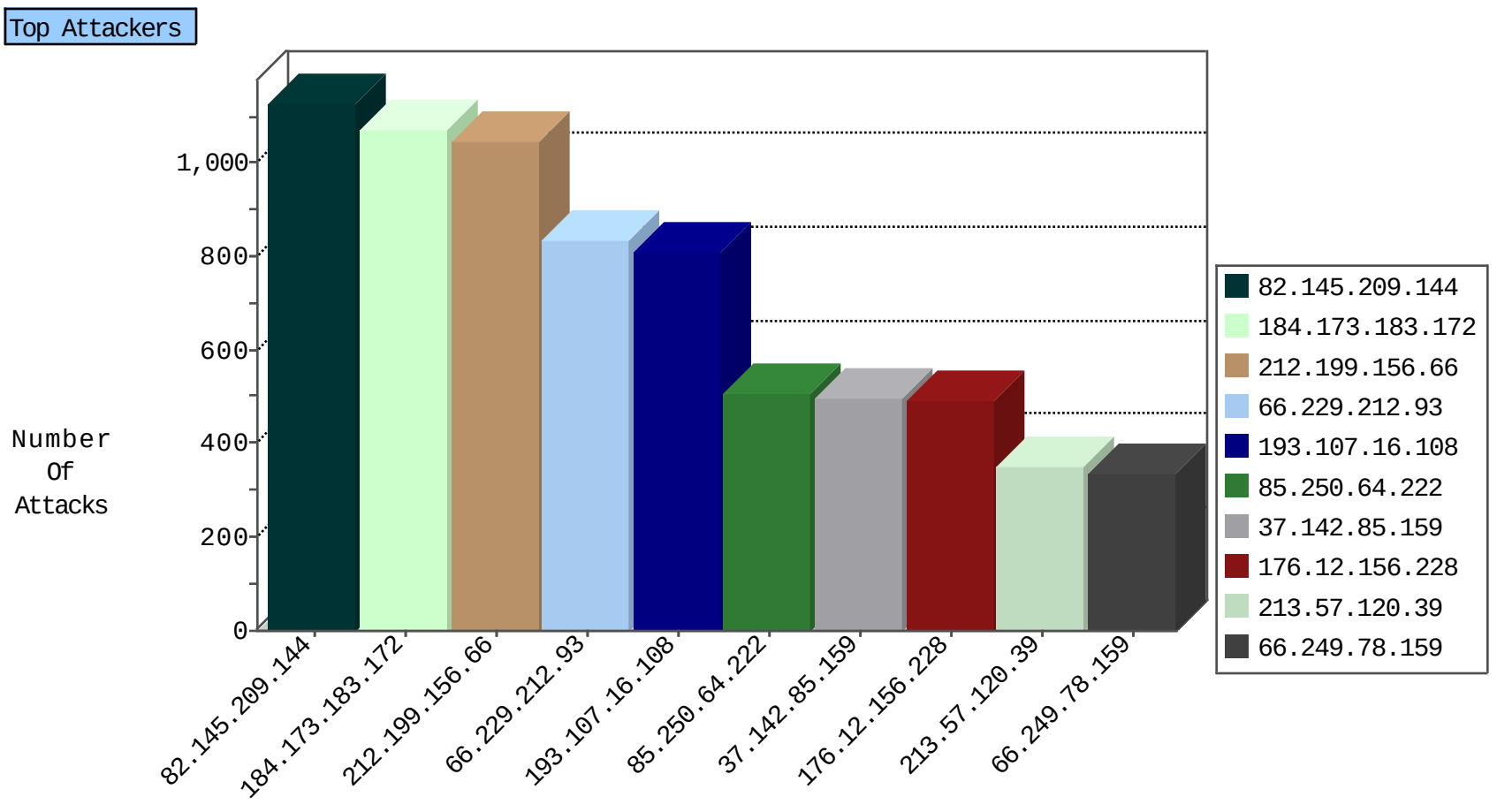
01-23-2015-00:00:08 to 01-24-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-23-2015-00:00:08 to 01-24-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
87.69.132.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1582
213.57.140.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1515
82.80.156.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1052
109.64.127.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	742
46.120.95.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	611
87.69.148.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	429
79.178.52.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	395
89.138.206.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	308
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
46.116.236.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
84.111.181.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
109.186.184.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
83.130.103.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.183.6.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
46.116.55.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
77.126.134.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
109.186.154.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
93.172.138.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
194.54.168.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.180.153.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
93.173.103.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.19.85.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
37.142.227.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
217.132.73.182	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	103
109.65.183.187	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	95
109.160.135.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
149.88.124.251	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
87.69.72.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.85.212	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
79.181.191.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
185.32.176.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
77.127.250.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
46.117.237.87	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
46.117.88.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
109.66.22.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
109.160.251.198	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	73
79.176.177.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	69
109.160.224.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.86.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
80.246.141.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.177.149.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
46.19.86.54	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
82.102.141.216	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
176.12.144.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
77.127.250.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	42
109.65.183.187	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	41

01-23-2015-00:00:08 to 01-24-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.199.156.66	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	1048
82.145.209.144	Europe	147.237.72.167	ishurim.aka.idf.il	Rep_Notify_Only_Tehila	Permit	1025
66.229.212.93	United States	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	834
193.107.16.108	Russian Federation	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	661
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	435
184.173.183.172	United States	147.237.76.42	refuah.idf.il	Rep_Notify_Only_Tehila	Permit	338
128.242.249.12	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	311
184.173.183.172	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	299
193.107.16.108	Russian Federation	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	151
78.52.3.179	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	147
82.145.209.144	Europe	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	77
213.8.242.98	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
82.145.209.144	Europe	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	28
95.130.15.251	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
176.31.190.158	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
178.33.193.136	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
77.95.229.11	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
194.0.236.89	Europe	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
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
109.65.188.17	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
71.6.165.200	United States	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	7
46.19.85.98	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.110	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.123	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	5
71.6.167.142	United States	147.237.72.217	e.idf.il	Block_Level_70_100	Block	5
85.25.103.50	Germany	147.237.77.234	halag.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	Block_Level_70_100	Block	5
37.142.254.96	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	5
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	5
213.57.185.98	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.77.233	atal.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	4
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	Block_Level_70_100	Block	4
213.151.44.86	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	4
190.39.181.133	Venezuela	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	4
109.201.152.227	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Rep_Notify_Only_Tehila	Permit	4
117.216.233.158	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	4
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	Block_Level_70_100	Block	4

01-23-2015-00:00:08 to 01-24-2015-00:00:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	300
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	141
109.169.45.231	United Kingdom	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	9
109.169.45.231	United Kingdom	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	9
109.169.45.231	United Kingdom	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
109.169.45.231	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
109.169.45.231	United Kingdom	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
109.169.45.231	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
107.167.110.60	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	5
109.169.45.231	United Kingdom	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
79.179.2.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
93.172.136.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
207.46.13.87	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
109.169.45.231	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
115.231.218.23	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	3
109.169.45.231	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
222.186.15.202	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
109.169.45.231	United Kingdom	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.169.45.231	United Kingdom	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3

01-23-2015-00:00:08 to 01-24-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
41.203.69.33	Nigeria	147.237.77.216	dover.idf.il		drop	drop	142
82.102.141.202	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	105
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	96
178.165.129.146	Austria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
82.102.141.202	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	70
190.24.146.71	Colombia	147.237.77.216	dover.idf.il		drop	drop	66
197.33.200.243	Egypt	147.237.77.216	dover.idf.il		drop	drop	58
84.229.157.143	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
176.228.215.178	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	49
94.160.182.245	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
85.130.245.207	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	44
192.117.4.242	Israel	147.237.0.19	madim.atal.idf.il		drop	drop	42
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
201.38.159.194	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
79.181.115.235	Israel	147.237.77.216	dover.idf.il		drop	drop	33
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
92.253.96.59	Jordan	147.237.77.216	dover.idf.il		drop	drop	32
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
192.166.132.229	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
84.228.197.197	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
177.111.197.110	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
23.241.67.47	United States	147.237.72.166	aka.idf.il		drop	drop	28
84.133.231.63	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
140.153.173.93	United States	147.237.77.176	matpash.idf.il		drop	drop	26
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.210.186.115	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	23
85.130.245.207	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	23
66.249.64.120	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
207.46.13.81	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
157.55.39.217	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
104.42.25.0		147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	20
46.237.207.196	Germany	147.237.76.177	ncore.idf.il	SAM rule	drop	drop	19
79.180.177.232	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
46.237.207.196	Germany	147.237.76.176	test.ncore.idf.il	SAM rule	drop	drop	18
66.249.93.195	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
110.248.87.116	China	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	18
176.12.148.219	Israel	147.237.72.166	aka.idf.il	'Cookie' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	17
192.116.81.23	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
79.176.54.81	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
84.11.93.218	Satellite Provider	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	15
46.19.85.212	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	15

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.64.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	509
37.142.85.159	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.85.159	Block	494
176.12.156.228	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.156.228	Block	490
213.57.120.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	353
2.54.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	326
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	276
2.54.183.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	217
87.68.51.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	209
85.64.38.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	197
79.183.123.14	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.183.123.14	Block	185
109.253.141.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	158
185.32.177.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
80.246.137.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
84.229.56.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
94.159.253.172	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 94.159.253.172	Block	52
192.117.4.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.112.144	Block	39
149.78.179.187	United States	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 149.78.179.187	Block	38
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	36
79.178.62.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
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	34
66.249.64.116	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.116	Block	33
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	31
66.249.64.120	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.120	Block	29
14.201.114.4	Australia	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	29
66.249.64.124	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	27
207.241.237.211	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	26
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	21
46.120.210.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	18
5.29.11.36	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.11.36	Block	16
82.102.141.204	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 82.102.141.204	Block	16
95.86.113.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
188.120.148.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
37.142.184.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
79.178.164.164	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	11
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	11
95.86.113.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	10
2.54.59.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	10
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.65.191	Block	9
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.65.195	Block	9
84.228.250.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
66.249.67.158	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.67.158	Block	9
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.204.127.33	Block	9
207.46.13.19	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.67.142	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.67.142	Block	7
79.180.28.83	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.180.28.83	Block	7
95.86.65.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
212.76.123.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
37.115.186.0	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//1498-en/dover.aspx/	Block	7