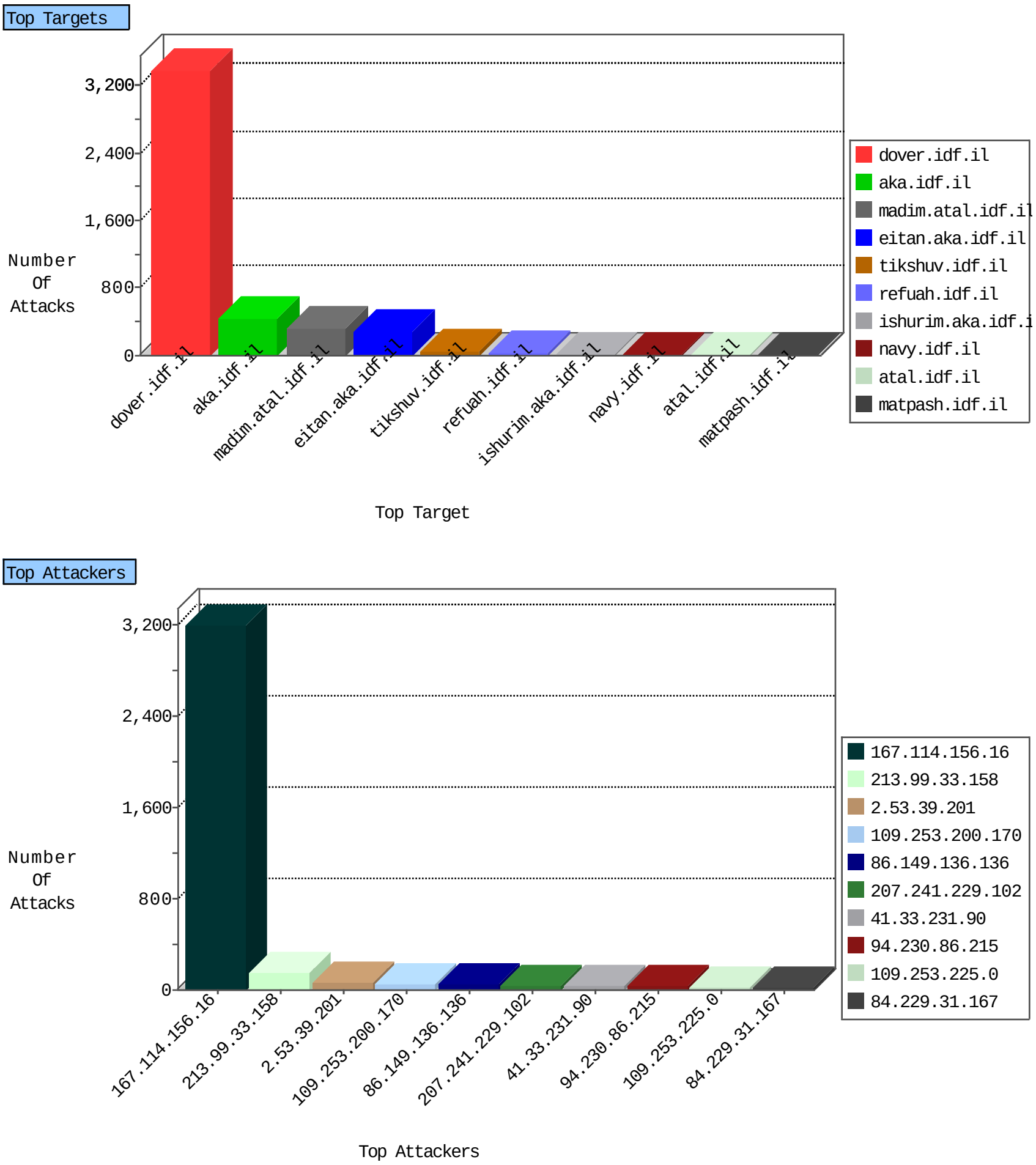
04-17-2016-22:04:08 to 04-17-2016-23:04:08

IDF Under Attack
Daily Report



04-17-2016-22:04:08 to 04-17-2016-23:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3209
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
79.183.119.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
101.201.147.32	China	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.163.144.28	Germany	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
112.95.149.171	China	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
93.174.93.50	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
112.95.149.171	China	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Http	drop	1

04-17-2016-22:04:08 to 04-17-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.39.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
213.57.33.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2

04-17-2016-22:04:08 to 04-17-2016-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3

04-17-2016-22:04:08 to 04-17-2016-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.99.33.158	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	64
213.99.33.158	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
86.149.136.136	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
207.241.229.102	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	39
94.230.86.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.229.31.167	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.154.151.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.253.196.144	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
84.229.34.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.99.33.158	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.81.223	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
66.249.81.217	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.179.19.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.11.118.116	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.15.195	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.81.220	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.216.5	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
84.228.245.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
84.108.67.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.201	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.67.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.199.169.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.55.136.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.28.17	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.66.21.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.230.86.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.248.147.94	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
185.3.144.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.67.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.179.217.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.169.37	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.176.28.17	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.76.114.182	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.199	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	drop		drop	4
5.28.133.115	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.129.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.7.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
5.102.254.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.96.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-17-2016-22:04:08 to 04-17-2016-23:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.178.96.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.178.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.96.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.39.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
109.253.200.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
109.253.225.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
109.253.224.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
109.253.224.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
109.253.224.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
37.26.147.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.224.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.224.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.224.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.224.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.253.224.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.253.224.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.253.224.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.224.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.221.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.224.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.148.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
131.253.25.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.224.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.86.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.225.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.224.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.220.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.67.171	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.108.67.171	Block	2
109.253.224.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.99.33.158	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.224.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.20.152	Israel	147.237.77.216	dover.idf.il	Redundant HTTP Headers from 176.13.20.152	Block	2
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.200.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.87.79.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
5.28.155.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/71725.pdf	Block	1
109.253.224.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
93.172.45.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
212.199.169.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
46.120.251.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.2.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.67.171	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/homepage/mobile	Block	1

04-17-2016-22:04:08 to 04-17-2016-23:04:08