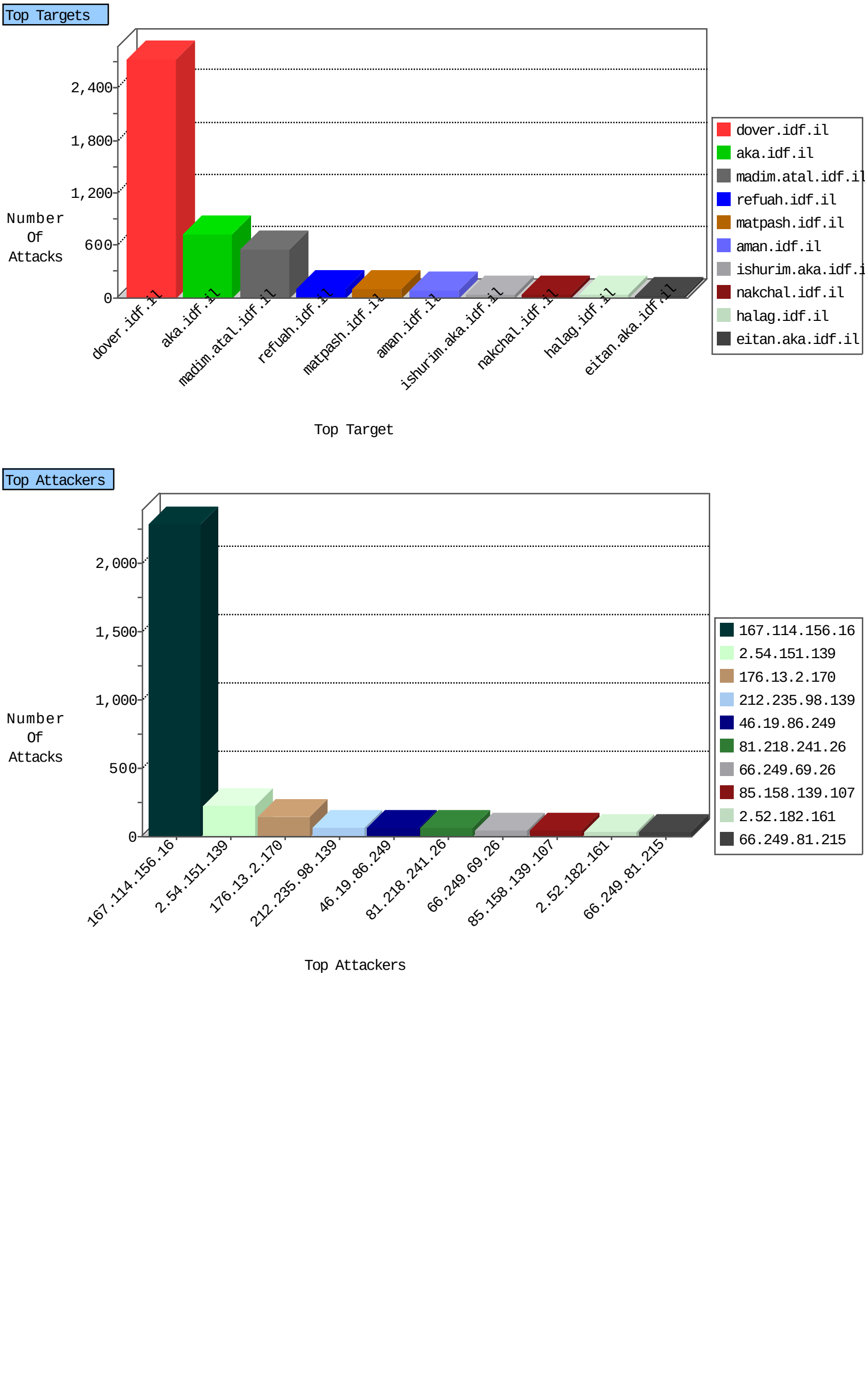
11-29-2015-09:04:03 to 11-29-2015-10:04:03

IDF Under Attack Daily Report



11-29-2015-09:04:03 to 11-29-2015-10:04:03

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	DOS-Tool-SwitchbladG	dest-reset	3356
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	267
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
81.218.105.235	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
38.229.1.13	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
195.154.188.28	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
118.193.23.46	China	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

11-29-2015-09:04:03 to 11-29-2015-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.54.130	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.54.155.181	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.210.148.233	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-29-2015-09:04:03 to 11-29-2015-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-29-2015-09:04:03 to 11-29-2015-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	63
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
85.158.139.107	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.52.182.161	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
66.249.81.215	Russian Federation	147.237.77.216	dover.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	34
100.100.84.58		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
2.54.165.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.76.53		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.10.110		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
80.246.133.114	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.180.150.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
100.100.85.78		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.54.161.158	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
89.138.170.189	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.163.68.111	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
79.177.18.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.229.2	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.97	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.154.91.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.46.13.91	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.183.0.123	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.19.85.240	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.0.123	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.140.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.65.42.116	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.181.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.173	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.155.190	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.135.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.178.136.221	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.228	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.22.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.64.32.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

11-29-2015-09:04:03 to 11-29-2015-10:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.151.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
176.13.2.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.2.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.54.151.139	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.151.139	Block	33
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.52.186.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.161.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
212.179.55.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	8
176.12.141.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
103.37.8.114	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
195.64.164.134	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.32.230.183	United Kingdom	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
216.120.237.104	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
177.85.102.169	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
83.145.246.174	Finland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
216.120.237.3	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
75.98.174.130	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
103.16.128.130	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
79.181.34.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	3
2.52.154.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	3
87.68.61.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
75.98.174.130	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
198.1.87.23	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
75.98.174.130	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 75.98.174.130	Block	3
195.29.89.8	Croatia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
2.52.181.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.141.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.55.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
192.254.137.108	United States	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
176.13.2.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.39.48	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
173.254.123.131	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
128.192.22.58	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.221.250.10	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
89.107.184.213	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.144.43.65	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
208.77.156.165	Canada	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
89.139.176.245	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
87.236.105.62	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
78.46.9.159	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
154.0.162.180	South Africa	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
209.204.64.36	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
75.98.174.130	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
128.192.22.58	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2

11-29-2015-09:04:03 to 11-29-2015-10:04:03