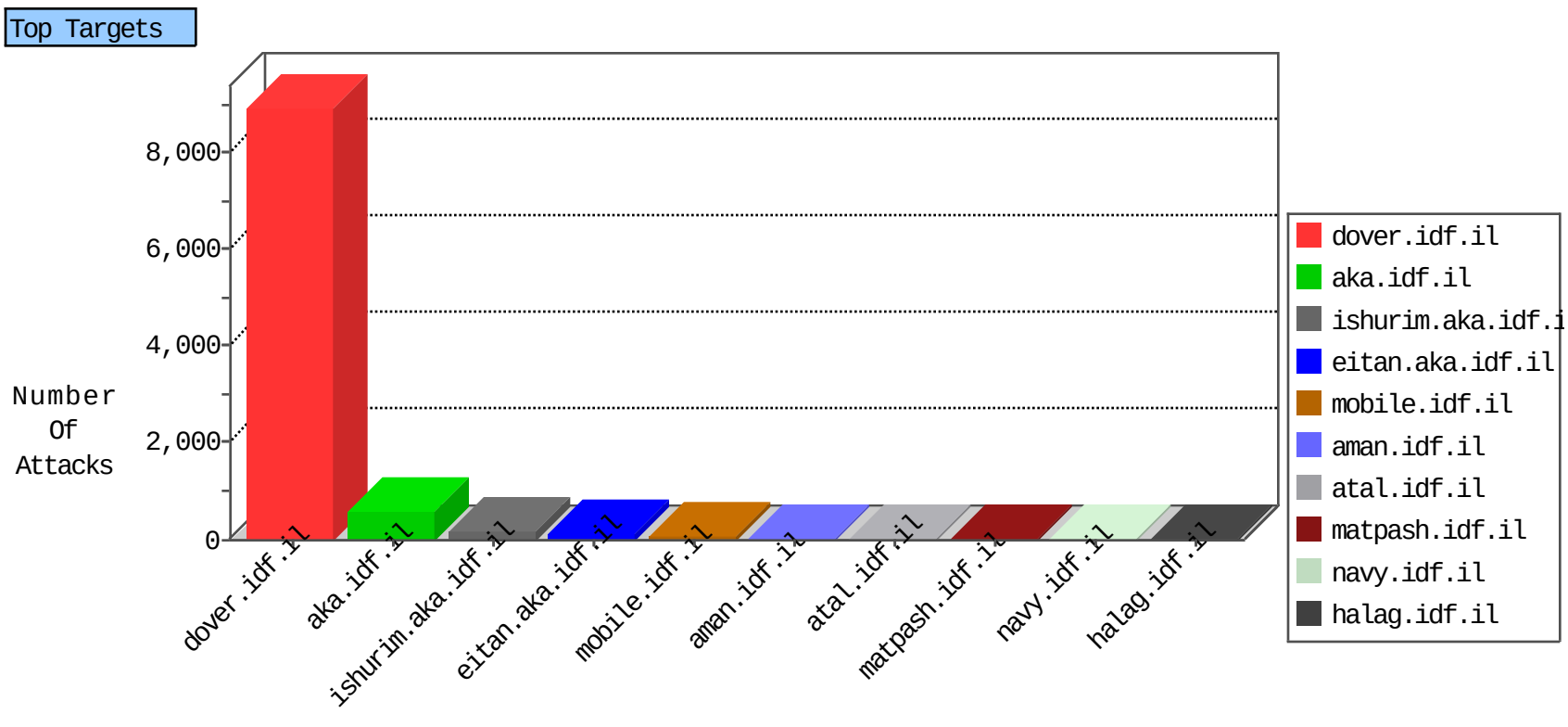
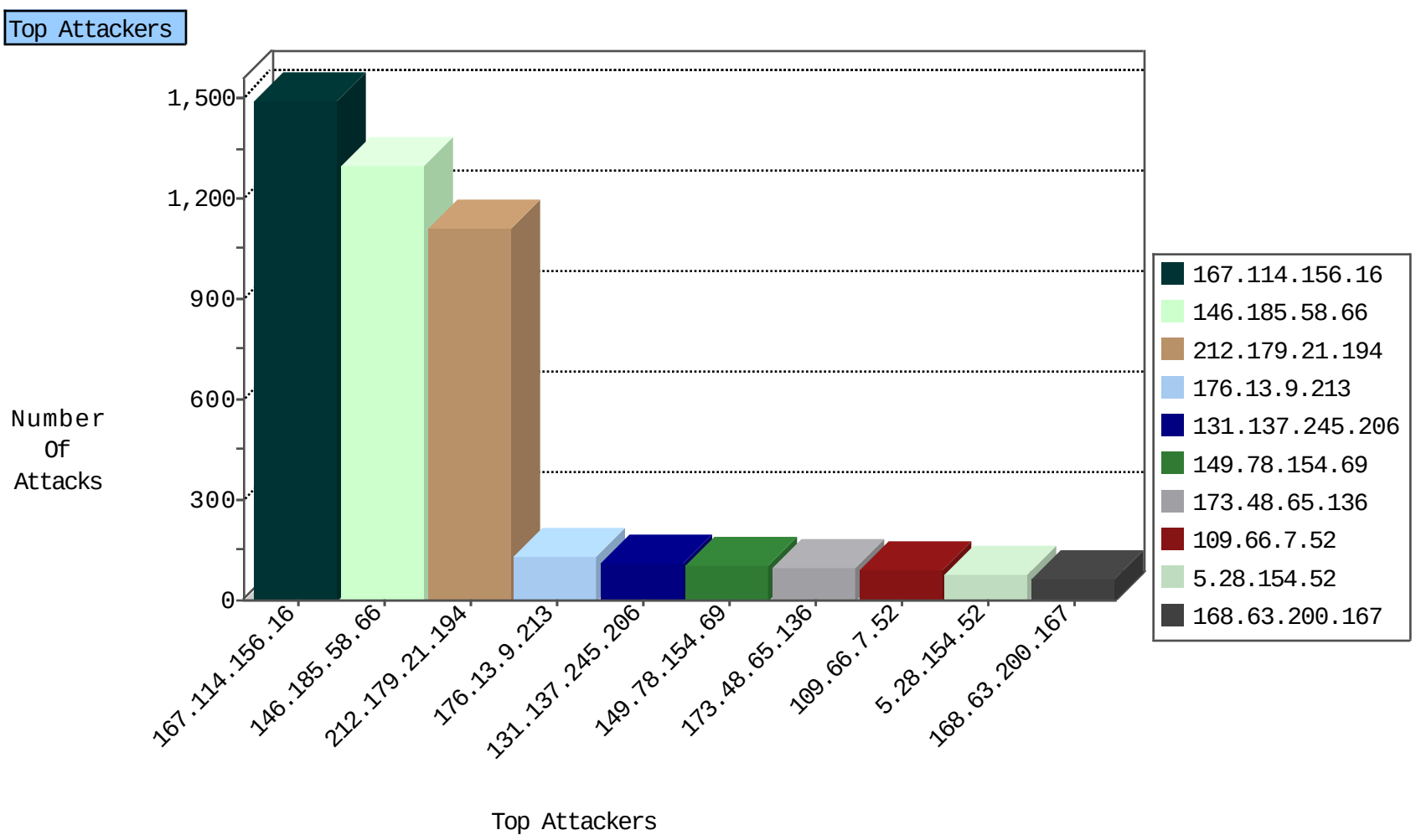
11-03-2015-16:04:00 to 11-03-2015-17:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-03-2015-16:04:00 to 11-03-2015-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3247
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2543
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1683
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	299
5.28.154.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	134
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	51
79.183.125.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
213.151.40.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
46.120.138.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
84.109.107.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.54.131.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
79.180.130.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.26.147.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
213.57.224.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
87.69.79.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
77.127.160.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
2.52.185.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
77.127.201.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
87.69.109.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.85.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.66.174.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.125.86.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.131.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
77.127.201.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.54.154.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.138.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.46.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.169.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.179.177.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.26.147.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.94.103.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.153.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.26.147.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
212.179.23.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.32.179.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.1.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.68.166.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.63.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.85.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.78.25.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.10.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
37.26.149.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
132.72.15.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.63.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
91.143.227.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-03-2015-16:04:00 to 11-03-2015-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
148.177.1.218	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.25.79.205	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-03-2015-16:04:00 to 11-03-2015-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.8	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
5.102.254.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.100.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.147.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.61.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
79.179.11.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.63.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.133.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.138.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-03-2015-16:04:00 to 11-03-2015-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
146.185.58.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1301
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1052
176.13.9.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
131.137.245.206	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
173.48.65.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
109.66.7.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
168.63.200.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.86.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.235	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
93.40.235.72	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
213.151.53.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
2.54.154.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
84.228.239.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.86.142	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
5.28.154.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
85.130.201.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
207.46.13.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
157.56.2.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
79.182.202.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
160.62.4.100	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
62.209.9.14	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.179.177.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.138.133.72	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
84.109.107.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
192.117.179.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
176.12.148.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
77.127.201.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
23.27.248.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.166.22.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.83.168	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
37.26.146.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
109.67.165.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.54.71		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
192.114.91.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
79.183.125.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
95.86.115.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.39.79		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
185.37.12.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	23
213.57.183.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

11-03-2015-16:04:00 to 11-03-2015-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.83.218	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
87.69.87.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.87.158	Block	13
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
95.86.115.228	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
66.249.83.210	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
138.134.102.16	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.102.16	Block	10
66.249.83.214	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
213.57.157.76	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
213.57.157.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	8
213.57.157.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
84.228.164.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	6
66.102.9.79	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
31.154.91.114	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
84.228.164.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
66.102.9.89	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
31.154.91.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	6
31.154.91.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
84.228.164.80	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
176.12.144.129	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	5
87.69.87.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	4
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	4
46.19.85.102	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
81.218.251.251	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 81.218.251.251	Block	3
66.102.9.71	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
80.246.140.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	2
85.65.224.80	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
85.65.224.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
85.65.224.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 207.232.27.5 (Unknown SSL Session)	None	1
66.249.65.75	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.247.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
176.13.18.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
79.176.209.145	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.149.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.41.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
84.228.2.8	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
79.183.23.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
149.78.18.73	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.64.172.57	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.64.172.57	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
46.229.164.100	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
176.13.18.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.179.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.179.186.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
37.142.148.238	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19815-he/idfgdover.aspx	Block	1
213.57.157.192	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1

11-03-2015-16:04:00 to 11-03-2015-17:04:00