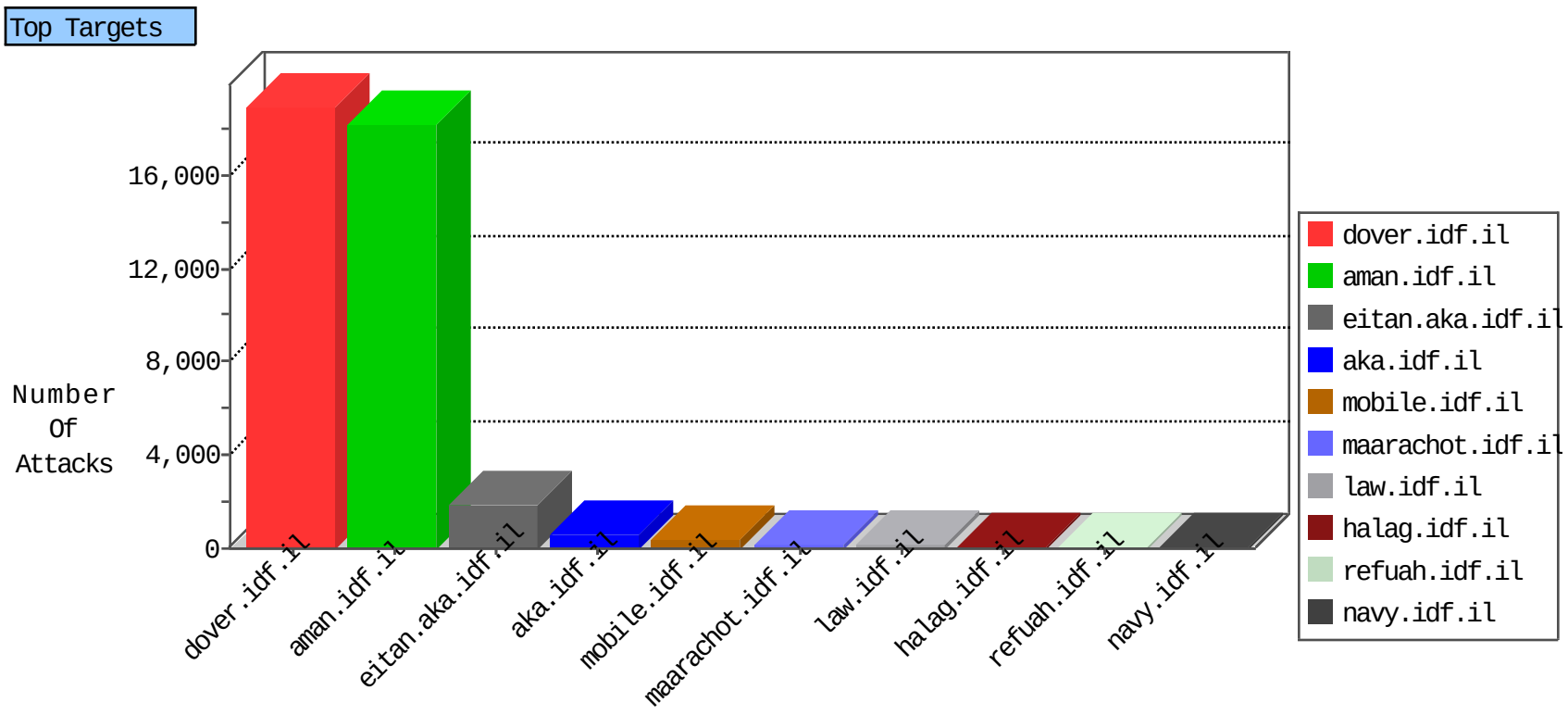
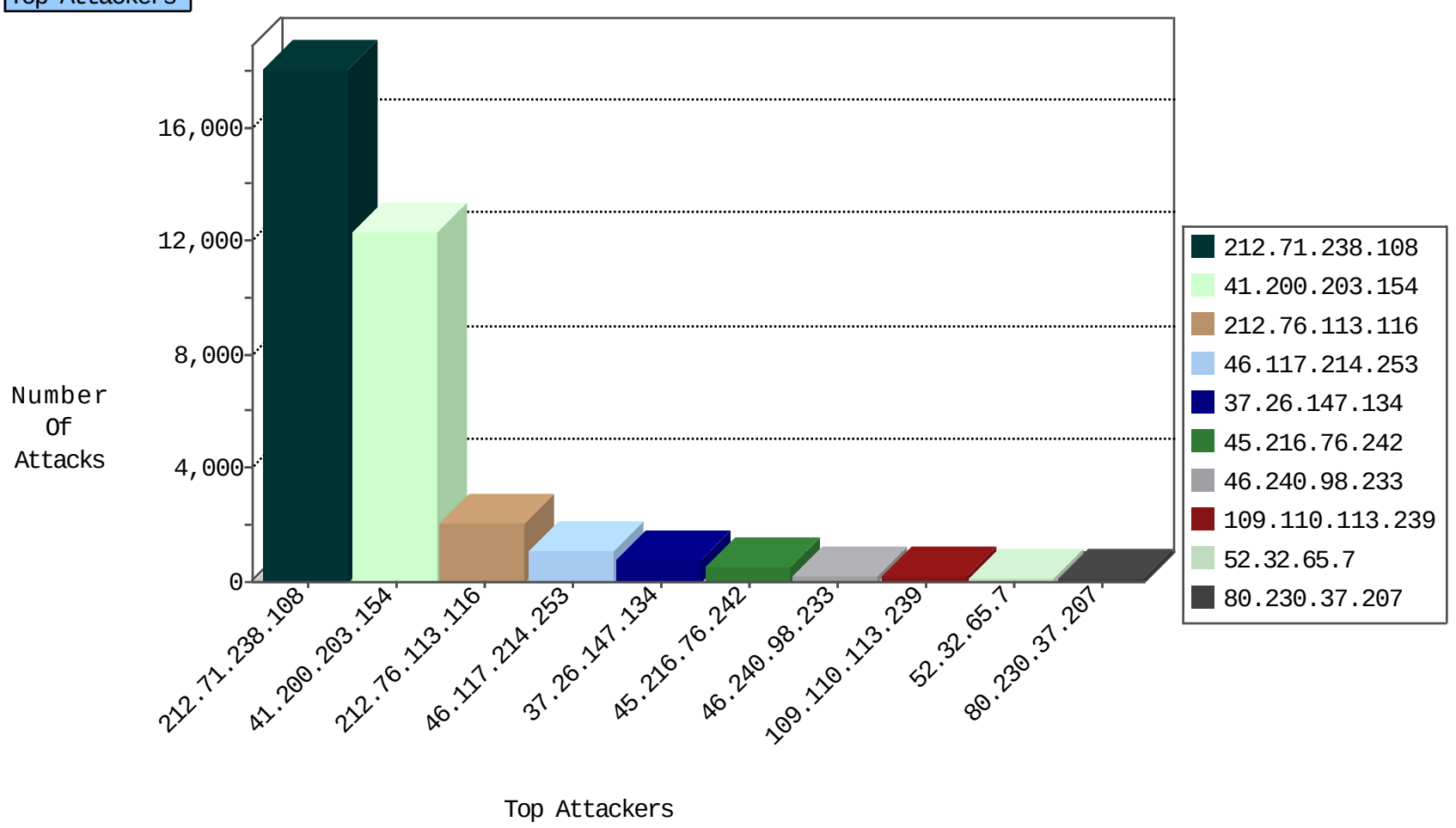
10-31-2015-23:04:03 to 11-01-2015-00:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-31-2015-23:04:03 to 11-01-2015-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	25179
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	16542
80.130.29.187	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16529
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	13444
52.32.65.7	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12247
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8805
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7749
92.238.125.81	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7531
178.38.77.193	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5795
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5228
41.200.203.154	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4617
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3921
185.88.24.70		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3804
66.249.78.54	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	3463
66.249.81.212	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3214
105.109.107.115	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3157
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2997
185.88.25.220		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2762
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2681
37.26.148.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2655
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2494
66.249.75.106	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2339
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2045
123.125.71.42	China	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1670
185.88.24.121		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1271
185.88.24.117		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1091
185.88.25.137		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1026
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	327
149.255.208.15	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	225
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	172
79.178.23.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	165
176.228.166.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	61
220.181.108.119	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	52
79.183.3.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	48
109.110.113.239	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
89.138.227.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
41.200.203.154	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	27
79.183.36.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
173.84.92.52	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
79.176.168.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
79.177.35.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
212.14.228.122	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.15.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	16
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
5.29.234.23	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.178.23.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.116.177.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10

10-31-2015-23:04:03 to 11-01-2015-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-23:04:03 to 11-01-2015-00:04:03

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	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4

10-31-2015-23:04:03 to 11-01-2015-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.200.203.154	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12264
212.76.113.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2064
37.26.147.134	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	750
45.216.76.242	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	561
46.240.98.233	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	213
109.110.113.239	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	197
80.230.37.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
52.32.65.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
80.130.29.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
94.230.86.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
105.188.234.168	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
2.54.163.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
31.210.181.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.120.229.31	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
174.95.94.184	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
149.255.208.15	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
95.86.79.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
81.178.198.161	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
185.88.24.61		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
70.215.15.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.228.166.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
176.13.4.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.177.35.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.183.36.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
176.13.3.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
149.78.251.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.117.214.253	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
185.88.24.87		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.66.132.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
185.88.24.62		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
185.88.25.137		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.158.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.183.3.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.88.24.121		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
178.63.165.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
88.231.199.243	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.71.238.108	United Kingdom	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 212.71.238.108	Block	18035
46.117.214.253	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.214.253	Block	1046
5.29.214.197	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.214.197	Block	45
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	45
176.12.145.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
176.228.166.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
46.120.229.31	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	30
89.139.186.224	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 89.139.186.224	Block	30
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
5.29.214.197	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	30
89.139.186.224	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/admin.aspx	Block	30
88.231.199.243	Turkey	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	30
46.116.177.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
37.60.43.5	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	30
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	30
176.13.21.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
212.71.238.108	United Kingdom	147.237.72.156	aman.idf.il	Distributed Admin Blocking	Block	30
89.139.186.224	Israel	147.237.72.156	aman.idf.il	Multiple Admin Blocking from 89.139.186.224	Block	30
85.250.230.212	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.250.230.212	Block	30
157.55.39.106	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.137.225.218	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/a2billing/customer/iridium_threed.php	Block	15
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7666-he/nakhal.aspx	Block	15
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
109.64.134.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
87.68.156.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
212.71.238.108	United Kingdom	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/61415dotjpg	Block	15
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	15
46.116.120.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	15
79.177.35.97	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/webresource.axd	Block	15
207.46.13.57	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
149.78.40.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	15
31.154.92.95	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.78.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	15
176.13.4.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/resources/scripts/generalfunctions.js	Block	15
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	15
109.64.11.231	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
79.182.12.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18189-he/dover.aspx	Block	15
212.71.238.108	United Kingdom	147.237.72.156	aman.idf.il	/warez/ access	Block	15
149.88.155.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15