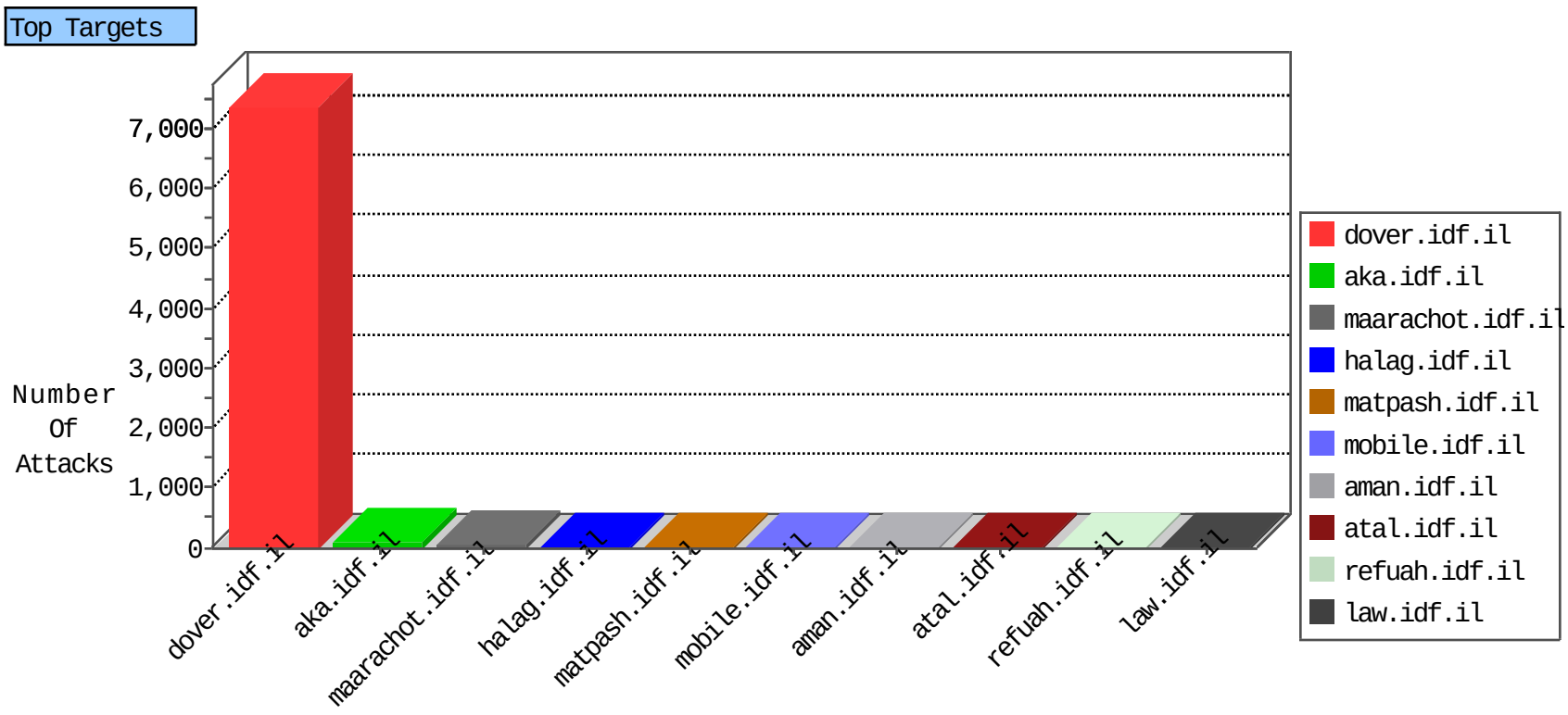
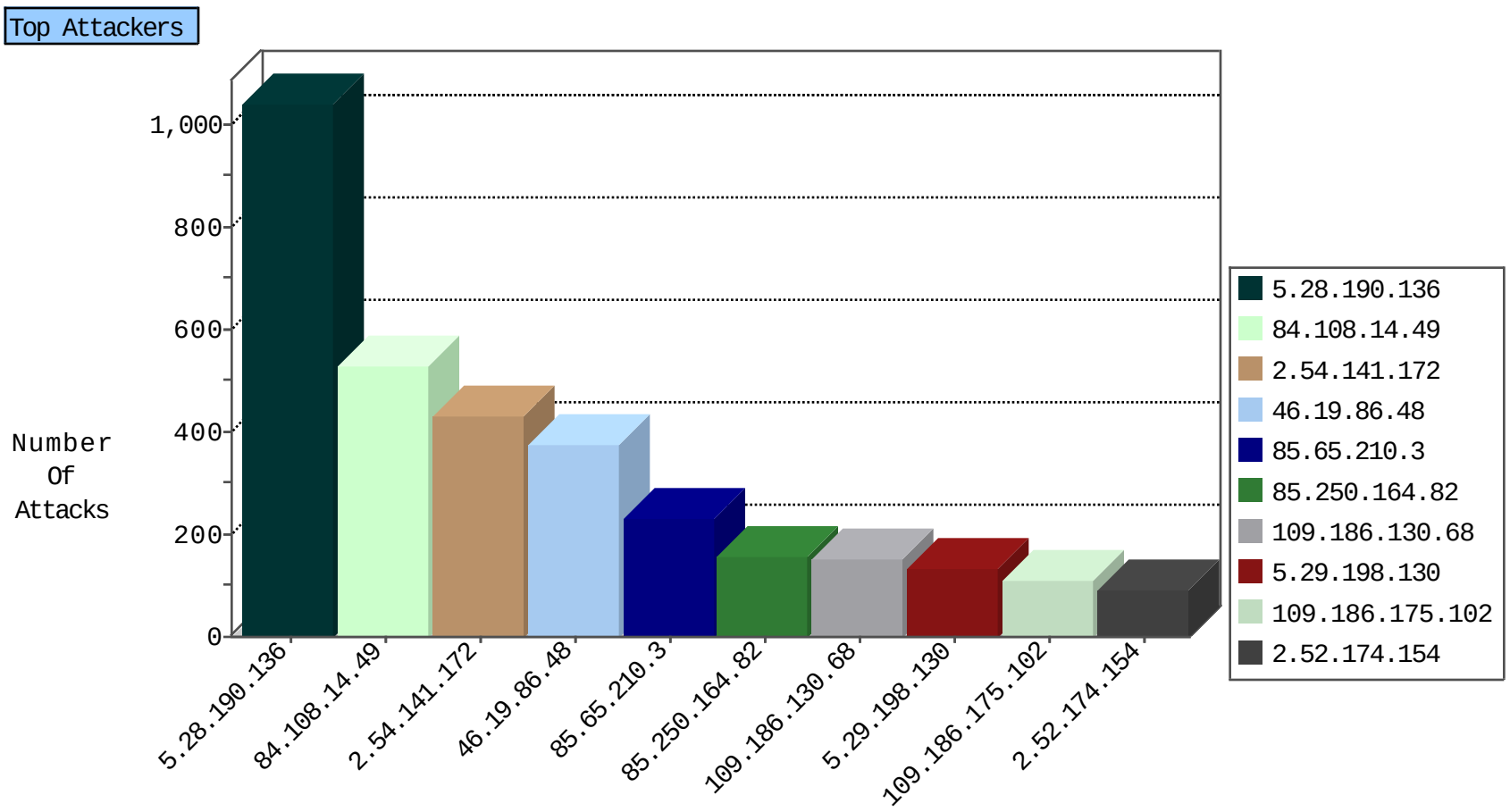
04-18-2015-19:03:02 to 04-18-2015-20:03:02

IDF Under Attack
04-18-2015-19:03:02

Top Targets



Top Attackers



04-18-2015-19:03:02 to 04-18-2015-20:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
93.172.165.93	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
82.102.141.253	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	10
109.67.177.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
89.133.44.108	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
46.121.244.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.117.129.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
195.37.190.86	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
94.98.35.136	Saudi Arabia	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
41.239.215.38	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.228.224.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-18-2015-19:03:02 to 04-18-2015-20:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
205.134.224.235	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	6
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
79.181.198.139	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.231	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
81.123.183.253	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
46.117.75.171	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.64.240.67	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.149.253	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
77.127.204.119	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.174	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
79.180.173.74	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-19:03:02 to 04-18-2015-20:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.145.223.139	Europe	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.178.13.41	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
182.72.40.18	India	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.130.46	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.17.72	Russian Federation	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.39.131	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
79.183.148.75	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.38	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-18-2015-19:03:02 to 04-18-2015-20:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.28.190.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1042
84.108.14.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	529
2.54.141.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	427
46.19.86.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	374
85.65.210.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	229
85.250.164.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	154
109.186.130.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	152
5.29.198.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	135
109.186.175.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
2.52.174.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
46.116.85.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
109.253.140.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
46.117.220.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
79.177.105.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
2.54.146.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	51
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
109.253.138.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
79.179.16.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
109.186.129.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
85.250.74.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
89.138.220.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
109.253.159.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
81.123.183.253	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
176.12.151.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
77.125.222.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.137.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
2.52.170.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
46.19.86.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
2.54.54.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.121.153.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
79.180.191.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
149.78.26.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
99.126.53.208	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
82.102.141.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.182.163.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
84.228.205.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
49.228.70.245	Thailand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
84.228.114.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.253.138.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
2.52.52.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
84.111.154.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
109.253.141.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	15
134.249.53.8	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	Block	5
89.139.181.202	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	4
178.137.85.64	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
77.127.229.185	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication	Block	2
85.248.226.28	Slovakia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
190.215.113.246	Chile	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
170.75.152.146		147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
109.186.154.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
178.254.36.72	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
2.54.189.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
108.178.202.110	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
87.253.162.5	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.128.48.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter 03ebfc30 in aka.idf.il/iturim/asp/results.asp	None	1
85.248.226.28	Slovakia	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
79.179.192.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
49.212.169.50	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//old/wp-admin/	Block	1
190.215.113.246	Chile	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
82.161.176.208	Netherlands	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.39.85.81	France	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
170.75.152.146		147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
109.186.56.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/main/giyus/general.aspx	None	1
79.180.16.251	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
46.117.75.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
178.254.36.72	Germany	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0706-1.stm	Block	1
107.77.94.96	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
49.228.70.245	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
82.161.176.208	Netherlands	147.237.72.166	aka.idf.il	Unknown Parameter DocID=61864 in www.aka.idf.il/edim/library/generaldoc.asp	None	1
5.39.85.81	France	147.237.72.156	aman.idf.il	Illegal HTTP Version + url + ' HTTP/1.1	Block	1
79.177.32.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.60.111	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
80.246.130.141	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.117.230.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
68.142.232.8	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wordpress/wp-admin/	Block	1
108.178.202.110	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored4.stm	Block	1
49.228.70.245	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1