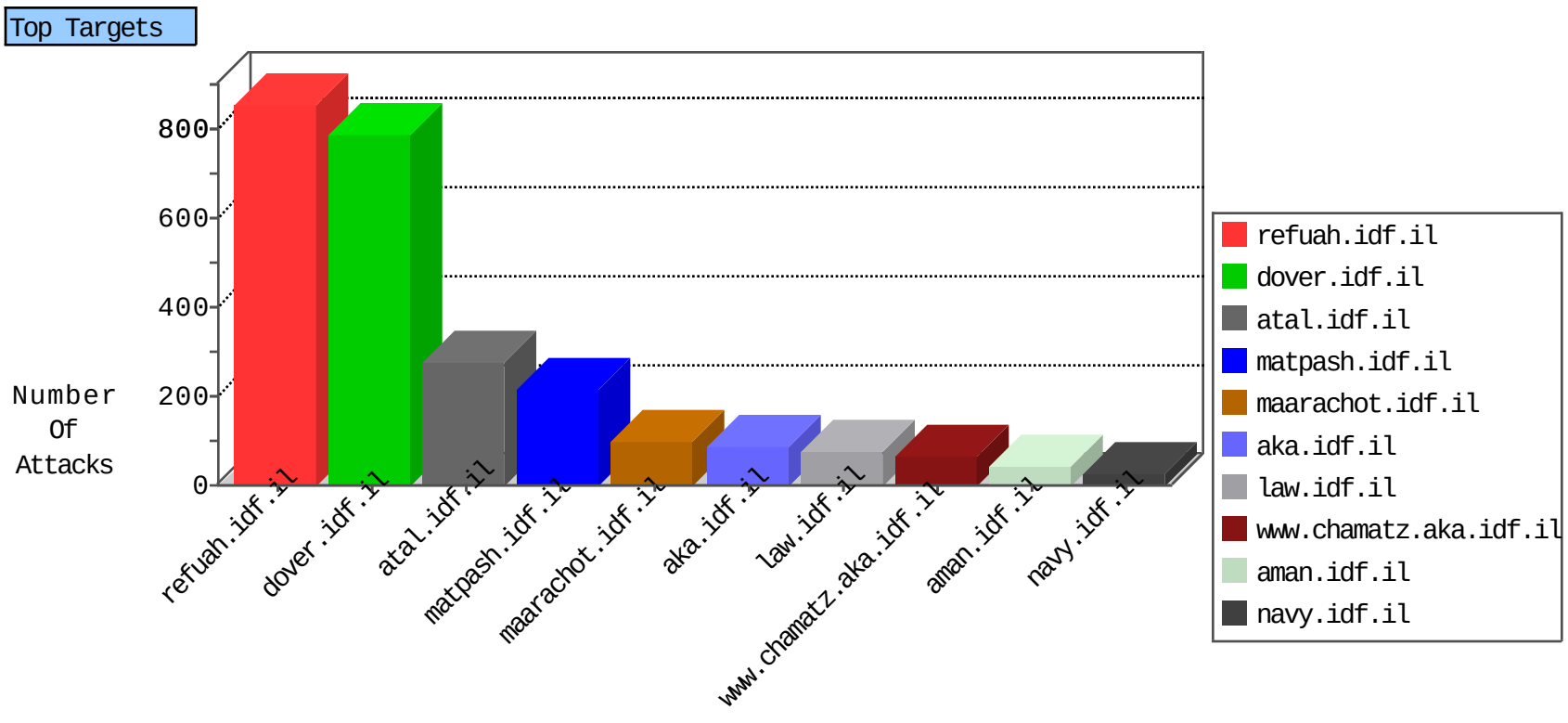
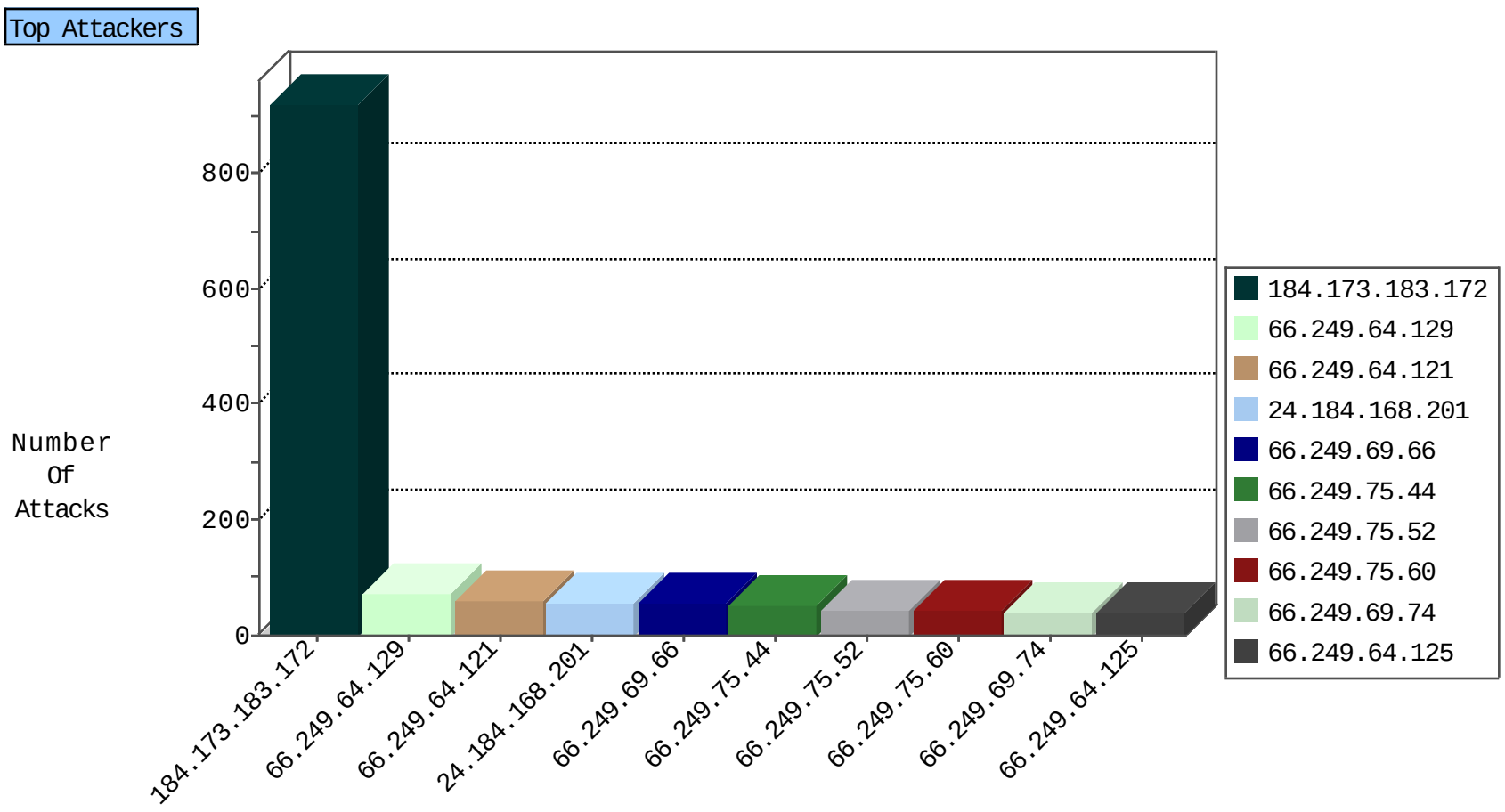
04-08-2015-04:03:01 to 04-08-2015-05:03:01

IDF Under Attack
04-08-2015-04:03:01





04-08-2015-04:03:01 to 04-08-2015-05:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.110.86.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	69
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	57
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	54
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	53
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	45
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	44
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	41
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	35
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	28
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	21
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	17
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.78.134	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.67.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	9
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.64.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.64.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.67.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4

04-08-2015-04:03:01 to 04-08-2015-05:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	612
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	165
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	145
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
112.216.26.252	Korea, Republic of	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.idf.	DVRep_B-N_60_100	Block	1

04-08-2015-04:03:01 to 04-08-2015-05:03:01

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
222.69.94.13	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.130		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
27.50.132.61	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
222.69.94.13	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
222.69.94.13	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
193.107.16.206	Russian Federation	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
69.12.92.160	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.61	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2015-04:03:01 to 04-08-2015-05:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
24.184.168.201	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
174.252.194.20	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
75.73.52.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
50.82.62.234	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
97.106.119.244	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.253.130.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
108.80.129.239	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
73.194.197.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
172.56.30.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
176.12.137.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.26.147.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
108.246.13.29	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
91.200.12.28	Ukraine	147.237.77.74	law.idf.il	SAM rule	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
108.212.244.124	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
73.193.152.12	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
108.31.241.56	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
68.187.248.97	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.54.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
40.135.5.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
65.188.229.84	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.174	Israel	147.237.76.31	nakchal.idf.i	Invalid ACK number	Bad TCP sequence	monitor	4
85.65.220.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.58.124.246	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
180.248.39.121	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
23.233.70.189	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.173.233.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
142.196.32.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
23.113.168.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.253.144.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.169.145.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.153	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.157.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
73.51.235.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
65.19.138.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
105.237.77.46	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.236.201.115	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.193.158.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-08-2015-04:03:01 to 04-08-2015-05:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.244.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	2
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	2
84.228.103.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
208.54.87.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.136	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
62.201.208.14	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
109.253.159.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0302-1.stm	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
178.162.203.244	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.5	Block	1
136.243.36.88	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.116.244.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.109.233.48	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.118.119.63	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8948-he/refuah.aspx	Block	1

04-08-2015-04:03:01 to 04-08-2015-05:03:01