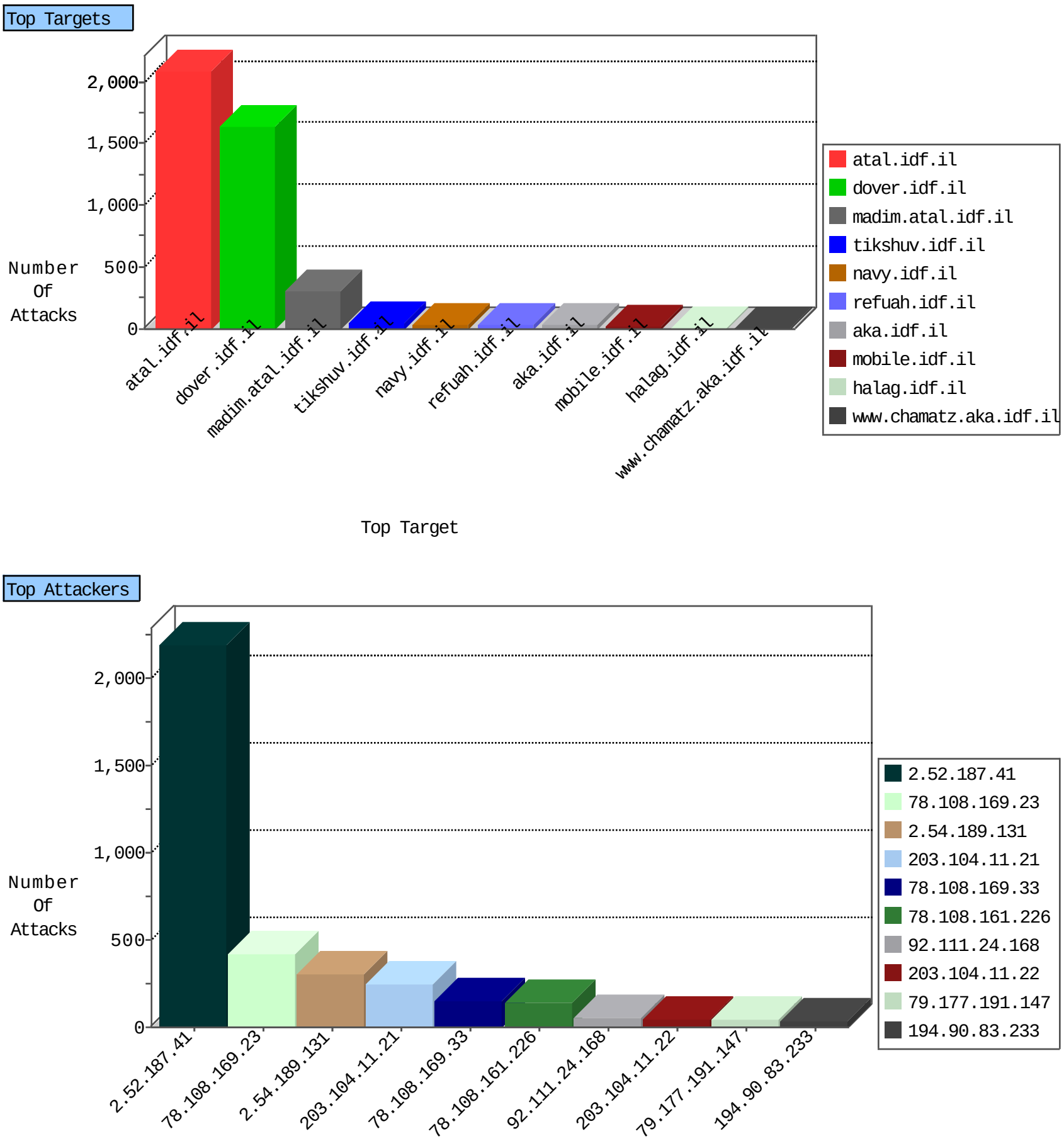
05-05-2015-07:03:07 to 05-05-2015-08:03:07

IDF Under Attack
05-05-2015-07:03:07



05-05-2015-07:03:07 to 05-05-2015-08:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
12.250.253.110	United States	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1

05-05-2015-07:03:07 to 05-05-2015-08:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.187.41	Israel	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	2078
2.52.187.41	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	117
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
79.177.99.23	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.75	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
79.179.110.20	Israel	147.237.76.42	refuah.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

05-05-2015-07:03:07 to 05-05-2015-08:03:07

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	4
176.12.139.255	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.102.60.140	Netherlands	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.5.191		147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
203.113.9.143	Thailand	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
203.113.9.143	Thailand	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
142.54.181.100	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.56.205	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
203.113.9.143	Thailand	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
142.54.181.100	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1

05-05-2015-07:03:07 to 05-05-2015-08:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
78.108.169.23	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	415
203.104.11.21	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
92.111.24.168	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
203.104.11.22	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	45
79.177.191.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	33
78.108.161.226	Lebanon	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	27
207.34.76.162	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
2.54.189.131	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
147.236.30.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
2.54.15.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.64.26.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
82.80.50.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.143.167	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
47.17.236.202	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.66.126.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.179.46.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
212.199.57.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
87.68.83.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.87.119.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
91.4.8.75	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.228.12.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.179.239.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
80.246.130.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
203.104.11.21	Australia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
74.73.151.222	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
78.108.161.226	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	5
2.54.3.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
111.93.44.123	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
194.90.134.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
78.108.161.226	Lebanon	147.237.77.234	halag.idf.il	First packet isn't SYN	drop	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.189.131	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.189.131	Block	282
85.250.8.24	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
109.253.142.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
69.113.153.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
149.78.124.10	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
61.141.252.22	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
180.76.6.134	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/kenya.stm	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.112.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/sites/resources/chinuch/styles/klali.asp	None	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.186.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
99.162.90.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
184.173.183.174	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-8271-he/dover.aspx&usg=alkjrhhcv2pe8yd6dazuyv7neep4yiacew	Block	1
66.249.64.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.126.229.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/sites/resources/chinuch/styles/mador.asp	None	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	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
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
188.138.17.205	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	1
66.249.64.247	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
79.179.110.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1387-he/atal.aspx	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
157.55.39.158	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
115.25.81.72	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza>Ñ?Ð¿ÐµÑ†Ð¸Ð°Ð»ÑŒ Ð½Ð¾Ð¼ÐµÑ€ Ñ?Ð°Ð¹Ñ‚Ð¾Ð², Ñ?Ð¾Ð·Ð´Ð°Ð½Ð¸Ð¸ Ð´Ð»Ñ? Ñ?Ñ‚Ð¾Ð»Ð±Ñ†Ð¾Ð². <p> <table cellspacing=	Block	1
66.249.93.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0302-2.stm	Block	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71822-he/maarachot.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.219.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
176.12.147.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	1