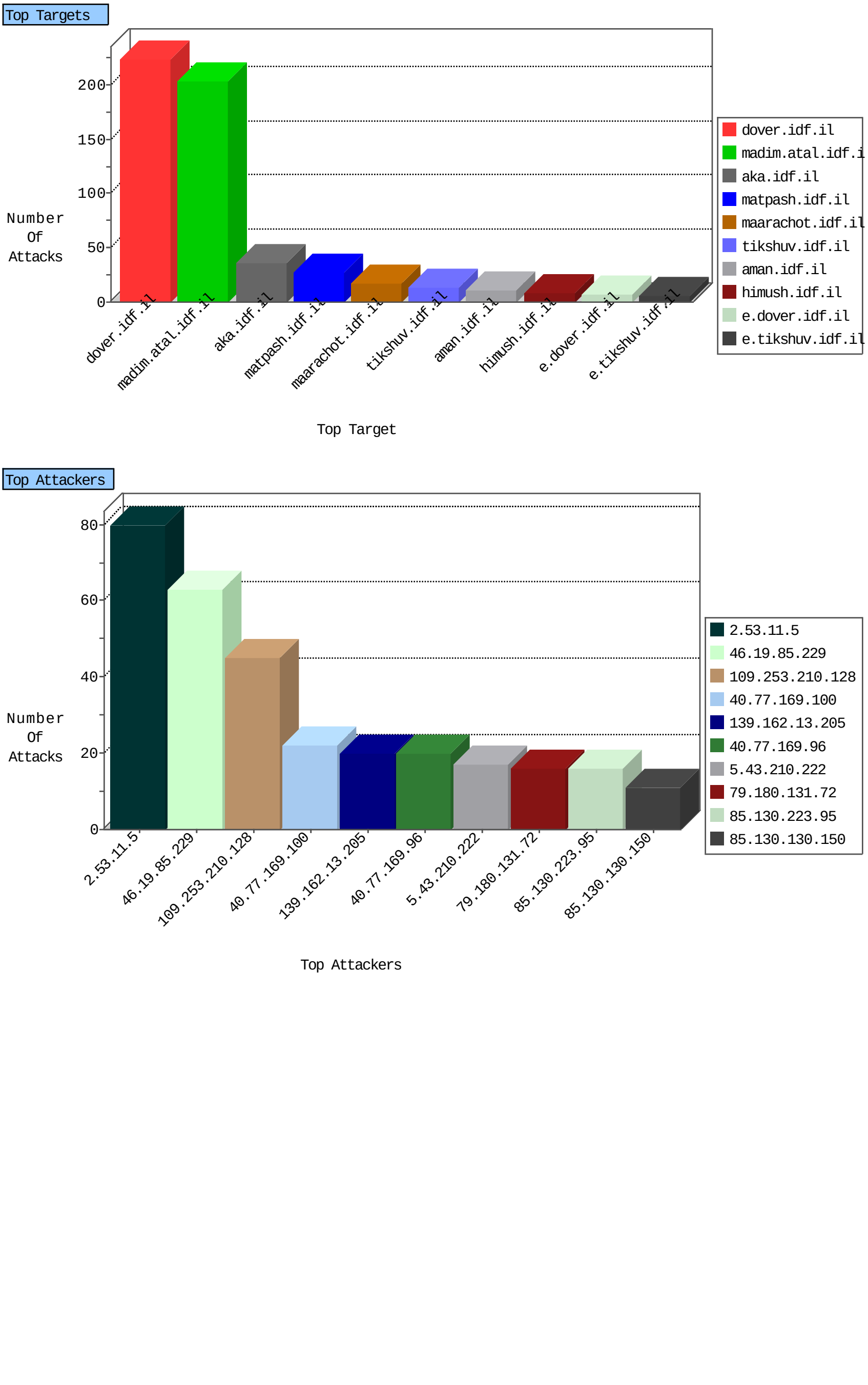
08-24-2016-14:04:03 to 08-24-2016-15:04:03

IDF Under Attack Daily Report



08-24-2016-14:04:03 to 08-24-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	8
109.253.217.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
212.179.64.162	Israel	147.237.72.156	aman.idf.il	Black List	drop	3
115.230.125.146	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.200.193.6	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
104.148.55.162	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-24-2016-14:04:03 to 08-24-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.137.160.45	Ukraine	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1
178.137.160.45	Ukraine	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	1

08-24-2016-14:04:03 to 08-24-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.194.170.194	147.237.77.216	Netherlands	dover.idf.il	Xenu Link Sleuth User Agent	1

08-24-2016-14:04:03 to 08-24-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
5.43.210.222	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
85.130.223.95	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
85.130.130.150	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	11
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	drop	SAM rule	drop	7
139.162.13.205	Singapore	147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	7
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.43.112.217	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
185.79.100.122	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
139.162.13.205	Singapore	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	6
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.41	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	5
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.50.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.223.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.132.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.111.89.69	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.2.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
100.92.156.222		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.210.128	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
41.36.156.11	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.179.115.198	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.249.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.238	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
129.56.2.38	Nigeria	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.7.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
210.56.212.18	China	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.16.153	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.216.64	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
85.130.223.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.11.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
109.253.210.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
79.180.131.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.180.131.72	Block	15
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
176.13.14.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.150.236.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.148.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.30.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.143.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.174.197	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.174.197	Block	3
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
89.169.86.36	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.55.42.108	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.8.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
84.95.45.92	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/	Block	1
5.102.242.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	1
207.46.13.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtcld1fe	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
46.117.128.18	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
89.139.221.152	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
77.139.19.93	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
64.41.200.105	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.250.137.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_stor	Block	1
31.13.100.114	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/-arr	Block	1
66.249.69.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.41.200.105	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.105 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
37.26.148.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
157.55.39.140	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.41.200.105	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.105 (Unsupported Cipher)	None	1
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;c in www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	None	1
89.187.219.147	Lebanon	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/113381.pdf.	Block	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
195.200.205.35	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/close_text.gif	Block	1