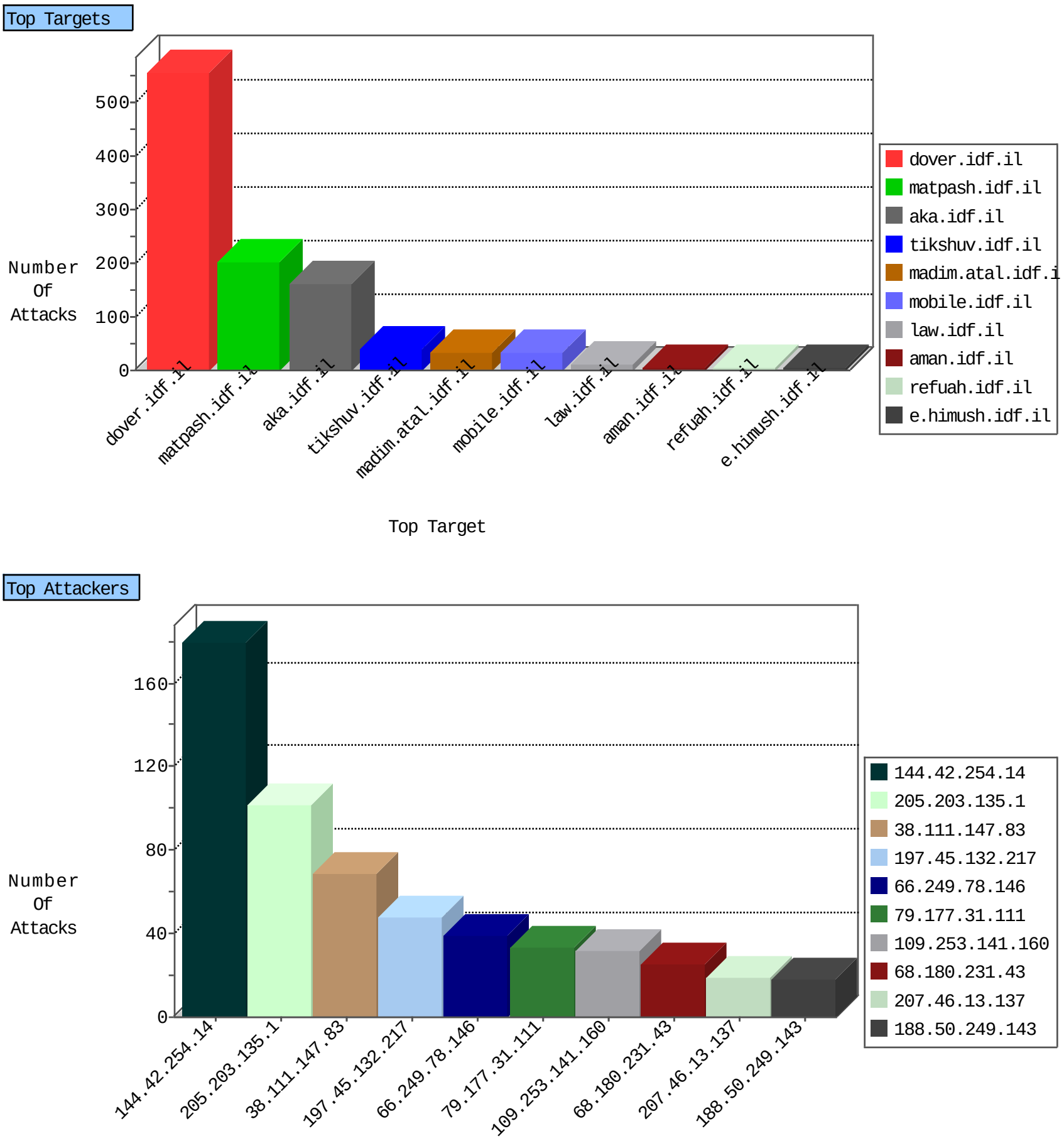
04-29-2016-00:04:08 to 04-29-2016-01:04:08

IDF Under Attack Daily Report



04-29-2016-00:04:08 to 04-29-2016-01:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.153.197.115	Hong Kong	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-00:04:08 to 04-29-2016-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-00:04:08 to 04-29-2016-01:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
68.115.186.146	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
93.189.26.18	147.237.8.24	Austria	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.216.60	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
71.6.216.53	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
68.115.186.146	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
96.36.97.78	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.47	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.216.60	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
158.255.5.147	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
96.36.97.78	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1

04-29-2016-00:04:08 to 04-29-2016-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
144.42.254.14	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	180
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
38.111.147.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
79.177.31.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.188.243.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.214.182.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.40.89.71	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
172.56.40.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.50.249.143	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.161.15.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.195.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
97.74.24.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.104.139.206	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.147.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.41.30.33	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
82.41.30.33	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.201.101.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.154.173.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
41.3.178.75	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.137.139.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.56.72.73	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
209.6.44.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-00:04:08 to 04-29-2016-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.141.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
89.138.109.204	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	14
82.80.135.141	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	4
93.109.218.123	Cyprus	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
65.55.210.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
64.71.32.22	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.22	Block	2
46.19.85.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	2
199.30.25.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.31.111	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
84.228.235.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
199.30.24.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.99.44.141	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.228.235.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.166.242.178	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
192.110.214.2	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
85.250.185.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
72.10.32.34	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
64.71.32.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/blog/wp-admin/	Block	1
132.74.145.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.185.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.31.140.19	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
75.141.65.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
64.71.32.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.26	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/gadna	Block	1
149.88.229.75	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.228.235.199	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.228.235.199	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
64.71.32.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
213.8.204.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/12.asp	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
46.43.68.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1

04-29-2016-00:04:08 to 04-29-2016-01:04:08