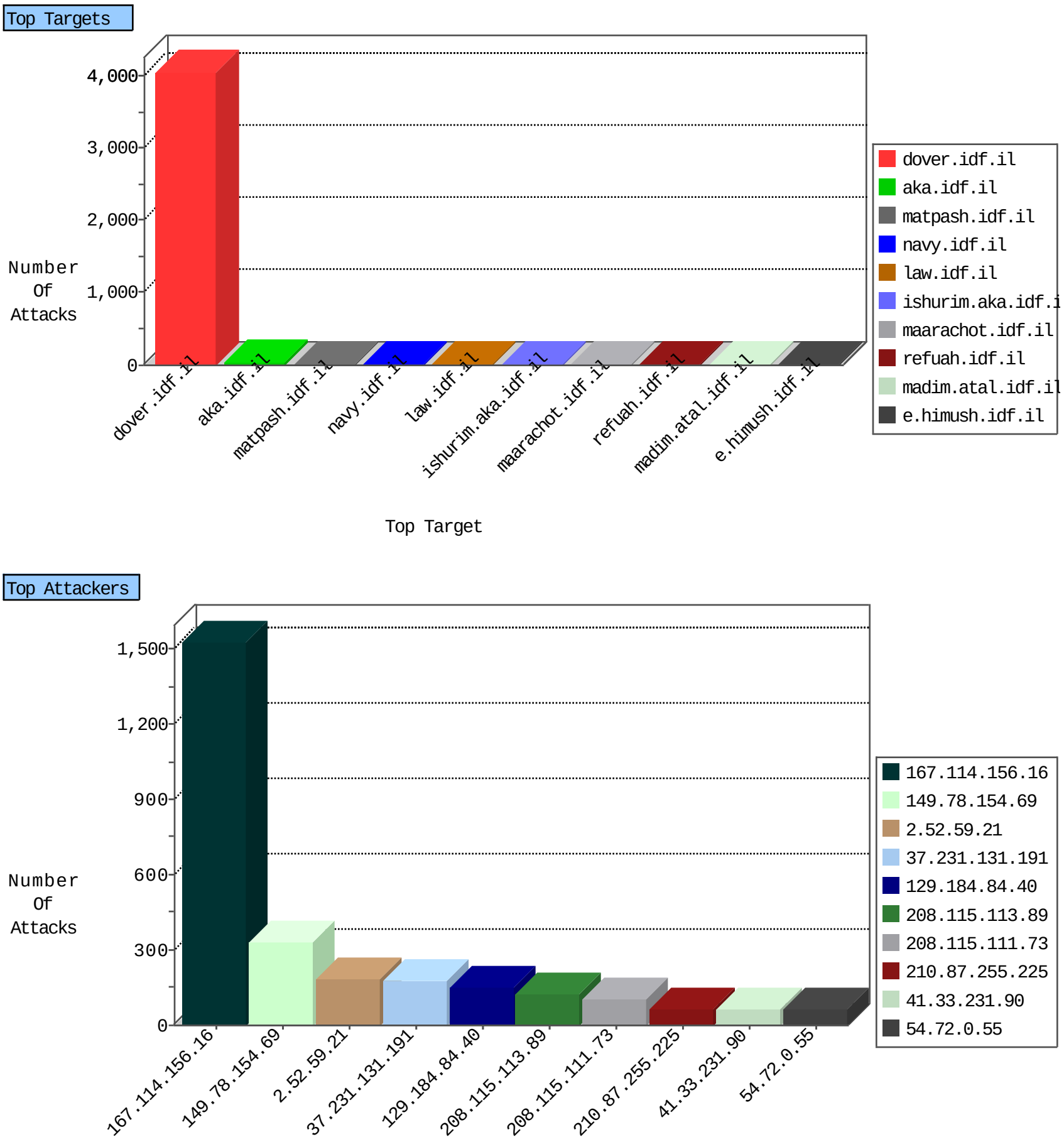
11-03-2015-05:04:01 to 11-03-2015-06:04:01

IDF Under Attack Daily Report



11-03-2015-05:04:01 to 11-03-2015-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2886
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	340
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
112.175.228.16	Korea, Republic of	147.237.76.34	yohalan.idf.il	Invalid TCP Flags	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.216.44	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
112.175.228.16	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.45	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
112.175.228.16	Korea, Republic of	147.237.76.202	e.halag.idf.il	Invalid TCP Flags	drop	1
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
112.175.228.16	Korea, Republic of	147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	1

11-03-2015-05:04:01 to 11-03-2015-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-03-2015-05:04:01 to 11-03-2015-06:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
108.61.222.183	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -f -sS	1
222.186.56.32	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.235.48.150	147.237.8.46	Poland	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.10.134	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
124.122.33.51	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.123.112.210	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
119.123.112.210	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
108.61.222.183	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.56.32	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.32	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.10.134	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
119.123.112.210	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
119.123.112.210	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
108.61.222.183	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1

11-03-2015-05:04:01 to 11-03-2015-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	329
2.52.59.21	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	186
37.231.131.191	Kuwait	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	175
129.184.84.40	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	149
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	122
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	101
210.87.255.225	Hong Kong	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
46.19.85.104	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
46.19.85.211	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
75.66.86.46	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
46.120.169.142	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
24.228.189.141	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
157.55.39.118	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
207.46.13.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
141.209.209.144	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
46.19.85.57	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
204.237.0.104	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
46.19.85.25	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
79.178.112.130	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
107.170.63.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.97.200		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
207.46.13.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.77.167.40	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
157.55.39.236	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
64.233.172.155	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
85.64.69.38	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.69.42	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
2.52.136.33	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
202.10.90.150	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-03-2015-05:04:01 to 11-03-2015-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.108.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.251	Block	2
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/main/home/default.aspx	None	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
207.46.13.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2254.jpg	Block	1
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71553-he/maarachot.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/81e359d56918044eb131f43270c06e55/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
82.221.105.7	Iceland	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71625-he/maarachot.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/	Block	1
66.249.65.125	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	1
157.55.39.164	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/home/default.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

11-03-2015-05:04:01 to 11-03-2015-06:04:01