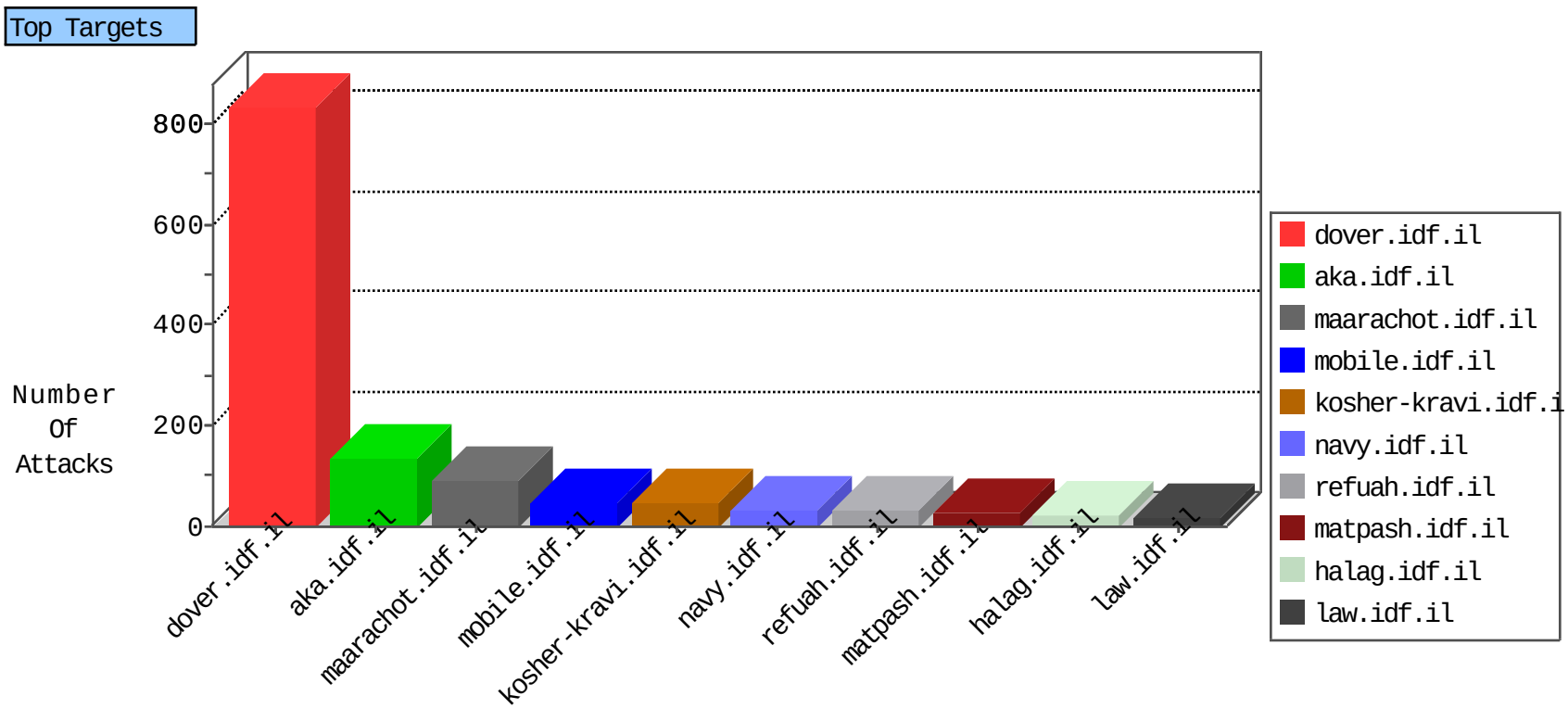
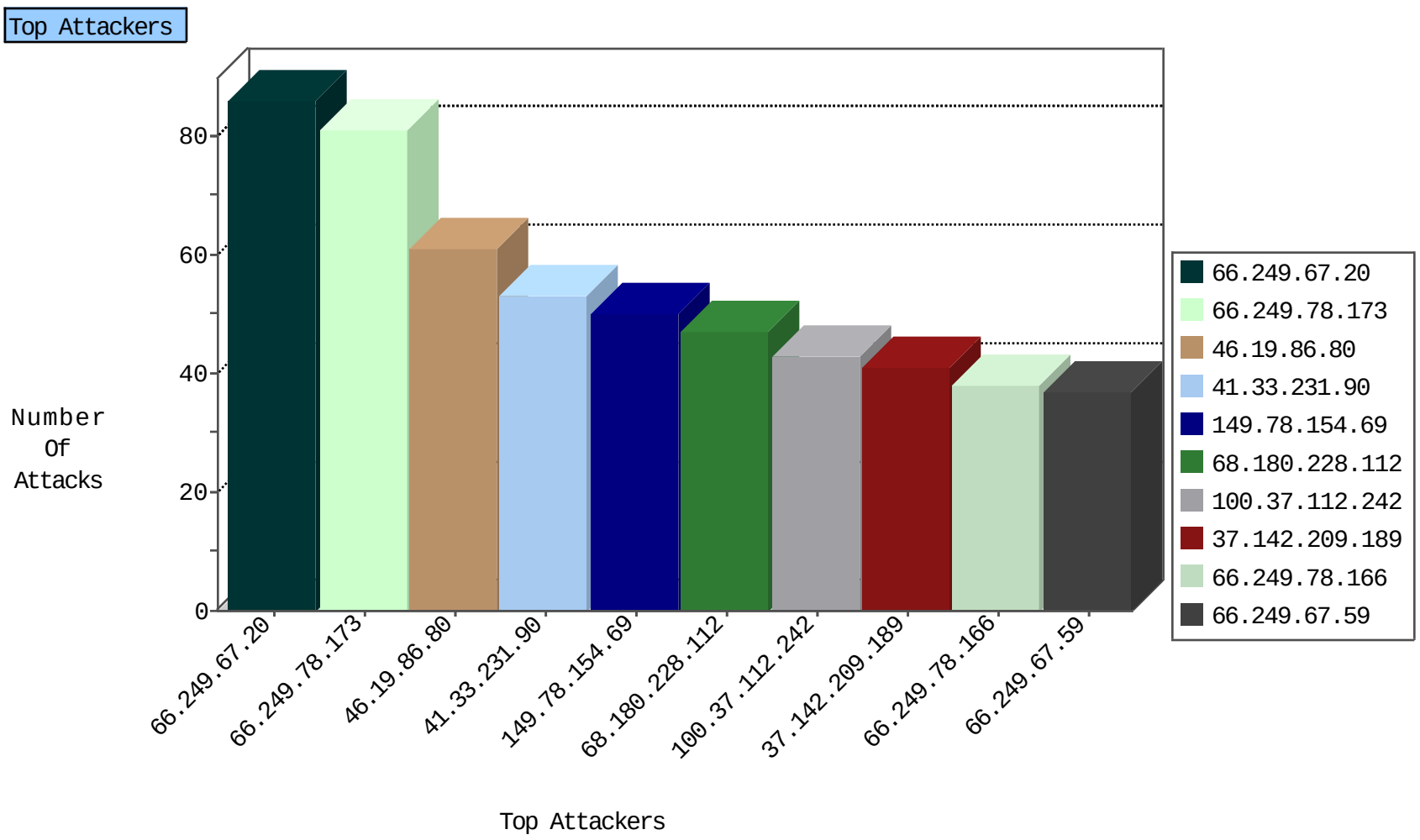
11-01-2015-05:04:07 to 11-01-2015-06:04:07

IDF Under Attack Daily Report





11-01-2015-05:04:07 to 11-01-2015-06:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6524
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	945
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	448
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	155
66.249.74.98	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	55
100.37.112.242	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
151.80.31.112	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
24.13.45.210	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
67.42.82.149	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
192.168.14.187		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.116.119.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
49.183.70.16	Australia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
185.115.124.16		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

11-01-2015-05:04:07 to 11-01-2015-06:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.12.168.26	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	13
109.65.108.86	Israel	147.237.0.34	tikshuv.idf.i	C1000004: HTTP: options method (Microsoft)	Block	4
204.12.168.26	United States	147.237.72.166	aka.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

11-01-2015-05:04:07 to 11-01-2015-06:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
204.12.168.26	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	16
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
223.4.244.13	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
14.215.130.20	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
223.4.244.13	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.147	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sS window 3072	1
210.50.197.147	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -f -sS	1
201.158.203.53	147.237.76.177	Mexico	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
119.146.130.25	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
223.4.244.13	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
223.4.244.13	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.147	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sS window 2048	1

11-01-2015-05:04:07 to 11-01-2015-06:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
46.19.86.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.142.209.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
100.37.112.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
47.20.25.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
67.42.82.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.13.15.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
97.125.190.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
49.183.70.16	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.66.119.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.54.25.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
201.52.177.87	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.120.126.32		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.87.78.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.108.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
66.249.65.125	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.194.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.68.65.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
131.253.25.141	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.210.242.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.137.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.228.97.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
70.196.73.165	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-01-2015-05:04:07 to 11-01-2015-06:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	30
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	15
66.249.67.38	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
182.69.48.166	India	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	15
2.54.25.143	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
185.120.126.32		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.54	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/links/links.aspx	Block	15
52.91.173.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Parameter Type Violation utm_source in www.idf.il/1133-20998-he/dover.aspx	Block	15
66.249.78.222	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	15
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
207.46.13.184	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	15
66.249.78.228	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	15
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1258-he/refuah.aspx	Block	15
87.69.137.150	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	15

11-01-2015-05:04:07 to 11-01-2015-06:04:07