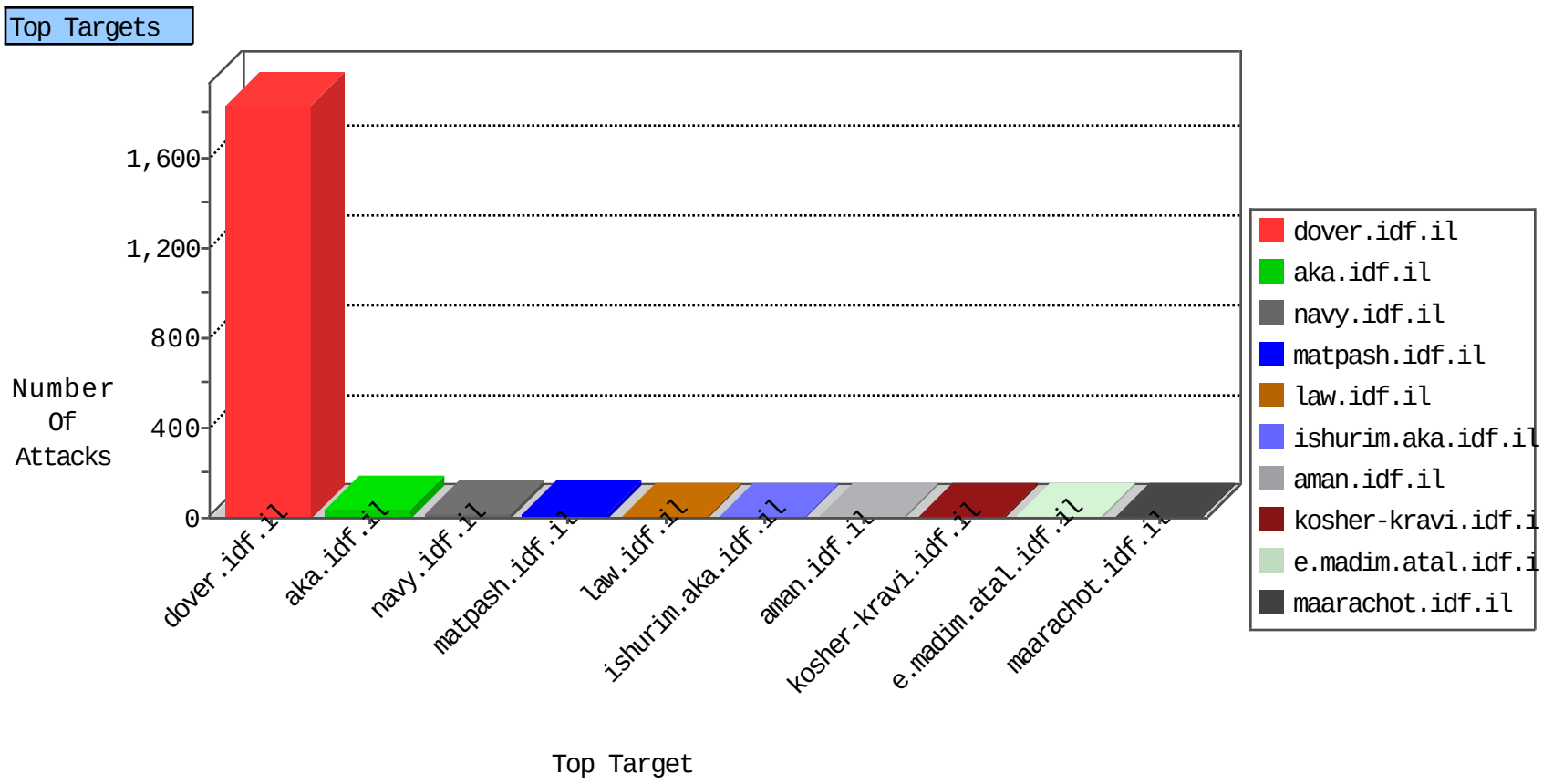
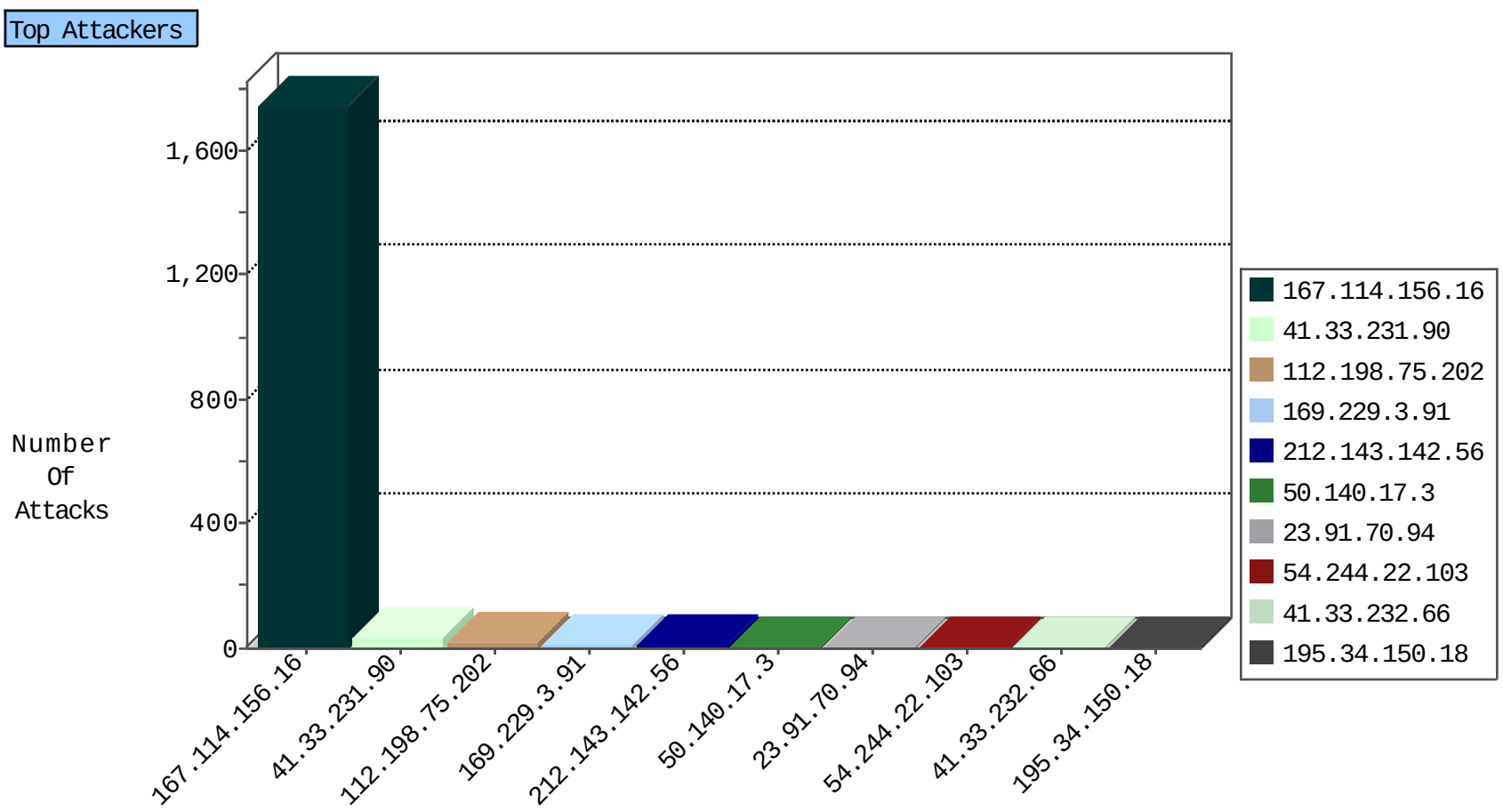
01-11-2016-05:04:05 to 01-11-2016-06:04:05

IDF Under Attack Daily Report





01-11-2016-05:04:05 to 01-11-2016-06:04:05

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	3167
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	53
185.130.5.228		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
23.95.248.111	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-05:04:05 to 01-11-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.74.38.14	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
200.59.205.238	Argentina	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
216.185.43.135	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
87.106.179.116	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-11-2016-05:04:05 to 01-11-2016-06:04:05

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	2
201.68.47.159	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.180.37.251	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
5.39.222.196	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

01-11-2016-05:04:05 to 01-11-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.140.17.3	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
104.35.157.251	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
23.91.70.94	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.65.30.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
177.185.192.50	Brazil	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
136.243.98.54	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.223	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
158.255.6.220	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.34	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.80	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
190.218.53.12	Panama	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
184.105.139.82	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
141.212.122.110	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
177.185.192.50	Brazil	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
216.218.206.107	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.114	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.111	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.20.47.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.223	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
73.218.120.240	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
23.91.70.94	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
184.105.139.79	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	4
84.228.35.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.31	Block	2
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
208.115.111.74	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
40.77.167.102	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/csp/dtag	Block	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/contact	Block	1
23.91.70.94	United States	147.237.72.167	ishurim.aka.idf.il	Multiple signatures from 23.91.70.94	Block	1
109.65.30.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
45.55.152.128		147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
157.55.39.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm)	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20236-he/idfgdover.aspx	Block	1
199.30.24.11	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.3	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
114.97.195.242	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1026-he/shared/usercontrols/headerupper/	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
216.218.206.67	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.137	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1766	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.3	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/plus/url_qrcode.php	Block	1
141.212.122.97	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /x	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
177.185.192.50	Brazil	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.74.109	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
40.77.167.44	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter qid in www.eitan.aka.idf.il/templets/js/iasklist.js	None	1
150.101.217.28	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
177.185.192.50	Brazil	147.237.72.166	aka.idf.il	Multiple signatures from 177.185.192.50	Block	1
23.91.70.94	United States	147.237.72.167	ishurim.aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

01-11-2016-05:04:05 to 01-11-2016-06:04:05