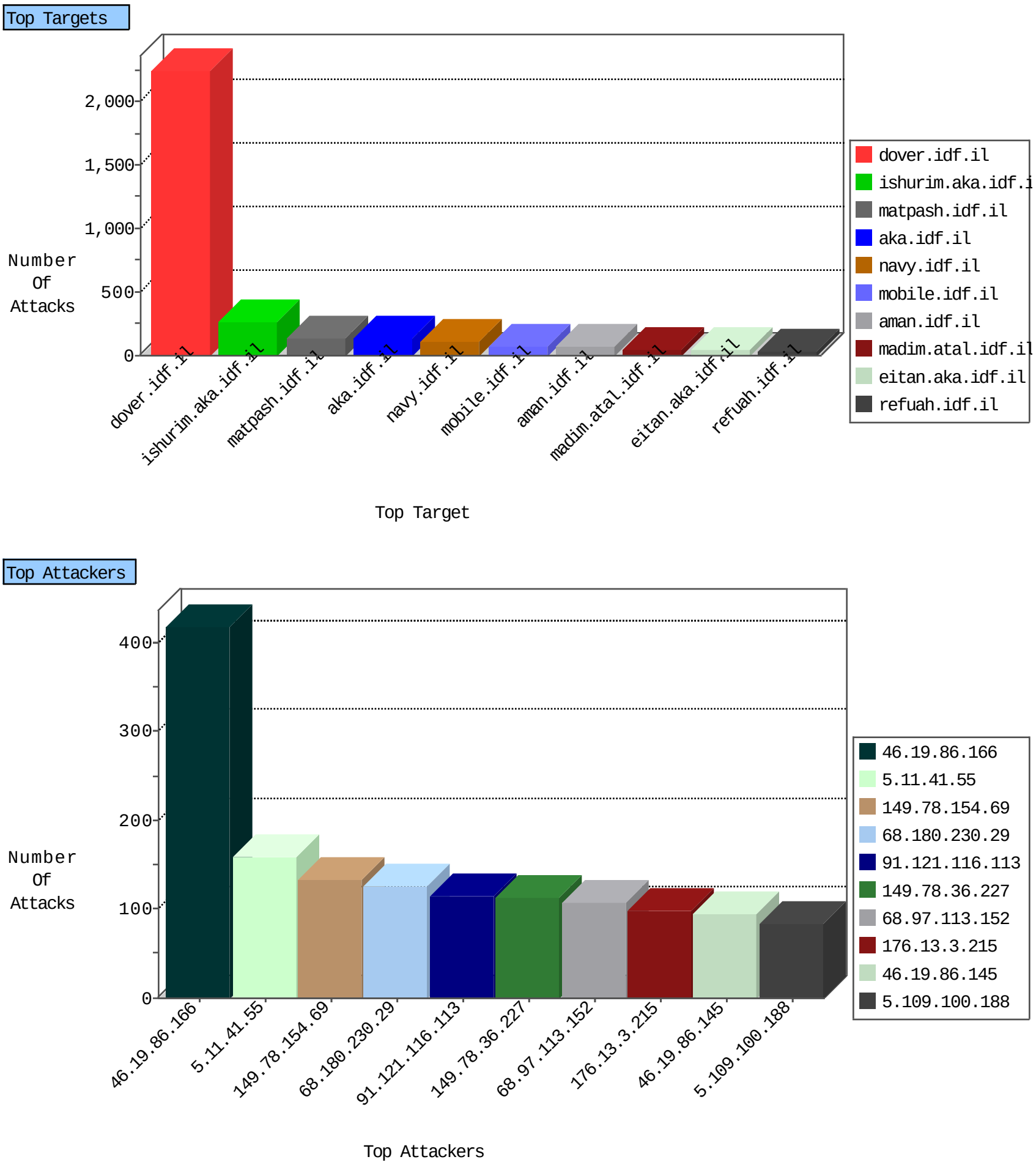
10-23-2015-01:04:05 to 10-23-2015-02:04:05

IDF Under Attack Daily Report



10-23-2015-01:04:05 to 10-23-2015-02:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.187.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
50.199.38.173	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.182.119.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.228.77.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.182.119.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-23-2015-01:04:05 to 10-23-2015-02:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-01:04:05 to 10-23-2015-02:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.84	147.237.76.86	Israel	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	35
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
210.61.150.154	147.237.8.45	Taiwan	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
61.174.13.64	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
138.47.27.43	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	1
61.174.13.64	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.174.13.64	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.16	Italy	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.8.45	Taiwan	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
61.174.13.64	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
114.34.33.33	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.143.82.50	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
61.174.13.64	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.200	Italy	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.15	Italy	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.174.13.64	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.8.45	Taiwan	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
61.174.13.64	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1

10-23-2015-01:04:05 to 10-23-2015-02:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.166	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	258
5.11.41.55	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	159
46.19.86.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
91.121.116.113	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
149.78.36.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
68.97.113.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
46.19.86.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
5.109.100.188	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
186.5.75.212	Ecuador	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
37.26.147.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
100.35.145.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
65.55.219.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
24.88.91.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.228.144.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
174.29.161.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
81.132.124.151	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
188.3.228.156	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
5.22.129.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.250.205.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.52.12.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.88.243.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
128.230.139.232	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	10
128.230.139.232	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
107.77.89.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.159.96	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
176.13.3.215	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-23-2015-01:04:05 to 10-23-2015-02:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-he/cogat.aspx	Block	84
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	56
176.13.3.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	42
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	42
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
176.13.3.215	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.3.215	Block	28
128.230.139.232	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
84.215.32.250	Norway	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	14
157.55.39.13	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	14
84.228.253.43	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.75.7	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
157.55.39.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15512-he/dover.aspx	Block	14
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	14
91.224.119.189	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.75.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	14
176.13.3.215	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	14
207.46.13.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	14
93.173.31.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
66.249.75.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list5.htm	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	14

10-23-2015-01:04:05 to 10-23-2015-02:04:05