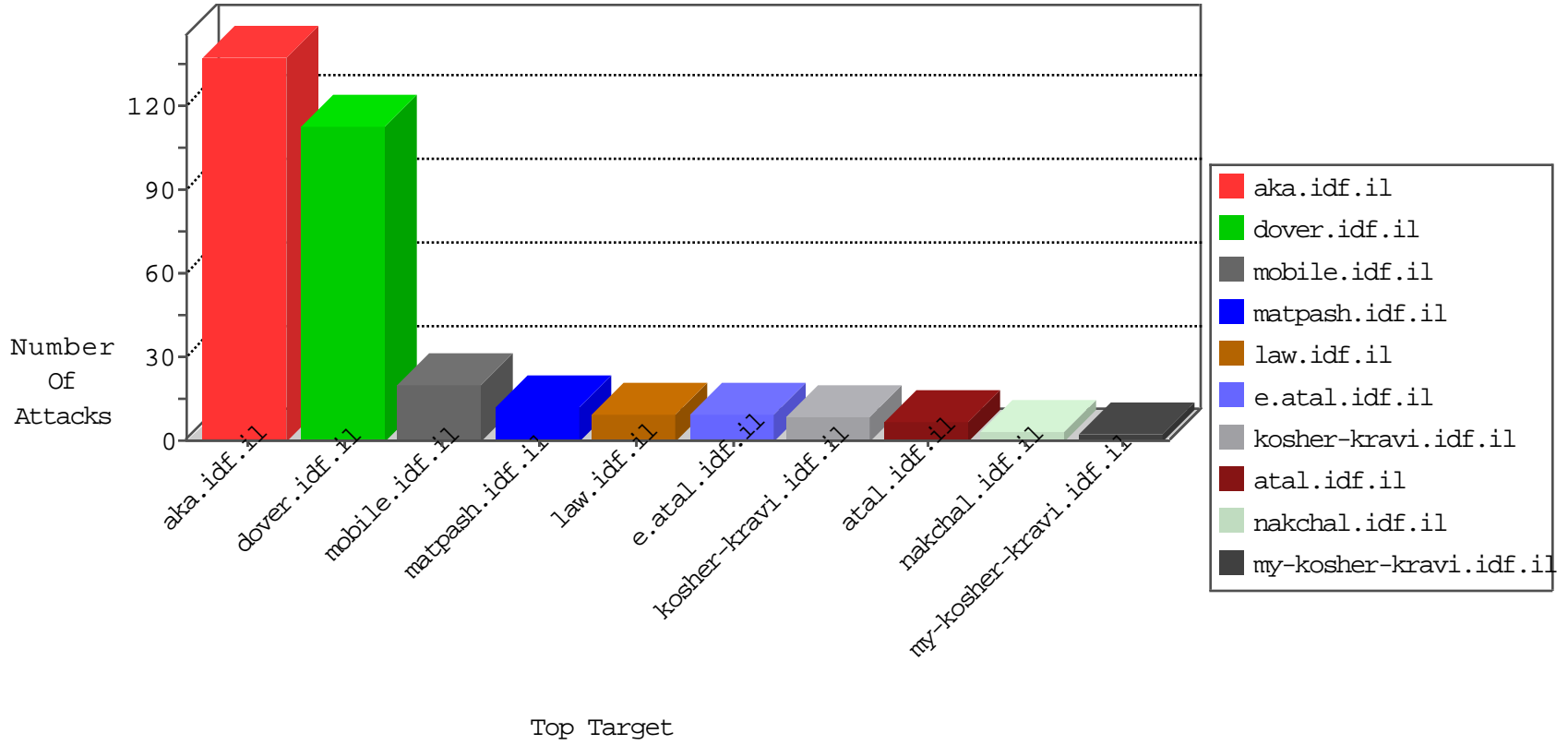


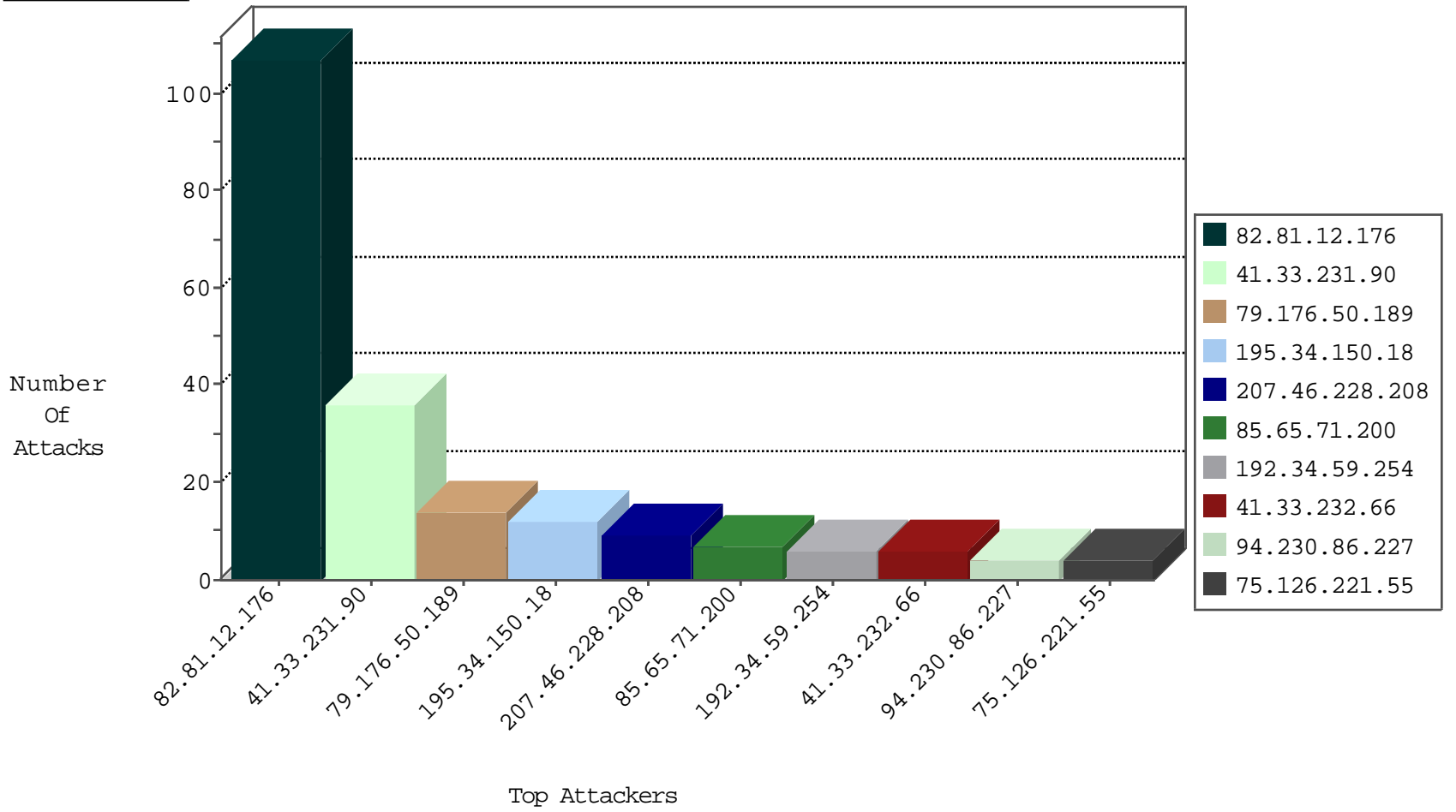
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
175.171.122.21	China	147.237.77.227	e.hamaz.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP_Page_Flood_Attack	drop	2
85.104.2.230	Turkey	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
1.55.118.188	Vietnam	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
85.104.2.230	Turkey	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
217.146.91.36	United Kingdom	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
1.55.118.188	Vietnam	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.45.137.67	147.237.76.176	Turkey	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
182.16.64.15	147.237.77.74	Hong Kong	law.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.76.177	Vietnam	ncore.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.161.40.120	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
209.126.230.74	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.171.23.126	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Potential SSH Scan	1

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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
207.46.228.208	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
79.176.50.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.34.59.254	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.65.71.200	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.212.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.186.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.71.200	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.197.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.207.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.147.244.138	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
173.252.115.87	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.22.126.119	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
173.252.115.84	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
173.252.115.86	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
193.90.12.87	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
162.247.72.199	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
217.132.99.226	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
198.1.101.123	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
70.211.128.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.61.147.146	Portugal	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
92.222.25.220	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.107.85.62	Iceland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
173.208.213.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
104.232.3.33		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.44	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.217.187.39	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.85.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
198.1.101.123	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.50.189	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.50.189	Block	4
89.161.202.147	Poland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.161.202.147	Block	3
79.176.50.189	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
79.183.97.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
188.143.232.35	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1283-en/dover.aspx	Block	2
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
134.119.45.15	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
84.229.129.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1
8.37.70.143	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/dover.aspx&usg=alkjrhg2size0wtylt8ydsbpk8-b1pxwkq	Block	1
192.241.141.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	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
79.176.50.189	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
150.70.173.46	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
150.70.173.46	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.161.202.147	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.84	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
110.170.29.146	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
68.142.232.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
157.55.39.36	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
93.158.152.202	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/webresource.axd	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
134.119.45.15	Germany	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
81.223.254.34	Austria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	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
106.68.207.59	Australia	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1