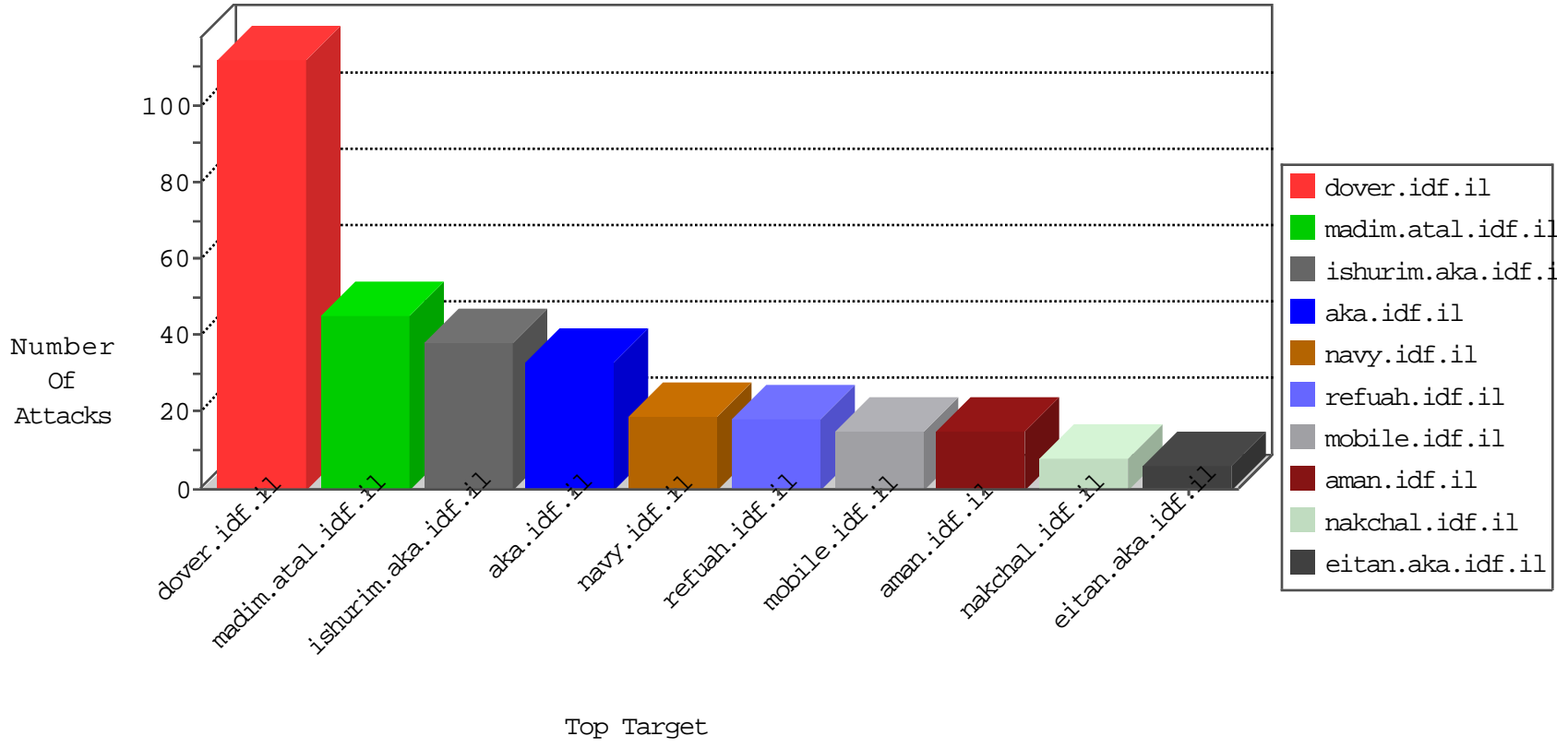


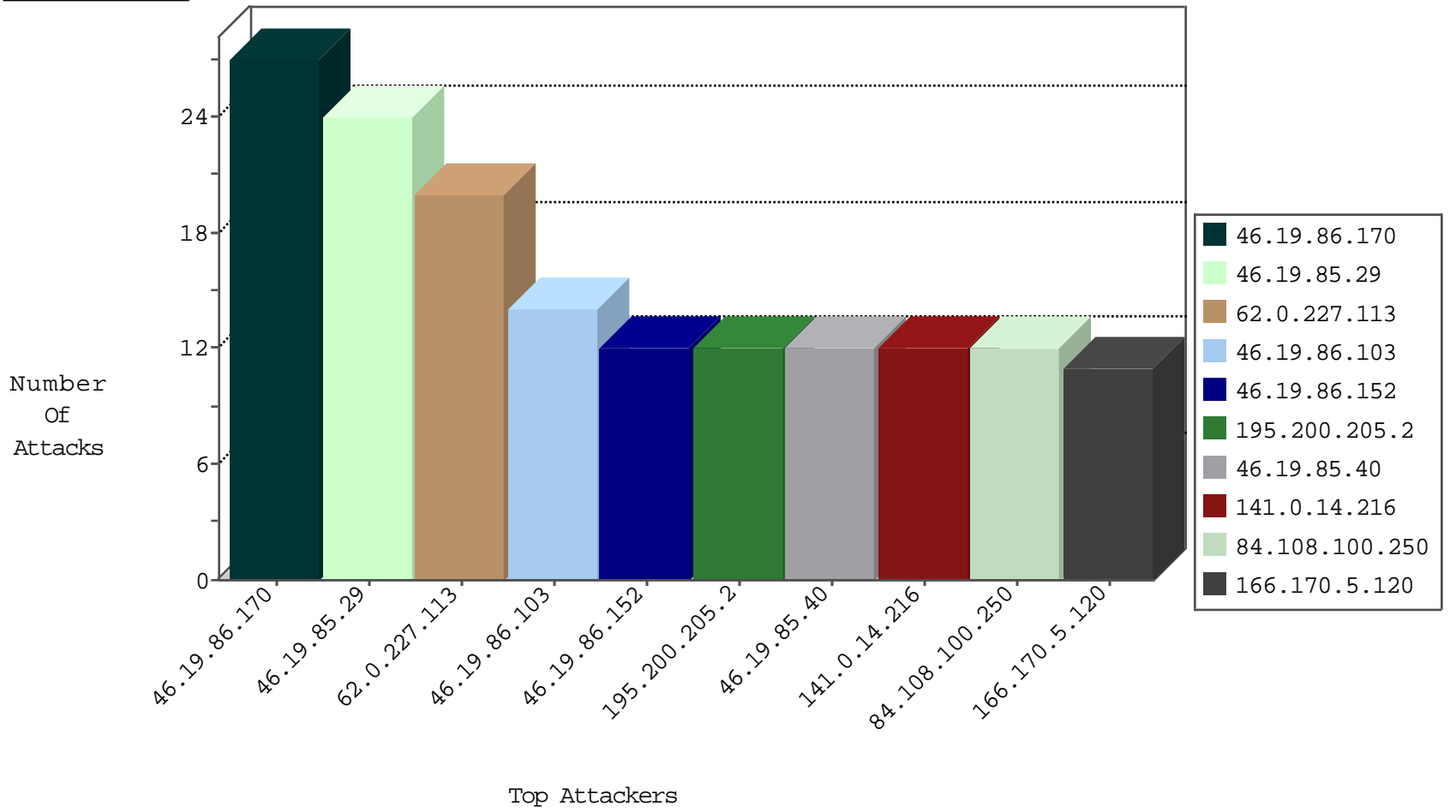
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
84.109.104.55	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
113.240.250.154	China	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
113.240.250.154	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
80.178.173.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
193.193.68.67	147.237.72.156	Poland	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
79.182.138.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.168.128	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.161.18.9	147.237.77.19	Taiwan	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
206.246.150.226	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.77.19	Latvia	law-forum.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.0.19	Singapore	madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.236.86.32	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
77.127.95.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.65.165	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
61.12.86.235	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.240.243	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
206.246.150.226	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
47.88.4.204	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
190.92.65.79	147.237.76.148	Honduras	ggcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.166.86.136	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.232.110.28	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.227.113	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	16
141.0.14.216	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.200.205.2	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.100.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.100.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
166.170.5.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
166.170.5.120	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.190.84	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
108.212.133.54	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.147.243	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.227.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.146.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
87.69.49.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.49.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.215.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.207	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
89.139.66.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.184	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.131.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.130.161.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.8.80	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.243	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.74	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
88.159.67.80	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.91.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.147.243	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.29.142.64	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.137.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.18	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
95.35.197.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.8.80	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.147.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.32	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.199.31	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
206.246.150.226	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.53.132.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	5
2.53.44.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.56.179	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
109.253.215.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.84	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.84	Block	2
89.139.66.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.173.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
139.162.13.205	Singapore	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.178.173.21	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.53.56.179	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.56.179	Block	1
191.96.143.6	United States	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
46.19.85.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
89.139.197.235	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.65.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1233-he/atal.aspx	Block	1
191.96.143.6	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/blog/wp-login.php	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
217.194.197.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.153.73.3	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmilum/templates/home.asp	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.229.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
89.138.24.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/31082010masaiyot.aspx	Block	1