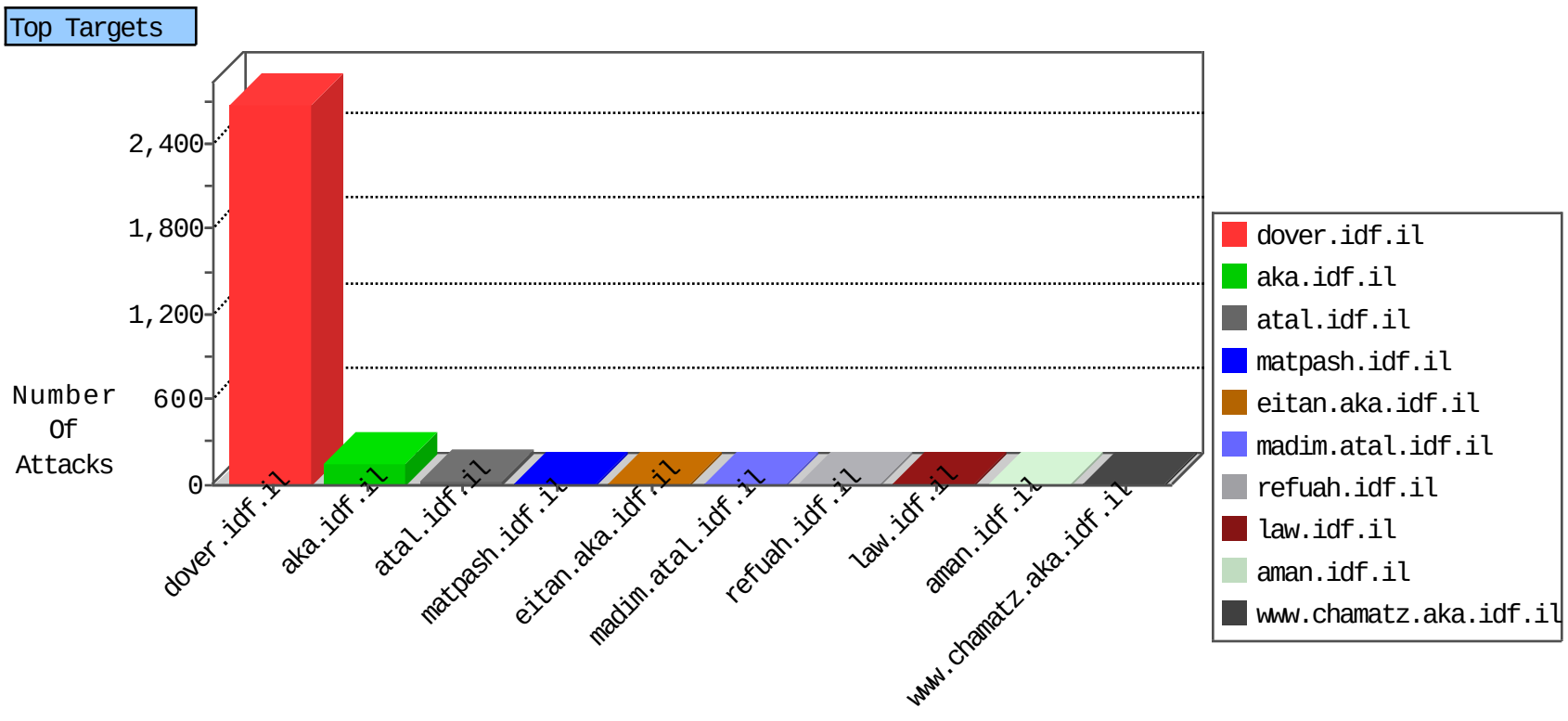
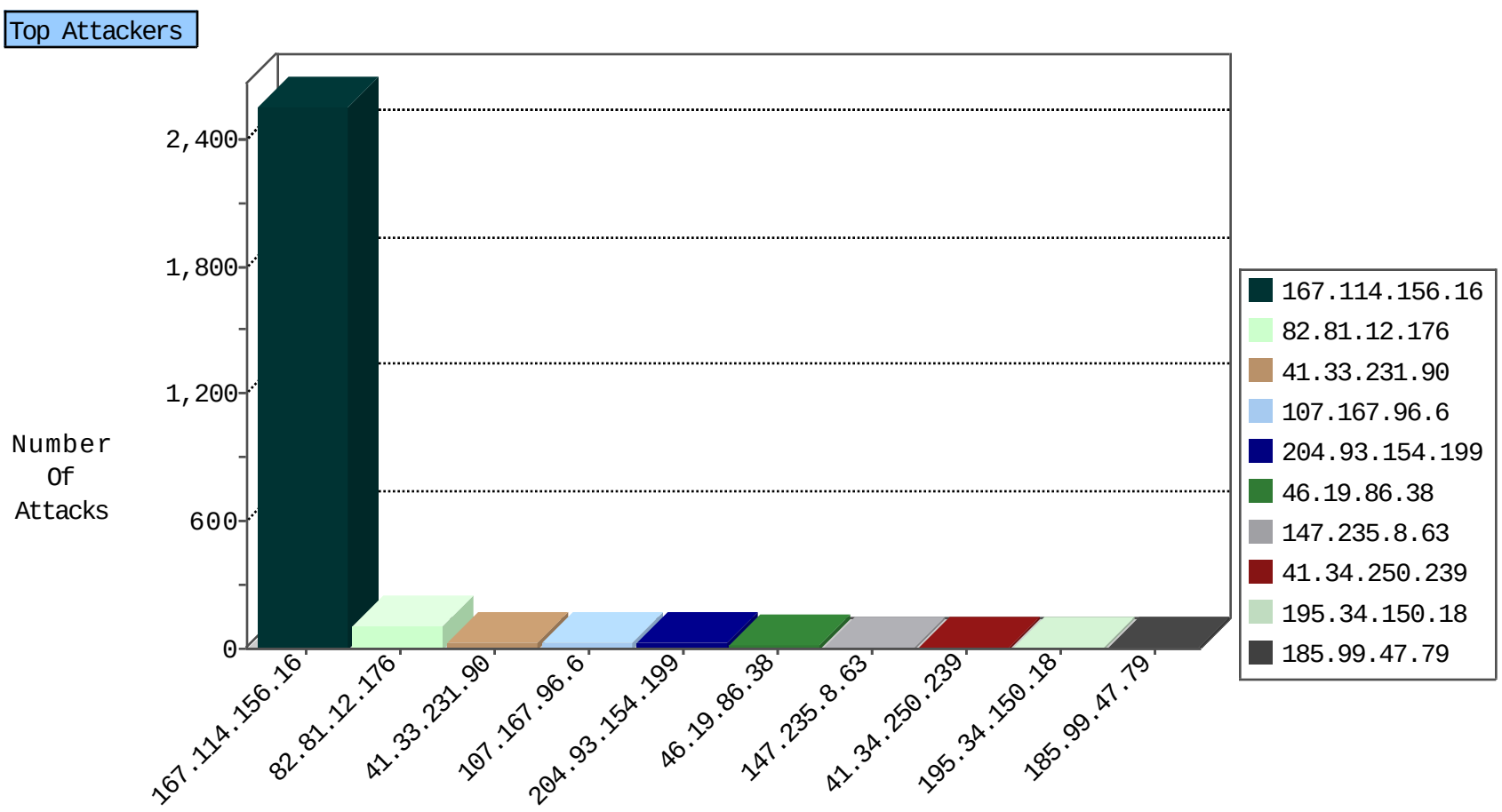
01-25-2016-02:04:00 to 01-25-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-25-2016-02:04:00 to 01-25-2016-03:04:00

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	3043
204.93.154.199	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	194
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
218.84.232.121	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
112.204.201.238	Philippines	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
218.84.232.121	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
112.204.201.238	Philippines	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-25-2016-02:04:00 to 01-25-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-25-2016-02:04:00 to 01-25-2016-03:04:00

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	3
37.143.82.50	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
193.105.134.220	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
188.166.245.249	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.83.135.131	147.237.72.166	Georgia	aka.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.72.14	Georgia	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
50.23.96.210	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -f -sS	1
188.166.245.249	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
80.83.135.131	147.237.72.217	Georgia	e.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.72.156	Georgia	aman.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1

01-25-2016-02:04:00 to 01-25-2016-03:04:00

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	30
107.167.96.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.86.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.102.9.71	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.71	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.99.47.79		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.34.250.239	Egypt	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
147.235.8.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
41.34.250.239	Egypt	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
83.244.50.117	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
147.235.8.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
41.34.250.239	Egypt	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
174.37.79.58	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
41.34.250.239	Egypt	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
147.235.8.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
147.235.8.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.120	United States	147.237.0.33	idf.il	drop		drop	1
37.26.148.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.166.100.163	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.99.47.79		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
204.93.154.199	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.148.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.121	United States	147.237.0.33	idf.il	drop		drop	1
185.99.47.79		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.46.38.78	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.177.150.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
208.43.206.15	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.148.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.121	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.95.88.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.99.47.79		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
147.235.8.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.113	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.246.136.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.18.206.194	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.148.243	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.122	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
147.235.8.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.208.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.75.160.133	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
150.70.173.55	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.210.20.27	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.65.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1085-he/nakhal.aspx	Block	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
212.76.110.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.113.151.67	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 69.113.151.67	Block	1
65.132.59.34	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.12	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
84.109.165.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
130.193.51.51	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.113.151.67	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
65.132.59.34	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/320-en/patzar.aspx	Block	1
185.68.109.226	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
98.130.0.140	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
141.212.122.112	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	1
72.184.141.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/62953.jpg	Block	1
195.154.226.90	France	147.237.77.233	atal.idf.il	Illegal HTTP Version HTTP/	Block	1
2.54.168.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
64.46.23.242	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspxfa	Block	1
150.70.173.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.145.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1776	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
5.29.202.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1