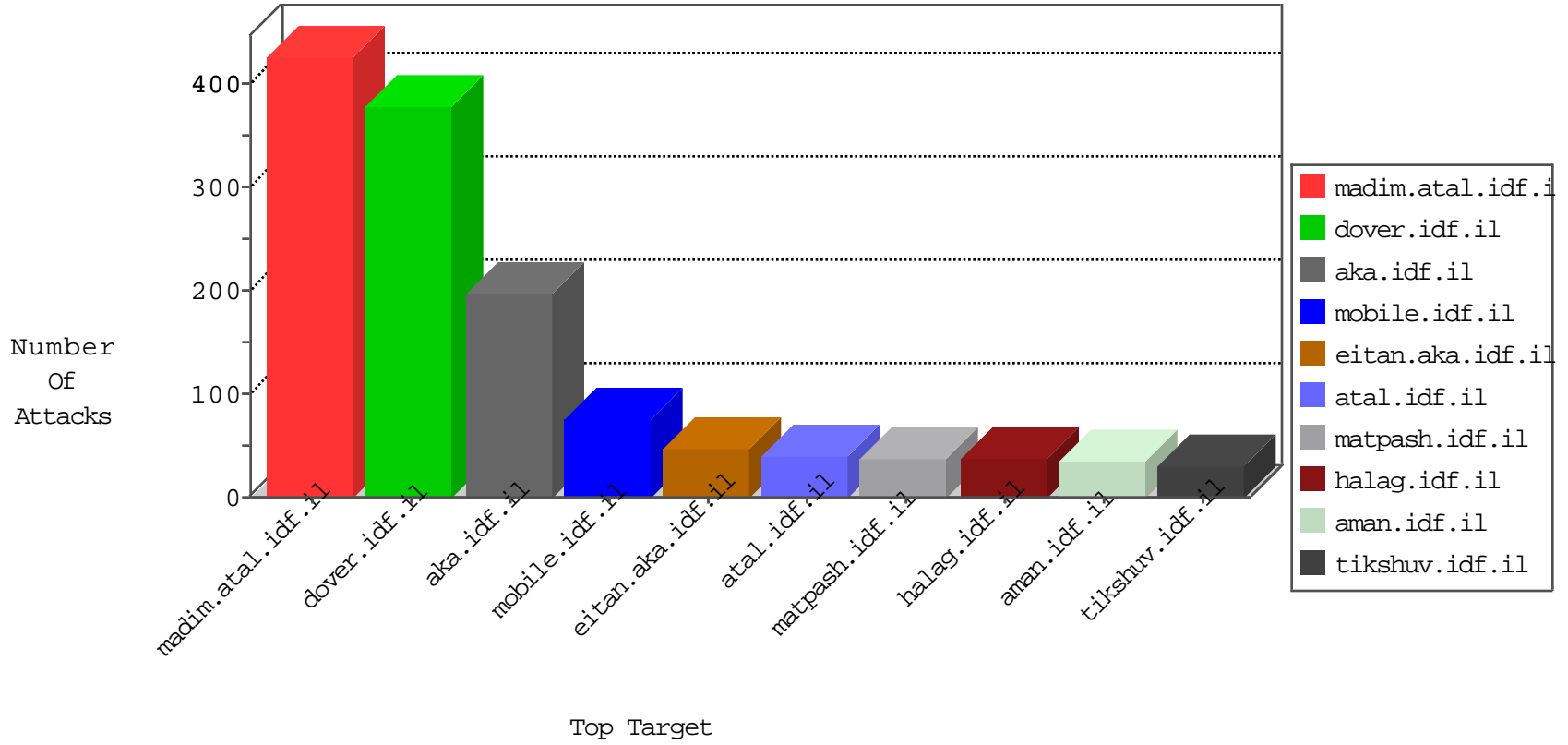


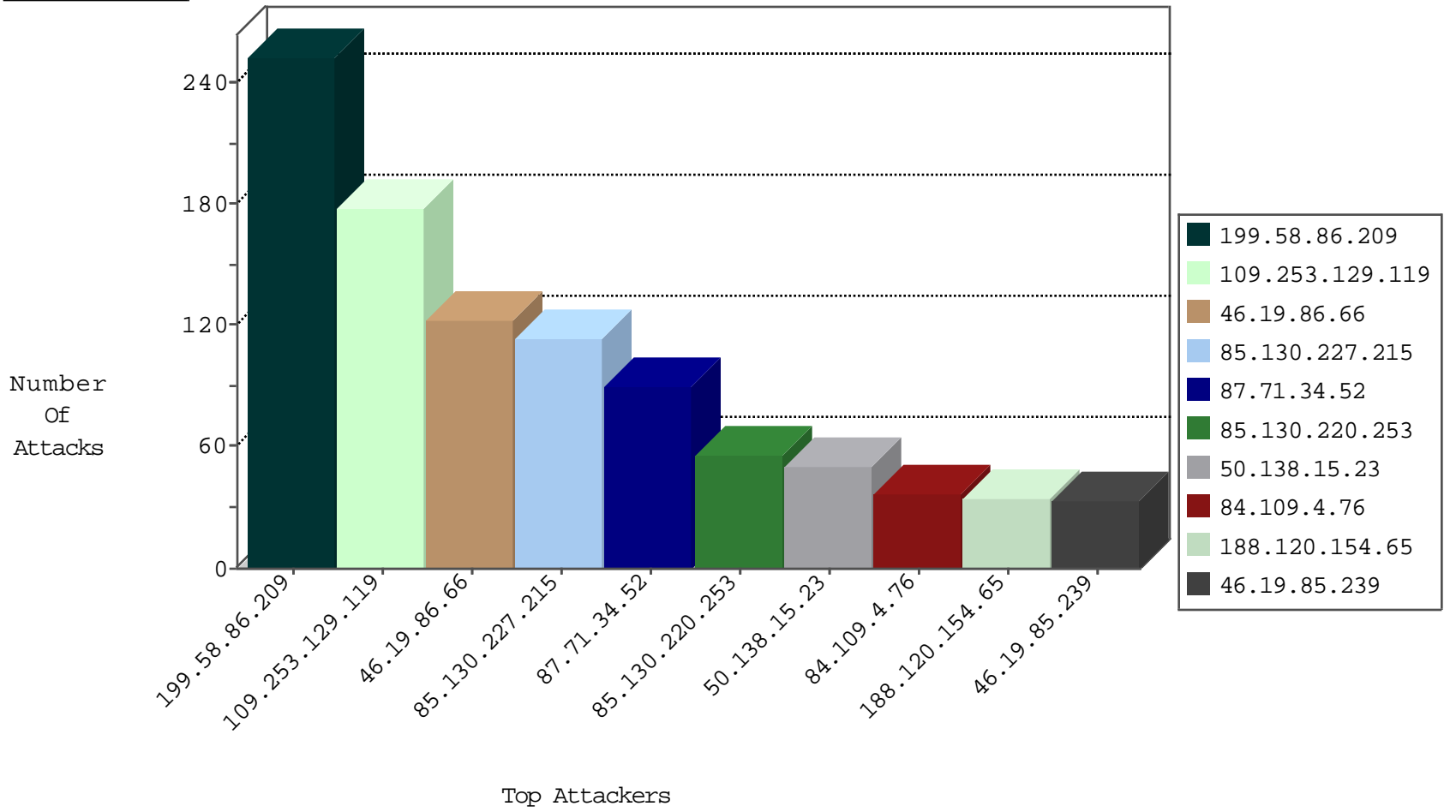
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	238
199.58.86.209	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.209	United States	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
128.232.110.28	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.218	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
219.146.251.139	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
219.146.251.139	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
219.146.251.139	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
128.232.110.28	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.176	Ukraine	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
72.27.202.48	147.237.77.216	Jamaica	dover.idf.il	ET SCAN NMAP -sS window 3072	1
219.146.251.139	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.74	Indonesia	law.idf.il	ET SCAN NMAP -sS window 4096	1
219.146.251.139	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
219.146.251.139	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
182.253.45.17	147.237.8.50	Indonesia	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
84.200.84.187	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.109.4.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
85.130.227.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
85.130.227.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	31
223.24.41.53	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
85.130.227.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
50.138.15.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
50.138.15.23	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
85.130.220.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
85.130.220.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
85.130.220.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.53.186.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.254.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.178.254.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.178.254.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
79.181.186.196	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
85.130.227.215	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.227.215	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
132.64.30.183	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.11.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.6.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.227.215	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.168.126.9	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.126.9	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
94.226.186.213	Belgium	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
79.177.37.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.138.253.3	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.138.120.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.120.4.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.229.46	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
46.116.196.238	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.30.94	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.181.186.196	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.16.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.147.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
176.13.235.233	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.147.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
185.3.147.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	177
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
87.71.34.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
42.123.65.19	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 42.123.65.19	Block	17
42.123.65.19	China	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	6
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.249.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.6.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.6.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
5.29.51.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	3
176.13.12.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.92.155	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
85.65.235.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.27.105.92	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
80.246.137.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.109.56.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3141.jpg	Block	1
157.55.39.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
77.138.106.149	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/kiosk/printablekiosk.aspx	Block	1
180.76.15.135	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.75.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/www.israelbar.org.il	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
42.123.65.19	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
176.13.11.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
89.138.230.199	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
42.123.65.19	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to ww.eitan.aka.idf.il/index.asp	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1391-12626-en/dover.aspx	Block	1
77.138.33.114	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1