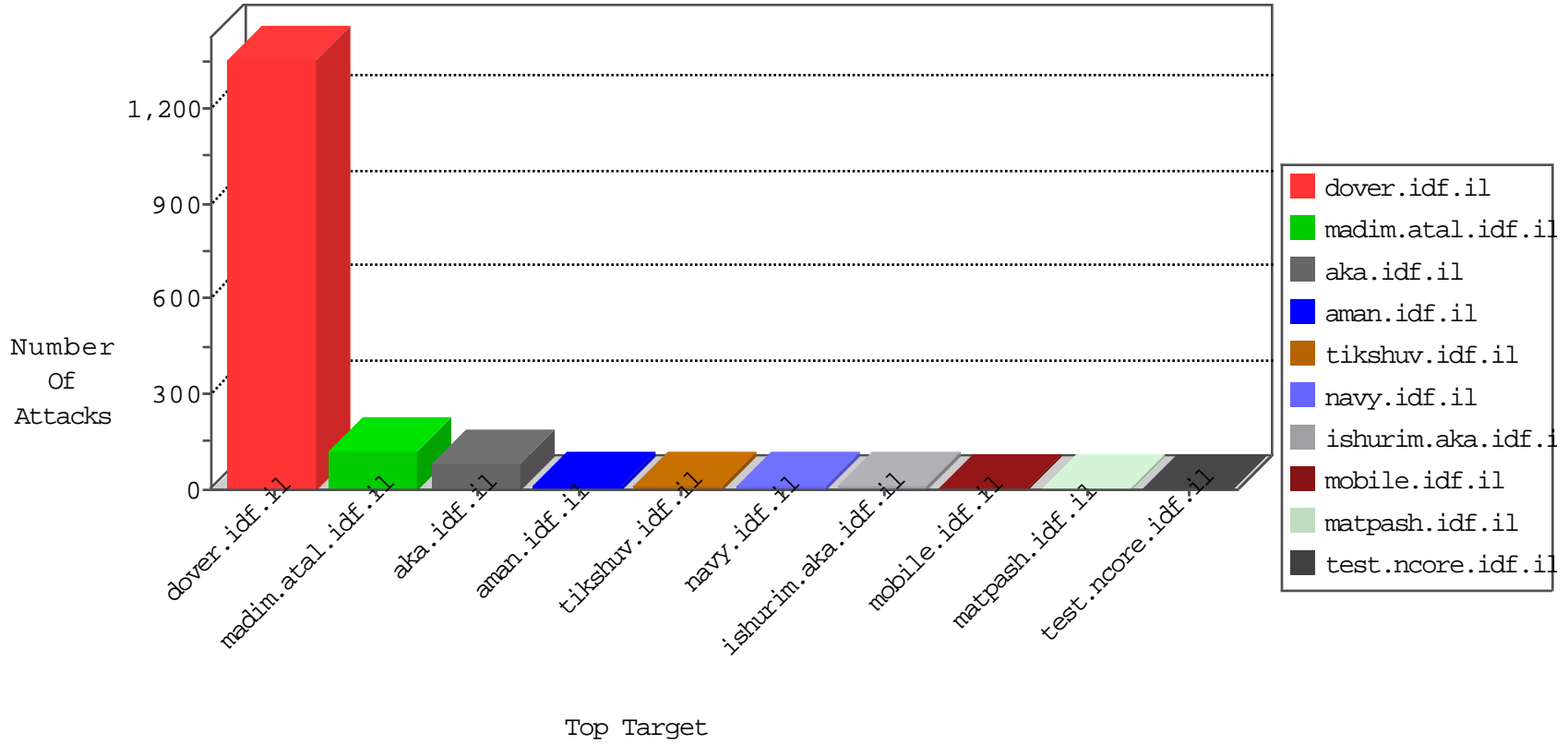




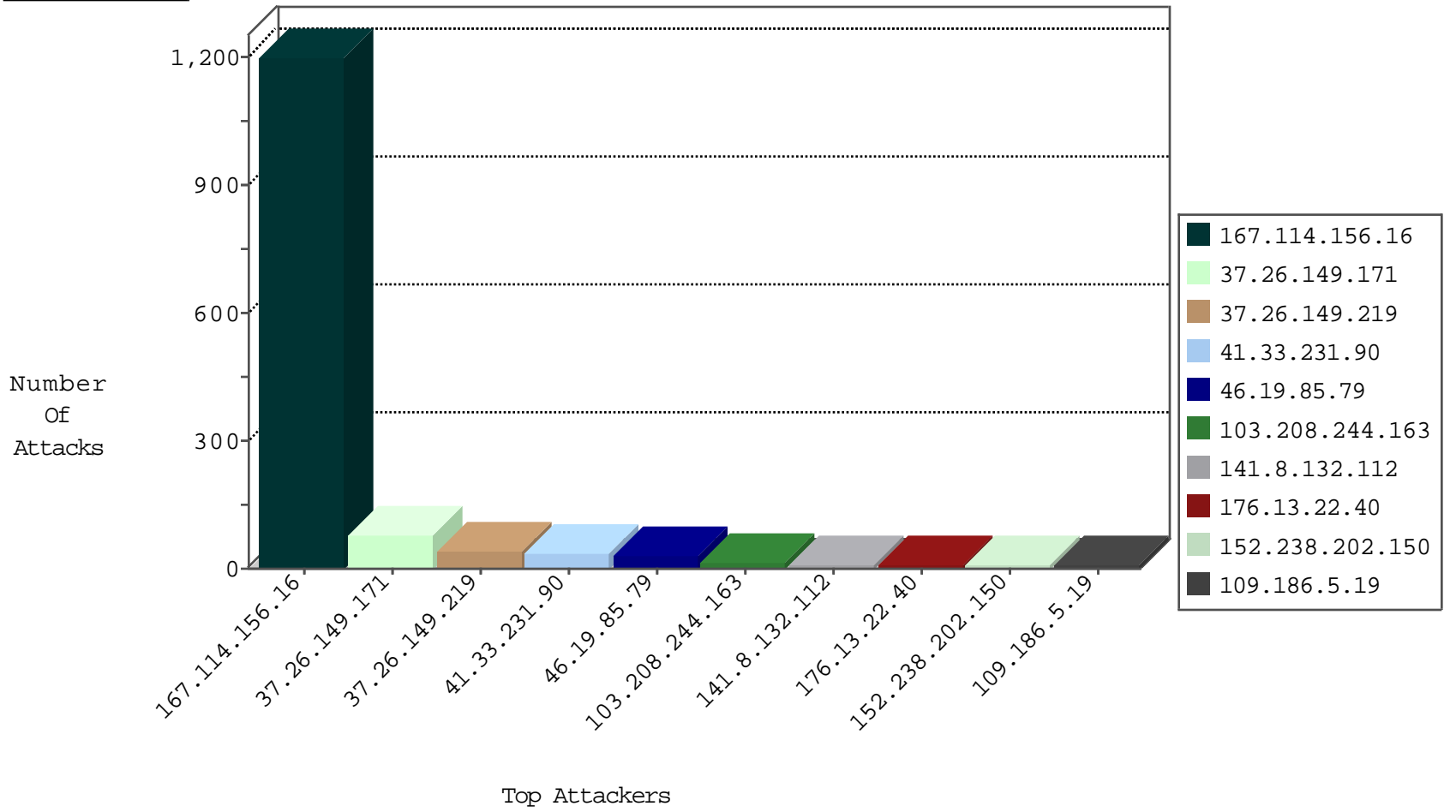
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Tp_Web_In	drop	1203
109.67.38.238	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
89.248.172.201	Netherlands	147.237.8.46	e.chiruch.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.201	Netherlands	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.105.155	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
40.77.167.85	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
103.208.244.163		147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

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	4
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
107.158.255.194	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.163	147.237.77.216		dover.idf.il	SERVER-WEBAPP admin.php access	1
78.109.24.107	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.171	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
125.212.232.165	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.34	Canada	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
42.113.132.39	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.22.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
152.238.202.150	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.179.185.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.148.144	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.186.5.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
73.171.202.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	4
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
79.182.51.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.244.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.165.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.119.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.13.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.218.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.61.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.186.5.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.25.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	2
2.53.187.23	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.76.98.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.29	United Kingdom	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.40	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.177.21.26	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
83.110.149.22	United Arab Emirates	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
188.36.120.189	Hungary	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.21.26	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.146.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
87.69.62.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.177.142.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.137	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.18.93	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
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
103.208.244.163		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.208.244.163	Block	5
103.208.244.163		147.237.77.216	dover.idf.il	PHP Attempt	Block	4
103.208.244.163		147.237.77.216	dover.idf.il	Multiple Admin Blocking from 103.208.244.163	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.79	Block	1
199.47.81.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1413-10820-	Block	1
103.208.244.163		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1133-he/dover.aspx parameter PageNum	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
93.172.150.76	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.79	Block	1
109.64.51.241	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1
197.41.120.111	Egypt	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method aa.1452424986.4.1460671361.1460671114.; in URL _pk_ses.20.8afc=*	Block	1
131.253.25.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.79	Block	1
197.41.120.111	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
52.91.239.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
37.146.191.124	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
85.65.116.235	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.79	Block	1
198.58.103.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1