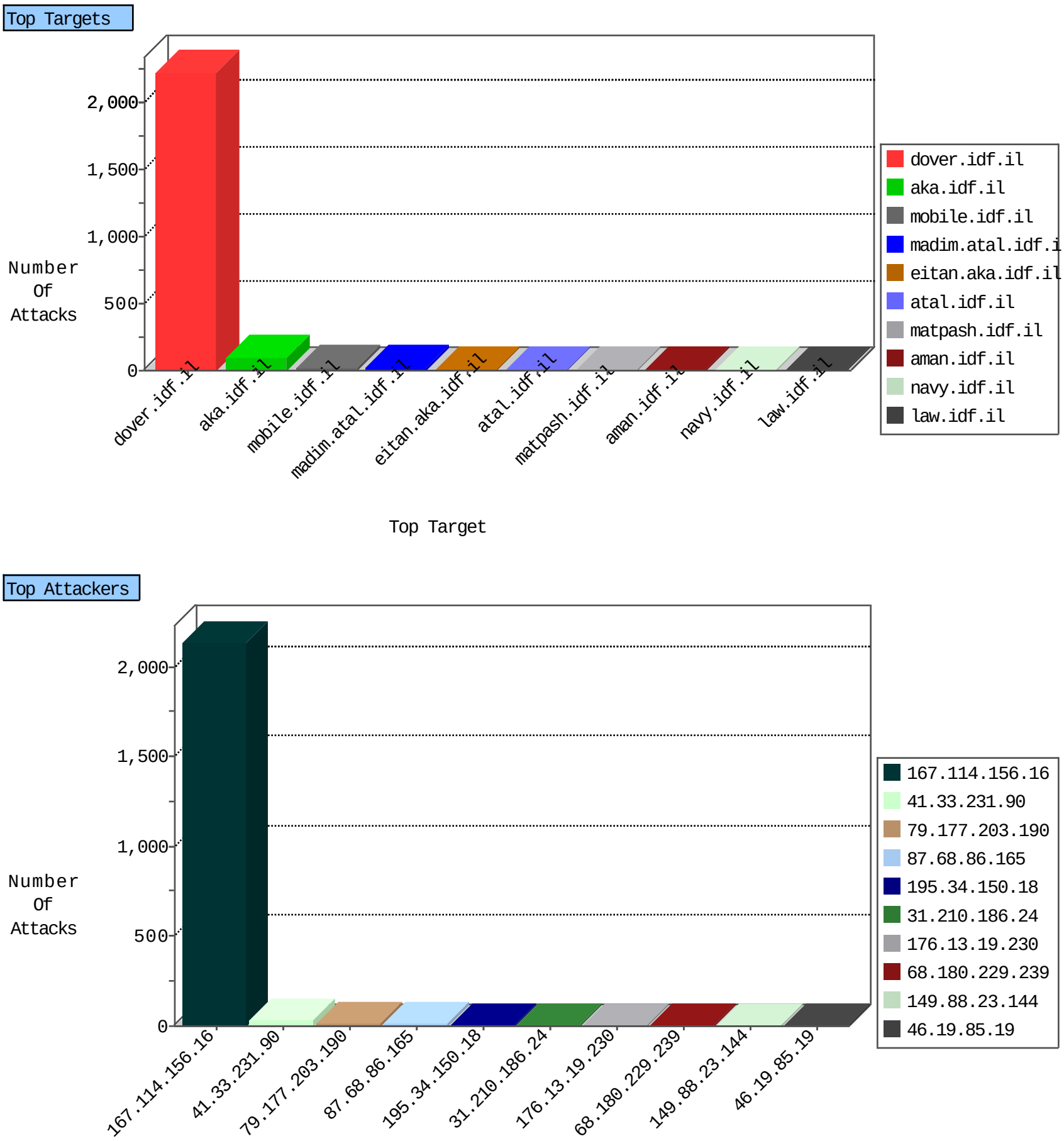
01-22-2016-07:04:09 to 01-22-2016-08:04:09

IDF Under Attack Daily Report



01-22-2016-07:04:09 to 01-22-2016-08:04:09

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	3068
200.35.95.235	Venezuela	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
201.211.226.101	Venezuela	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

01-22-2016-07:04:09 to 01-22-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
172.245.218.130	United States	147.237.77.233	atal.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-22-2016-07:04:09 to 01-22-2016-08:04:09

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
66.249.93.99	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
213.204.101.24	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
184.173.48.221	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
159.8.109.19	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1

01-22-2016-07:04:09 to 01-22-2016-08:04:09

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
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.85.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.184.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
149.88.23.144	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
23.113.204.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
206.253.226.7	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.36.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.205.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.67.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.176.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.9.122.203	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.86.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.241.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
40.77.167.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.233.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.86.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
204.79.180.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.179.3.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
190.120.108.226	Argentina	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
213.204.101.24	Lebanon	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
190.120.108.226	Argentina	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.183.27.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.93.239	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
87.68.86.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
79.179.3.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
66.240.236.119	United States	147.237.0.33	idf.il	drop		drop	1
190.120.108.226	Argentina	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.94.67.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.236	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.186.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.56	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.186.129.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.157.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
87.68.86.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.32.179.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
40.77.167.69	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
180.76.15.31	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.178.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.210.186.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
103.248.80.3	India	147.237.77.74	law.idf.il	PHP Attempt	Block	2
103.248.80.3	India	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
109.253.128.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.140.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.216.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
107.77.94.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/dover/site/mainpage.asp	Block	1
66.249.78.184	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
5.29.109.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
61.183.148.136	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
176.13.15.1	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	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
5.29.117.24	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.29.117.24 (sigalgs DoS Attack)	None	1
204.79.180.225	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
66.249.65.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
176.13.19.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.126.63.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.78.169.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /login	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.176	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/109335.pdf×³Â¦×³×Ÿ Â¿Â½×³Â?-×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â¦×³×ŸÂ¿Â½×³×ŸÂ¿Â½	Block	1
104.128.144.131	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
198.137.20.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1