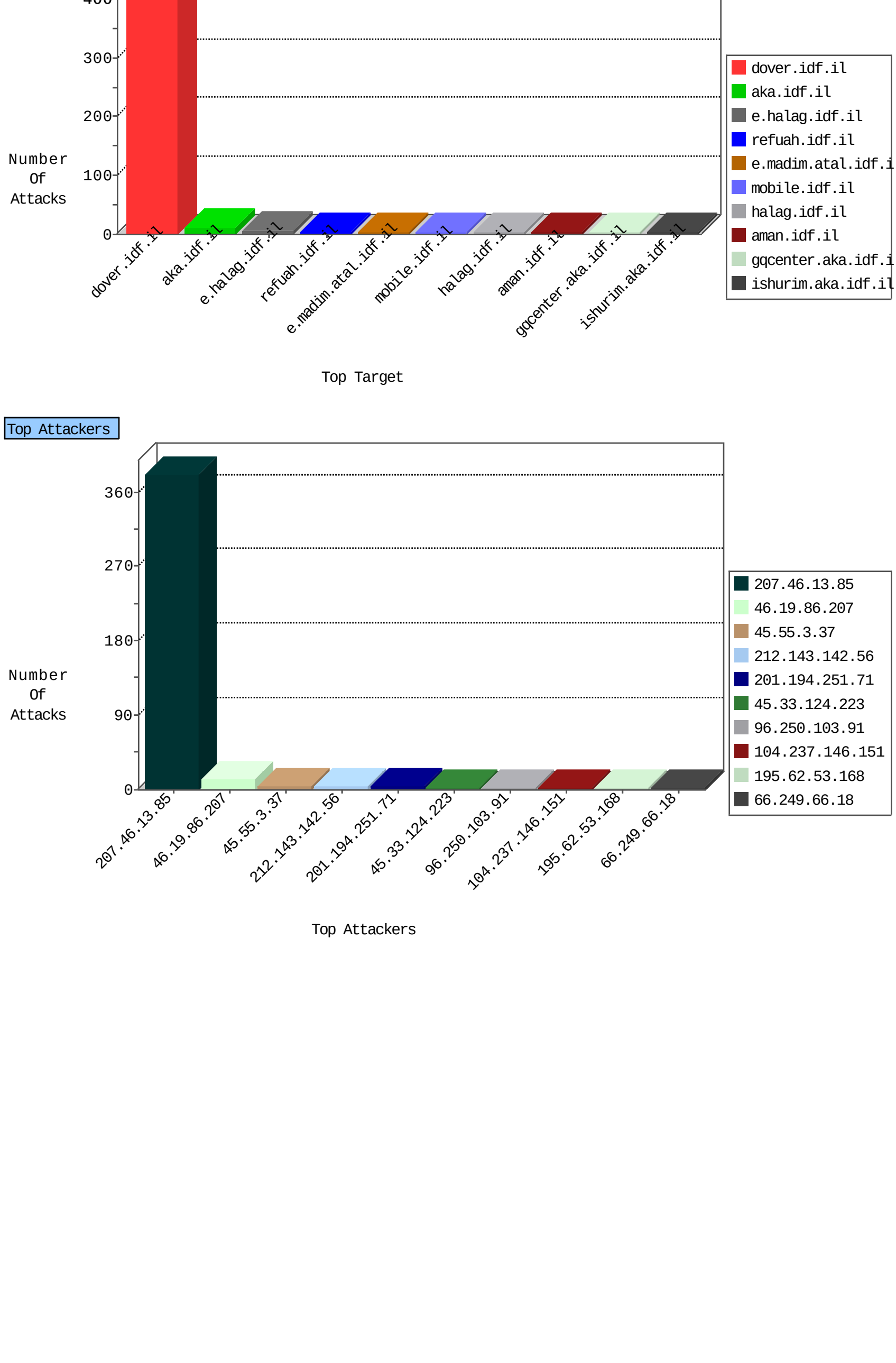
10-05-2016-05:04:08 to 10-05-2016-06:04:08

IDF Under Attack Daily Report



10-05-2016-05:04:08 to 10-05-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
93.174.94.235	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

10-05-2016-05:04:08 to 10-05-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-05-2016-05:04:08 to 10-05-2016-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
58.220.2.5	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
50.254.111.193	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.229.223.8	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.3.37	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1
45.55.3.37	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
45.55.3.37	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
163.172.11.244	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.210.243.100	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
49.50.79.18	147.237.77.178	India	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
46.172.91.20	147.237.72.166	Ukraine	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.55.3.37	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.3.37	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
183.7.112.77	147.237.76.202	China	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.152.59.11	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.210.243.100	147.237.0.35	France	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

10-05-2016-05:04:08 to 10-05-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	382
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
201.194.251.71	Costa Rica	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
183.129.160.229	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
45.33.124.223	United States	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.88	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
139.162.160.132	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.243	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.92.20.154	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
177.23.177.146	Brazil	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
139.162.246.121	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
104.237.146.151	United States	147.237.76.196	e.sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
198.58.110.199	United States	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
45.33.124.223	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.79	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.89	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
139.162.160.132	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.72	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.61	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.252	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
23.239.31.132	United States	147.237.0.35	akaws.idf.il	drop		drop	1
178.79.141.130	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.43	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.103	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.95	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.168.200	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
96.250.103.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.0.86.147	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.239.31.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
178.79.141.130	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.44	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
201.194.251.71	Costa Rica	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.115	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
174.106.51.1	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
139.162.168.200	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.110	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.58.110.199	United States	147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
104.237.146.151	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
45.33.124.223	United States	147.237.0.33	idf.il	drop		drop	1
178.79.141.130	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.80	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-05-2016-05:04:08 to 10-05-2016-06:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
137.226.113.7	Germany	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
184.105.247.243	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-05-2016-05:04:08 to 10-05-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.250.103.91	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
40.77.167.52	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
201.194.251.71	Costa Rica	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.19	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/mobile/	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza>специальном сайте, с озданном для этих целей .</p> #012#012#012#012#012 #012#012<table cellspacing=	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9694-he/refuah.aspx	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/שקופית 12	Block	1
183.129.160.229	China	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8898-he/refuah.aspx	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/שקופית 13	Block	1
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/general/default.asp	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1

10-05-2016-05:04:08 to 10-05-2016-06:04:08