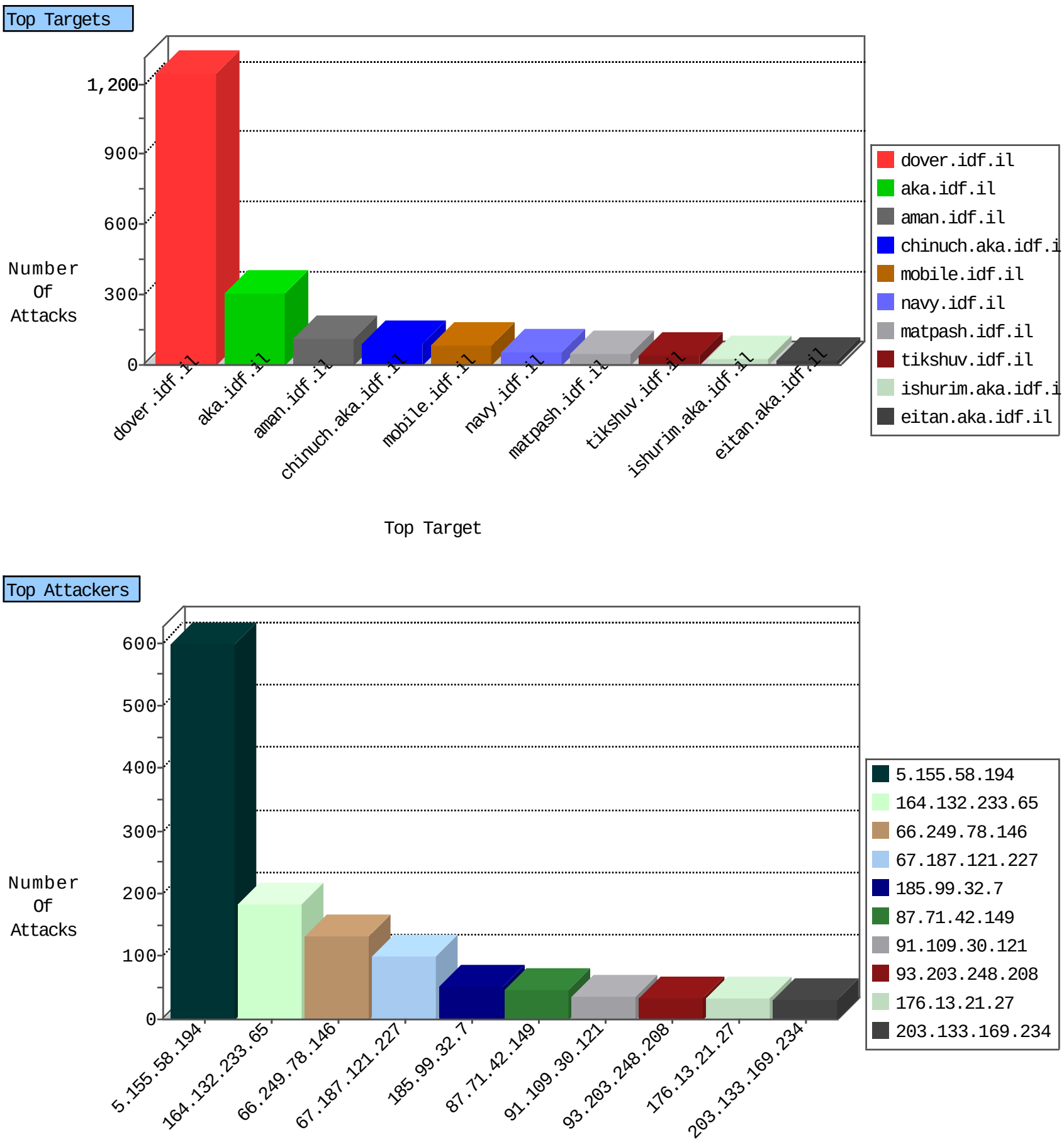
04-28-2016-14:04:02 to 04-28-2016-15:04:02

IDF Under Attack Daily Report



04-28-2016-14:04:02 to 04-28-2016-15:04:02

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	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
104.255.70.247	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
104.255.70.247	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-28-2016-14:04:02 to 04-28-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-14:04:02 to 04-28-2016-15:04:02

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
161.202.120.146	147.237.77.234	Japan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.34.99	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
190.153.238.58	147.237.0.19	Chile	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-14:04:02 to 04-28-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.155.58.194	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	426
5.155.58.194	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop		drop	153
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
67.187.121.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
164.132.233.65	Italy	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	92
164.132.233.65	Italy	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	92
185.99.32.7	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
91.109.30.121	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	35
93.203.248.208	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.13.21.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
87.71.42.149	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	32
203.133.169.234	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
104.46.236.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
188.120.153.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.195.121.145	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
37.46.38.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.53.28.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.229.29.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.156.88.184	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.22.131.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.120.154.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
41.42.25.28	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.195.121.145	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.155.58.194	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
5.155.58.194	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.120.148.194	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.137.200.61	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.238.152.14	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.238.152.14	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
108.171.129.162	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.71.42.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.160.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.71.42.149	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.144.9	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.235.98	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 62.90.235.98	Block	3
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.122.157	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
37.46.38.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.184	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.13.19.184	Block	2
149.78.197.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
176.13.21.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1306-he/atal.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8942-he/refuah.aspx	Block	1
192.115.103.128	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
40.77.167.36	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.88.38.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
85.65.186.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
62.90.235.98	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
31.129.174.36	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily'a=0	Block	1
178.210.133.131	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
82.137.200.61	Syrian Arab Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/dover.aspx„'¦' :•'½„¿„¯„'½„¿„¯„'½„¿„¯	Block	1
2.53.45.6	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
85.250.104.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
178.210.133.131	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
109.67.51.106	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.111.122.157	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.111.122.157	Block	1
46.121.208.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
167.114.36.152	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
2.53.134.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
91.210.164.117	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
178.210.133.131	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
109.67.178.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
84.111.122.157	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
5.155.58.194	Syrian Arab Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
104.46.236.214	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
37.128.186.113	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
188.120.154.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default	Block	1

04-28-2016-14:04:02 to 04-28-2016-15:04:02