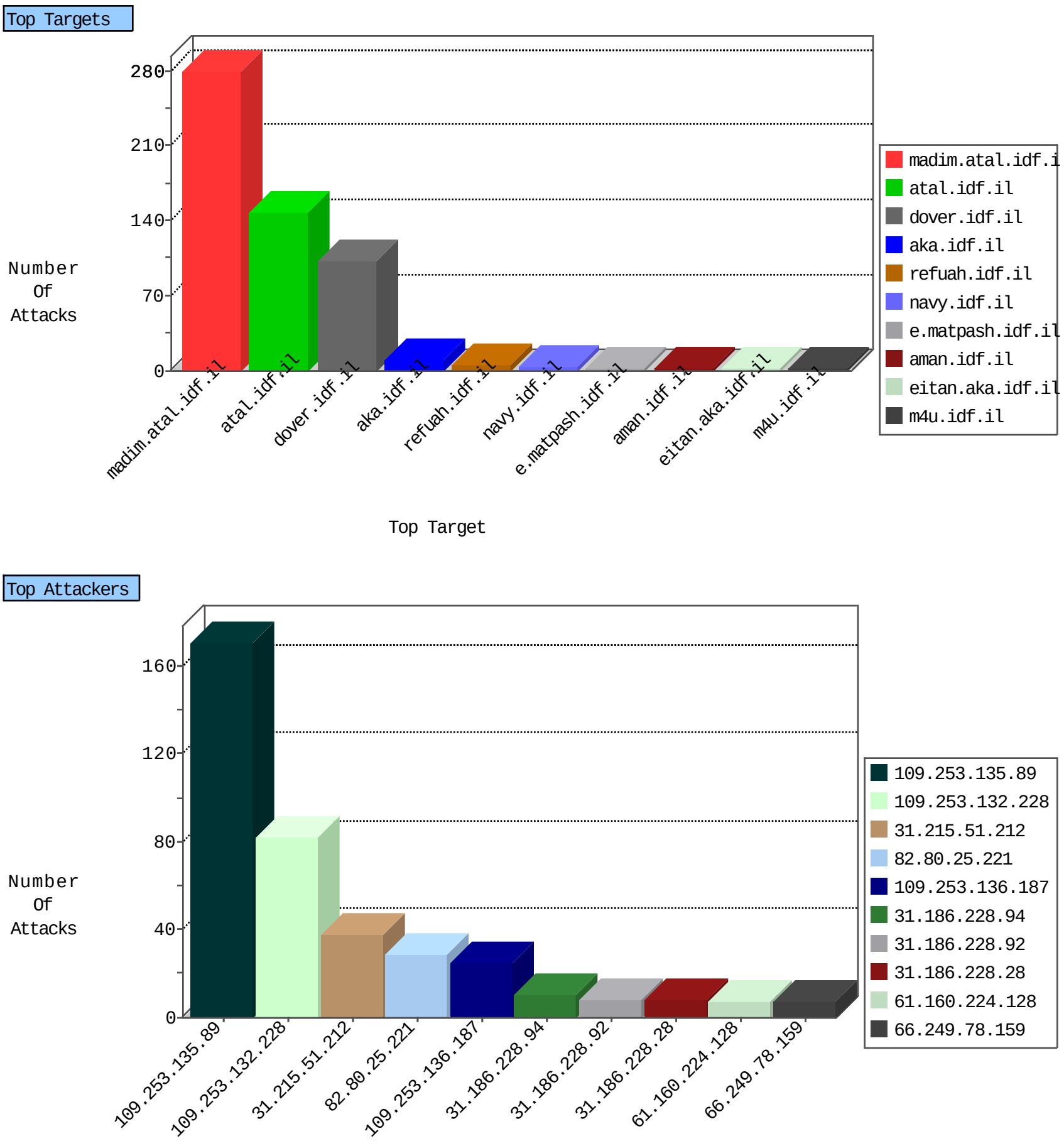
03-29-2015-05:03:07 to 03-29-2015-06:03:07

IDF Under Attack
03-29-2015-05:03:07



03-29-2015-05:03:07 to 03-29-2015-06:03:07

Top Attackers In DDoS-Defence

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

03-29-2015-05:03:07 to 03-29-2015-06:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
37.130.227.133	United Kingdom	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-29-2015-05:03:07 to 03-29-2015-06:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
222.69.94.13	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -f -sS	1
115.231.218.147	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

03-29-2015-05:03:07 to 03-29-2015-06:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.215.51.212	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.132.228	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
31.186.228.94	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.28	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.92	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.27	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.62	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.89	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.63	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
109.253.135.89	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.64	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.23	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.26	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.57	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.88	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.29	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.67	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.30	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.59	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.90	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.31	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.60	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.32	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.87	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.61	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.66	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.93	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.68	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.95	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.86	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.24	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.58	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.25	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.91	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.65	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.96	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.170	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	2
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
188.138.1.218	Germany	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
216.218.206.122	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.0.33	idf.il		drop	drop	1
46.19.86.119	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
129.121.177.94	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
188.138.17.205	France	147.237.76.34	yohalan.idf.il		drop	drop	1
141.212.122.50	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
85.130.248.104	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.56	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

03-29-2015-05:03:07 to 03-29-2015-06:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.135.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
109.253.132.228	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.132.228	Block	71
109.253.136.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
109.65.185.65	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.65.185.65	Block	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	3
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	2
109.253.138.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
109.253.146.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.113.183	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.138.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
188.143.232.19	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
109.65.185.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	1
176.12.138.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/december/4.stm	Block	1
109.253.132.228	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/february/0218-2.stm	Block	1
66.249.75.113	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
180.76.4.147	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
109.253.142.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
41.189.161.61	Ghana	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.189.161.61	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
217.69.133.229	Russian Federation	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1
66.249.78.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim1/news/news.asp	Block	1
180.76.6.150	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/	Block	1
109.253.143.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.23.45.196	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
41.189.161.61	Ghana	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/1217-6.stm	Block	1
157.55.39.159	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
188.143.232.19	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	1

03-29-2015-05:03:07 to 03-29-2015-06:03:07