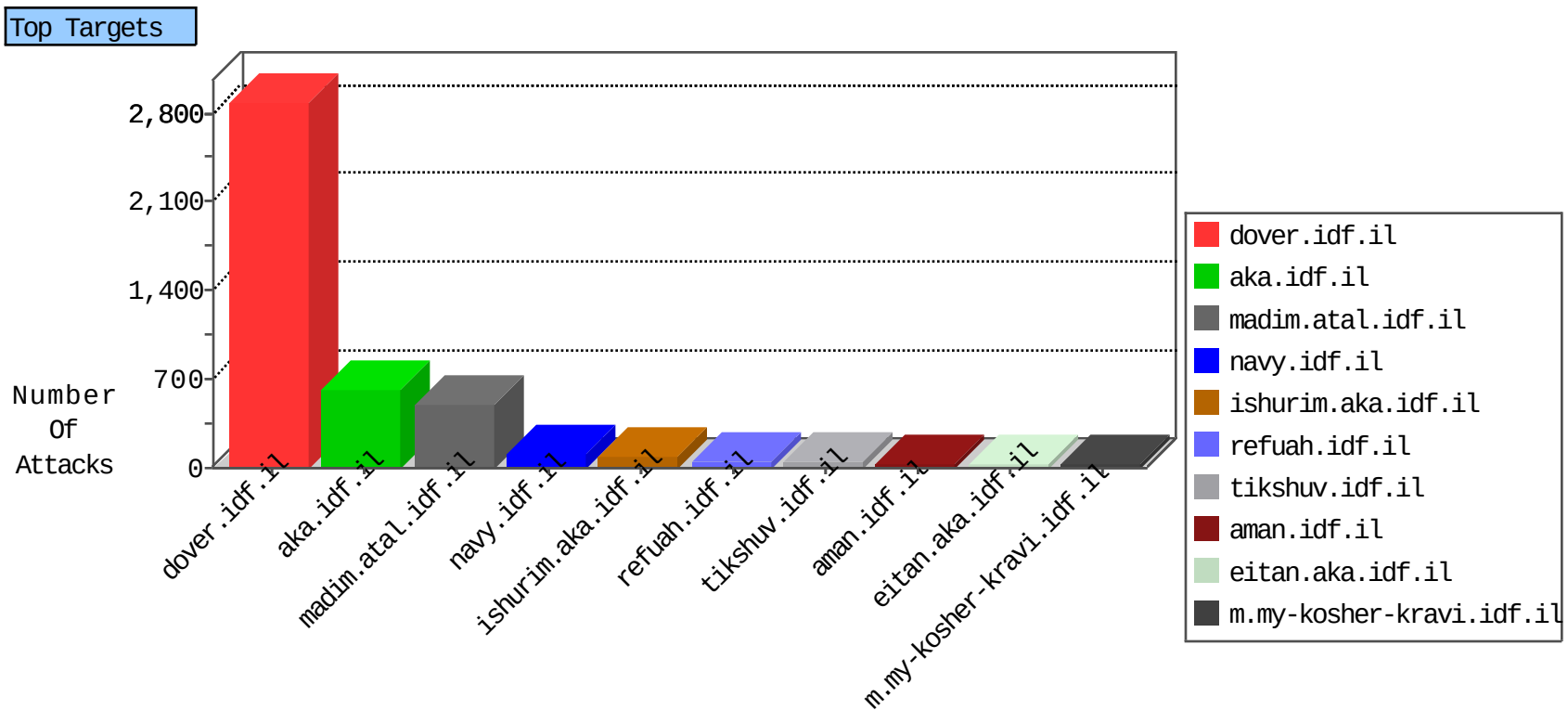
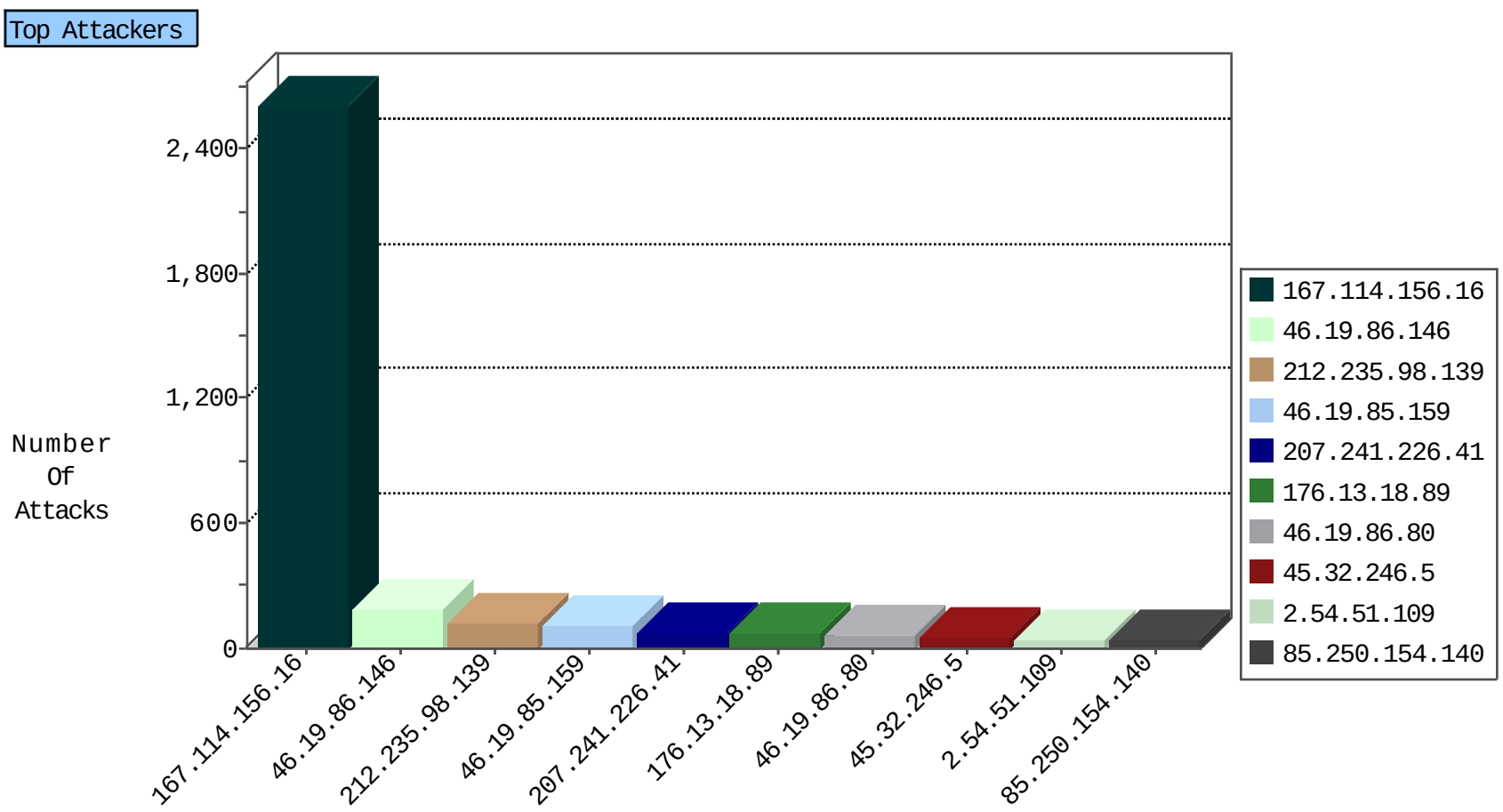
12-08-2015-14:04:01 to 12-08-2015-15:04:01

IDF Under Attack
Daily Report



Top Target



Top Attackers

12-08-2015-14:04:01 to 12-08-2015-15:04:01

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	3331
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
45.32.246.5		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	12
93.174.93.138	Netherlands	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
71.6.216.41	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
210.77.180.10	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-08-2015-14:04:01 to 12-08-2015-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-08-2015-14:04:01 to 12-08-2015-15:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

12-08-2015-14:04:01 to 12-08-2015-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	107
46.19.86.210	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
85.250.154.140	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
2.54.52.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.51.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.86.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
177.235.143.150	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
85.250.154.140	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.19.85.10	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
62.90.236.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.206.132	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
45.32.246.5		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
91.186.252.94	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.8	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
45.32.246.5		147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
40.77.167.65	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.52.25.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.52.33	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	9
2.54.10.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
89.138.76.38	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.241.226.39	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
212.150.161.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.91	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
94.230.86.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.28.146.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.51.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
45.32.246.5		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
45.32.246.5		147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
5.28.146.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.51.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.201	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.13.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.120.148.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.100.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.151.52	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	6
149.88.13.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.18.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.60.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.34.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.251.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.31.58.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.175.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.244.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.228.100.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.250.56.199	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.91.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

12-08-2015-14:04:01 to 12-08-2015-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
176.13.18.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
207.241.226.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	68
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
2.54.177.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
176.13.20.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	9
2.54.54.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
212.150.161.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
31.168.213.225	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
79.177.57.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.18.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
207.241.226.41	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	3
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.186.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.28.151.52	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
176.12.147.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.179.83.94	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.116.170.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.17.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.89.33	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$ in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
213.57.163.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.169.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.102	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/css/base/css/fetchcss	Block	1
37.26.147.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.124.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.154.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il./style/shared/reset.css	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3241.jpg	Block	1
176.13.23.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.146	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.149	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/css/base/css/fetchcss	Block	1
84.111.25.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.136.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
186.202.87.94	Brazil	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
93.173.255.35	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/110581.pdf	Block	1
46.116.251.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.120.92	Israel	147.237.77.233	atal.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 85.65.120.92	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
222.163.195.4	China	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
109.67.153.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
105.200.22.41	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

12-08-2015-14:04:01 to 12-08-2015-15:04:01