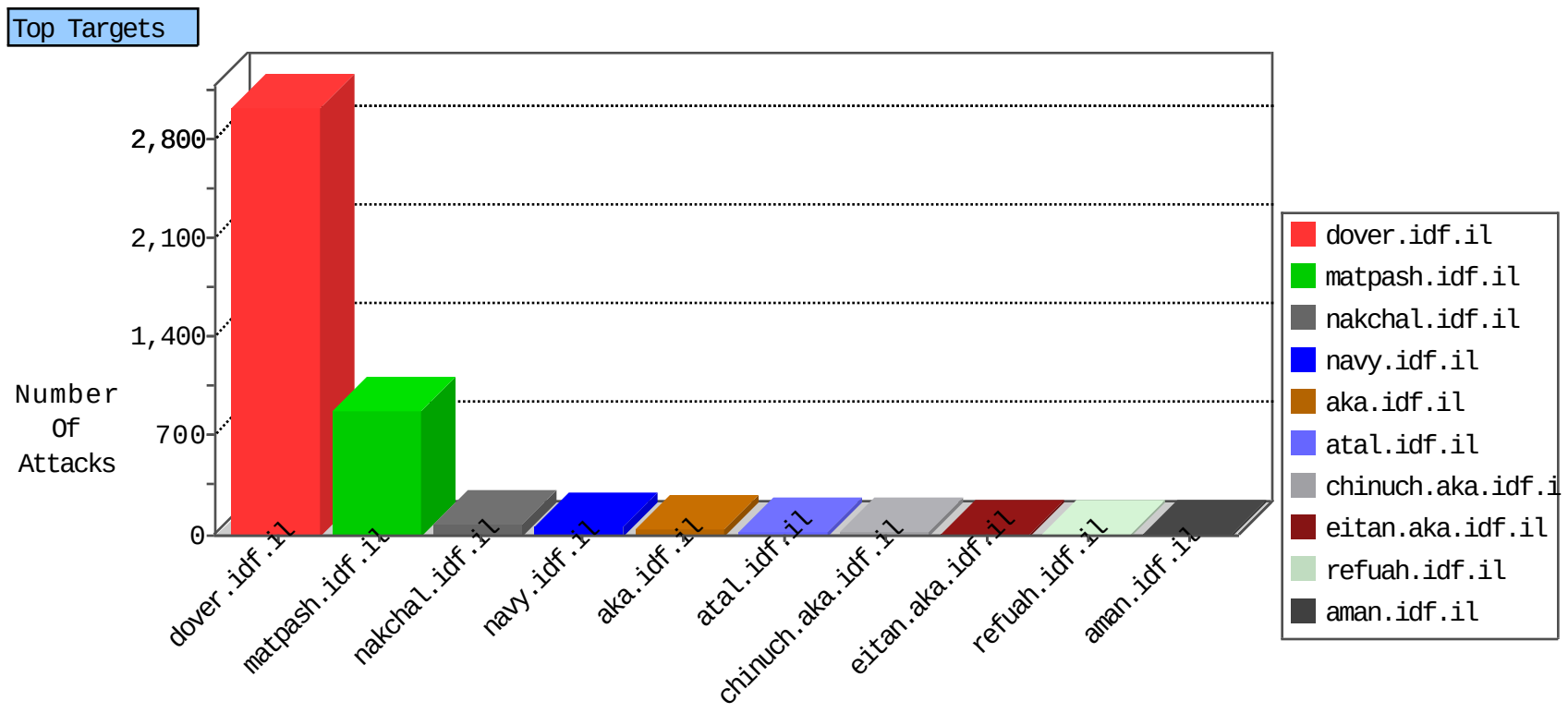
10-25-2015-03:04:04 to 10-25-2015-04:04:04

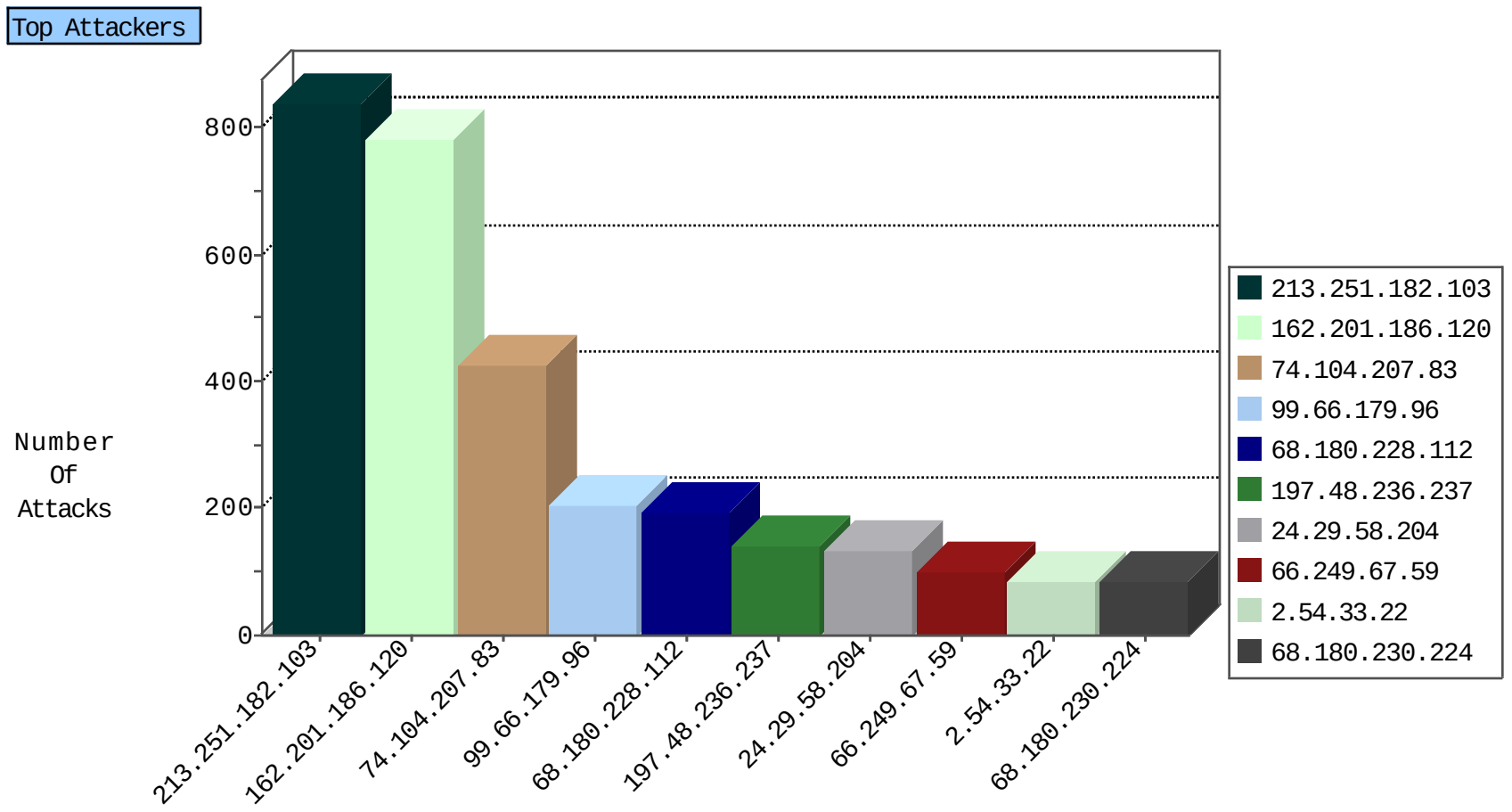
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-25-2015-03:04:04 to 10-25-2015-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.91.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
115.231.222.40	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.231.222.40	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
58.177.117.113	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
115.197.104.21	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
119.236.193.213	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
24.57.113.65	Canada	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
115.205.229.114	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1

10-25-2015-03:04:04 to 10-25-2015-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-03:04:04 to 10-25-2015-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.162.116.221	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.8	147.237.8.27	Ukraine	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
210.50.197.147	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 4096	1
37.143.82.50	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
210.50.197.147	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -f -sS	1
37.143.82.50	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -f -sS	1
193.107.17.72	147.237.76.86	Seychelles	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
190.124.35.115	147.237.76.38	Nicaragua	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
188.68.224.151	147.237.77.243	Poland	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
185.100.84.253	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
78.181.207.63	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.162.116.221	147.237.76.38	Sweden	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.147	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 2048	1
37.143.82.50	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
193.107.17.72	147.237.76.86	Seychelles	navy.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.76.38	Nicaragua	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
190.124.35.115	147.237.8.24	Nicaragua	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
188.68.224.151	147.237.8.14	Poland	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.76.148		gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1

10-25-2015-03:04:04 to 10-25-2015-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.201.186.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	781
74.104.207.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	427
99.66.179.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	204
197.48.236.237	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
24.29.58.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
2.54.33.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
131.253.25.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
174.61.103.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
71.191.165.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	27
179.105.188.94	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
73.1.106.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
74.56.229.13	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
85.250.52.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.241.226.144	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	15
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
134.191.232.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
108.59.253.71	United States	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
70.208.75.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.155.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
134.191.232.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.33	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
222.153.95.196	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.18.21.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.26.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.204.34.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.67.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-25-2015-03:04:04 to 10-25-2015-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	840
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	84
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	56
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	53
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	28
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
188.143.232.43	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
91.200.12.53	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18893-he/dover.aspx	Block	14
45.35.71.179		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20594-he/dover.aspx	Block	14
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
40.77.167.43	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
157.55.39.255	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	14
71.13.39.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	14
41.189.32.61	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	14
188.143.232.35	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
41.189.32.61	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	12

10-25-2015-03:04:04 to 10-25-2015-04:04:04