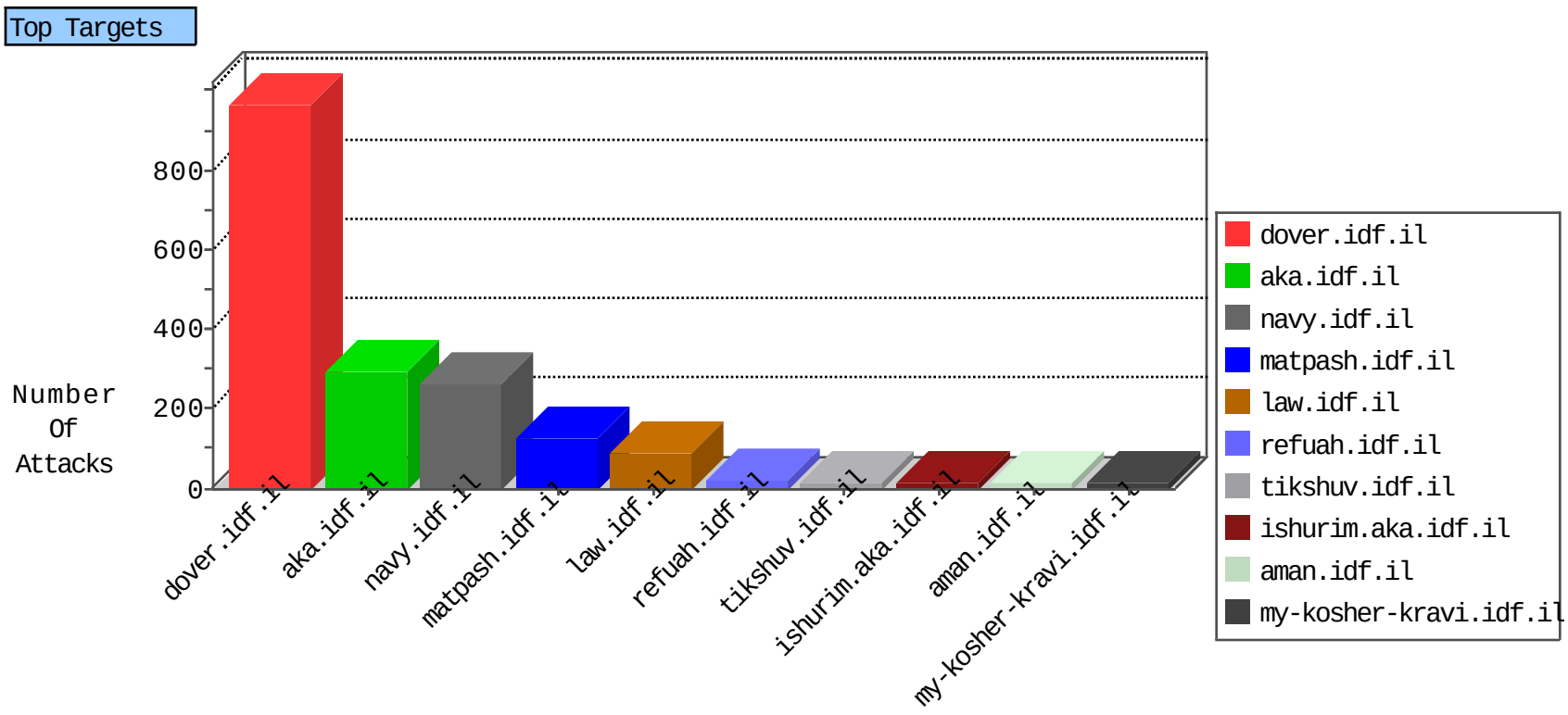
10-30-2015-04:04:00 to 10-30-2015-05:04:00

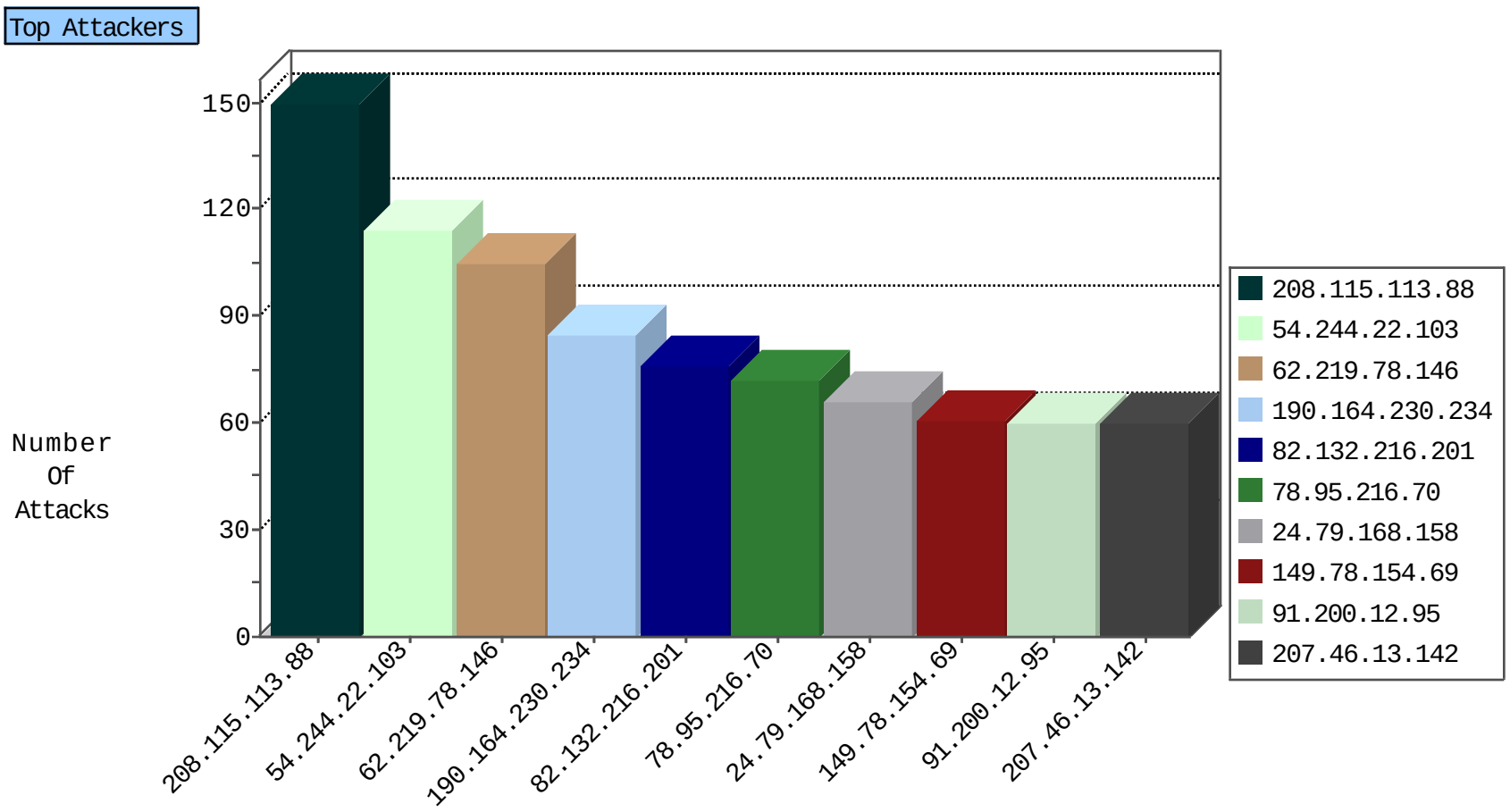
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-30-2015-04:04:00 to 10-30-2015-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	843
66.249.75.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	32
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
188.120.134.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	3
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	3
54.187.55.213	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
69.64.32.110	United States	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
117.172.26.162	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
120.37.169.19	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

10-30-2015-04:04:00 to 10-30-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.60.127.93	Spain	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-30-2015-04:04:00 to 10-30-2015-05:04:00

Top Attackers In IDS

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

10-30-2015-04:04:00 to 10-30-2015-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
82.132.216.201	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
78.95.216.70	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
24.79.168.158	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
79.182.188.240	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
74.14.50.145	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
188.247.78.100	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
78.95.237.238	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.180.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.184.77.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
118.173.112.185	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
190.164.230.234	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.12.145.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
96.23.211.159	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.149	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
79.181.147.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.125.104.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
128.232.110.28	United Kingdom	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
24.182.106.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
202.106.38.21	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.232.110.28	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
204.237.0.104	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.159.194.182	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.113.117.206	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.123	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
108.44.233.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.20.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.75.38	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	135
190.164.230.234	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/social/undefined	Block	60
207.46.13.142	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.142	Block	45
62.219.78.146	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	45
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.139	Block	30
91.200.12.95	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	30
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	30
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	30
5.29.195.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	30
62.219.78.146	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	30
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
178.49.154.143	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	15
41.130.1.232	Egypt	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 41.130.1.232 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	15
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	15
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.132	Block	15
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	15
91.200.12.95	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.95	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	15
190.164.230.234	Chile	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 190.164.230.234	Block	15
62.219.78.146	Israel	147.237.77.176	matpash.idf.il	Admin Blocking	Block	15
109.66.144.49	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
157.55.39.22	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/haredim/gallery.aspx	None	15
66.249.69.76	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	15
62.219.78.146	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 62.219.78.146	Block	15
141.212.122.64	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /x	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx	Block	15
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/www.sviva.gov.il	Block	15
157.55.39.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/miluim/default.aspx	Block	15
91.200.12.95	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/307.pdf/xmlrpc.php	Block	15
66.249.69.92	Israel	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	15
149.88.129.216	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	15
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.251	Block	15
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	15
93.173.152.243	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	15
66.249.73.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list3.htm	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/14570.jpg	Block	15
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	15
89.138.59.47	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15

10-30-2015-04:04:00 to 10-30-2015-05:04:00