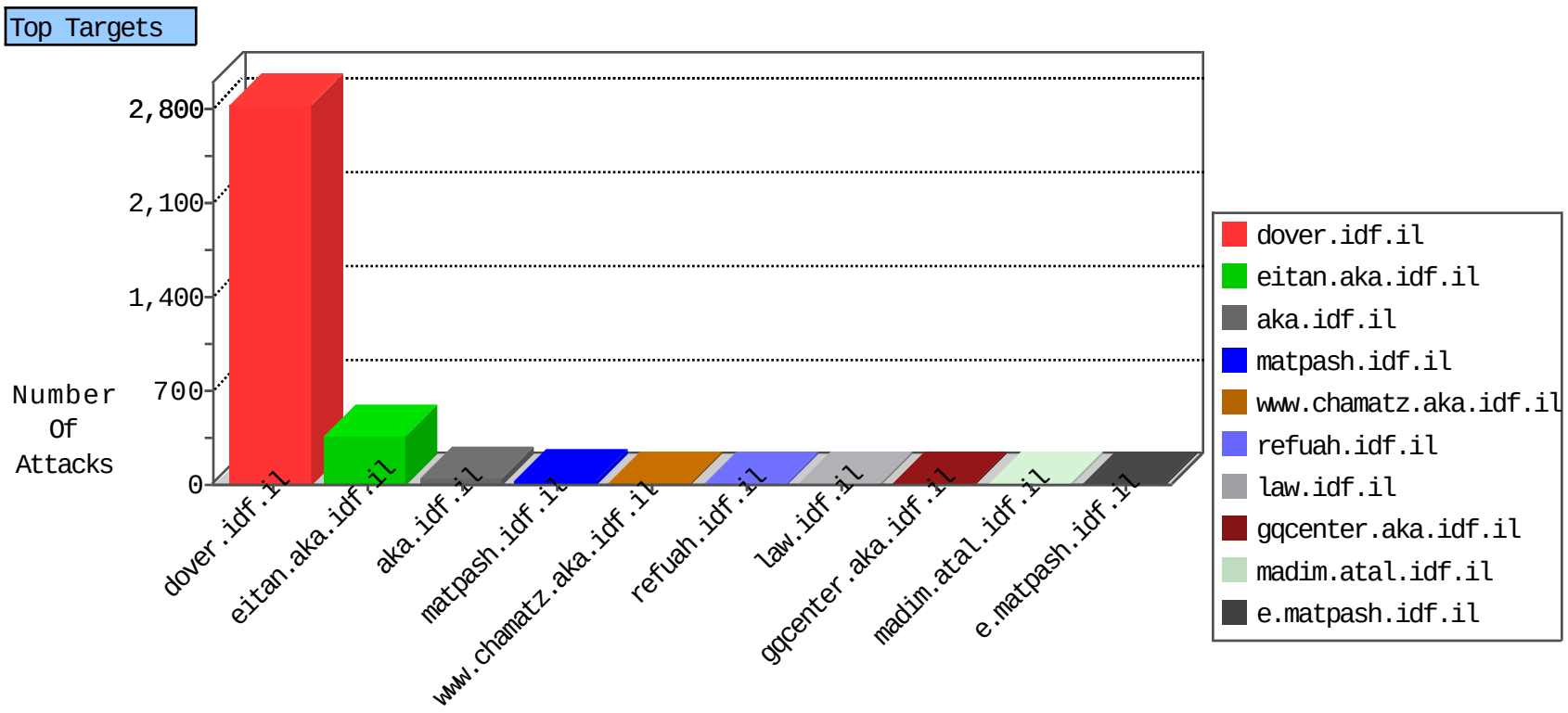
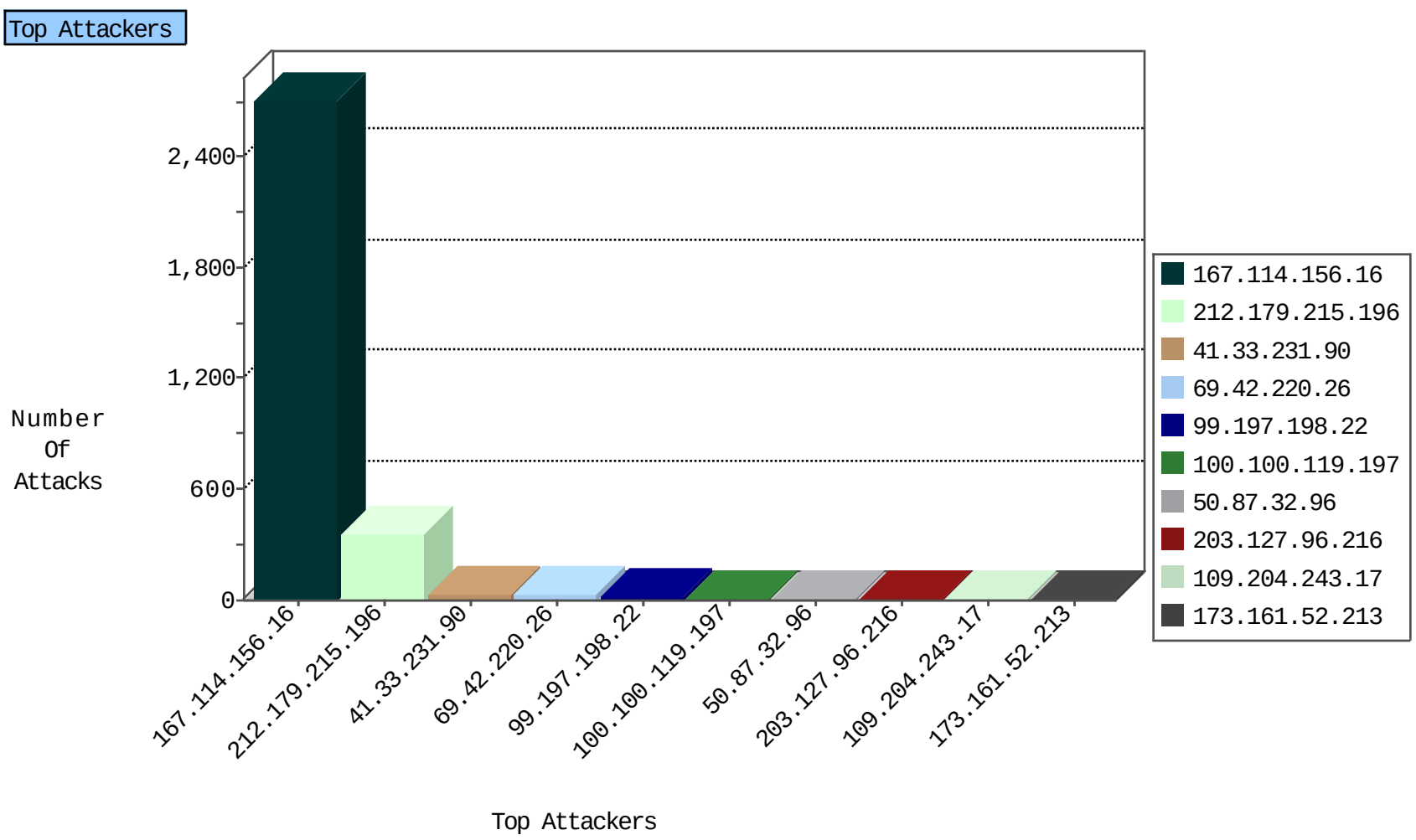
12-03-2015-02:04:01 to 12-03-2015-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-03-2015-02:04:01 to 12-03-2015-03:04:01

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	3658
69.42.220.26	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	11
69.42.220.26	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	2
94.23.220.137	France	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-03-2015-02:04:01 to 12-03-2015-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-03-2015-02:04:01 to 12-03-2015-03:04:01

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
69.42.220.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
197.157.244.243	147.237.76.148	Somalia	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.42	Canada	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
89.219.56.200	147.237.77.234	Estonia	halag.idf.il	ET SCAN NMAP -f -sS	1
210.50.197.154	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
197.157.244.243	147.237.77.212	Somalia	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.219.56.200	147.237.77.234	Estonia	halag.idf.il	ET SCAN NMAP -sS window 2048	1

12-03-2015-02:04:01 to 12-03-2015-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	78
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	25
100.100.119.197		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
69.42.220.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
99.197.198.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.226.44.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.0.139.227	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.32.98		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
99.197.198.22	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
199.30.25.217	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.106.227.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.163.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.31.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.229.31.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
69.42.220.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.200	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.128.144.131	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.172.157.109	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.161.52.213	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
213.57.151.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.88.179.210	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
31.154.92.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.201	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.196.184.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.102.49.54	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.161.52.213	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
209.126.116.147	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.88.179.210	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.8.70.76	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.201	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.87.32.96	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
109.204.243.17	Finland	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.204.243.17	Finland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.204.243.17	Block	2
82.205.108.35	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
141.8.142.29	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
50.87.32.96	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
50.87.32.96	United States	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
150.70.173.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.204.243.17	Finland	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 109.204.243.17	Block	1
54.153.33.152	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
173.161.52.213	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
112.208.62.103	Philippines	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
78.1.169.73	Croatia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
208.52.122.212	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
150.70.173.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
58.59.236.99	China	147.237.0.19	madim.atal.idf.i	PHP Attempt	Block	1
173.161.52.213	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
37.8.70.76	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/	Block	1
113.88.74.158	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
50.87.32.96	United States	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 50.87.32.96	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
58.59.236.99	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/wp-content/plugins/login-wall-ysqow/login_wall.php	Block	1
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Illegal URL Path Encoding www.idf.il/%	Block	1
37.142.64.4	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
50.87.32.96	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.87.32.96	Block	1
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	1
173.161.52.213	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
109.204.243.17	Finland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
37.142.164.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=2cf2ca42kkkkkkk_2cf2ca42	Block	1
149.88.94.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.161.52.213	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
112.208.62.103	Philippines	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
78.1.169.73	Croatia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

12-03-2015-02:04:01 to 12-03-2015-03:04:01