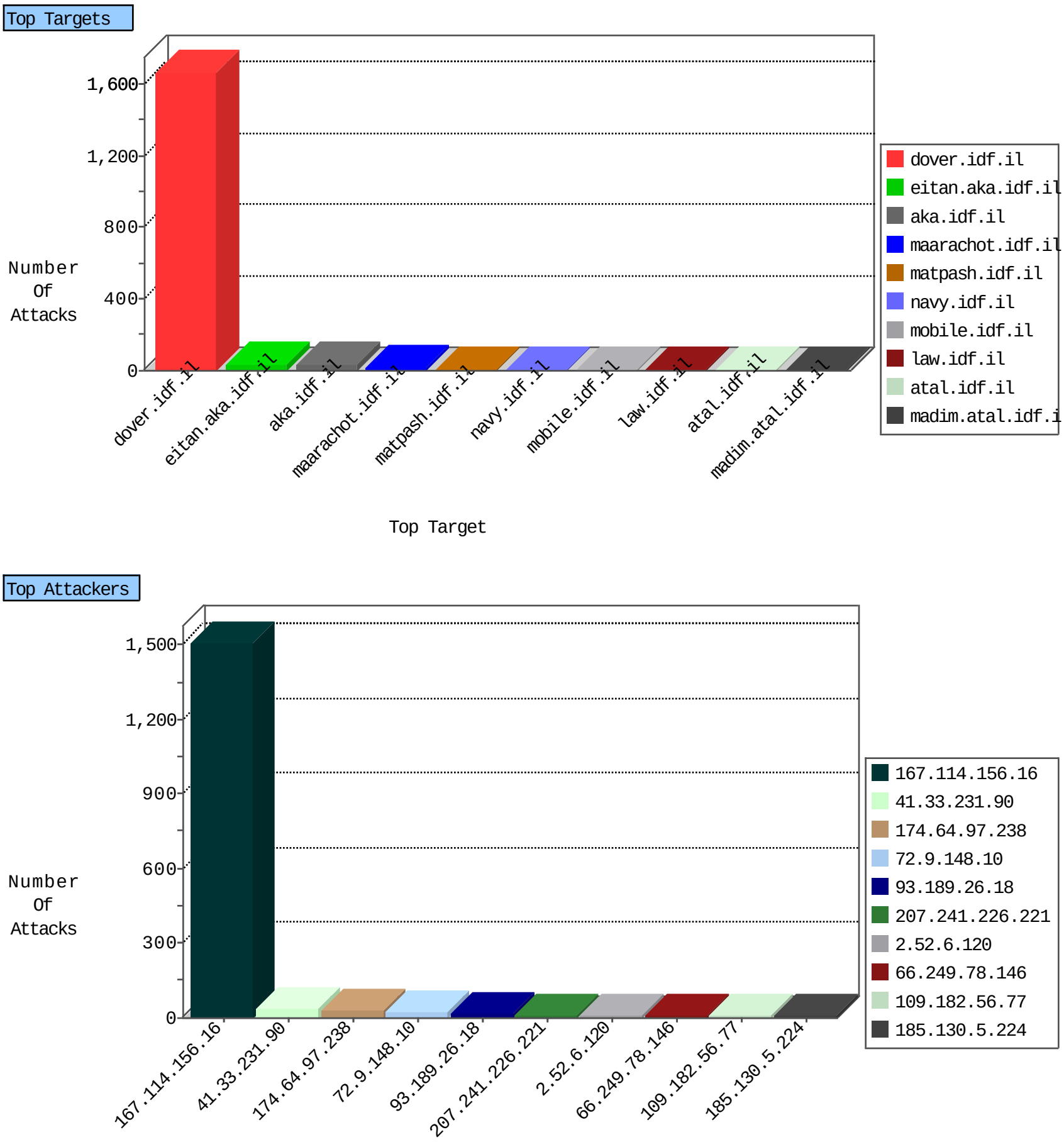
01-02-2016-04:04:08 to 01-02-2016-05:04:08

IDF Under Attack Daily Report



01-02-2016-04:04:08 to 01-02-2016-05:04:08

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	3562
106.75.199.192	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

01-02-2016-04:04:08 to 01-02-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.141.216	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

01-02-2016-04:04:08 to 01-02-2016-05:04:08

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
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.178	Austria	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
162.222.185.165	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.235	Austria	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.8.46	Austria	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.196	Ukraine	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.64	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

01-02-2016-04:04:08 to 01-02-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
174.64.97.238	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
207.241.226.221	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
109.182.56.77	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
77.127.243.193	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
49.229.84.204	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
67.55.90.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.6.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
64.246.165.150	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
77.126.152.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.231.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.114.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.130.5.224		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	2
41.233.205.234	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.130.5.224		147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	2
67.55.90.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
94.230.86.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
76.170.97.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
2.52.6.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
74.82.47.20	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.69.18	Israel	147.237.0.33	idf.il	drop		drop	1
93.189.26.18	Austria	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.115.117.117	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.175.26.46	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
2.52.6.120	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.120	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.104	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.189.26.18	Austria	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
195.154.227.118	France	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
2.52.6.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
185.130.5.224		147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
74.82.47.24	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.72	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.189.26.18	Austria	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
199.115.117.117	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.189.26.18	Austria	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.224		147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

01-02-2016-04:04:08 to 01-02-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.146.93	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.65.122.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
41.40.5.150	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.78.198	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/mobile/	Block	1
66.249.66.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
207.46.13.160	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catID\u003d42697\u0026docID\u003d42736 in www.aka.idf.il/yohalan/main/main.asp	None	1
41.233.205.234	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1414-17439-he/kkkkkkk=cfd127f5kkkkkkk_cfd127f5	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
66.249.66.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	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
108.175.150.166	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId59034 in www.aka.idf.il/main/rabanut/general.aspx	None	1
185.27.105.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.90.126	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.249.66.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
2.54.170.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
108.175.150.166	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
46.166.186.222	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
199.115.117.117	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/themes/elastixneo/ie.css	Block	1
77.127.90.126	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
66.249.73.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/03042011agrigatim.aspx	Block	1
41.40.5.150	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/patzar/news/	None	1
46.182.106.190	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
199.115.117.117	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/themes/elastixneo/ie.css	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-02-2016-04:04:08 to 01-02-2016-05:04:08