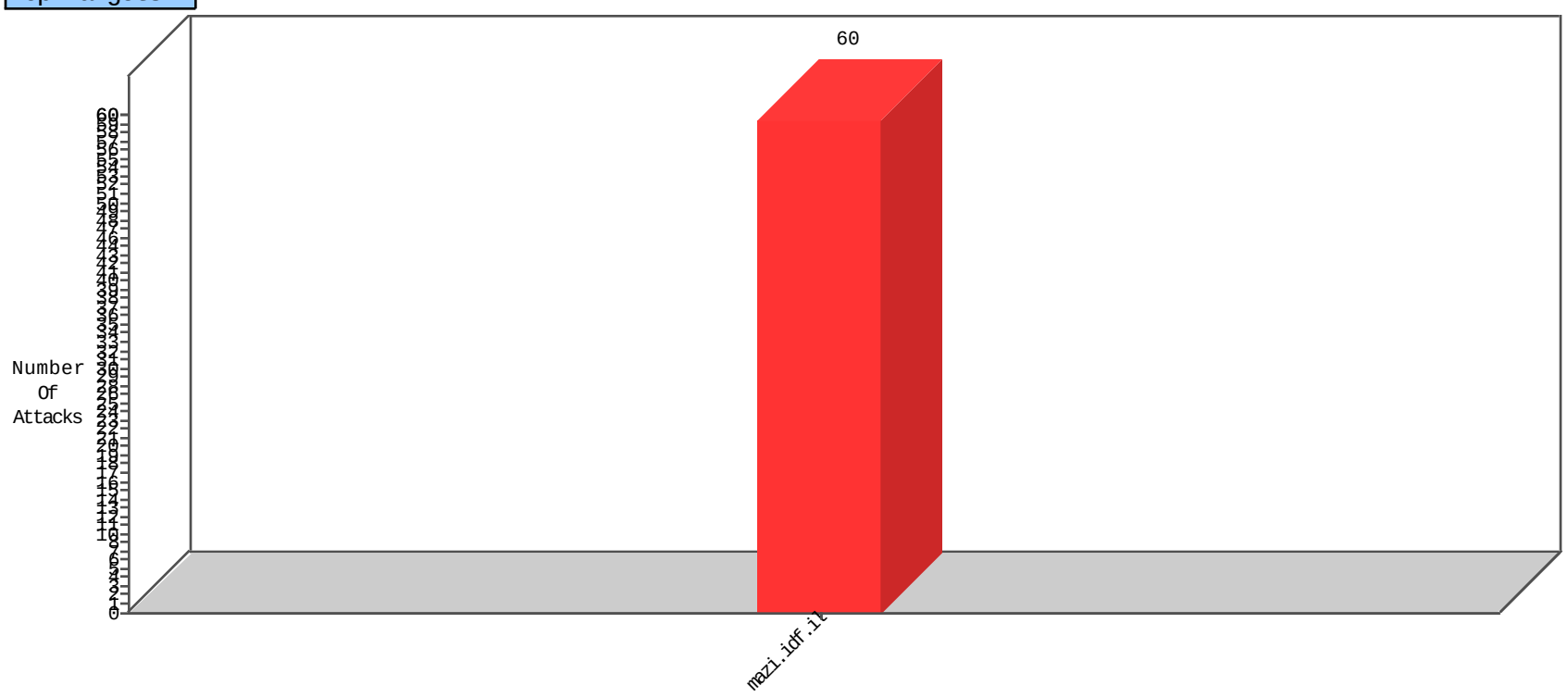
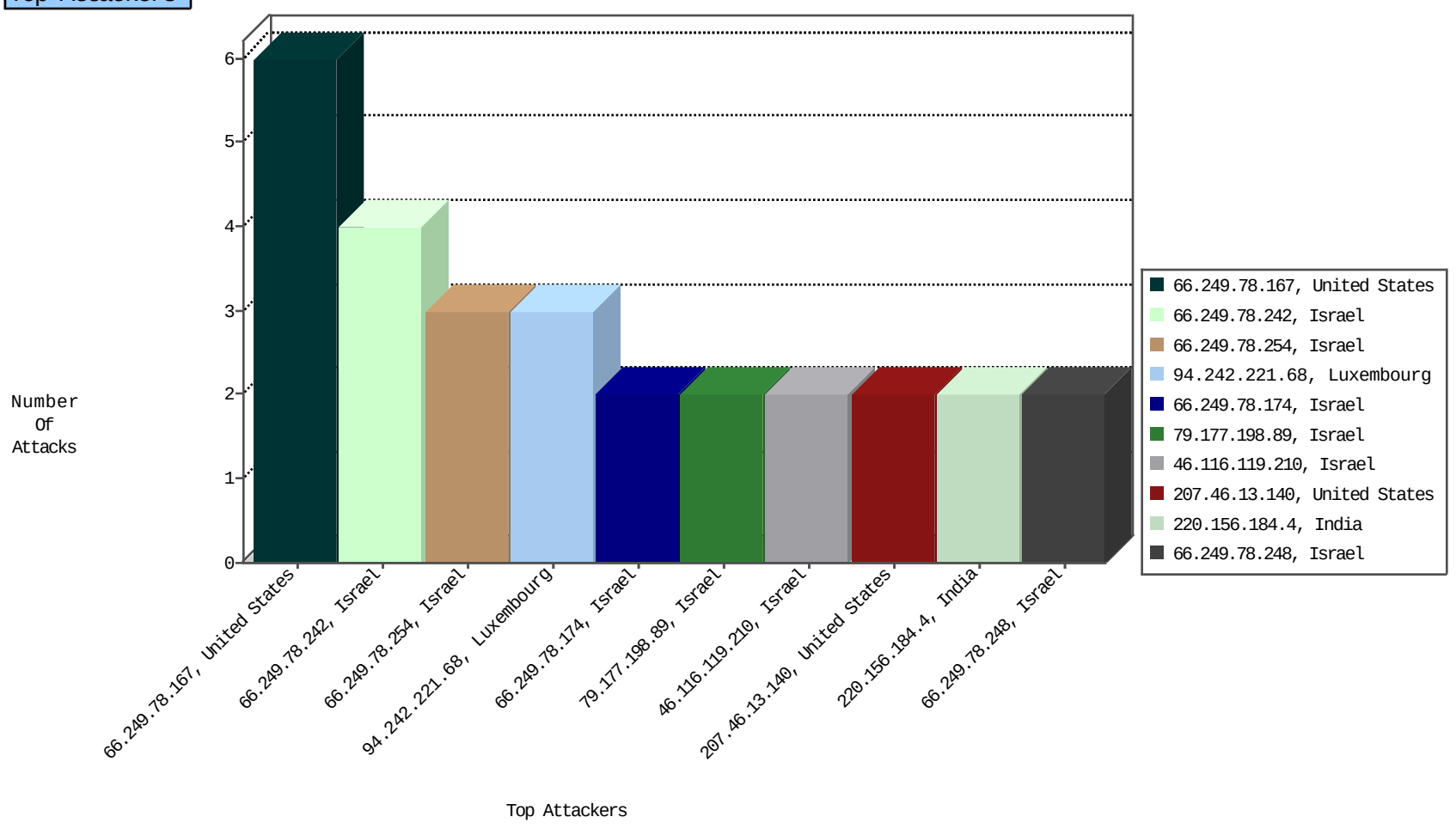
12-06-2015 to 12-07-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-06-2015 to 12-07-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2
167.88.7.233	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

12-06-2015 to 12-07-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2

12-06-2015 to 12-07-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.78.167	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	6
45.32.24.122		147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.17	mazi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	Netherlands	147.237.77.17	mazi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
187.160.92.160	Mexico	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.151.29.209	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
5.42.38.207	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
114.32.119.74	Taiwan	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	United States	147.237.77.17	mazi.idf.i	ET DROP Dshield Block Listed Source	1

12-06-2015 to 12-07-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.235.98.139	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1369
213.57.175.169	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	246
46.19.85.54	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
46.19.85.54	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	81
2.52.5.226	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	80
46.19.86.17	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
2.52.5.226	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
2.52.5.226	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
82.166.100.2	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.5.226	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
85.65.197.159	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.125	Israel	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	12
46.19.86.145	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.65.165.181	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.149.194	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.180.138.152	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.57.137.185	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.171.228.231	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.69.67.228	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.137	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	4
213.57.137.185	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
84.108.185.15	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.133.178	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
71.204.146.106	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.22.106	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.223	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.197.159	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
207.46.13.140	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.2.203	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.142.127.161	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.181.26.145	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.148.192	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.176	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.230	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.248	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.126	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.157	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.8.170	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.149.171	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.15	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.128.172	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
31.168.71.249	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.16.158	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.77	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.198	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
46.19.86.19	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.181.26.145	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.192	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

12-06-2015 to 12-07-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
91.228.248.251	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
79.177.198.89	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5772-8117-he/igf.aspx	Block	1
46.19.86.74	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
212.112.126.13	Kyrgyzstan	147.237.77.17	mazi.idf.i	Distributed Parameter Type Violation on igf.idf.il/3775-he/igf.aspx parameter pagenum	Block	1
95.86.93.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
79.181.138.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-8444-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9280-he/igf.aspx	Block	1
14.163.170.46	Vietnam	147.237.77.17	mazi.idf.i	Parameter Type Violation tabnum in mazi.idf.il/3775-he/igf.aspx	Block	1
207.46.13.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
94.242.221.68	Luxembourg	147.237.77.17	mazi.idf.i	Distributed Parameter Type Violation on igf.idf.il/3775-he/igf.aspx parameter pagenum	Block	1
79.177.198.89	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
212.199.224.24	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 212.199.224.24	Block	1
46.116.119.210	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
157.55.39.15	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-8134-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
31.184.132.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
207.46.13.140	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
94.242.221.68	Luxembourg	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/3775-he/igf.aspx	Block	1
79.181.6.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5551-6908-he/igf.aspx	Block	1
213.57.175.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
46.116.119.210	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
2.54.17.156	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
207.46.13.28	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
91.205.66.166	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation tabnum in mazi.idf.il/3775-he/igf.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-8411-he/igf.aspx	Block	1
40.77.167.10	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/stream/generate	Block	1
207.46.13.140	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/	Block	1
94.242.221.68	Luxembourg	147.237.77.17	mazi.idf.i	Parameter Type Violation pagenum in igf.idf.il/3775-he/igf.aspx	Block	1
79.181.138.25	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.121.86.235	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hir .	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
207.46.13.95	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1

12-06-2015 to 12-07-2015