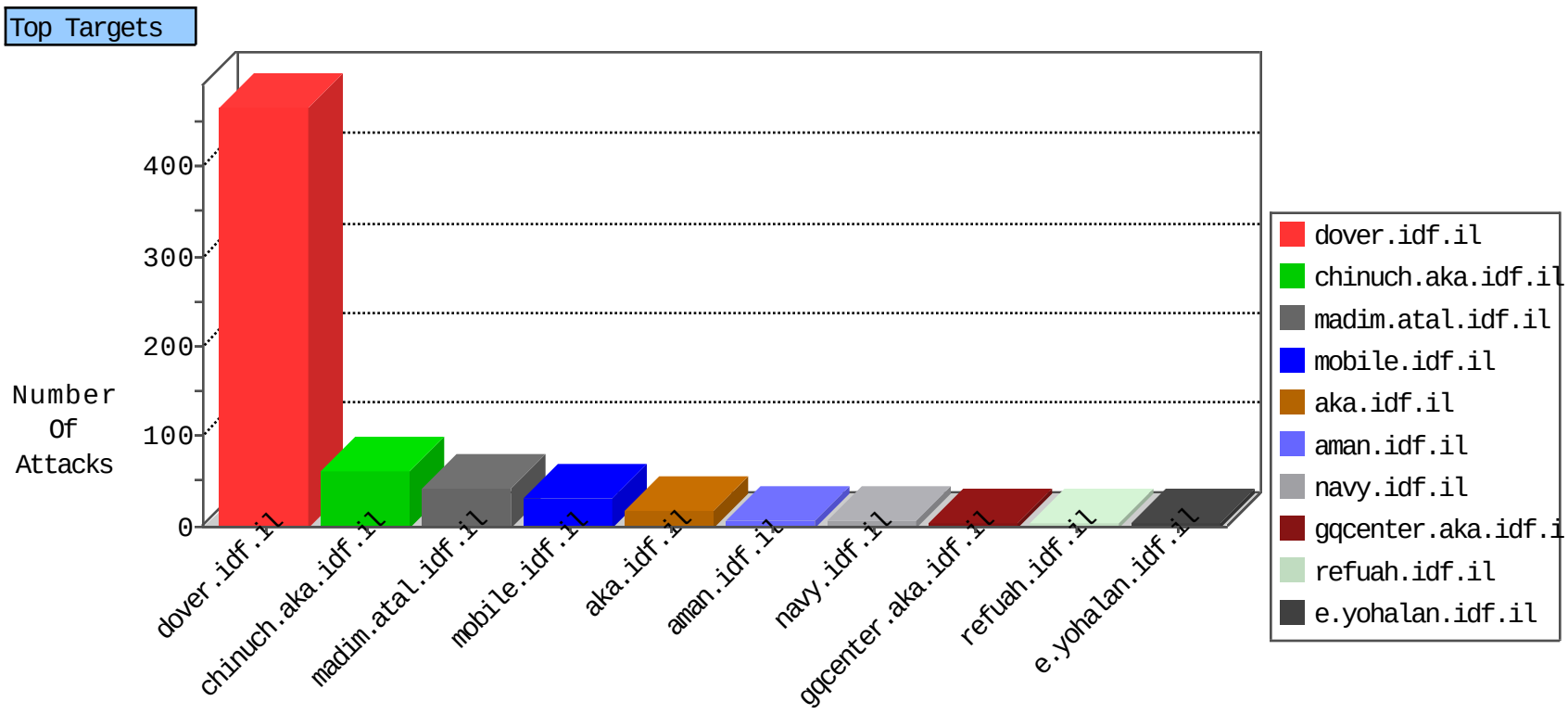
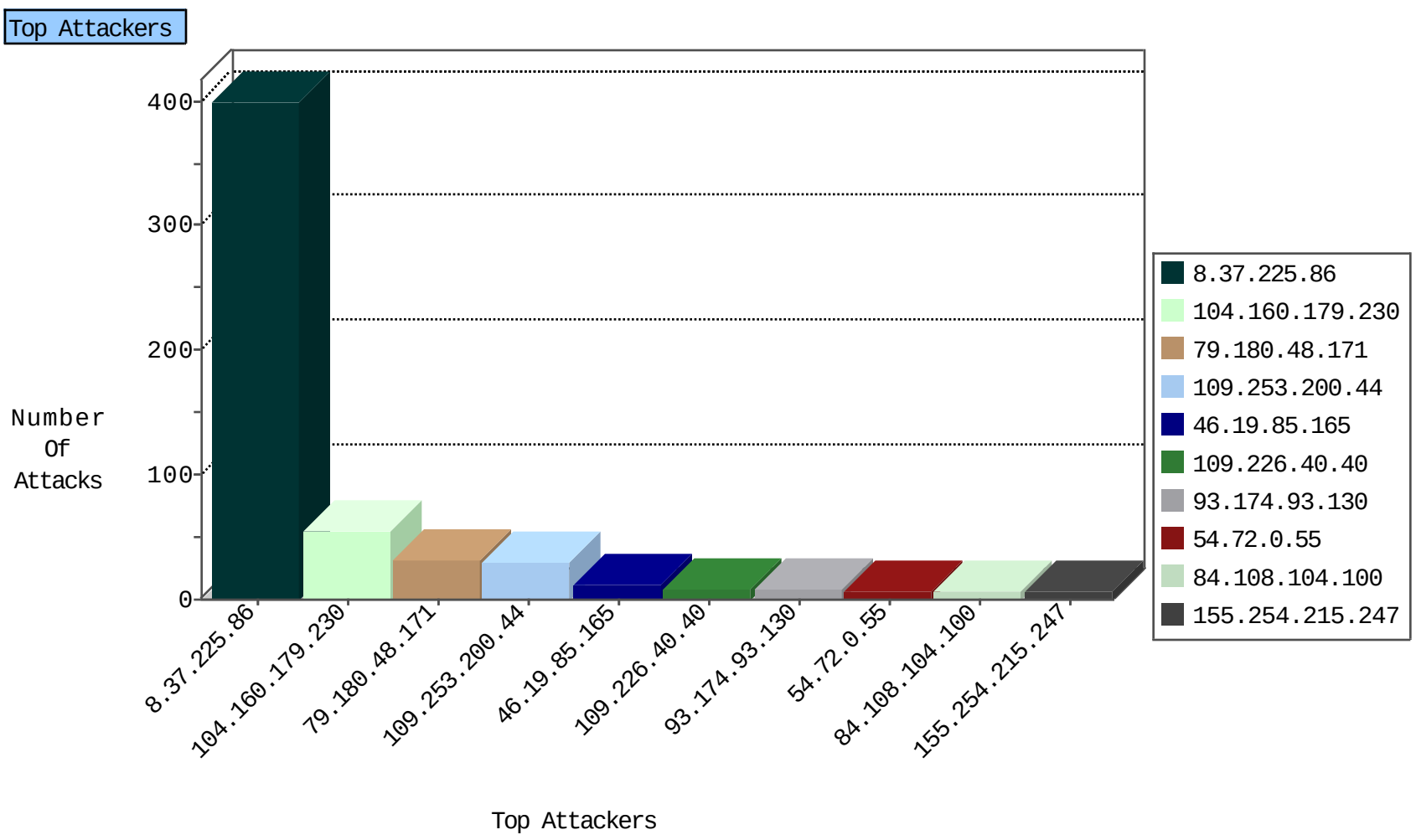
09-24-2016-08:04:04 to 09-24-2016-09:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-08:04:04 to 09-24-2016-09:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.136.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
8.37.225.86	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-24-2016-08:04:04 to 09-24-2016-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.77.76.152	Taiwan	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.69.74	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-24-2016-08:04:04 to 09-24-2016-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.174.93.130	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.130	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.149.244.79	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
185.153.198.10	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
179.43.141.221	147.237.8.27	Switzerland	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.130	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.130	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.130	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.130	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
179.43.141.221	147.237.77.212	Switzerland	e.dover.idf.il	ET SCAN Potential SSH Scan	1
81.170.162.82	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
140.246.105.194	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.187.89	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.130	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.130	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-24-2016-08:04:04 to 09-24-2016-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
8.37.225.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	50
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
155.254.215.247	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.9.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.226.217.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
122.170.22.189	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.139.161.235	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.108.104.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
187.87.204.200	Brazil	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.108.104.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
109.64.172.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
194.58.73.192	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.125.48.7	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
194.58.73.192	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.147.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
131.253.29.133	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
198.20.69.74	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.74	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.43	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
216.218.206.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
79.178.0.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.51	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
120.132.68.87	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.92	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.217.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.58	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1

09-24-2016-08:04:04 to 09-24-2016-09:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.48.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
157.55.39.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
213.57.223.65	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.66.10	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
188.32.178.199	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/994-9043-he/refuah.aspx	Block	1
207.46.13.188	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3294.jpg	Block	1
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.165 (Open Mode)	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
213.8.204.67	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
66.249.75.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
5.22.134.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.8.204.67	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
46.121.208.103	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1

09-24-2016-08:04:04 to 09-24-2016-09:04:04