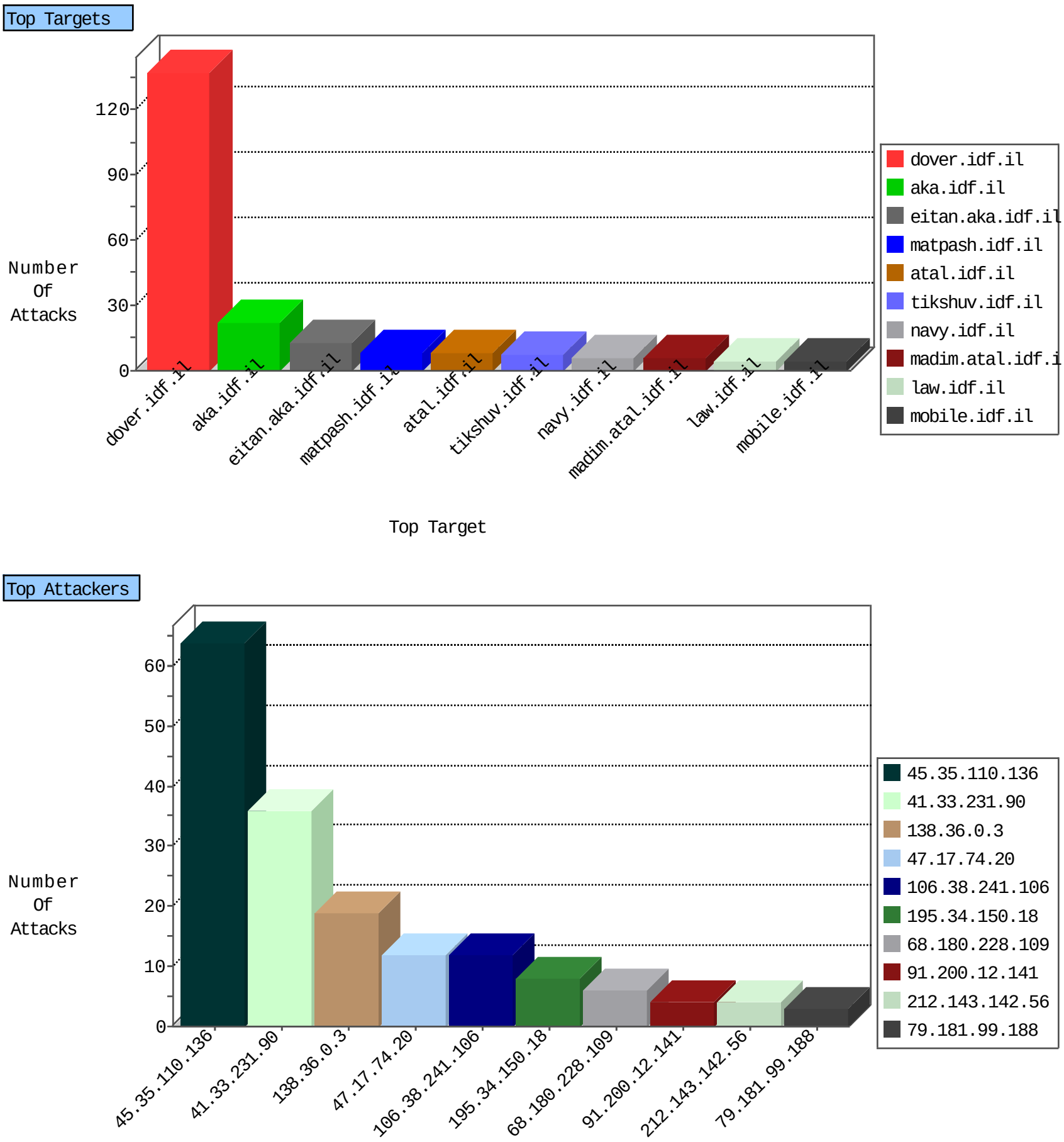
02-27-2016-06:04:09 to 02-27-2016-07:04:09

IDF Under Attack
Daily Report



02-27-2016-06:04:09 to 02-27-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.104	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.219	Switzerland	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
174.90.123.196	Canada	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.124	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-27-2016-06:04:09 to 02-27-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.35.110.136		147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	10
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
122.152.167.156	Japan	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

02-27-2016-06:04:09 to 02-27-2016-07:04:09

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
138.36.0.3	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.76.200	Netherlands	eitan.aka.idf.i	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
138.36.0.3	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
179.32.200.181	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-27-2016-06:04:09 to 02-27-2016-07:04:09

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
45.35.110.136		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
47.17.74.20	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.118.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.99.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.115.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
40.77.167.63	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.133	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
78.47.62.212	Germany	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.8.24	e.lifestyle.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.223	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.11	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.77	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
182.50.130.133	Singapore	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
66.147.244.138	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
138.36.0.3		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.31	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
123.125.71.77	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.99	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.108	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.35	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.75.103.242	Russian Federation	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.111	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.112	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-27-2016-06:04:09 to 02-27-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.35.110.136		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.35.110.136	Block	25
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
87.69.143.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/payslips/viewslipaspdf.asp	Block	2
95.211.187.82	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/wp/wp-admin/	Block	1
1.4.167.136	Thailand	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.35.110.136		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
194.226.6.252	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
98.139.204.40	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/wp-admin/	Block	1
2.54.14.159	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
157.7.105.223	Japan	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/old/wp-admin/	Block	1
50.62.176.236	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/	Block	1
204.79.180.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
99.32.153.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
45.35.110.136		147.237.77.216	dover.idf.il	Admin Blocking	Block	1
157.55.39.249	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/templates/inner.asp	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
204.79.180.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
113.76.90.196	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
45.35.110.136		147.237.77.216	dover.idf.il	Multiple Admin Blocking from 45.35.110.136	Block	1
184.172.172.26	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/blog/wp-admin/	Block	1
1.4.167.136	Thailand	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 1.4.167.136 (Open Mode)	None	1
204.79.180.252	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.226.6.252	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1

02-27-2016-06:04:09 to 02-27-2016-07:04:09