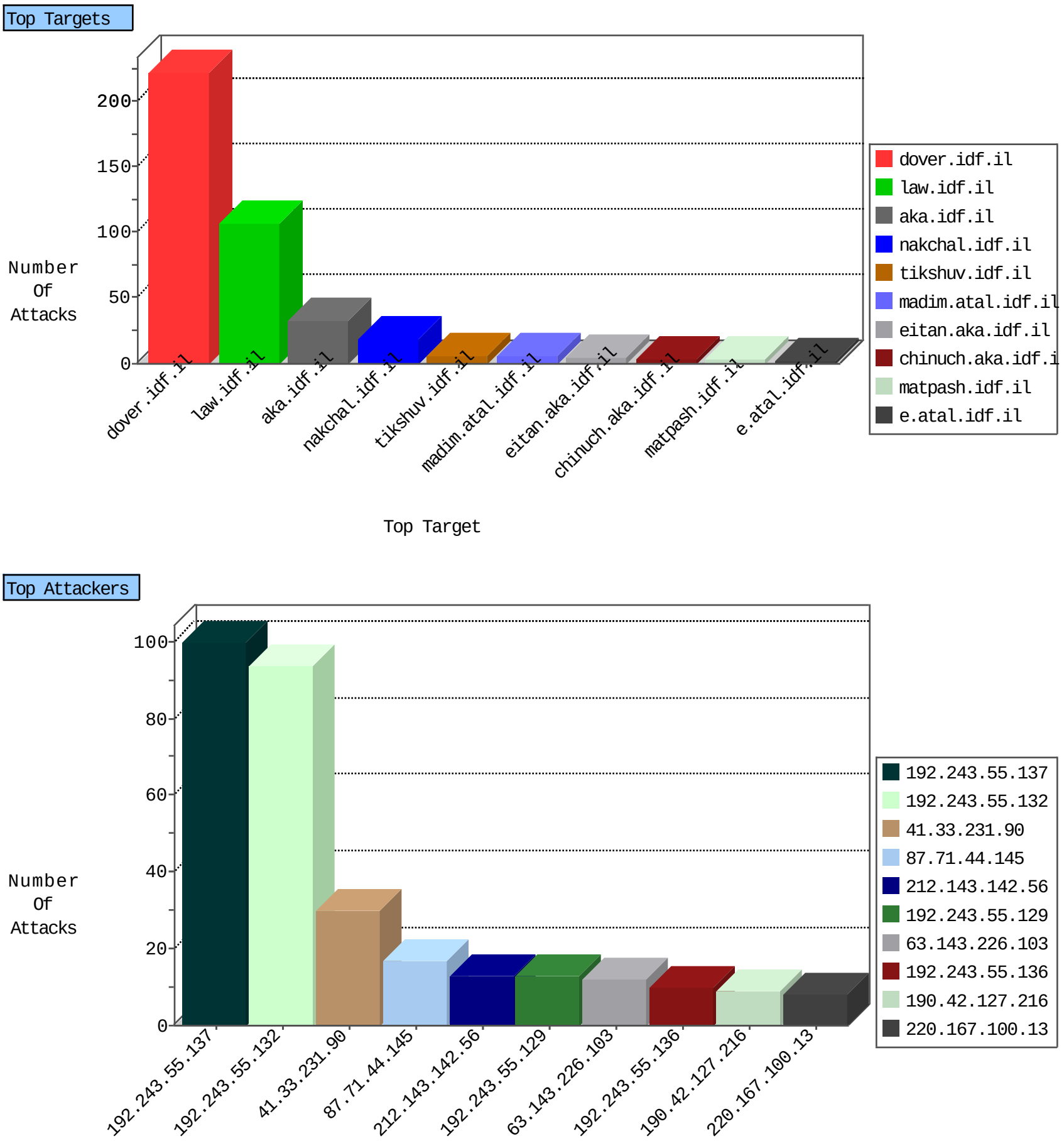
04-12-2016-06:04:07 to 04-12-2016-07:04:07

IDF Under Attack Daily Report



04-12-2016-06:04:07 to 04-12-2016-07:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.132	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.12.160.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.93.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.181.215.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-12-2016-06:04:07 to 04-12-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
54.183.93.152	United States	147.237.77.176	matpash.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1

04-12-2016-06:04:07 to 04-12-2016-07:04:07

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	2
185.130.5.86	147.237.72.156	Lithuania	aman.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
220.167.100.13	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
14.102.100.2	147.237.0.33	India	idf.il	ET SCAN Potential SSH Scan	1
220.167.100.13	147.237.0.19	China	madim.atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.86	147.237.77.216	Lithuania	dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.44	Lithuania	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
220.167.100.13	147.237.0.34	China	tikshuv.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
2.53.25.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.167.100.13	147.237.0.19	China	madim.atal.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.86	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1

04-12-2016-06:04:07 to 04-12-2016-07:04:07

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	30
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
63.143.226.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
209.6.148.106	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.208.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
63.143.226.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.169.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
190.42.127.216	Peru	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
149.78.47.50	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
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
190.42.127.216	Peru	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
190.42.127.216	Peru	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.194	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
41.47.113.119	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
149.78.47.50	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
98.165.177.28	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.47.50	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
131.253.25.222	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

04-12-2016-06:04:07 to 04-12-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.44.145	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
87.71.44.145	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.71.44.145	Block	6
65.55.210.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.16	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.66.33	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
199.30.24.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.44.145	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	2
199.30.24.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.208.17	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
207.46.13.41	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
216.218.206.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17938-he/dover.aspx<span style='font-family:tahoma	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
220.167.100.13	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/manager/html	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.167.100.13	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/manager/html	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1

04-12-2016-06:04:07 to 04-12-2016-07:04:07