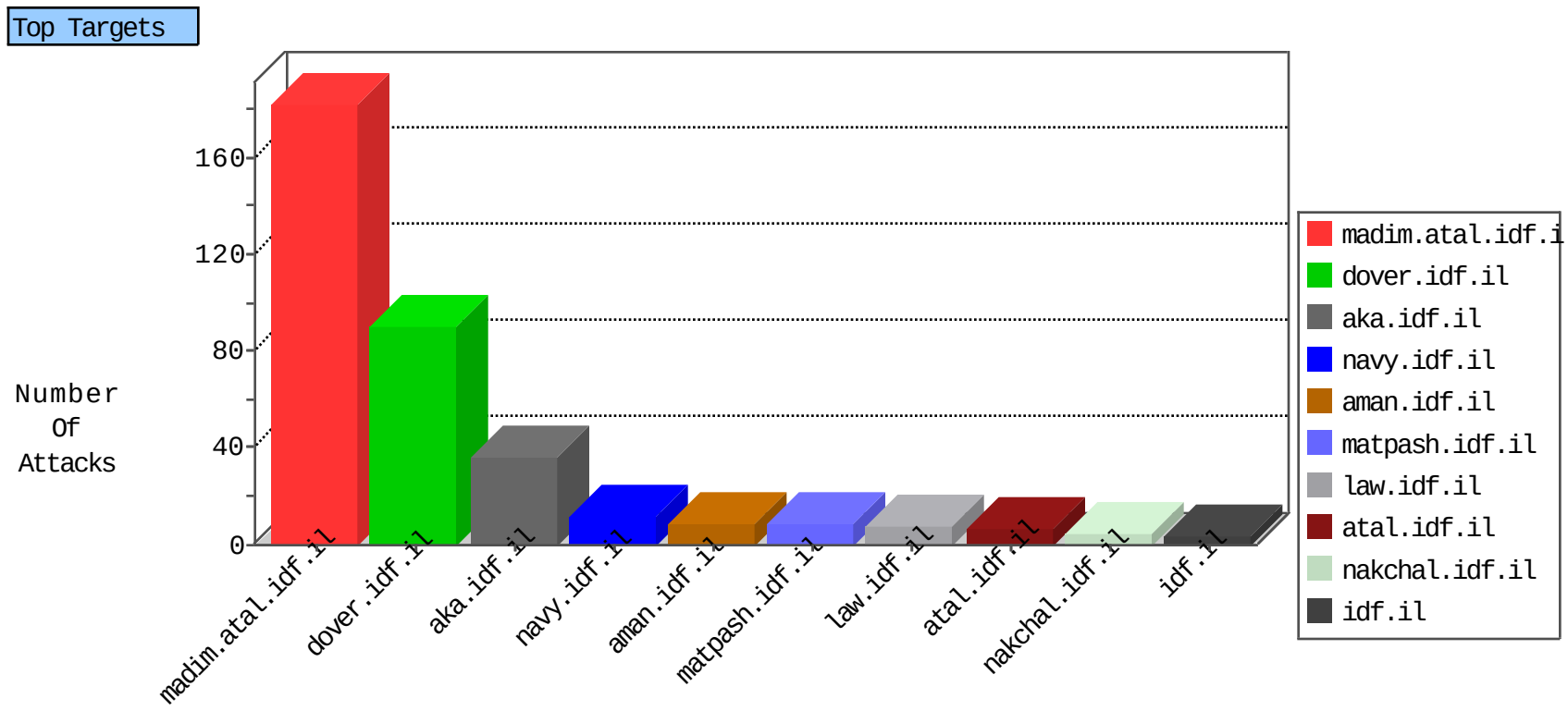
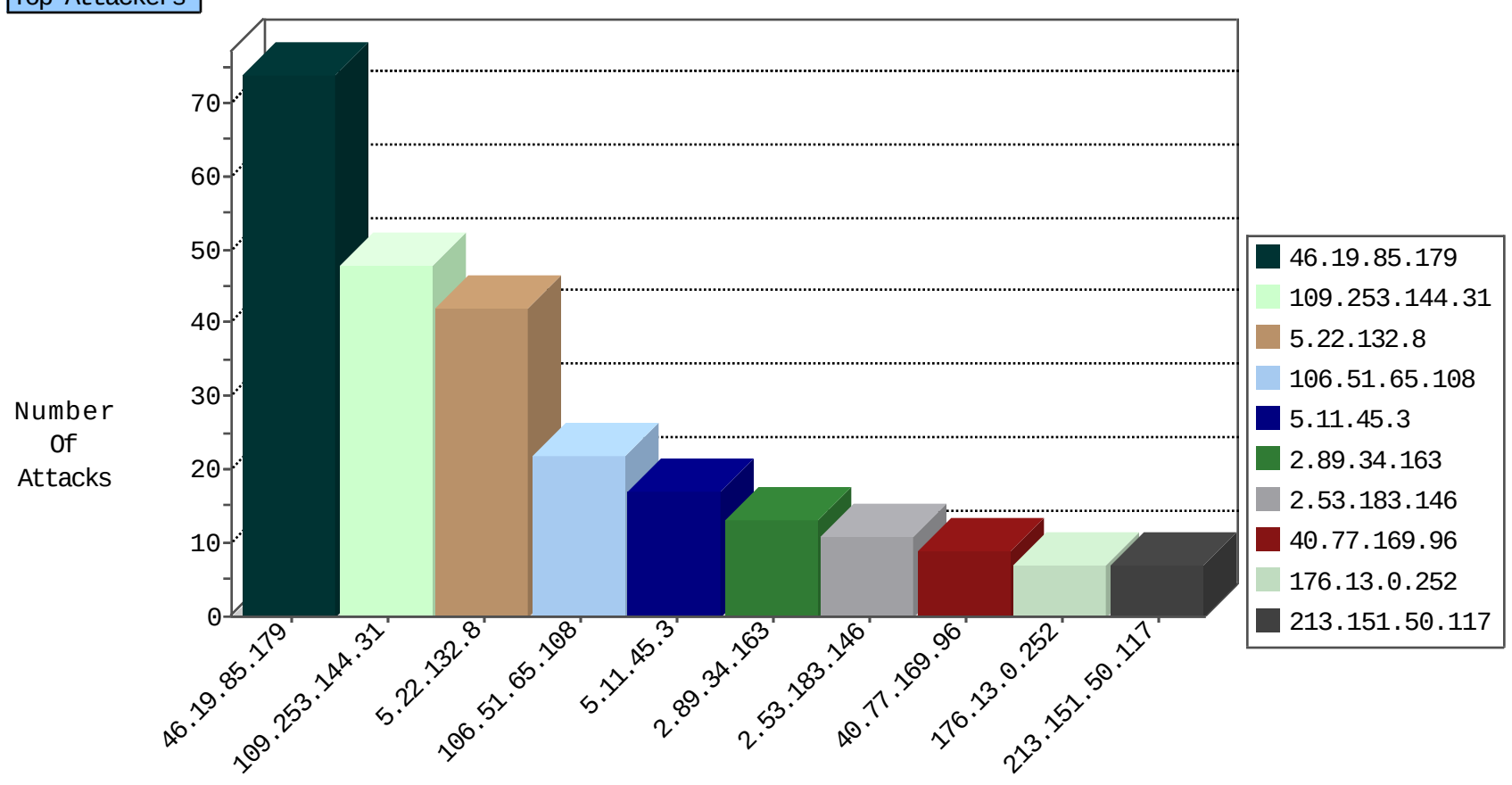
08-24-2016-21:04:07 to 08-24-2016-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-24-2016-21:04:07 to 08-24-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	6
123.59.59.52	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
80.82.70.230	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
141.0.15.36	Norway	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
80.82.70.230	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
158.69.43.169	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-24-2016-21:04:07 to 08-24-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
51.255.65.25	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.171	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.85	Italy	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-24-2016-21:04:07 to 08-24-2016-22:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
106.51.65.108	147.237.77.61	India	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
106.51.65.108	147.237.76.86	India	navy.idf.il	ET SCAN Potential SSH Scan	2
106.51.65.108	147.237.76.39	India	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
106.51.65.108	147.237.77.205	India	prisha.idf.il	ET SCAN Potential SSH Scan	2
106.51.65.108	147.237.76.177	India	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.102.9.185	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
40.77.169.96	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
106.51.65.108	147.237.76.202	India	e.halag.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.56.80.144	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.76.176	India	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.77.233	India	atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.98	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
106.51.65.108	147.237.77.170	India	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.77.19	India	law-forum.idf.il	ET SCAN Potential SSH Scan	1
106.51.65.108	147.237.76.200	India	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.80.144	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.0.35	Japan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.76.44	India	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
106.51.65.108	147.237.77.234	India	halag.idf.il	ET SCAN Potential SSH Scan	1
101.178.206.92	147.237.76.200	Australia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.65.108	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
77.138.52.97	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
106.51.65.108	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1

08-24-2016-21:04:07 to 08-24-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.89.34.163	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.11.45.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
156.198.186.164	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.0.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
66.102.9.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.11.45.3	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
176.13.18.147	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.224.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
198.179.95.131	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.241.117	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
107.170.125.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.128.48.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.127.77.46	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.228.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
100.92.106.20		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
141.212.122.26	United States	147.237.0.33	idf.il	drop		drop	1
77.40.0.13	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
133.242.3.168	Japan	147.237.0.33	idf.il	drop		drop	1
141.212.122.16	United States	147.237.0.200	m4u.idf.il	drop		drop	1
212.235.2.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.17	United States	147.237.0.200	m4u.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.3.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.251.97	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.25	United States	147.237.0.33	idf.il	drop		drop	1
77.40.0.13	Russian Federation	147.237.0.33	idf.il	drop		drop	1
37.26.149.222	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.253.144.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
5.22.132.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.53.183.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
213.151.50.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	7
80.178.202.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
77.126.30.174	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 77.126.30.174	Block	2
94.187.48.1	Lebanon	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/smalim/html/12.asp	Block	2
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
109.66.150.31	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
80.246.139.208	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.138.254.110	France	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
37.142.201.232	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
85.65.186.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	1
194.219.51.241	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.20.159	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
37.142.201.232	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
172.56.2.40	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
77.126.30.174	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8	Block	1
208.99.252.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
46.116.0.222	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.27.104.50	Block	1
109.65.191.82	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/spotting/spotting.asp	Block	1
77.127.43.240	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 77.127.43.240	Block	1
46.117.116.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.182	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	1
5.29.7.169	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.46.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2689.jpg	Block	1
31.168.107.244	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.205	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.230.171	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
109.66.182.60	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1

08-24-2016-21:04:07 to 08-24-2016-22:04:07