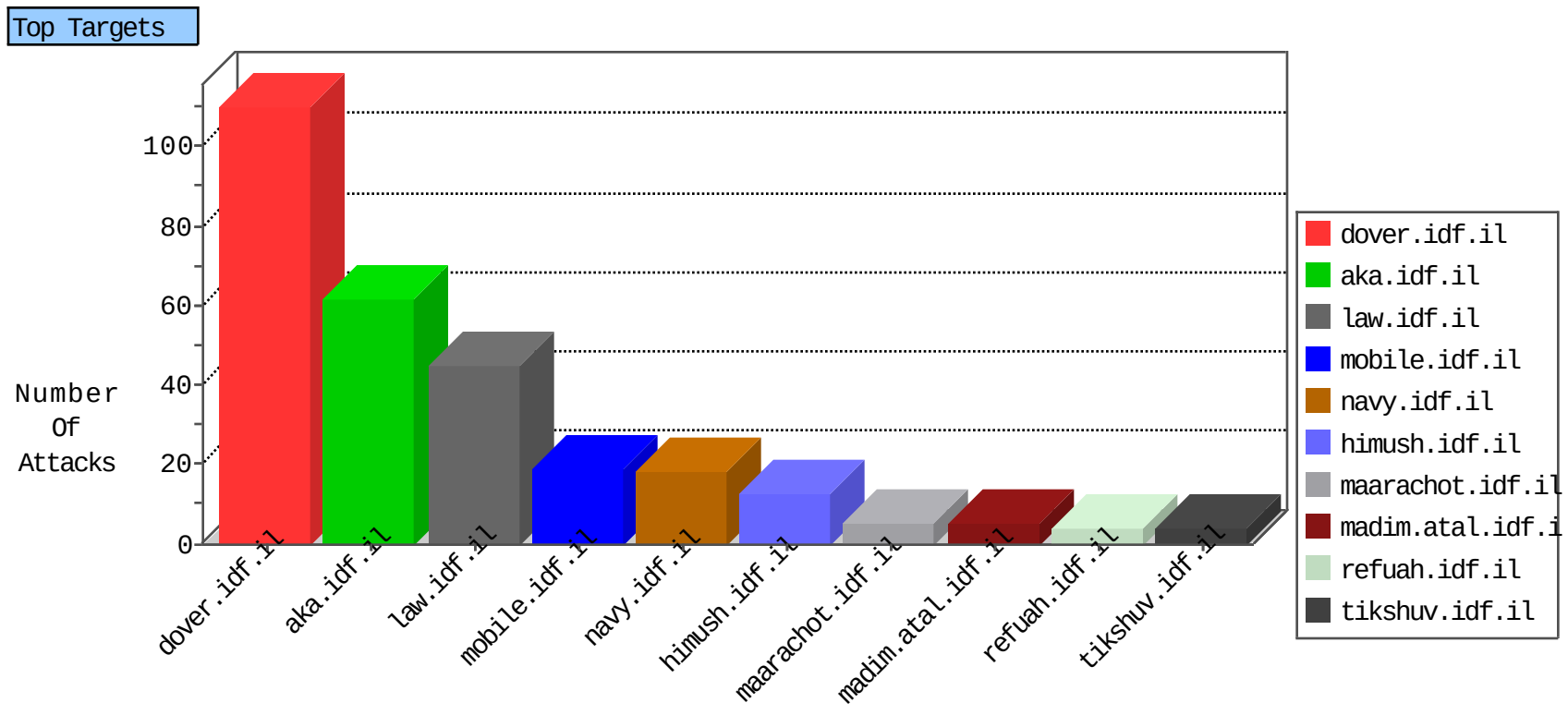
02-04-2016-02:04:06 to 02-04-2016-03:04:06

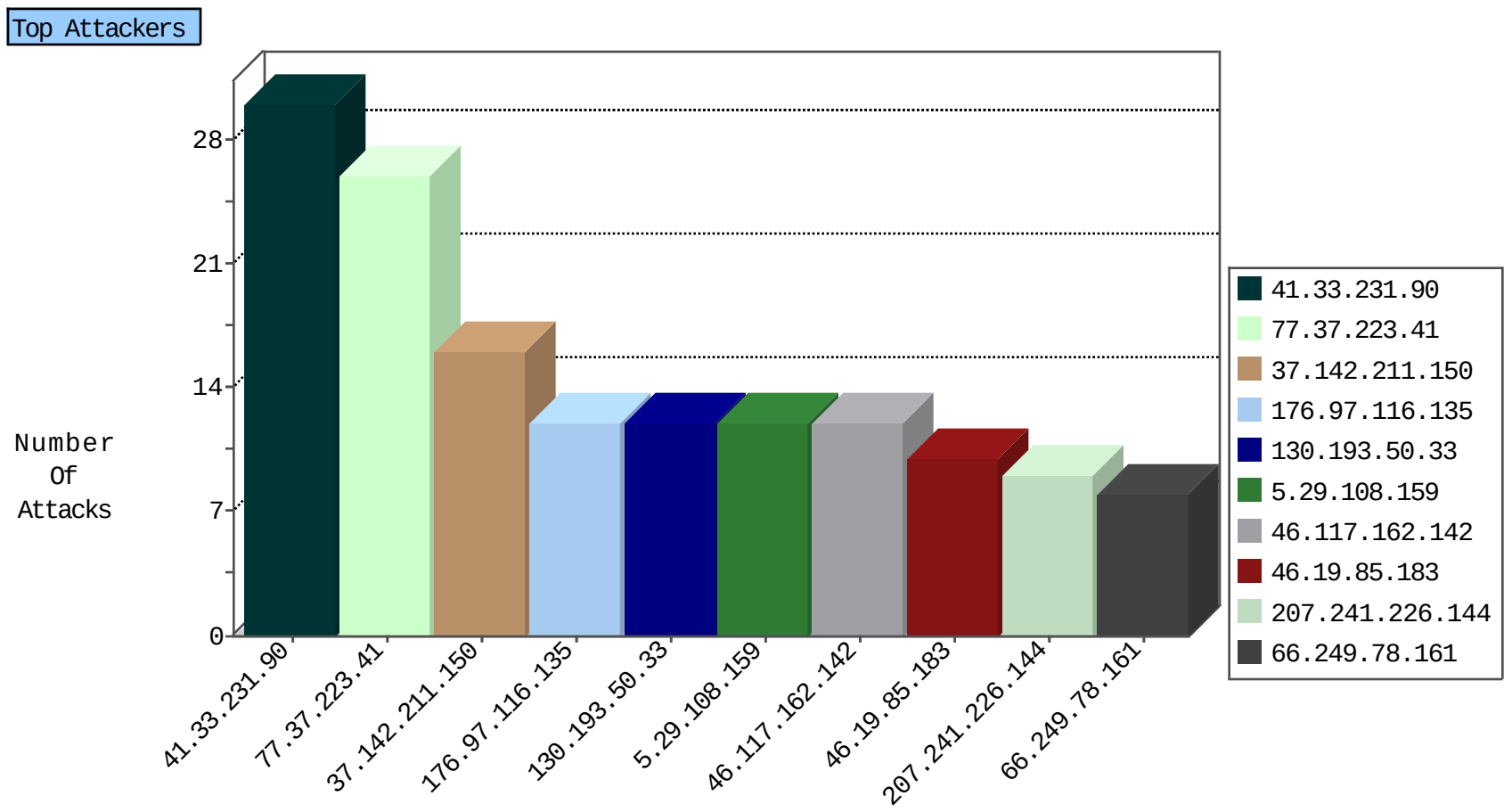
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-04-2016-02:04:06 to 02-04-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
142.54.169.162	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
54.67.38.74	United States	147.237.76.42	refuah.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
74.91.28.62	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
142.54.169.165	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
54.67.38.74	United States	147.237.77.170	maarachot.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
74.91.28.62	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
54.67.38.74	United States	147.237.77.234	halag.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
142.54.160.214	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-04-2016-02:04:06 to 02-04-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-04-2016-02:04:06 to 02-04-2016-03:04:06

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.76.176		test.ncore.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
111.193.243.62	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
123.249.35.30	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

02-04-2016-02:04:06 to 02-04-2016-03:04:06

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
77.37.223.41	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
46.117.162.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
5.29.108.159	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
207.241.226.144	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	9
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.146.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.0.14.177	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
198.182.56.5	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.154	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
181.211.249.18	Ecuador	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.38.62	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.111.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.63.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.220	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.24	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
118.173.249.251	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
176.228.26.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.108.159	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.39.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
177.82.205.98	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
177.82.205.98	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
42.62.74.71	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
37.142.211.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.73.209	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.38.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.i	drop	SAM rule	drop	1
5.22.135.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.181.133.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.33	China	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.181.133.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
187.153.158.147	Mexico	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.211.150	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	7
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.97.116.135	Block	5
37.142.211.150	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.142.211.150	Block	4
109.67.197.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
37.142.211.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.192.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
45.53.19.69		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
84.108.90.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.46.38.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general.aspx	Block	1
137.99.229.183	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1084-en/eitan.aspx	None	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
218.25.89.100	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/home	Block	1
84.108.90.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
142.54.169.166	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.99yyzz.com/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9180-he/refuah.aspx	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=1%7C5; __atuvs=56b29dc544ae68f5000; __atssc=facebook%3B2	Block	1
218.25.89.100	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/home	Block	1
84.108.90.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
76.126.242.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=a011996f0452e06b.1448626810.1.1448626810.1448626810.;	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17154-he/dover.aspx	Block	1
79.177.185.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$27 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method %22%5D; in URL _pk_id.20.8afc=a011996f0452e06b.1448626810.1.1448626810.1448626810.	Block	1

02-04-2016-02:04:06 to 02-04-2016-03:04:06