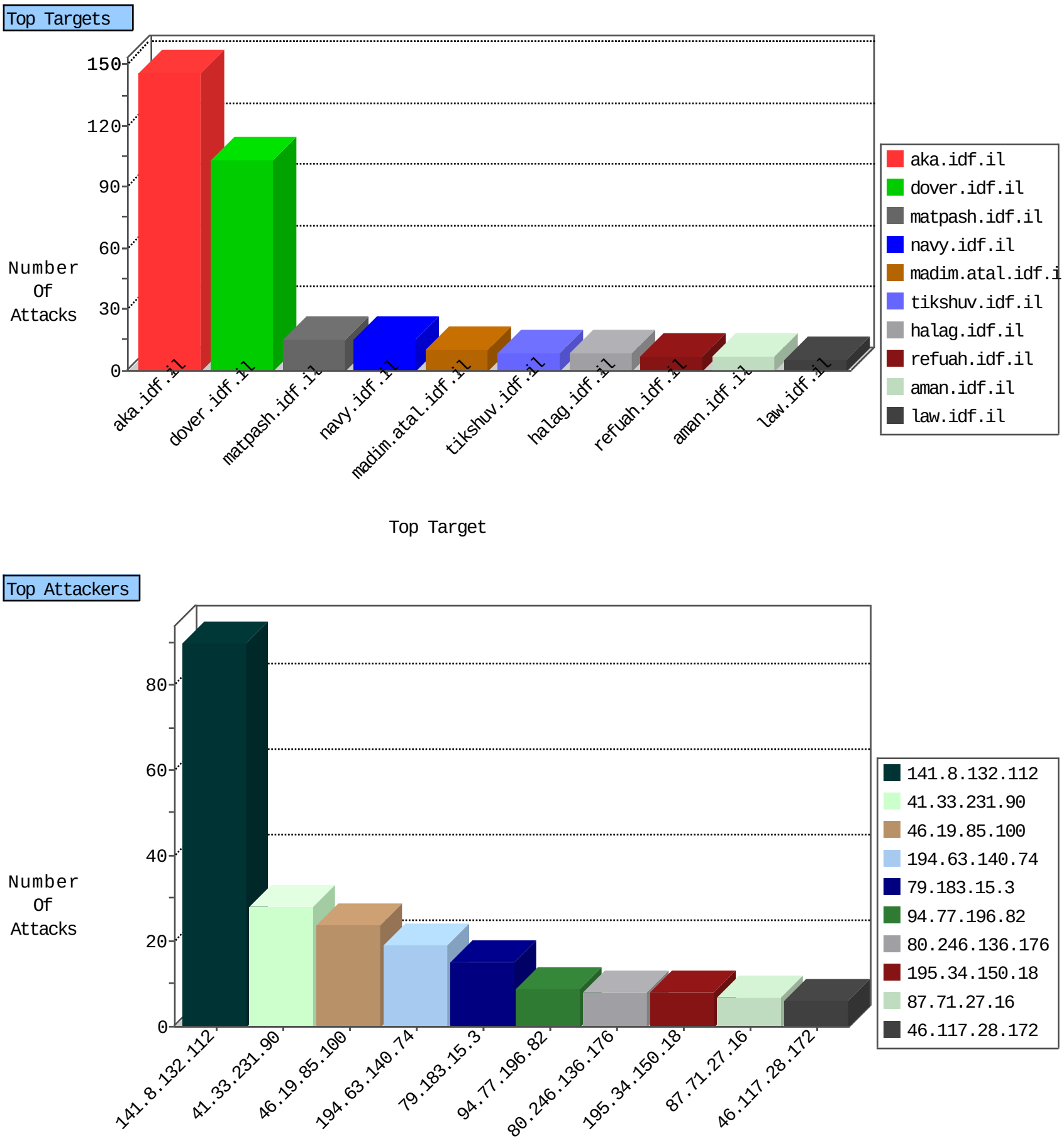
02-17-2016-01:06:37 to 02-17-2016-02:06:37

IDF Under Attack
Daily Report



02-17-2016-01:06:37 to 02-17-2016-02:06:37

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-01:06:37 to 02-17-2016-02:06:37

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-01:06:37 to 02-17-2016-02:06:37

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
194.63.140.74	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
194.63.140.74	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
69.197.145.242	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.0.34	Indonesia	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
194.63.140.74	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.1	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
212.116.207.66	147.237.0.19	Saudi Arabia	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
194.63.140.74	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1

02-17-2016-01:06:37 to 02-17-2016-02:06:37

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
79.183.15.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.117.28.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
87.71.27.16	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.138.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.194.94.231	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
177.235.124.135	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.119.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.207	Israel	147.237.76.42	refuah.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
37.26.149.187	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.62.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.116.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.211.4.182	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
108.167.133.30	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.149.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
192.185.4.108	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
40.77.167.36	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.114.65.67	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.116.49.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.79	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.149.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.172.51.127	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.186	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.116	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.71	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.148.172	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
123.125.71.79	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.176.217	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-17-2016-01:06:37 to 02-17-2016-02:06:37

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.176	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	8
178.137.93.235	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	6
79.176.177.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.177.250	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
79.176.177.250	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
2.52.10.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
87.71.27.16	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.168.19.222	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19484-he/idfgdover.aspx	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
180.76.15.31	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8915-he/refuah.aspx	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
79.176.177.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
207.46.13.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

02-17-2016-01:06:37 to 02-17-2016-02:06:37