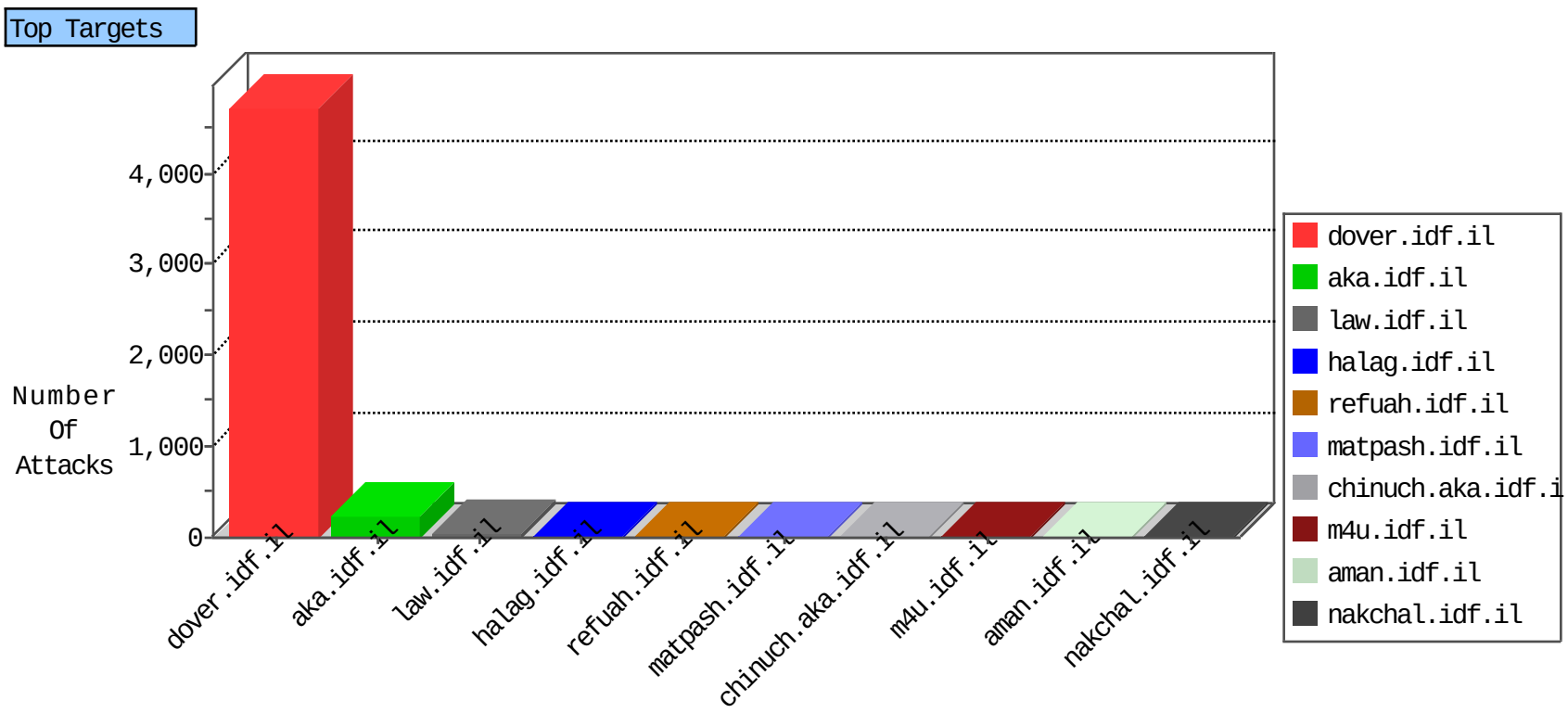
04-09-2016-02:04:09 to 04-09-2016-03:04:09

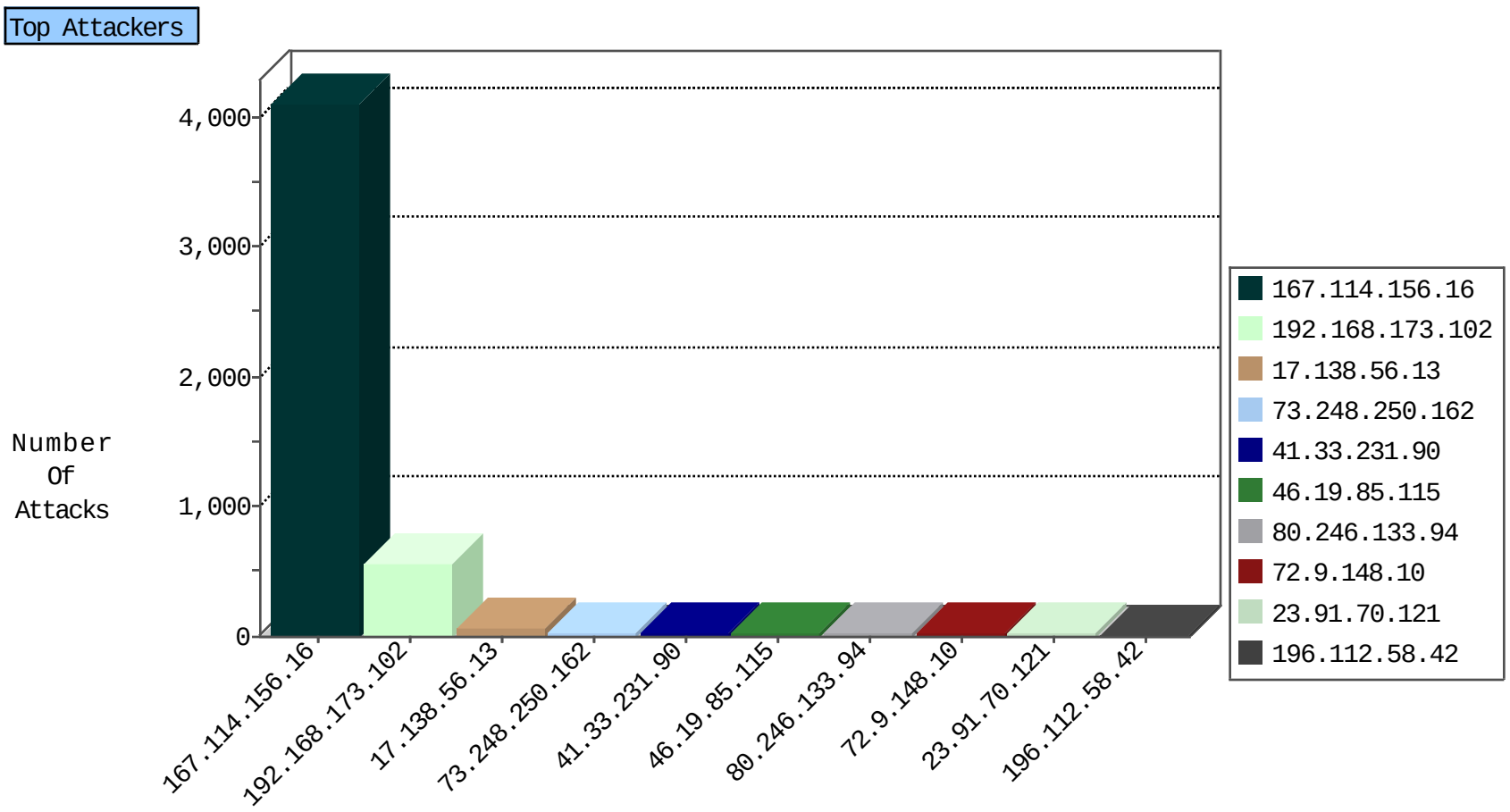
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-09-2016-02:04:09 to 04-09-2016-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4099
181.54.81.104	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3293
46.19.85.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2983
95.145.28.178	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1711
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1297
66.102.9.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	833
199.30.24.246	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	809
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	4
105.91.213.208	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
42.112.10.74	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
109.67.5.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.68	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
37.15.138.133	Spain	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.70	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.93	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1

04-09-2016-02:04:09 to 04-09-2016-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
23.91.70.121	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
23.91.70.121	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
51.254.141.46	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
23.91.70.121	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

04-09-2016-02:04:09 to 04-09-2016-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.121	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.171.122.176	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
104.128.144.131	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -f -sS	1
159.8.100.84	147.237.77.179	France	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
105.91.213.208	147.237.77.216	Egypt	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
104.128.144.131	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
180.76.170.207	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2016-02:04:09 to 04-09-2016-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	357
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	199
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
73.248.250.162	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
80.246.133.94	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
196.112.58.42	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
188.72.103.230	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
50.131.217.141	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
123.126.113.109	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
130.203.136.75	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
94.102.153.58	United Kingdom	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.103.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.106.92.47	Russian Federation	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	3
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
73.171.202.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
118.173.140.248	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.166	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.246.13	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.135.189.99	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
104.148.44.148	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
169.229.3.90	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.62.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
104.148.44.148	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.85.166	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.76.170.207	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
5.29.120.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.188.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.120.173.85	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
218.22.211.69	China	147.237.0.35	akaws.idf.il	drop		drop	1
120.132.68.73	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.207.132.173	Algeria	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
149.78.215.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.128.144.131	Canada	147.237.0.200	m4u.idf.il	drop		drop	1
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

04-09-2016-02:04:09 to 04-09-2016-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
157.55.39.60	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
178.214.94.131	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1226-	Block	1
5.31.187.83	United Arab Emirates	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/writetous/default.asp	None	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
208.115.111.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
5.31.187.83	United Arab Emirates	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
159.203.4.15	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
80.246.133.94	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
31.44.128.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
159.203.4.15	Canada	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/שקופית12	Block	1
123.59.59.52	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.elong.com/894-he/nakhal.aspx	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
169.229.3.90	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/ts.php	Block	1

04-09-2016-02:04:09 to 04-09-2016-03:04:09