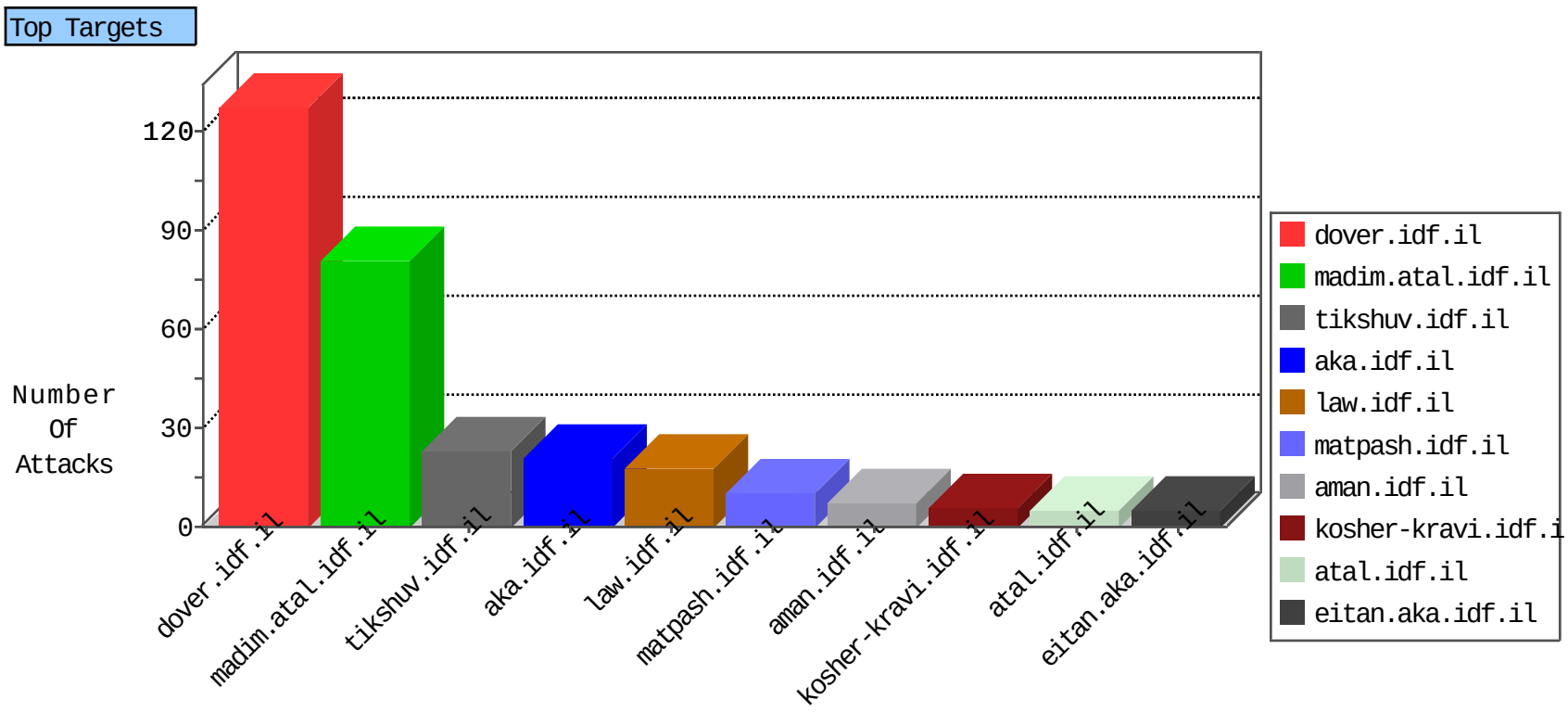
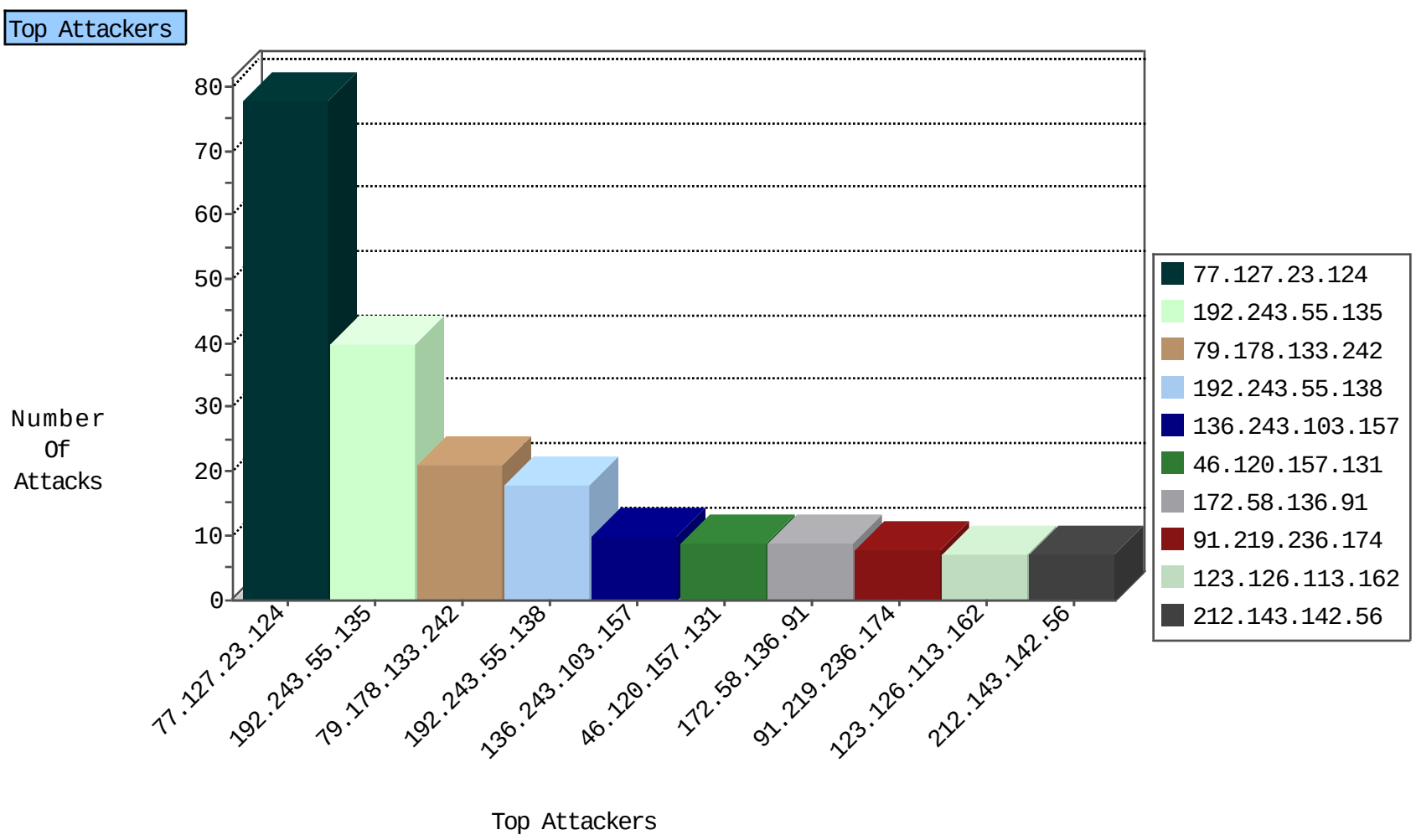
03-05-2016-01:09:27 to 03-05-2016-02:09:27

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-05-2016-01:09:27 to 03-05-2016-02:09:27

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Http	drop	2
61.160.6.152	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	JLM_Purple_Con_Limit_Http	drop	1
203.95.25.20	Japan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
203.95.25.36	Japan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
124.85.117.165	Japan	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

03-05-2016-01:09:27 to 03-05-2016-02:09:27

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
136.243.103.157	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.103.157	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.103.157	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
136.243.103.157	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
49.246.230.40	China	147.237.77.176	matpash.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
136.243.103.157	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

03-05-2016-01:09:27 to 03-05-2016-02:09:27

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
213.136.91.26	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
172.242.12.88	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.227	Canada	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
61.160.6.152	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
172.242.12.88	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-05-2016-01:09:27 to 03-05-2016-02:09:27

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.133.242	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
172.58.136.91	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
91.219.236.174	Hungary	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
63.249.66.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.25.36	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.120.157.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.120.157.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.23.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
78.40.177.35	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.169	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.120.157.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.120.157.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.250.172.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
123.126.113.162	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
190.237.183.224	Peru	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.149.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
123.125.71.54	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.71.235.23	United Kingdom	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.41.177.26		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
45.56.104.218		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.150.193.1	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.183.28.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
37.26.149.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.70	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
103.41.177.26		147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.56.104.218		147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
84.191.15.178	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
37.26.149.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
103.41.177.26		147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1

03-05-2016-01:09:27 to 03-05-2016-02:09:27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.23.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
151.226.168.14	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.89	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
37.142.68.90	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
207.241.229.222	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
77.75.79.11	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.66.64	Block	1
173.252.88.93	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.66.67	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/106675.pdf	Block	1
5.175.0.99	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
66.249.93.48	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/108906.pdf	Block	1
27.33.172.45	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.185	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
66.249.93.52	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
65.55.213.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
151.226.168.14	United Kingdom	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.66.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/5/1125.doc	Block	1
37.142.68.90	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
66.249.93.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1679-18967/dover.aspx	Block	1
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/new	Block	1

03-05-2016-01:09:27 to 03-05-2016-02:09:27