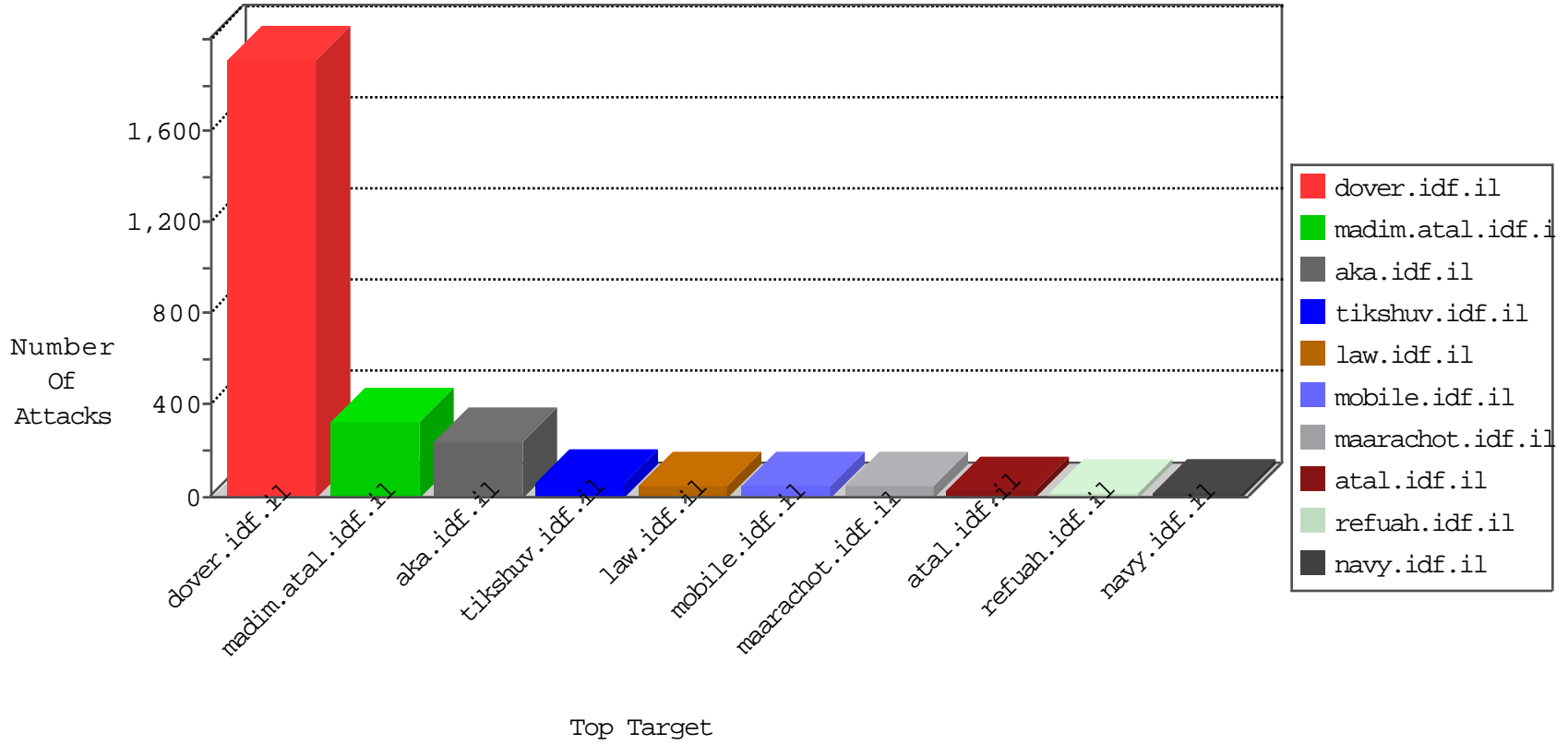


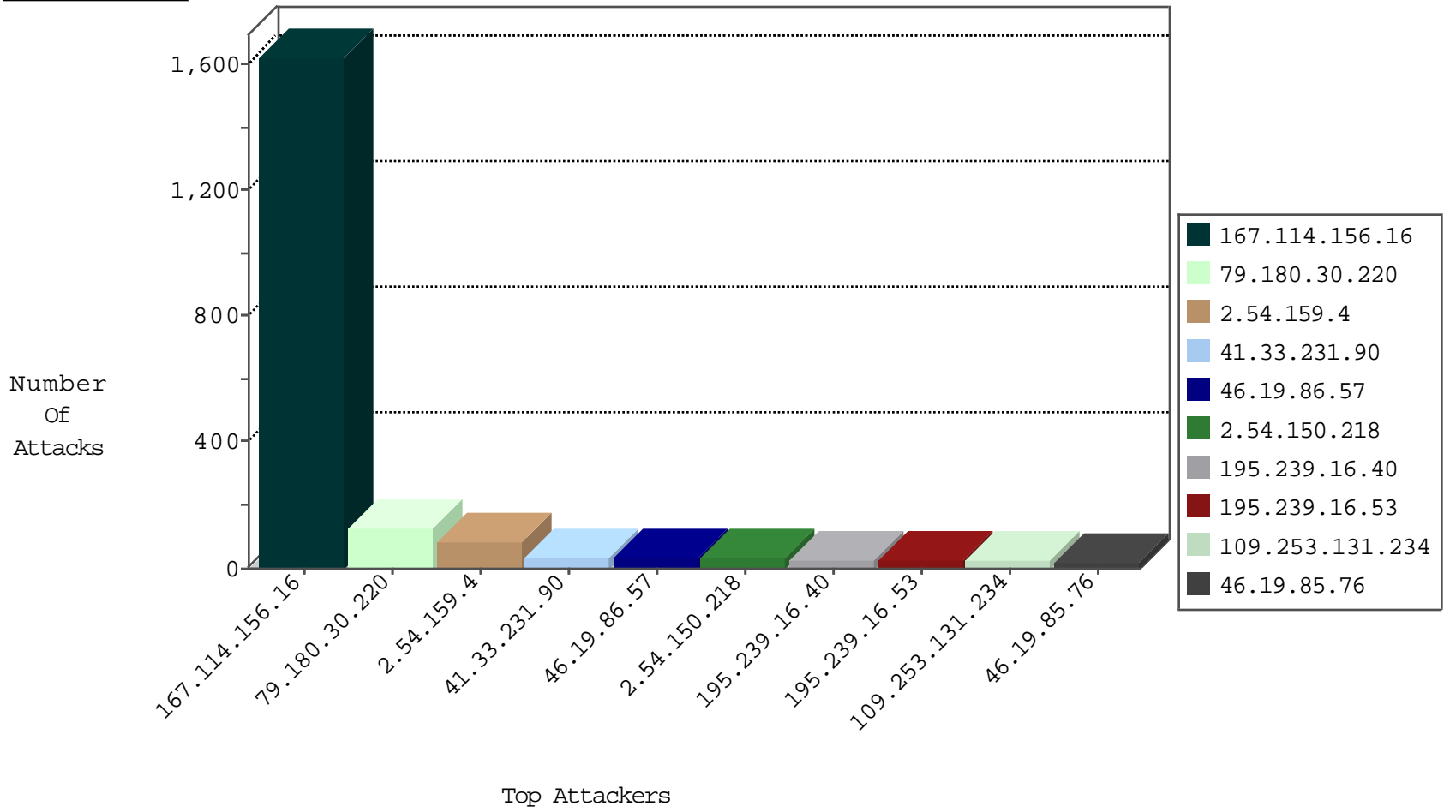
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	DOS-Tool-SwitchbladG	dest-reset	3103
79.181.162.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
77.247.178.132	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
42.2.176.241	Hong Kong	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
77.247.178.132	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

01-03-2016-23:04:06 to 01-04-2016-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.150.218	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	19
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4

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
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
93.172.172.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.131.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.131.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
79.181.162.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
2.54.150.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
217.132.131.205	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
159.203.243.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.254.183	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.159.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
208.54.44.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.130.240	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.173.157.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.215	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.126.225.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.217.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.13.112.122	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.120.130.11	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.180.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
71.199.155.178	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.147.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.127.52.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.117.157.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.124	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.252.89.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
31.13.112.118	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
84.108.62.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.187.251	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
190.105.168.61	Panama	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.13.112.119	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
173.252.89.53	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.54.156.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.30.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.30.220	Block	94
2.54.159.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.180.30.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.54.159.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
176.13.3.179	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.13.3.179	Block	18
109.253.158.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.10.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
94.159.146.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
79.178.198.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
85.65.122.174	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	6
79.180.102.69	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
109.64.138.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.191.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.7.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.160.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.115.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewifpjuzy7kahwdubqkhd3ocpaqfggumai&sig2=yjfyzyuja815dxl4mvo2bq&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	3
46.19.86.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
125.46.26.253	China	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
85.64.115.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
2.54.180.255	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
176.12.150.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	2
77.127.52.21	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
125.46.26.253	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/wp-admin/admin-ajax.php	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.142	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.136.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.22.37.142	Portugal	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=1%7C1; __atuv=568998c60bb40af9000; __atssc=facebook%3B2	Block	1
89.138.188.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
37.26.147.130	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1086-23059-he/dover	Block	1
2.54.174.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.230	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.201.154.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.70.60	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
223.240.126.139	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11435-he/cogat.aspx/trackback/	Block	1
37.46.39.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1086-23059-he/dover	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1