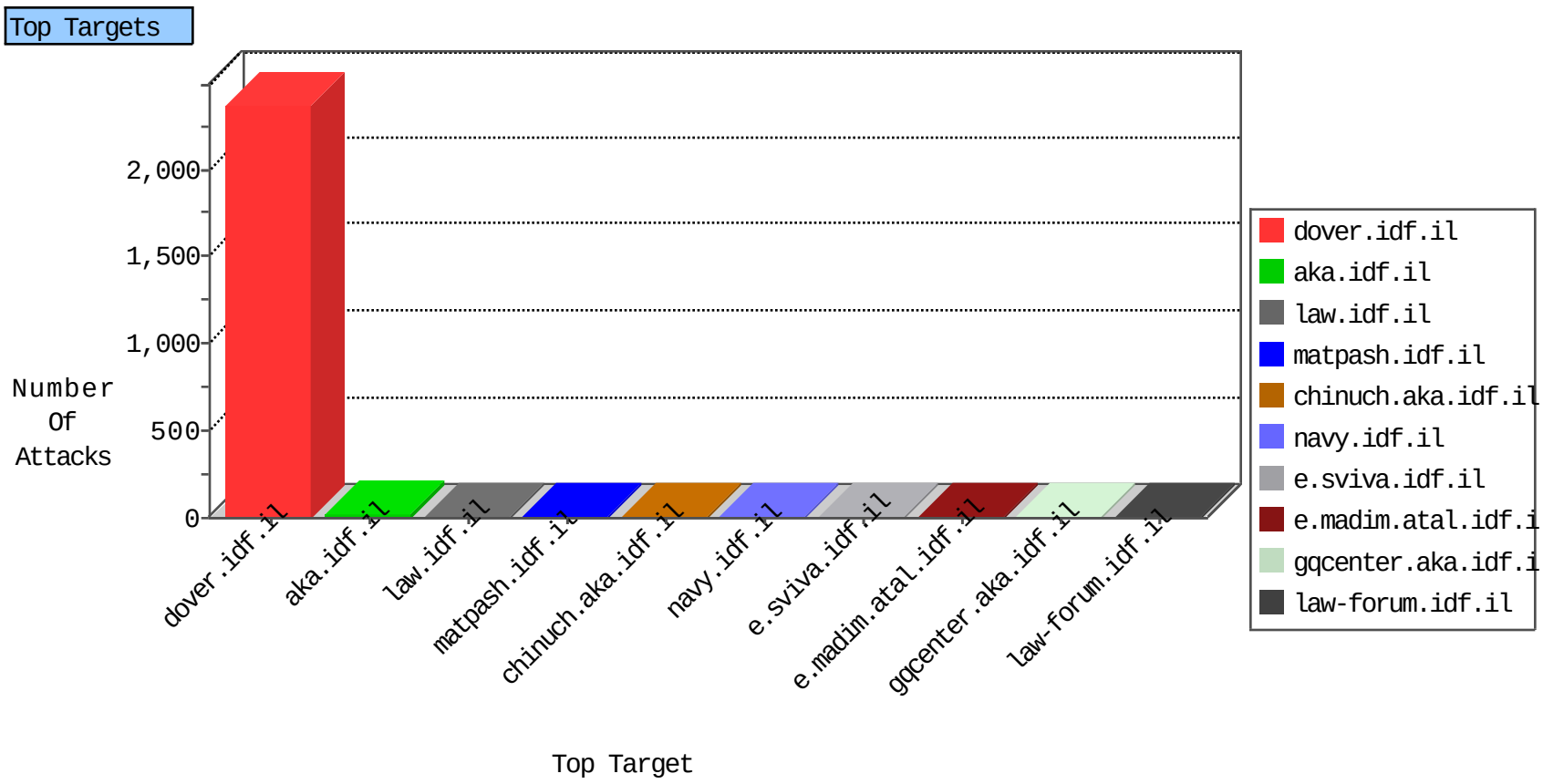
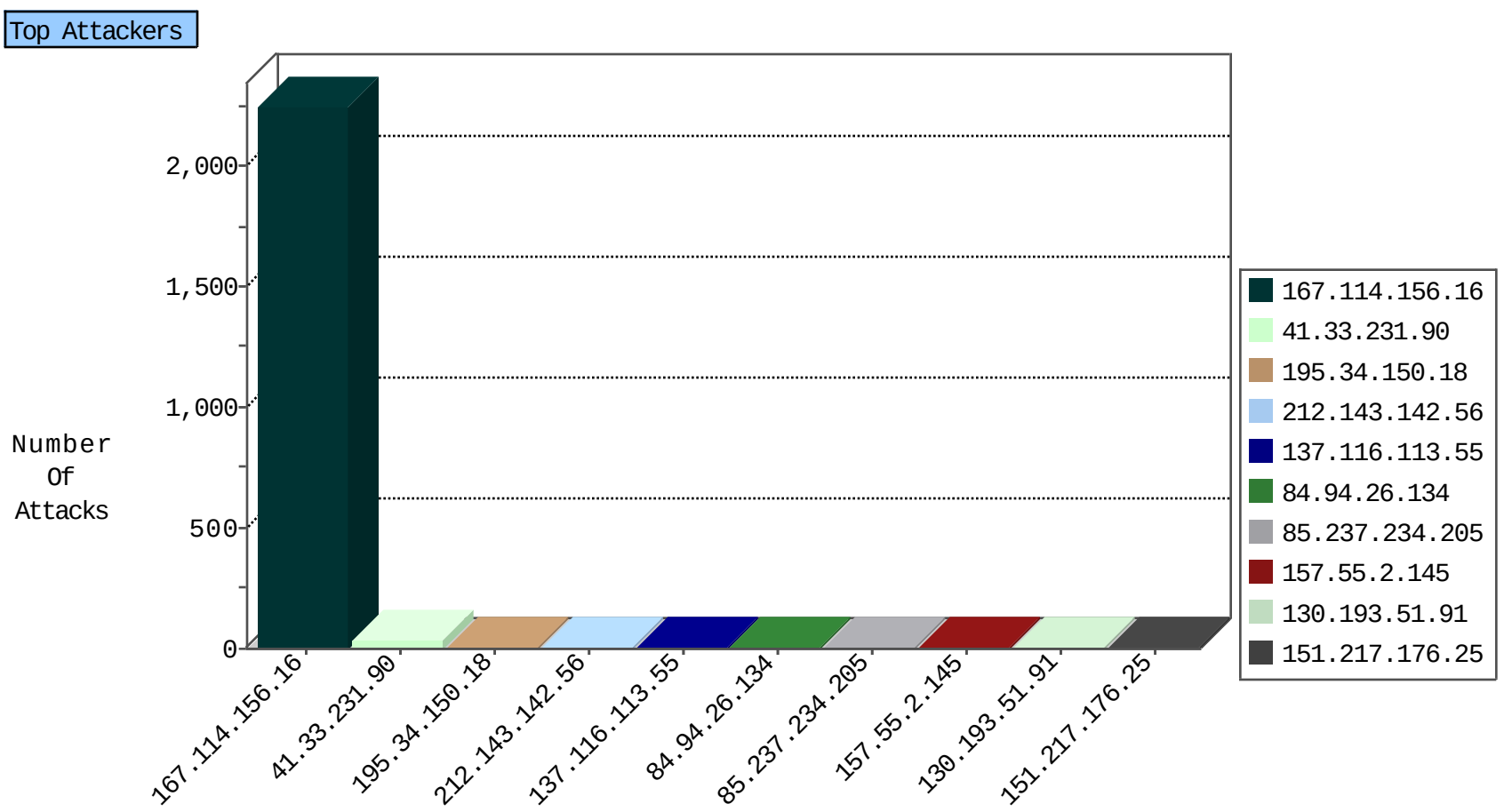
12-28-2015-03:04:01 to 12-28-2015-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015-03:04:01 to 12-28-2015-04:04:01

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	3470

12-28-2015-03:04:01 to 12-28-2015-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-03:04:01 to 12-28-2015-04:04:01

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
137.116.113.55	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
73.17.14.46	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.68	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.169.113.185	147.237.76.196	Singapore	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.36	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
151.217.176.25	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.176.25	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
137.116.113.55	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
137.116.113.55	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
137.116.113.55	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.114	147.237.77.74	Ukraine	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
151.217.178.68	147.237.77.176		matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.169.113.185	147.237.76.196	Singapore	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.63	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.36	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
151.217.176.25	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
137.116.113.55	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
137.116.113.55	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1

12-28-2015-03:04:01 to 12-28-2015-04:04:01

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	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.237.234.205	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
157.55.2.145	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.94.26.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.175.193.232	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.94.26.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.140.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.232.110.28	United Kingdom	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.53.21.212	Turkey	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.230.230.230	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.171	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.24.144	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
73.17.14.46	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.69.172.227	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.103	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
107.170.123.11	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
178.217.187.39	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.172	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.36.197	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
90.219.71.211	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.165.230.5	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.104	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.70	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.10.71.107	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
68.10.249.105	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
146.185.239.102	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
37.187.114.171	France	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.154.146.225	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.109	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.60.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.42.116.16	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
72.194.64.75	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.102	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.242.228.108	Luxembourg	147.237.77.216	dover.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

12-28-2015-03:04:01 to 12-28-2015-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.109	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
173.254.21.120	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
95.65.34.177	Moldova, Republic of	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
141.212.122.97	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
81.169.237.146	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
2.54.26.39	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
180.76.15.18	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.170.123.11	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
141.212.122.97	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
37.26.146.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.134	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.134	United States	147.237.72.166	aka.idf.il	Unknown Parameter 6683f660 in www.aka.idf.il/main/home/default.aspx	None	1
157.55.39.26	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
94.23.12.182	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
40.77.167.8	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/tz	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.254.21.120	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
94.23.12.182	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.234.59.32	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
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	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/home	Block	1

12-28-2015-03:04:01 to 12-28-2015-04:04:01