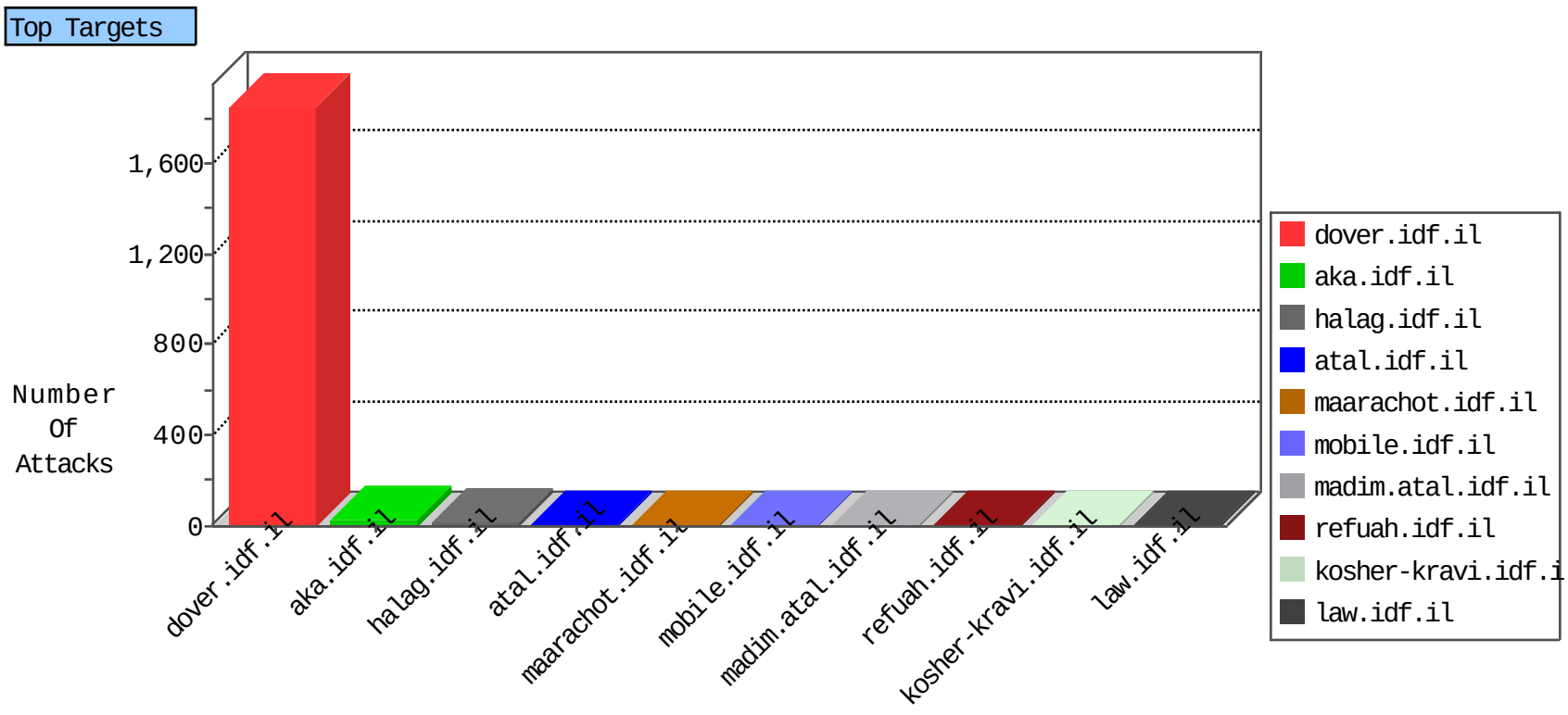
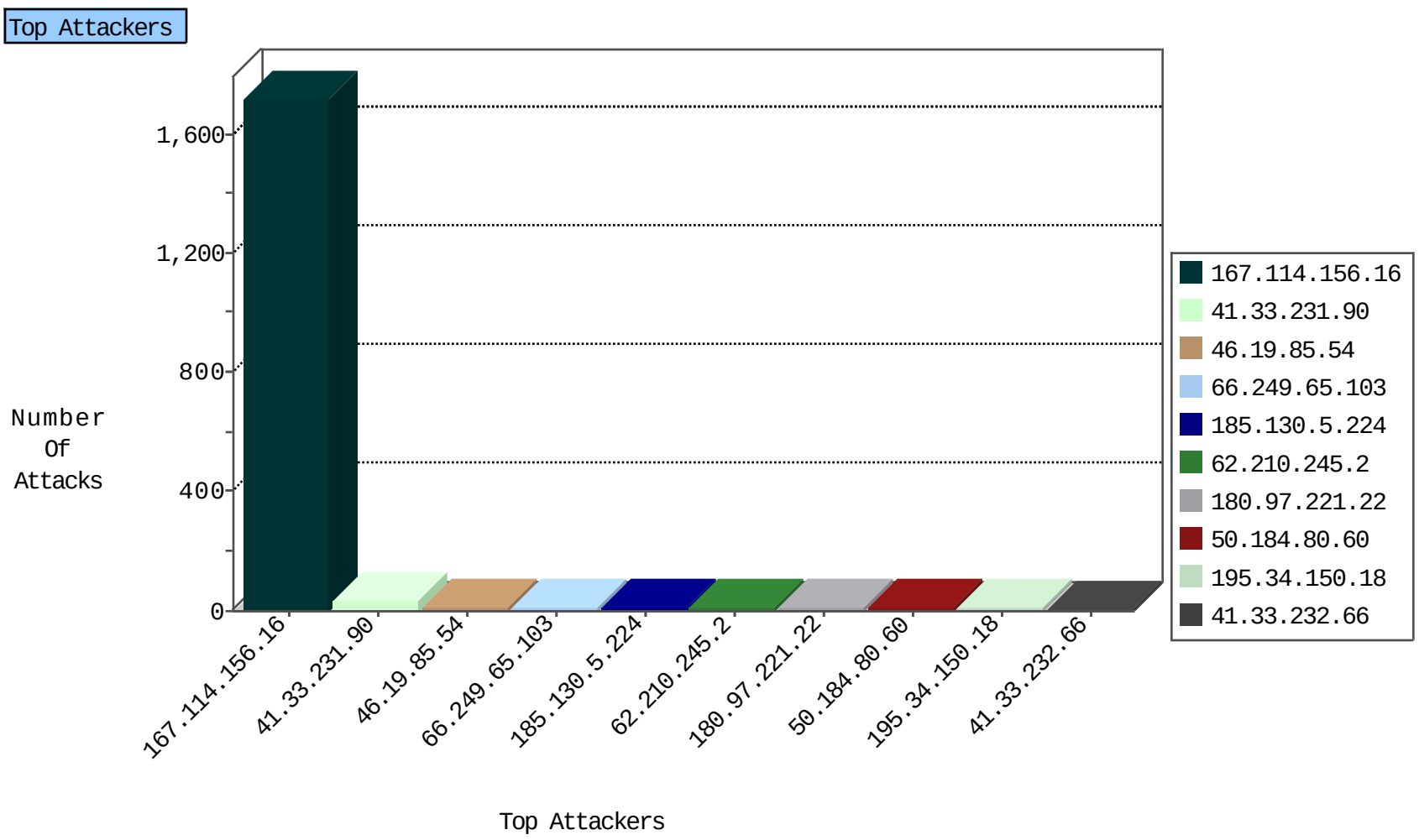
01-04-2016-03:04:09 to 01-04-2016-04:04:09

IDF Under Attack Daily Report





01-04-2016-03:04:09 to 01-04-2016-04:04:09

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	DOS-Tool-SwitchbladG	dest-reset	3198
66.249.69.93	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	556
50.172.79.15	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-04-2016-03:04:09 to 01-04-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-04-2016-03:04:09 to 01-04-2016-04:04:09

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
62.210.245.2	147.237.77.216	France	dover.idf.il	ET WEB_SERVER ColdFusion administrator access	1
62.210.245.2	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET WEB_SERVER ColdFusion administrator access	1
209.126.116.147	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
192.186.95.178	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.221.22	147.237.77.233	China	atal.idf.il	SQL generic sql with comments injection attempt - GET parameter	1
180.97.221.22	147.237.77.233	China	atal.idf.il	SQL 1 = 1 - possible sql injection attempt	1
180.97.221.22	147.237.77.233	China	atal.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	1
62.210.245.2	147.237.77.216	France	dover.idf.il	POLICY-OTHER Adobe ColdFusion admin interface access attempt	1
62.210.245.2	147.237.0.17	France	m.my-kosher-kravi.idf.il	POLICY-OTHER Adobe ColdFusion admin interface access attempt	1
52.48.37.125	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.221.22	147.237.77.233	China	atal.idf.il	SQL Injection - Select From	1
180.97.221.22	147.237.77.233	China	atal.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1
180.97.221.22	147.237.77.233	China	atal.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	1

01-04-2016-03:04:09 to 01-04-2016-04:04:09

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
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
50.184.80.60	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.54	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
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.127.233.192	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.208.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
96.224.13.26	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.187.253.17	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.114.91.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.19.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.30.238	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
66.249.65.109	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.45.132.180	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
37.26.147.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
216.218.206.80	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
157.55.39.240	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.230.151	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
84.109.116.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.210.245.2	France	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
185.130.5.224		147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
38.229.1.15	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
93.174.93.203	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.80	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.16	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.224		147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
5.102.254.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
108.168.102.23	Canada	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
85.65.6.28	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
62.210.245.2	France	147.237.0.33	idf.il	drop		drop	1
185.130.5.224		147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
149.254.235.106	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
95.35.54.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
172.56.18.239	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.24.185.147	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
85.65.6.28	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
62.210.245.2	France	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.23.210.58	France	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
109.201.152.24	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.94.176.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.210.245.2	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/cfide/administrator/	Block	1
37.142.226.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1
94.23.210.58	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
46.43.185.41	United Kingdom	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.43.185.41 (Unknown SSL Session)	None	1
180.97.221.22	China	147.237.77.233	atal.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 180.97.221.22	None	1
89.138.35.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
40.77.167.26	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
107.178.194.79	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	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
46.43.185.41	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.97.221.22	China	147.237.77.233	atal.idf.il	Multiple signatures from 180.97.221.22	Block	1
94.23.210.58	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
210.87.255.225	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 210.87.255.225	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
62.210.105.116	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
180.97.221.22	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/news/html/	Block	1
2.54.44.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.23.210.58	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19708-he/dover.aspx	Block	1
210.87.255.225	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.176.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.210.245.2	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/cfide/administrator/	Block	1
197.231.221.211	Liberia	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
37.142.68.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1