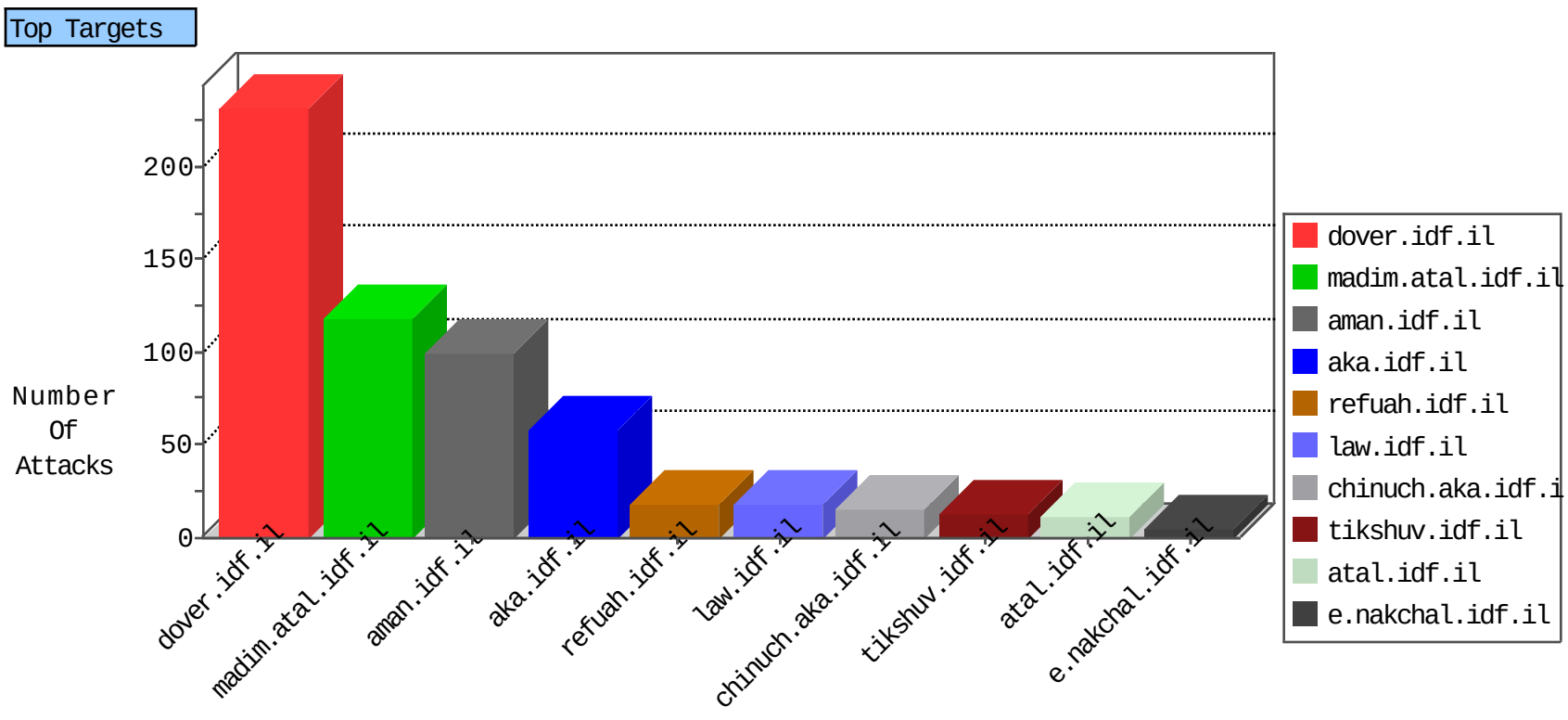
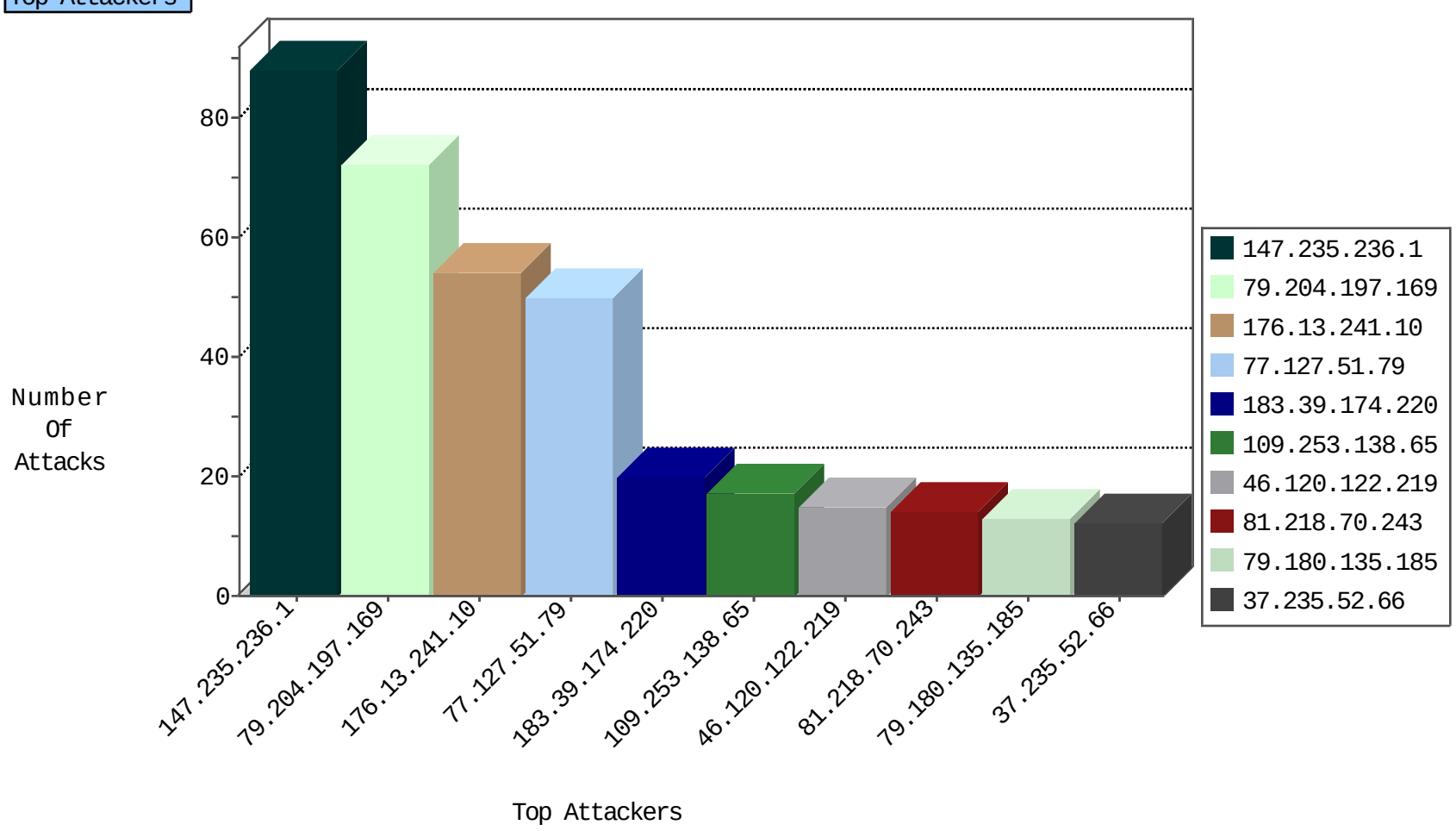
08-29-2016-17:04:01 to 08-29-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-29-2016-17:04:01 to 08-29-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.226.217.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.253.138.202	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
120.132.50.135	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
123.59.59.52	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
178.239.62.141	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
104.238.184.170	United Kingdom	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
109.241.231.15	Poland	147.237.77.243	mobile.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

08-29-2016-17:04:01 to 08-29-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.6.49	Lithuania	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.129.62.63	Denmark	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
185.130.6.49	Lithuania	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

08-29-2016-17:04:01 to 08-29-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.114.5	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	6
183.39.174.220	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	2
183.39.174.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
183.39.174.220	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	2
82.81.215.221	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
37.235.52.66	147.237.8.24	Chile	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
132.70.66.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.154.81.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.75.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.177.110	147.237.72.156	France	aman.idf.il	portscan: TCP Distributed Portscan	1
13.89.50.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.23.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.214.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.6.49	147.237.77.216	Lithuania	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
5.29.90.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.235.52.66	147.237.77.205	Chile	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
185.32.179.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.190.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.235.52.66	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
87.68.25.44	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
37.235.52.66	147.237.76.86	Chile	navy.idf.il	ET SCAN Potential SSH Scan	1
183.39.174.220	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
84.111.100.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
154.16.199.49	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
37.235.52.66	147.237.72.166	Chile	aka.idf.il	ET SCAN Potential SSH Scan	1
183.39.174.220	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.80.59.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.235.52.66	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.49	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.246.138.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.235.52.66	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.253.197.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.105.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
24.105.159.242	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.188.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.58.90	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
183.39.174.220	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
5.29.213.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.214.104	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
199.203.68.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.235.52.66	147.237.77.233	Chile	atal.idf.il	ET SCAN Potential SSH Scan	1

08-29-2016-17:04:01 to 08-29-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
147.235.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
79.204.197.169	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
109.253.138.65	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
79.180.135.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
192.95.22.82	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
12.27.109.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
131.82.74.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.212.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.54.104.126	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.198	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.100	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
109.66.9.96	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
176.13.228.69	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
46.120.122.219	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.199.105	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
46.253.93.137	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.3.223	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
217.10.240.82	Bulgaria	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.120.122.219	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
46.120.122.219	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
2.54.104.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
71.6.216.50	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.179	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.248	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
85.130.190.227	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
188.126.80.52	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.26.146.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.222.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.23.224	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
2.53.151.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.209.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
100.92.0.156		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
54.169.197.38	Singapore	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.210.94	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
54.169.197.38	Singapore	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
139.162.37.113	United States	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.136.212	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.251.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.211.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.241.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
77.127.51.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
85.65.165.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
109.253.193.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.67.27.210	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
89.164.11.68	Croatia	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
212.199.16.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	5
85.64.48.180	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
212.199.108.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.108.62	Block	4
2.53.169.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.118	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
195.200.205.35	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.225.134	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
89.139.96.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.3.123	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	2
2.55.9.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
158.194.110.11	Czech Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.132.124.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
176.13.228.69	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
99.31.227.98	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
109.65.3.43	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
212.199.16.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.16.193	Block	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/scroller/jquery.jcarousel.js	None	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
109.253.138.65	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
75.101.174.81	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
101.178.206.92	Australia	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/broadweb/bwroot.asp	Block	1
195.200.205.35	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 195.200.205.35	Block	1
148.75.91.245	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/jquery/global.js	None	1
109.65.188.91	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.187.91	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
37.26.147.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
192.118.27.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.118.27.253	Block	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/sidebar/sidebar.js	None	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/scriptresource.axd	None	1
101.178.206.92	Australia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 101.178.206.92	Block	1
77.126.68.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
82.81.50.127	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.200.205.35	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/6/	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/theproj/	Block	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/jquery/jquery-1.4.2.min.js	None	1
79.179.114.5	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
212.199.108.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/mitgaysim	Block	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/ui/ui.datepicker.js	None	1
192.118.27.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
81.218.70.243	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/shared/clientscripts/jquery.plugins/jquery.charts.js	None	1
109.253.205.245	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1