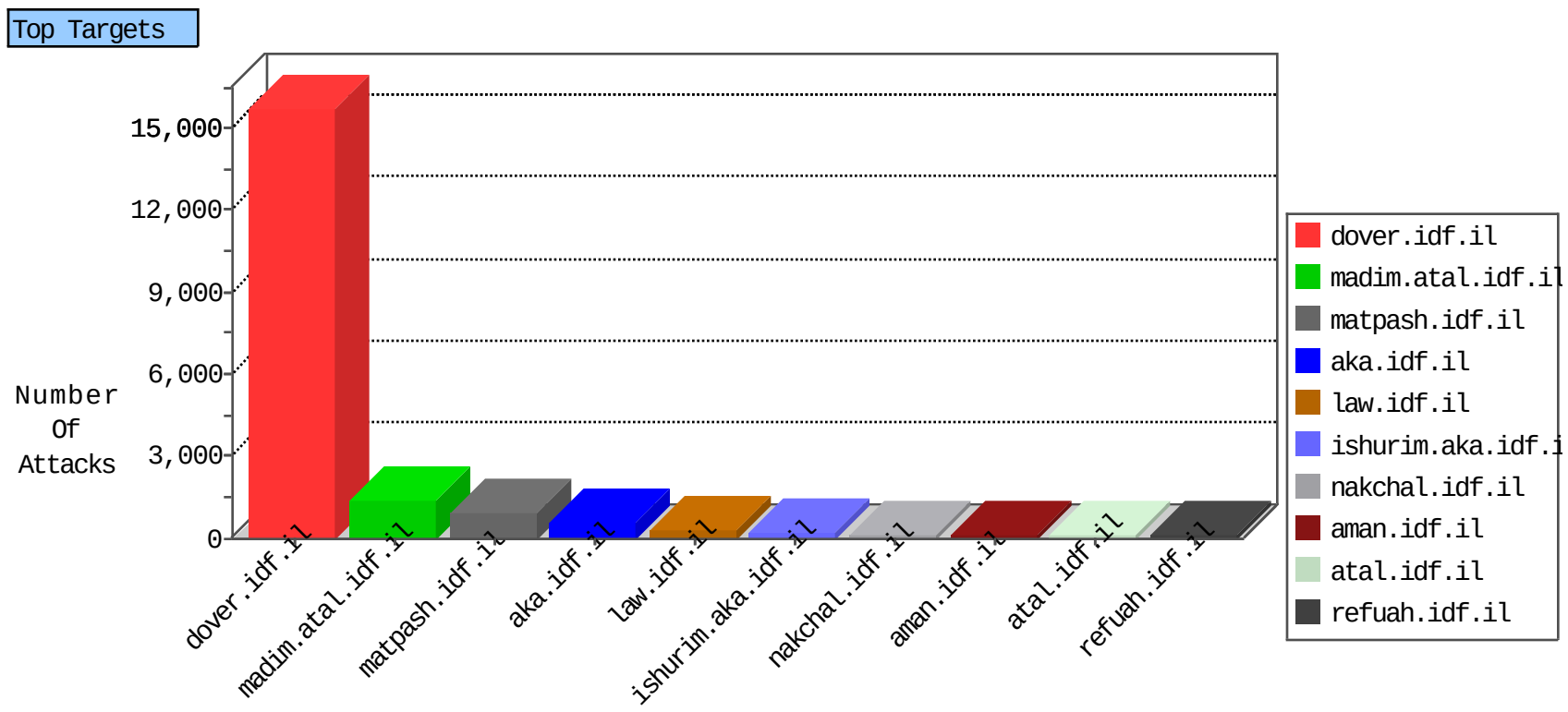
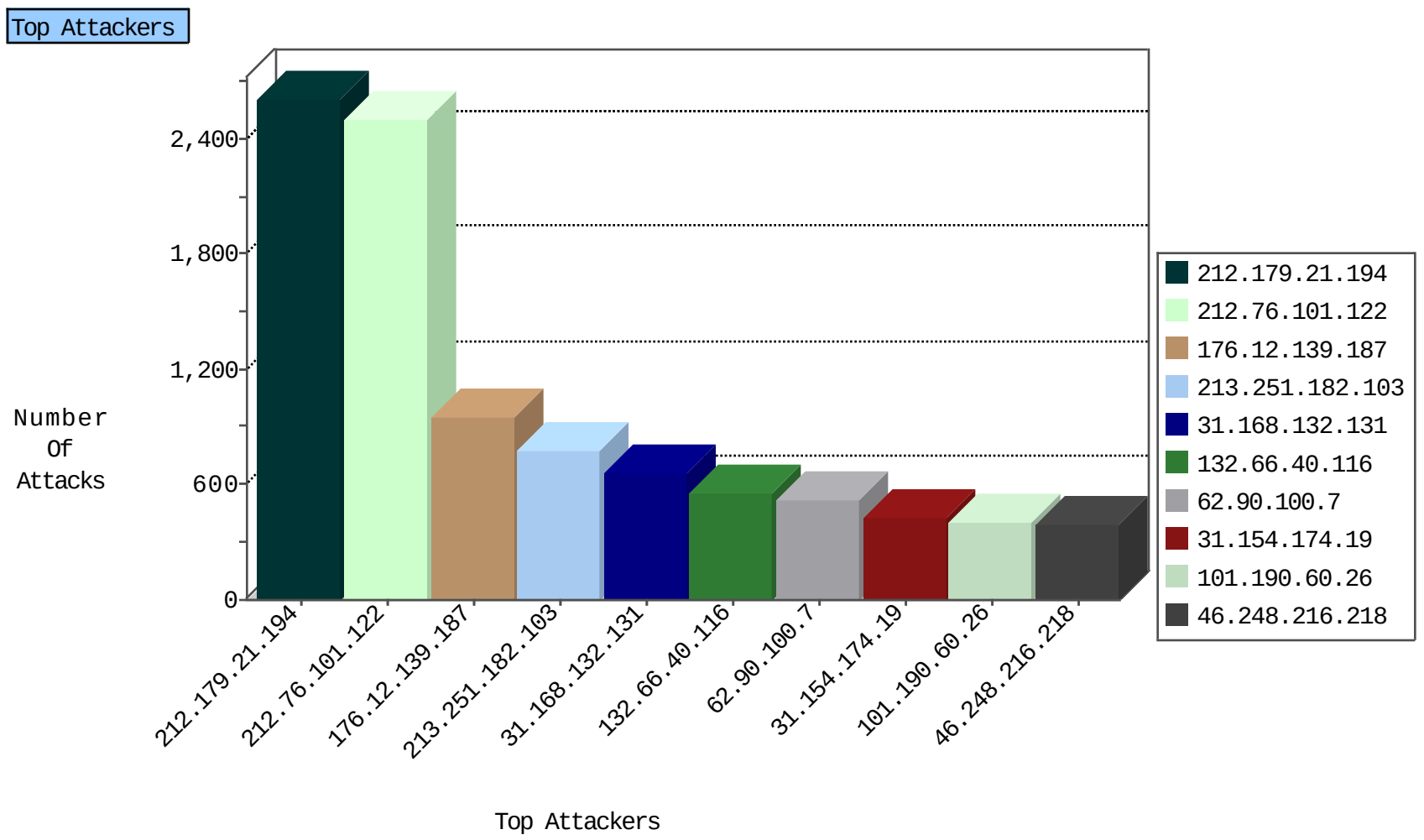
10-21-2015-12:04:08 to 10-21-2015-13:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-12:04:08 to 10-21-2015-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11960
80.246.139.208	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	100
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	84
2.54.31.199	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	42
109.64.56.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
81.218.116.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.182.125.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	22
176.13.7.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
176.12.148.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.12.150.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
109.66.41.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.43.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
77.158.88.40	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
94.76.42.77	Bahrain	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.179.131.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.244.83.216	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
107.6.142.106	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
197.44.184.20	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.154.165.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.179.62.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.133.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.13.231	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.157.141.171	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.180.147.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.64.208.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.47.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.137.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
85.114.104.171	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	3
37.208.141.60	Qatar	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.60.12.140	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.146.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
31.154.150.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.43.75.223	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.6.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.60.4.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.64.56.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
99.51.233.158	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.229.183.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.16.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.67.100.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
95.86.124.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.149.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.51.211.31	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
197.53.9.75	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-21-2015-12:04:08 to 10-21-2015-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.160.240.11	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-21-2015-12:04:08 to 10-21-2015-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.85	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
213.57.109.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.87.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.37.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.92.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.120.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.180.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-21-2015-12:04:08 to 10-21-2015-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2527
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2502
31.168.132.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	654
132.66.40.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	552
62.90.100.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	515
101.190.60.26	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	405
46.248.216.218	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	392
50.118.172.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	236
185.9.137.3	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	199
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	180
217.64.86.6	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
2.54.47.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	147
5.245.158.187	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
213.151.37.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
92.241.32.244	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
41.44.37.205	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
77.125.123.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
45.97.48.147		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
95.86.124.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
77.158.88.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
185.19.223.58	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
213.139.52.31	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
141.0.15.183	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
197.44.184.20	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
37.39.121.46	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
107.6.142.106	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
65.255.37.150	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
89.167.129.96	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
5.29.133.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
176.13.18.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
62.90.131.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.231.22.111	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.145.221.7	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.67.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.67.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
185.19.221.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.139.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	949
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	780
31.154.174.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	429
82.166.238.242	Israel	147.237.77.74	law.idf.il	Parameter Type Violation prefixText in www.mag.idf.il/webservices/wscity.asmx/getcities	Block	247
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	78
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	78
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	39
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	39
176.12.150.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	26
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	26
2.54.187.223	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/favicon.ico	Block	13
208.113.155.237	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	13
85.250.233.93	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
79.177.28.171	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	13
107.6.142.106	Netherlands	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	13
31.168.216.252	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	13
217.69.133.192	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	13
195.154.177.67	France	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	13
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
125.71.41.56	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15916-en/dover.aspx/trackback/	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	13
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
5.28.184.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	13
212.179.21.194	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	13
88.75.182.131	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
79.179.131.80	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	13
180.153.186.92	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js%3fsiteversion	Block	13
37.26.147.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
198.1.101.123	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
141.212.122.64	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	13
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
93.172.12.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
5.28.190.91	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	13
212.179.197.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
79.183.37.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
182.118.70.228	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/scriptresource.axd%3fd	Block	13
109.64.204.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	13
46.120.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	13
2.54.6.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
207.46.13.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
84.108.108.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
107.6.142.106	Netherlands	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 107.6.142.106 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	13
14.219.45.203	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/window.location.href	Block	13
79.183.50.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	13
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	13
109.66.41.225	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	13
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13