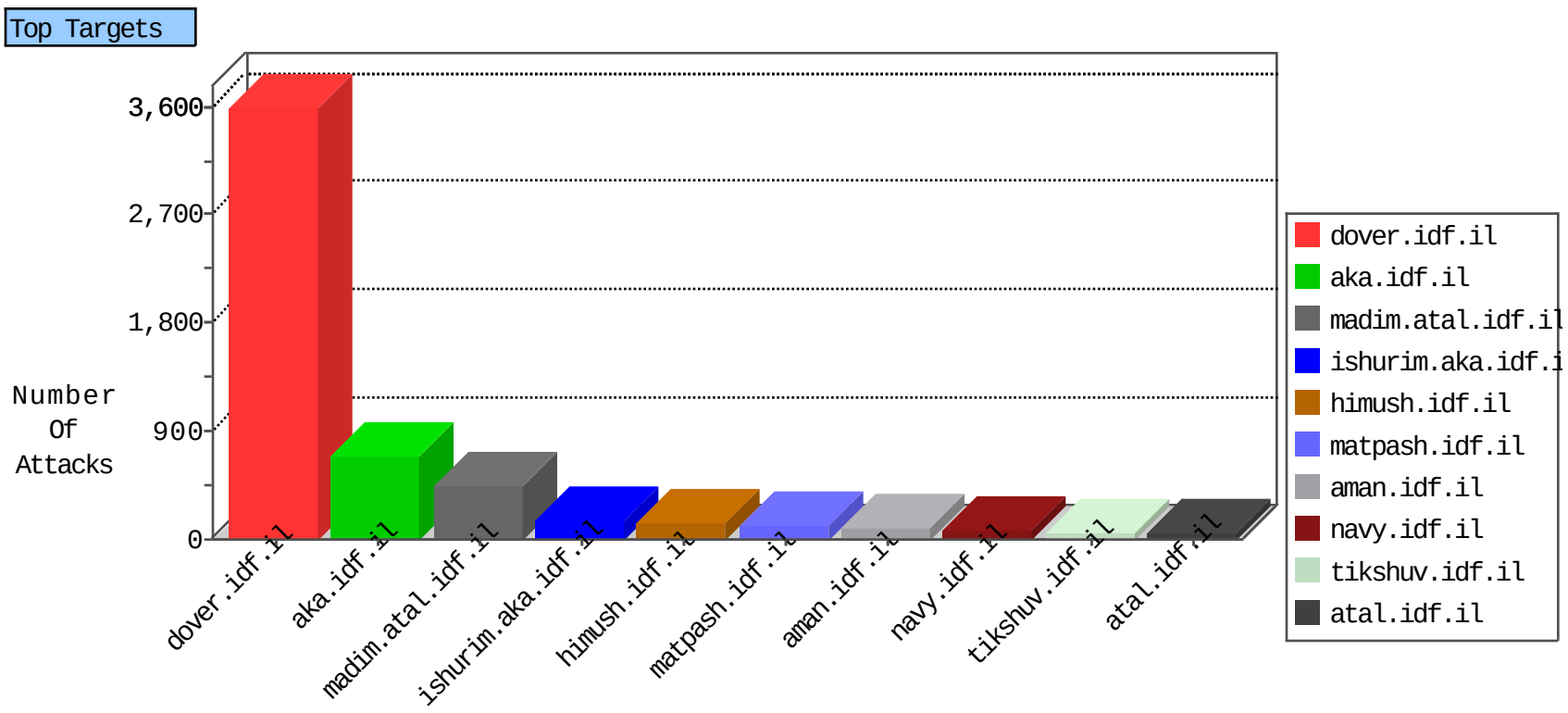
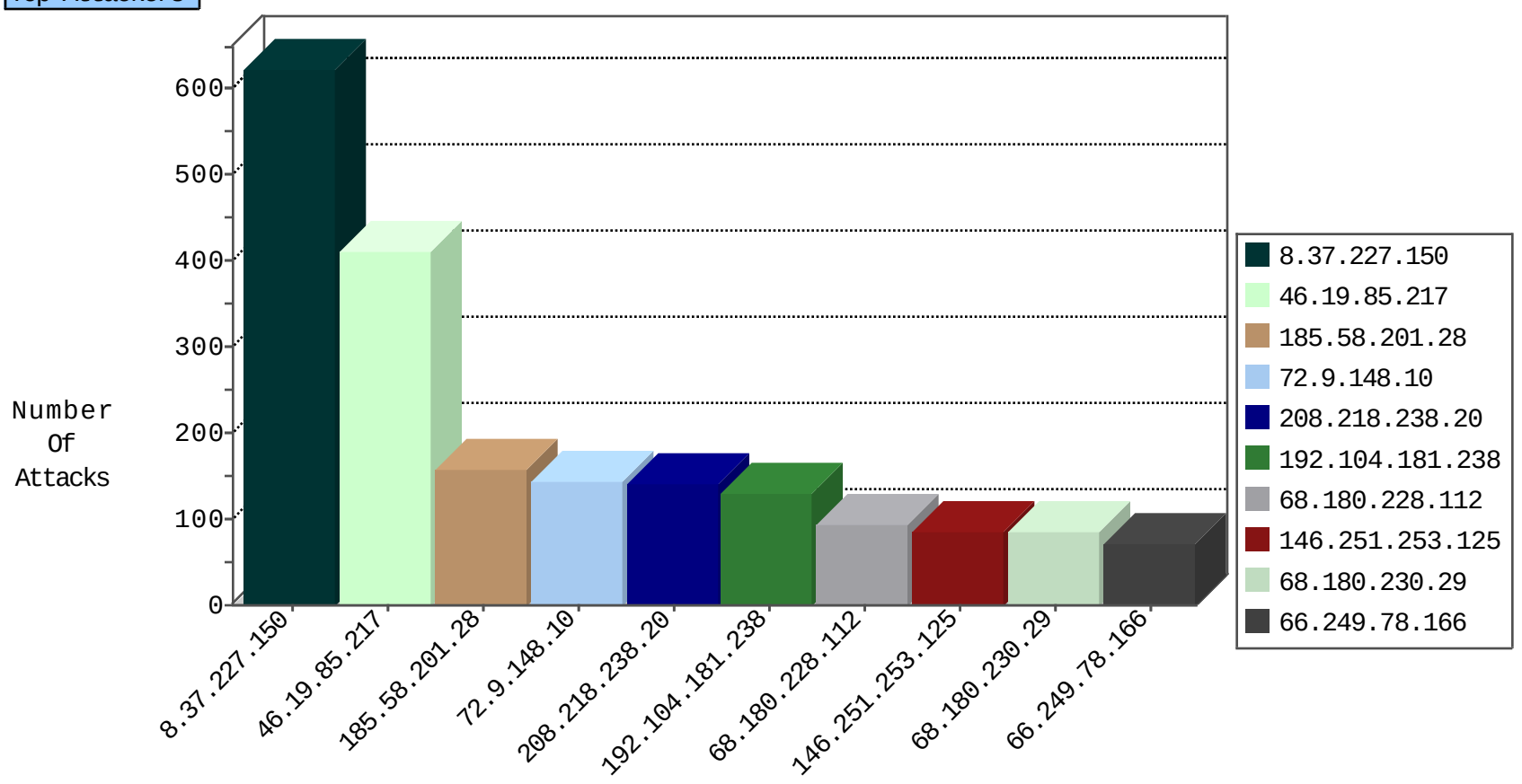
10-26-2015-22:04:07 to 10-26-2015-23:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-26-2015-22:04:07 to 10-26-2015-23:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.110	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	516
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	318
2.52.139.192	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	132
5.22.130.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	87
176.13.21.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	61
31.151.248.145	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
46.19.86.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.181.186.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.181.186.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	22
109.66.3.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
109.65.34.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
192.116.177.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
2.52.38.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
84.111.164.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
209.150.88.155	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
176.13.18.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.1.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.67.57.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
192.34.76.178	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.85.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.66.104.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.180.55.61	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.228.68.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.2.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
95.86.66.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.149.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.228.222.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.52.33.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.186.185.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.78.96.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.78.176.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
209.150.88.155	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.146.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.188.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.111.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.2.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
159.54.138.10	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.16.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.101.23.252	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.172.38.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.39.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.20.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.109.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.168.200.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.138.46.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.8.65.135	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.128.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.139.52.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-26-2015-22:04:07 to 10-26-2015-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.242	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
46.252.131.34	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

10-26-2015-22:04:07 to 10-26-2015-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-26-2015-22:04:07 to 10-26-2015-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.227.150	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	617
208.218.238.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
192.104.181.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	129
146.251.253.125	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	69
95.86.67.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
213.204.101.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
89.187.142.208	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
37.142.100.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
149.255.204.18	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
46.19.86.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.43.75.156	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
192.34.76.178	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
131.253.25.203	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
5.22.130.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.16.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
199.72.36.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
93.172.38.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.78.96.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
12.183.151.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.201.193.102	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.185.0.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.146.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.31.171		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
159.54.138.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.46.39.245	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.109.127.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.116.177.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.67.134.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.209.6.71	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.26.146.167	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
109.66.43.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12

10-26-2015-22:04:07 to 10-26-2015-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	406
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	70
93.125.99.34	Belarus	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.125.99.34	Block	56
72.9.148.10	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	56
84.228.200.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	56
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	56
80.179.141.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
75.139.60.176	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	28
72.9.148.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
84.111.241.179	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	28
178.62.209.185	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllyta2ltawms5kb2m=&infocenteritem=true	Block	14
79.176.126.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
148.251.137.43	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 148.251.137.43	Block	14
2.54.151.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
84.109.127.85	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	14
218.200.139.242	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	14
173.252.120.109	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	14
105.158.217.42	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	14
62.210.88.201	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.google.pl/search	Block	14
185.101.107.189		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	14
79.183.23.89	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
149.78.6.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
93.125.99.34	Belarus	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	14
84.110.145.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.12.141.94	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	14
109.64.126.50	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
87.69.124.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.165.15.108	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	14
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	14
149.88.8.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
93.172.110.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
84.111.180.70	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 84.111.180.70 (Open Mode)	None	14
176.13.0.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
109.65.34.118	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
2.54.16.167	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
81.218.151.16	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
195.154.227.118	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/	Block	14
173.252.90.229	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	14
93.172.188.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	14
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
84.111.180.70	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
176.13.22.238	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	14

10-26-2015-22:04:07 to 10-26-2015-23:04:07