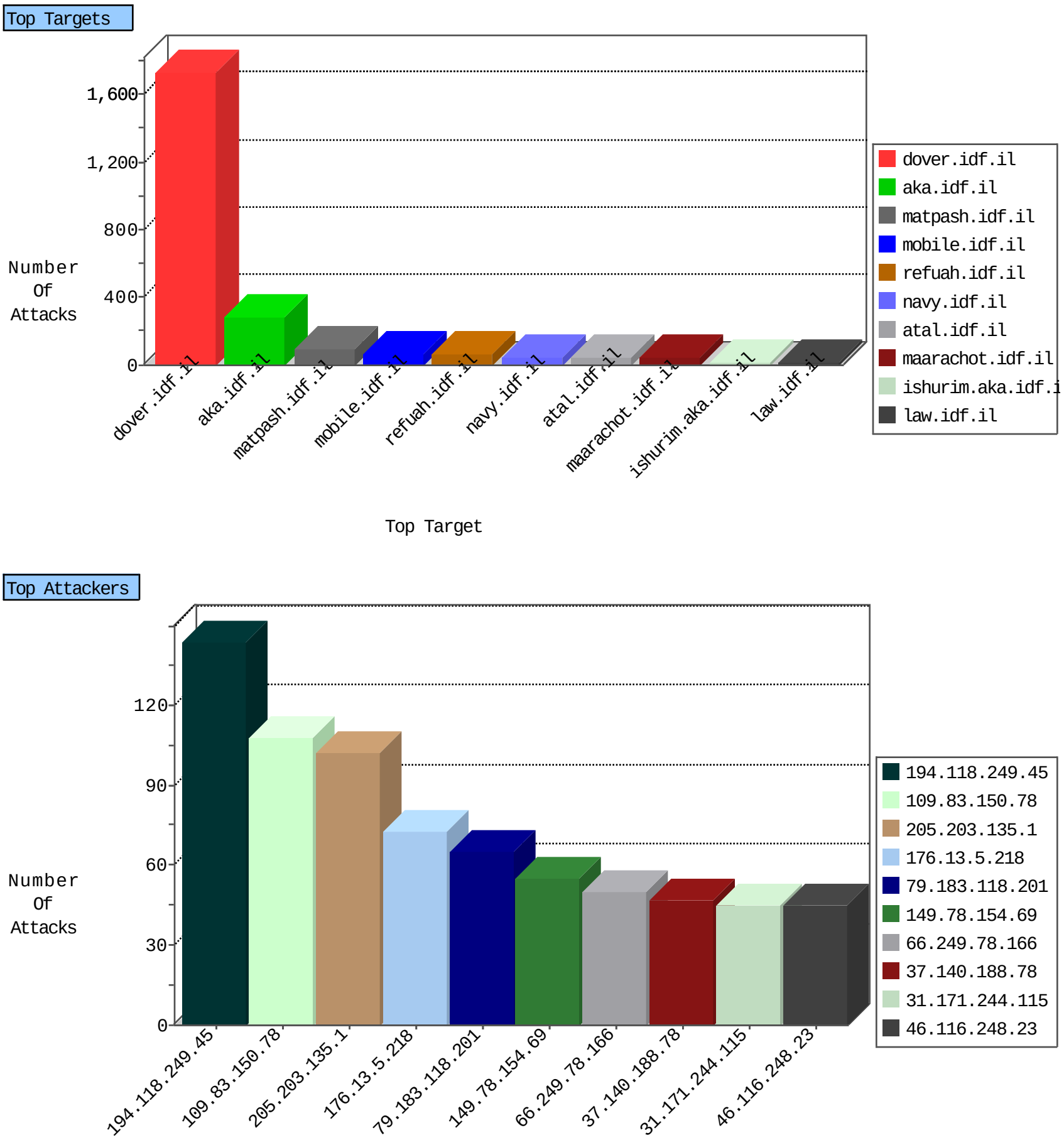
10-31-2015-09:04:08 to 10-31-2015-10:04:08

IDF Under Attack Daily Report



10-31-2015-09:04:08 to 10-31-2015-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3281
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1132
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	706
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
79.178.176.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
185.32.179.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
46.120.61.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
2.54.160.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
93.172.4.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.120.61.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
195.91.216.59	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
5.29.187.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.29.236.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.66.209.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.123.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.126.43.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.163.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.19.85.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.127.173.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.30.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.0.114.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.160.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
62.0.114.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.160.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.45.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.19.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.66.26.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.9.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
81.218.15.194	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.il	Block_Udp_All_Nets	drop	3
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
120.32.199.207	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
202.106.211.99	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
176.2.86.214	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.181.163.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.125.75.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.19.85.78	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
85.65.185.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
77.127.173.234	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.117.76.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.30.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

10-31-2015-09:04:08 to 10-31-2015-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.0.139.152	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	19
69.113.124.178	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-31-2015-09:04:08 to 10-31-2015-10:04:08

Top Attackers In IDS

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

10-31-2015-09:04:08 to 10-31-2015-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.118.249.45	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	144
109.83.150.78	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
176.13.5.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
79.183.118.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
46.116.248.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
62.198.213.171	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
77.125.14.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.220.68.242	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
41.220.68.243	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
185.32.179.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
195.91.216.59	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.29.187.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.4.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.130.165	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.220.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.183.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.90.128.174	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.57.128.221	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
168.235.195.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
117.193.74.179	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.2.86.214	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.66.190.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.18.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
5.28.133.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.76.214.224	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.75.77.123	Czech Republic	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.108.64		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.128.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	30
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
52.2.65.189	United States	147.237.77.176	matpash.idf.il	Directory Traversal - 16	Block	15
31.215.221.243	United Arab Emirates	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	15
184.105.139.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2883.pdf	Block	15
66.249.67.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/9/107829.pdf	Block	15
46.117.245.187	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
141.212.121.192	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	15
66.249.69.34	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1150-en/hamaz.aspx	Block	15
65.78.117.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	15
31.215.221.243	United Arab Emirates	147.237.77.216	dover.idf.il	eMail Hoarding	Block	15
188.40.123.141	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/test-for-404-page	Block	15
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2882.pdf	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
46.121.108.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
149.88.136.11	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	15
66.249.74.100	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/21032011sufa.aspx	Block	15
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	15
37.142.68.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/	None	15
207.46.13.100	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3367	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.121.113.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	15
207.46.13.113	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
37.142.68.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/main/home/default.aspx	None	15
79.177.183.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	15
66.249.67.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
52.2.65.189	United States	147.237.77.176	matpash.idf.il	Directory Traversal (In URL)	Block	15
2.54.160.181	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	15
176.12.148.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2881.pdf	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	15
213.57.251.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	15
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/departmentslobby/shared/usercontrols/promotioncube/	Block	15
85.250.225.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	15

10-31-2015-09:04:08 to 10-31-2015-10:04:08