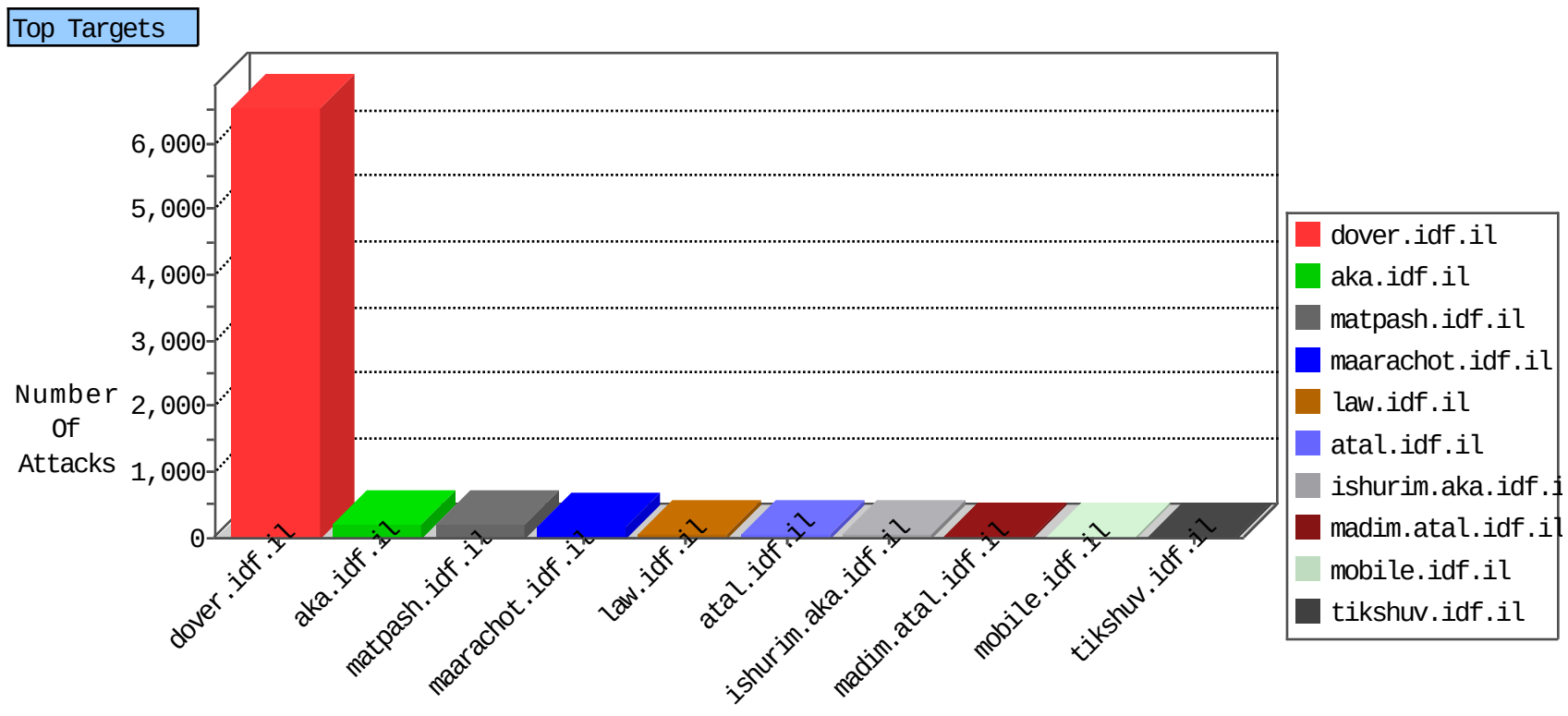
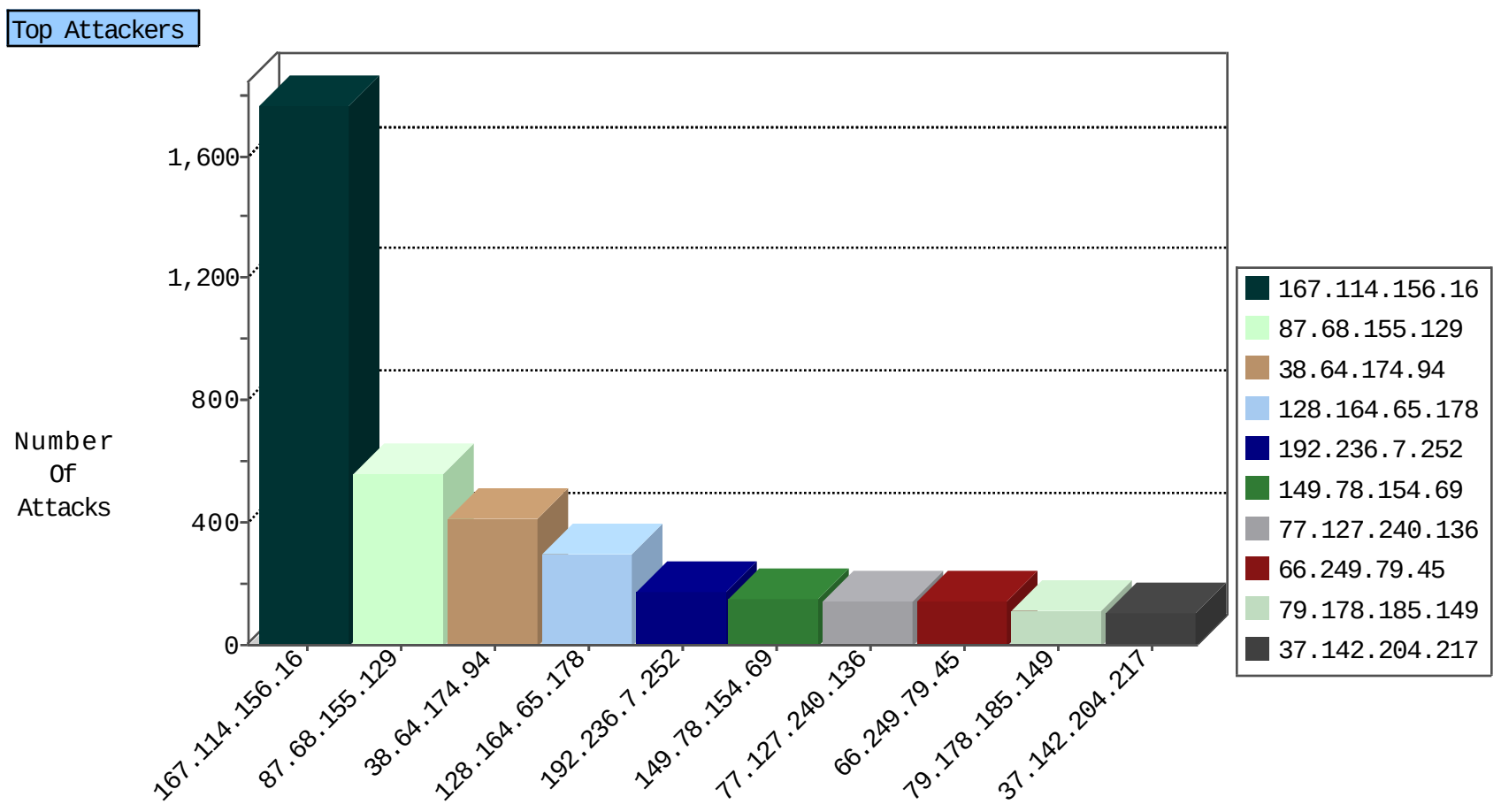
11-04-2015-23:04:06 to 11-05-2015-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-04-2015-23:04:06 to 11-05-2015-00:04:06

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	TCP handshake violation, first packet not syn	drop	119103
128.164.65.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28758
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	23292
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	17186
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	15973
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13121
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	12104
192.236.7.252	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	11909
192.198.151.45	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11435
37.26.148.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10981
178.238.182.254	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10767
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9815
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9338
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9277
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8673
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8257
38.64.174.94	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8215
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7985
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6810
54.244.22.103	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5560
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4977
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4678
104.131.199.242	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4330
41.129.101.155	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4299
66.249.93.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4193
136.243.5.203	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4187
37.237.160.88	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3969
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3759
144.24.20.230	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3380
97.74.24.187	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3003
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2649
50.116.30.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2584
168.61.42.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2436
94.32.217.246	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2388
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2370
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	656
84.94.180.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.181.60.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
93.172.137.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	20
2.54.57.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
79.181.2.149	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
84.110.84.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
83.130.101.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.126.54.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.131.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.67.194	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5
80.246.136.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.93.233	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5

11-04-2015-23:04:06 to 11-05-2015-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	10
95.86.74.153	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
61.160.213.11	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-04-2015-23:04:06 to 11-05-2015-00:04:06

Top Attackers In IDS

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

11-04-2015-23:04:06 to 11-05-2015-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	563
38.64.174.94	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	380
128.164.65.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	267
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
192.236.7.252	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	142
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
79.178.185.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
37.142.204.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
178.238.182.254	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
41.129.101.155	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
139.127.253.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
77.127.201.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
77.125.245.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
176.13.21.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.85.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
104.33.160.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
85.65.60.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
188.120.148.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.182.129.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
89.138.231.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.52.45.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.94.180.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.85.136		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
100.100.85.136		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.183.183.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
93.172.137.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.120.16		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
192.236.7.252	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
31.154.91.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
24.90.171.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.67.136.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.26.148.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.81.193.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.229.117.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.52.18.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15

11-04-2015-23:04:06 to 11-05-2015-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.36.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
50.63.138.151	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.63.138.151	Block	5
94.32.217.246	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
176.13.7.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
84.95.133.22	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.133.22	Block	3
159.203.137.192	United States	147.237.76.30	himush.idf.il	Unauthorized Method HEAD for www.chimush.atal.idf.il/	None	1
54.244.22.103	United States	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.49.66.27	United Arab Emirates	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
79.178.185.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
96.91.243.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.239.0.14	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
31.154.92.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
83.130.101.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
66.249.67.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1515-he/atal.aspx	Block	1
104.236.221.91		147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
45.55.228.253		147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.13.13.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/main/main.asp	Block	1
66.249.67.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/20092010maskorot.aspx	Block	1
141.212.122.112	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
46.117.59.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.126.43.78	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
195.90.103.48	Poland	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.237.160.88	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
66.249.79.232	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3213.pdf	Block	1
144.24.20.230	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.49.66.27	United Arab Emirates	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
77.126.235.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.238.70.47	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
95.86.74.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1772	Block	1

11-04-2015-23:04:06 to 11-05-2015-00:04:06