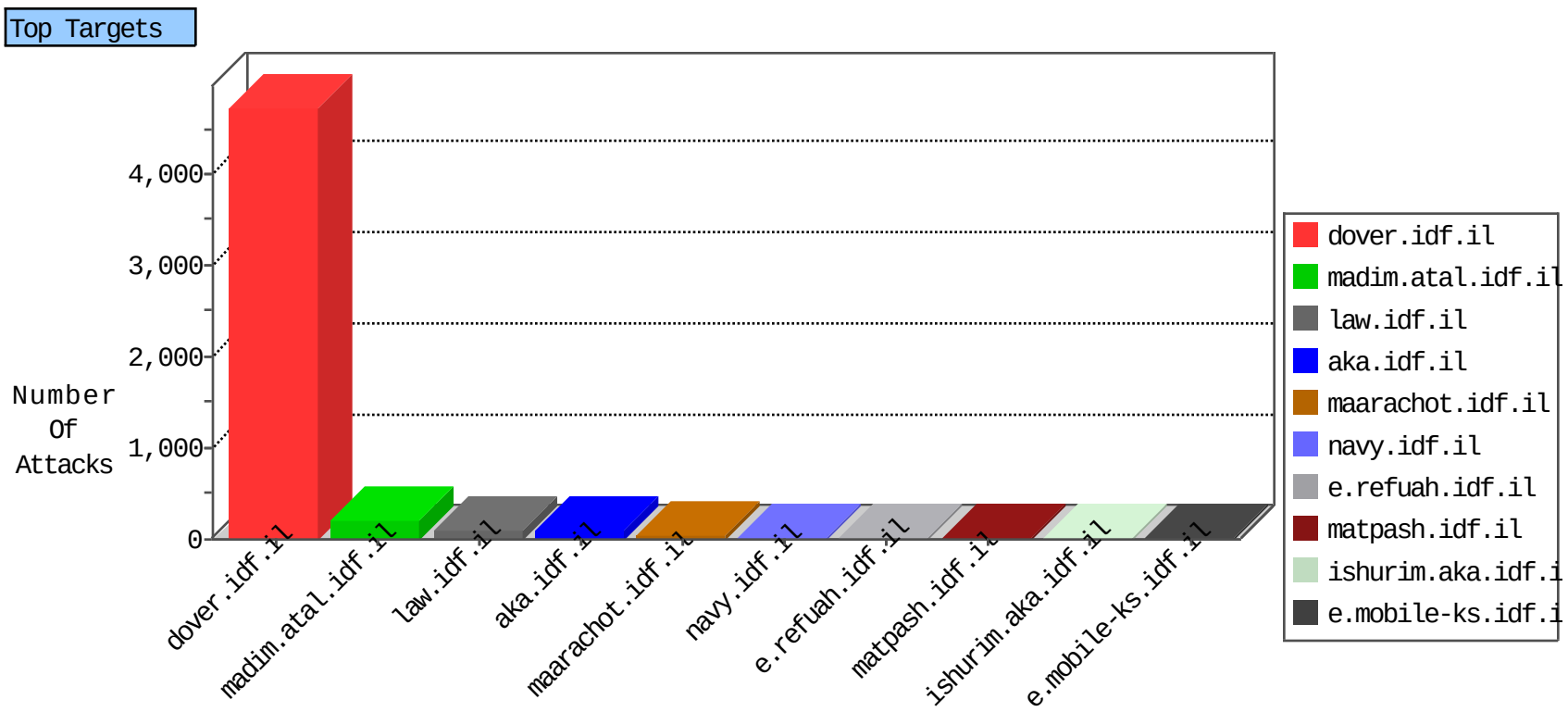
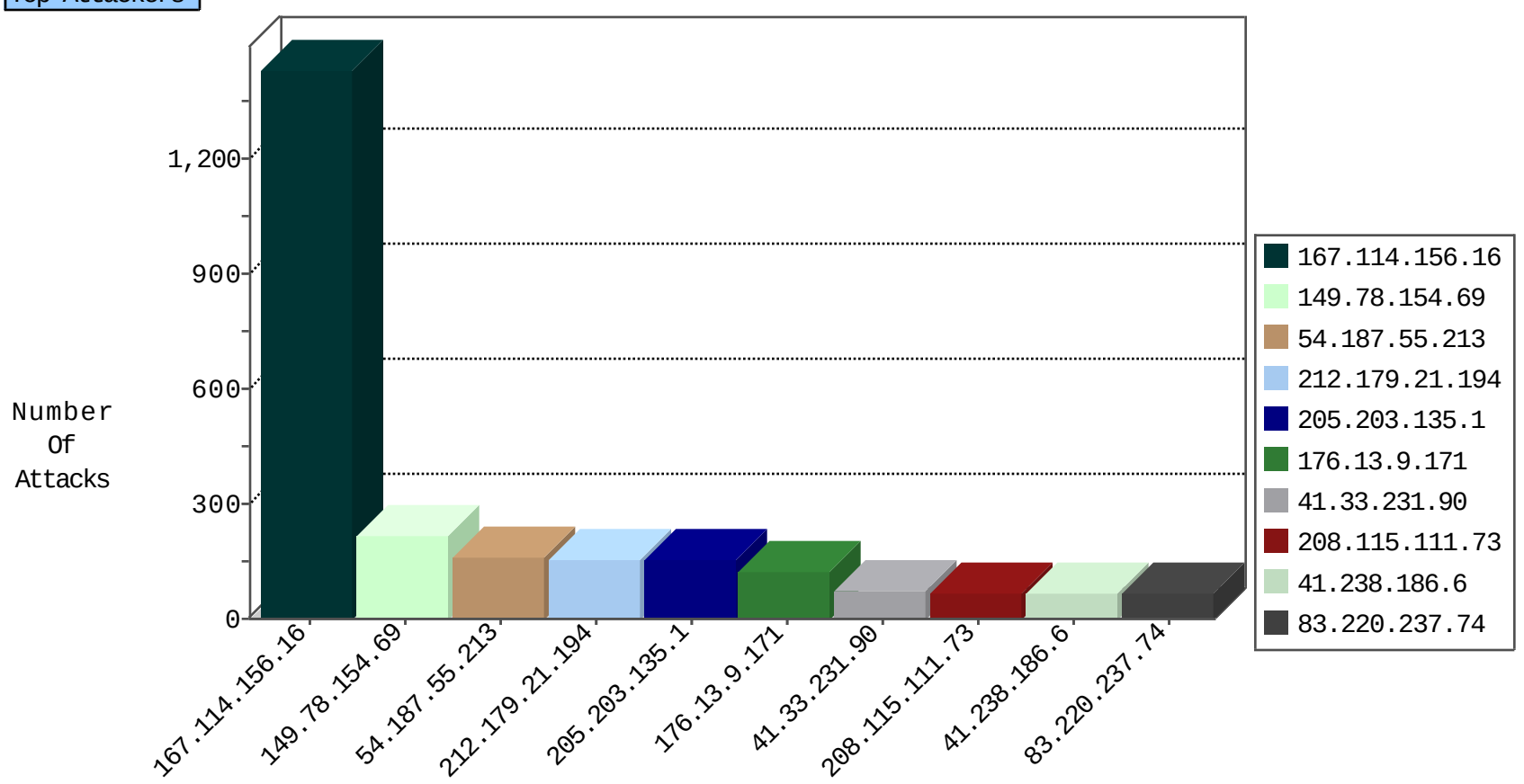
11-05-2015-07:04:00 to 11-05-2015-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-05-2015-07:04:00 to 11-05-2015-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3217
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2506
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1129
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1046
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1002
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	946
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	673
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	662
66.249.90.114	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	512
97.122.200.133	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	407
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	404
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	391
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	277
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	145
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	69
184.168.152.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	67
80.246.139.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	37
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
97.122.200.133	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
31.154.94.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.144.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
62.0.102.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
46.19.85.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
46.19.85.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.150.174.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
46.19.85.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.137.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.25.69.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.109.115.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.147.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
115.239.228.8	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Http	drop	2
176.13.2.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.118.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
192.115.248.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.186.90	United States	147.237.76.39	mobile.meitav.idf.i	Block_Ntp_All_Net	drop	1
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
58.152.250.99	Hong Kong	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
37.26.146.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.216.60	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
205.203.135.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

11-05-2015-07:04:00 to 11-05-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.113.143	France	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

11-05-2015-07:04:00 to 11-05-2015-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
62.210.113.143	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
62.210.113.143	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
92.247.120.60	147.237.76.39	Bulgaria	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.78	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.230.35.77	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.122	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
92.247.120.60	147.237.0.15	Bulgaria	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.178.78.130	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
178.48.138.165	147.237.0.33	Hungary	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-05-2015-07:04:00 to 11-05-2015-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	209
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	156
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	156
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	154
41.238.186.6	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
83.220.237.74	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
176.13.23.222	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
46.19.86.234	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
46.19.85.158	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
37.26.148.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
2.54.60.87	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
71.53.6.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
194.90.122.40	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
80.178.202.155	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
62.210.113.143	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
69.171.231.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
79.180.135.1	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
194.90.83.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
46.19.86.116	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
207.46.13.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
207.46.13.93	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
37.26.147.170	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
79.182.36.128	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
67.160.22.20	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
157.55.39.202	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
84.111.138.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
31.154.94.21	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
69.171.231.225	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
97.122.200.133	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
207.46.13.177	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
81.218.40.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
109.67.136.52	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

11-05-2015-07:04:00 to 11-05-2015-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.9.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.9.171	Block	45
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.13.10.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.12.142.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.12.148.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.51.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.4.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	2
79.178.178.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.190.74	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
212.143.96.222	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	2
147.235.236.1	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
176.12.151.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.245.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
223.81.196.72	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
52.89.52.221	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
167.114.184.98	Canada	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 167.114.184.98	Block	1
72.52.128.19	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 72.52.128.19	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1465-he/atal.aspx	Block	1
176.13.2.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
52.89.52.221	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
167.114.184.98	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/rss	Block	1
72.52.128.19	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
212.143.56.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$c in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
176.13.4.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.67.167.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
212.143.56.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$txtAnsw in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/112511.pdf	Block	1
109.186.147.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
64.246.165.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.117.155.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.9.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1

11-05-2015-07:04:00 to 11-05-2015-08:04:00